T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR VE LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ PROGRAMI

GÜVENLİ SES İLETİMİNDE MERKEZİ OLMAYAN BLOK ZİNCİR TABANLI KİMLİK DOĞRULAMA MEKANİZMASI

DOKTORA TEZİ

MUSTAFA KARA
3172202

TEZ DANIŞMANI: PROF.DR. HASAN HÜSEYİN BALIK
İKİNCİ TEZ DANIŞMANI: DOÇ.DR. MUHAMMED ALİ AYDIN

İSTANBUL
TEMMUZ 2022

T.C.
MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR VE LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ ANA BİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ PROGRAMI

GÜVENLİ SES İLETİMİNDE MERKEZİ OLMAYAN BLOK ZİNCİR TABANLI KİMLİK DOĞRULAMA MEKANİZMASI

DOKTORA TEZİ

MUSTAFA KARA
3172202

Tezin Enstitüye Verildiği Tarih: 19.07.2022
Tezin Savunulduğu Tarih: 01.07.2022

Tez Oy birliği ile başarılı bulunmuştur.

	Unvan Ad Soyad	İmza
Tez Danışmanı	Prof.Dr. Hasan Hüseyin BALIK	
İkinci Tez Danışmanı	Doç.Dr. Muhammed Ali AYDIN	
Jüri Üyeleri	Prof.Dr. Oğuz BAYAT	
	Doç.Dr. Şerif BAHTİYAR	
	Doç.Dr. Can EYÜPOĞLU	
	Dr.Öğr.Üyesi Ömer ÇETİN	

İSTANBUL
TEMMUZ 2022

ÖZGÜNLÜK RAPORU

Tez çalışmamın a) Kapak sayfası, b) Giriş, c) Ana bölümler ve ç) Sonuç kısımlarından oluşan toplam 134 sayfalık kısmına ilişkin, 01/07/2022 tarihinde şahsım tarafından Turnitin adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan özgünlük raporuna göre, tezimin benzerlik oranı % 4'tür.

Uygulanan filtrelemeler:

1- Kaynakça hariç
2- Alıntılar hariç
3- 5 kelimeden daha az örtüşme içeren metin kısımları hariç

Millî Savunma Üniversitesi Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü Lisansüstü Tez Çalışması Özgünlük Raporu Alınması ve Kullanılması Uygulama Usul ve Esasları'nı inceledim ve bu Uygulama Esasları'nda belirtilen azami benzerlik oranlarına göre tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Mustafa KARA

19/07/2022

ETİK BEYAN

Millî Savunma Üniversitesi Enstitüleri Lisansüstü Tez Hazırlama Kılavuzu'nda yer alan kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir; aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Bu tezdeki düşünce, görüş, varsayım, sav veya tezler bana aittir; Millî Savunma Bakanlığı, Millî Savunma Üniversitesi ve Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü sorumlu tutulamaz.

Mustafa KARA

19/07/2022

Değerli aileme…

ÖNSÖZ ve TEŞEKKÜR

Bu çalışma, Millî Savunma Üniversitesi Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalında yapılan "Güvenli Ses İletiminde Merkezi Olmayan Blok Zincir Tabanlı Kimlik Doğrulama Mekanizması" adlı doktora tez çalışmasını içermektedir. VoIP kullanıcıları arasında güvenli ve güvenilir iletim kanalı sağlayan merkezi olmayan blok zincir tabanlı kimlik doğrulama yöntemi geliştirilmiştir. Yaklaşımın tek nokta hatası gibi merkezi sistemin bazı dezavantajlarını önlediği ve VoIP iletişim güvenliğini iyileştirdiği kanıtlanmıştır. Bu çalışmanın, VoIP güvenlik mekanizması ve blok zincir teknolojisi ile ilgilenen araştırmacılara yarar sağlamasını ümit ederim.

Bu doktora eğitimim süresince doktora tezimin hazırlanmasında sahip olduğu engin bilgi birikimini ve deneyimlerini benimle paylaşan, kıymetli zamanını bana ayıran, bilgi ve tecrübesi ile büyük pay sahibi olan ve desteklerini hiçbir zaman esirgemeyen kıymetli tez danışmanlarım Prof.Dr. Hasan Hüseyin BALIK'a ve Doç.Dr. Muhammed Ali AYDIN'a sonsuz şükran ve teşekkürlerimi sunarım.

Doktora tez çalışmamda her türlü kolaylığı ve desteği sağlayan Millî Savunma Üniversitesi Hava Harp Okulu'ndaki çalışma arkadaşlarıma, yolladığım makaleleri göndermeden önce okuyarak bana fikirlerini söyleyen Sn. Şevki Gani ŞANLIÖZ'e ve Sn. Hisham R. J. MERZEH'e, tüm süreçte verdikleri destek ve hoşgörü nedeniyle değerli aileme teşekkürlerimi sunar, minnettarlığımı iletmek isterim.

İstanbul; Temmuz 2022 Mustafa KARA

İÇİNDEKİLER

Sayfa

Sayfa

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

Sayfa

SEMBOL LİSTESİ

E **:** Şifreleme
H : Özetleme Fonksiyonu
L **:** Paket Bit Uzunluğu
R **:** İletim Hızı
SHA3 : Güvenli Özetleme Algoritması
Z : Tam Sayılar Kümesi

KISALTMALAR

ADSL : Asimetrik Sayısal Abone Hattı (Asymmetric Digital Subscriber Line)
ATM : Eş zamansız Aktarım Modu (Asynchronous Transfer Mode)
CA : Sertifika Otoritesi (Certificate Authority)
CBC : Şifre Blok Zincirleme (Cipher Block Chaining)
CPU : Merkezi İşlem Birimi (Central Process Unit)
DDoS : Dağıtılmış Hizmet Reddi (Distributed Denial-of-Service Attack)
DSL : Dijital Abone Hattı (Digital Subscriber Line)
DSS : Dijital İmza Standardı (Digital Signature Standard)
ECC : Eliptik Eğri Şifreleme **(**Elliptic-Curve Cryptography)
ECDH : Eliptik Eğri Diffie-Hellman (Elliptic-Curve Diffie–Hellman)
ECDLP : Eliptik Eğri Ayrık Logaritma Problemi **(**Elliptic Curve Discrete Logarithm Problem)
ECDSA : Eliptik Eğri Dijital İmza Algoritması (Elliptic Curve Digital Signature Algorithm)
ETH : Ether
Gbps : Saniyede Aktarılan Gigabit Cinsinden Veri Sayısı (Gigabits per second)
GUI : Grafiksel Kullanıcı Arayüzü (Graphical User Interface)
HMAC : Özet Tabanlı Mesaj Doğrulama Kodu (Hash with Message Authentication Code)
IETF : İnternet Mühendisliği Görev Grubu (Internet Engineering Task Force)
IKE : İnternet Anahtar Değişimi (Internet Key Exchange)
IoT : Nesnelerin İnterneti **(**Internet of Things)
IP : İnternet Protokolü (Internet Protocol)
IPsec : İnternet Protokolü Güvenliği (Internet Protocol Security)
ISDN : Bütünleştirilmiş Sayısal Ağ Hizmetleri (Integrated Services Digital Network)
Jason API : Jason Uygulama Programlama Arayüzü (Jason Application Programming Interface)
MAC : Mesaj Doğrulama Kodu (Message-Authentication Code)
Mbps : Saniyede Aktarılan Megabit Cinsinden Veri Sayısı (Mega Bits Per Second)
MITM : Ortadaki Adam Saldırısı (Man-in-the-Middle Attack)
MIKEY : Multimedya İnternet Anahtarlama (Multimedia Internet KEYing)
MKI : Ana Anahtar Tanımlayıcısı (Master Key Identifier)
NAT : Ağ Adresi Dönüştürme (Network Address Translation)
PBFT : Pratik Bizans Hata Toleransı (Practical Byzantine Fault Tolerance)
PBX : Özel Telefon Santrali (Private Branch Exchange)
P2P : Eşler Arası (Peer-to-Peer)
PGP : Oldukça İyi Gizlilik (Pretty Good Privacy)
PKI : Açık Anahtar Altyapısı (Public Key Infrastructure)

PoC : Kavram İspatı **(**Proof of Concept)
PoS : Hisse İspatı **(**Proof of Stake)
PoW : İş Kanıtı **(**Proof of Work)
PSTN : Genel Aktarmalı Telefon Şebekesi (Public Switched Telephone Network)
QoS : Hizmet Kalitesi (Quality of Service)
RAM : Rastgele Erişim Belleği **(**Random Access Memory)
RBFT : Yedekli Bizans Hata Toleransı (Redundant Byzantine Fault Tolerance)
RPC : Uzaktan Yordam Çağrısı (Remote Procedure Call)
RSA : Rivest–Shamir–Adleman
RTP : Gerçek Zamanlı Aktarım Protokolü (Real-time Transport Protocol)
RTCP : Gerçek Zamanlı Aktarım Kontrol Protokolü (Real-time Transport Control Protocol)
S/MIME : Güvenli/Çok Amaçlı İnternet Posta Uzantıları (Secure/Multipurpose Internet Mail Extensions)
SAS : Kısa Kimlik Doğrulama Dizisi **(**Short Authentication String)
SBC : Oturum Sınır Kontrolörü (Session Border Controller)
SDES : Oturum Açıklaması Protokol Güvenlik Açıklamaları (Session Description Protocol Security Descriptions)
SDP : Oturum Tanımlama Protokolü (Session Description Protocol)
SIP : Oturum Başlatma Protokolü (Session Initiation Protocol)
SRTP : Güvenli Gerçek Zamanlı İletim Protokolü (Secure Real-time Transport Protocol)
SSL : Güvenli Giriş Katmanı (Secure Socket Layer)
TCP : Gönderim Kontrol Protokolü (Transmission Control Protocol)
TDM : Zaman Bölmeli Çoğullama (Time Division Multiplexing)
TLS : Taşıma Katmanı Güvenliği (Transport Layer Security)
TTP : Güvenilir Üçüncü Taraf (Trusted Third Party)
UDP : Kullanıcı Veri Protokolü (User Datagram Protocol)
UML : Birleşik Modelleme Dili (Unified Modeling Language)
VANET : Araçsal Tasarsız Ağlar (Vehicular Ad-Hoc Networks)
VLAN : Sanal Yerel Alan Ağı (Virtual Local Area Network)
VoD : Talep Üzerine Görüntü (Video on Demand)
VoIP : İnternet Protokolü Üzerinden Ses (Voice over Internet Protocol)
VPN : Sanal Özel Ağ (Virtual Private Network)
WSNs : Kablosuz Sensör Ağları (Wireless Sensor Networks)
ZRTP : Z ve Gerçek Zamanlı Aktarma İletişim Protokolü (Composed of Z and Real-time Transport Protocol)

ÖZ

Güvenli Ses İletiminde Merkezi Olmayan Blok Zincir Tabanlı Kimlik Doğrulama Mekanizması

Mustafa KARA

Millî Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü

İstanbul, Temmuz, 2022

İnternet Protokolü Üzerinden Ses (VoIP), iletişimde daha düşük maliyet ve daha fazla esneklik sağlar ve haberleşme yükünü en aza indirir. VoIP haberleşme teknolojisi, sayısallaştırılmış ses verilerini bir IP ağı üzerinden iletir. Çağrı sisteminin tam işlevselliği, VoIP teknolojisi ile kullanıcıya IP ağına bağlı olan her yerde ölçeklenebilir, esnek ve uygun maliyetli bir iletişim altyapısı sağlar. Bununla birlikte, IP ağına bağlantı, internet ortamındaki güvenlik ve gizlilik açıklarını ve kötü niyetli saldırıları ortaya çıkarır. Böylece gizlilik, bütünlük, erişilebilirlik, kimlik doğrulama ve inkâr edememe unsurlarının birlikte sağlanması güvenli iletişim için en yüksek öncelik haline gelmektedir. Ancak kimlik doğrulama, tüm bu güvenlik unsurlarının arasında savunma mekanizmasının ilk hattıdır. Ne yazık ki, geleneksel merkezi tek taraflı kimlik doğrulama, zayıf ve kırılgandır. Böylece Tek Nokta Hatası (SPF) ve mahremiyet sorunları gibi çeşitli güvenlik açıkları nedeniyle güvenli iletişim ortamı sağlanamamaktadır. Ayrıca, Sertifika Yetkilisi (CA) ve Güvenilir Üçüncü Taraf (TTP) gibi anahtar dağıtım mekanizmalarına körü körüne güvenmek, önemli güvenlik sorunlarını beraberinde getirecektir. Çünkü kimlik doğrulama mekanizması için yanlış türde sertifika yayınlayabilir ve dijital sertifikaların ele geçirilmesine, sahteciliğine ve tahrif edilmesine karşı savunmasızdır. Bu tez çalışması, belirtilen dezavantajlara bir çözüm olarak VoIP için merkezi olmayan blok zincir tabanlı bir kimlik doğrulama mekanizması sunmaktadır. Önerilen kimlik doğrulama mekanizması, VoIP uygulamalarında veri mahremiyeti ve güvenli iletişim sağlamak için blok zincir platformunun değişmezlik, şeffaflık ve hata toleransı gibi temel özelliklerini kullanır. Tüm deneyler, sanal Ethereum platformu ve Python dili kullanılarak gerçek bir uygulama ortamında gerçekleştirilmiştir. Deneysel sonuçlara göre, önerilen şemanın VoIP iletişiminde merkezi olmayan bir kimlik doğrulama mekanizması olarak VoIP çağrı süreci için güvenli, etkili ve uygun maliyetli bir çözüm olduğu tespit edilmiştir. Ayrıca, eşler arası güvenli arama performansı, ortalama zaman gecikmesi açısından mevcut blok zincir tabanlı kimlik doğrulama mekanizmalarından %30-70 oranında daha iyi performans göstermiştir. Önerilen şema, taraflar arasında kimlik doğrulaması yapmak için Taşıma Katmanı Güvenliği (TLS) yönteminden neredeyse on kat daha hızlıdır. Ayrıca, SIP kimlik doğrulaması üzerinden gerçekleştirilen hızlı ancak daha az güvenli yöntemlerle karşılaştırıldığında kabul edilebilir gecikme süresine sahiptir ve SIP kimlik doğrulama sistemine alternatif olabilecek yöntem önerilmiştir.

Anahtar Sözcükler: Blok zincir, VoIP, Kimlik doğrulama, Güvenli haberleşme, Ağ güvenliği.

Bilim Kodu : 92403

Sayfa Sayısı : 151

Tez Danışmanı : Prof.Dr. Hasan Hüseyin BALIK, Doç.Dr. Muhammed Ali AYDIN

ABSTRACT

Decentralized Blockchain-Based Authentication Mechanism for Secure Voice Communication

Mustafa Kara

National Defence University, Atatürk Strategic Studies And Graduate Institute

Istanbul, July, 2022

The Voice over Internet Protocol provides lower cost and more flexibility in transmission and minimizes communication overhead. VoIP communication technology transmits digitized voice data over an IP network. The calling system's full functionality provides a scalable, flexible, and cost-effective communication infrastructure wherever connected to the IP network with this technology. Nevertheless, the connection to the IP network exposes security and privacy vulnerabilities and malicious attacks. Thus, confidentiality, availability, integrity, authentication, and non-repudiation, when together, became the top priority for secure communication. However, authentication is the first line of defense amongst all these security parameters. Unfortunately, several authentication mechanisms in the traditional centered single-side authentication are weak and fragile, which cannot provide secure communication due to various vulnerabilities such as Single Point of Failure (SPF) and privacy issues. Furthermore, blindly trusting key distribution mechanisms such as Certificate Authority (CA) and Trusted Third Party (TTP) will bring significant security problems. The authentication mechanism may issue the wrong type of certificate and are vulnerable to hacking, forgery, and falsification of digital certificates. This thesis presents a decentralized blockchain-based identity authentication mechanism for VoIP as a solution to these drawbacks. The authentication mechanism utilizes the main features of the blockchain platform, such as immutability, transparency, and fault tolerance, to provide data privacy and secure communication in VoIP applications. All experiments were performed as an actual implementation using the virtual Ethereum platform and Python language. The experimental results show that the proposed scheme is a secure, efficient and cost-effective solution for the call process as a decentralized identity authentication system in VoIP. In addition, peer-to-peer secure call performance outperforms the existing blockchain-based authentication mechanisms by 30%–70% in terms of average time delay. The proposed scheme is almost ten times faster than the TLS process to authenticate between parties. Moreover, it has an acceptable time delay in a call process compared to fast but less secure basic methods over the SIP authentication.

Keywords **:** Blockchain, VoIP, Authentication, Secure communication, Network security.

Science Code : 92403

Pages : 151

Supervisor : Prof.Dr. Hasan Hüseyin BALIK, Doç.Dr. Muhammed Ali AYDIN

1. GİRİŞ

İnternet Protokolünün (IP) yönlendirme işlevi sayesinde güvenlik, kamera, haberleşme sistemleri yanında daha birçok sistemin altyapı ağında bu protokol yaygın olarak kullanılmaktadır. IP altyapısı üzerine kurulu İnternet Üzerinden Ses Protokolü (VoIP) son yıllarda popülaritesi yüksek bir ivme ile artan ve temelde telefon görüşmesi imkanı tanıyan ve tarafları ortak bir ağ üzerinden birbirine bağlayarak iletişim altyapısı sunan bir internet protokolüdür. Bu popülarizmin en önemli sebebi VoIP uygulamalarının gözle görülür bir şekilde düşük maliyetinin yanında yüksek performans ve ölçeklenebilirlik sağlamasıdır. VoIP iletişim altyapısının önemli bir parçasıdır. VoIP sayesinde üzerine ilgili yazılımlar kurulmuş internet bağlantılı bir telefon veya bir bilgisayar üzerinden telefon görüşmesi yapılabilmektedir. VoIP kullanımı için üzerine VoIP yazılımı kurulmuş bir bilgisayar cihazı IP telefonu (VoIP telefon, SIP telefonu veya yazılım tabanlı telefonlar) olarak adlandırılır ve tamamen internet altyapısı üzerinden sağlanan telefon uygulaması hizmetidir (Singh ve diğ, 2014). Genel Aktarmalı Telefon Şebekesi (PSTN) benzeri geleneksel telefon sistemleri ile karşılaştırıldığında VoIP sistemler düşük maliyetli, esnek, ölçeklenebilir iletişim teknolojisi sunmaktadır. Ancak VoIP sistemi elektronik iletişim hattı olan internet üzerinden görüşmeler gerçekleştirdiği için internet ortamındaki olası tüm saldırı modelleri VoIP içinde geçerlidir (Dhillon ve Kalra, 2019).

VoIP internet bağlantısı kullanan aramalar için en yaygın kullanılan iletişim modülüdür. Ancak gerçek zamanlı bir teknoloji olan VoIP uygulaması, genel ağ üzerinden veri akışını sağladığı için ciddi saldırılara maruz kalır (Keromytis, 2010; Dhillon ve Kalra, 2019; L. Zhang ve diğ., 2016; Y. Chen ve diğ, 2021). Bu nedenle VoIP haberleşmesinde güvenlik önemli bir sorundur ancak sistemdeki her VoIP kullanıcısı potansiyel bir güvenlik açığı noktasıdır (Dantu ve diğ, 2009). VoIP uygulamalarının kullanımı esnasında internet ağının iyi bilinen tehditleri (tekrarlama saldırısı, internet telefonu üzerinden spam gönderme, ortadaki adam saldırısı (MITM) vb.) nedeniyle taraflar arasında bir güvenilirlik sorunu oluşmaktadır (Pecori ve Veltri, 2016; Ntantogian ve diğ, 2019).

Güvenlik unsurlarından biri olan kimlik doğrulama, VoIP gibi gerçek zamanlı uygulamalarda güvenli iletişimin merkezinde yer alır ve internetteki çeşitli güvenlik açıkları nedeniyle önemli bir rol oynar (Alqassem ve Svetinovic, 2014). Ayrıca, VoIP iletişimi gizlilik ve güvenilirlik açısından da birçok güvenlik unsuruna karşı ele alınmalıdır (Dantu ve diğ, 2009). Bu bağlamda, güvenlik ve gizlilik sağlamak için kullanıcılar arasındaki güvenilirlik sorunu kimlik doğrulama yoluyla giderilmelidir.

Güvenli görüşme için güvenlik unsurları yani temel olarak gizlilik (confidentiality), bütünlük (integrity), erişilebilirlik (avaliablity), inkâr edememe (non-repudiation), erişim kontrolü (access control) ve kimlik doğrulama (authentication) bir bütün halinde sağlanmalıdır (Ferrag ve diğ, 2020). Ancak kimlik doğrulama güvenlik unsurları arasında savunma mekanizmasının ilk hattıdır. VoIP dahil internet multimedya haberleşme sistemlerinde kullanıcı ve cihaz kimliğinin doğrulanması yetkilendirme öncesinde gereklidir (Sukma ve Chokngamwong, 2017). Çünkü arayan kimliği bilgisi bir aramada taklit edilebilir ve VoIP haberleşme altyapısına saldırı olarak kullanılabilir. Başka bir ifadeyle arayan kişi (caller) ve aranan kişi (callee) kimlik doğrulamaları gerçekleşmediği takdirde kimliği taklit edilebilir (Nikooghadam ve Amintoosi, 2020). Böylece tekrarlama veya ortadaki adam saldırısı benzeri saldırılar üzerinden haberleşmeyi yönetmek, değiştirmek ve iptal etmek gibi sorunlara sebep olur. Bu açıdan gerçek ses verisinin iletildiği katman (media transport layer) güvenliği esasen oturum anahtarlarının gizliliğine ve oturum katılımcılarının kimliklerinin doğrulanmasına bağlıdır (Gupta ve Shmatikov, 2007). Kimlik doğrulama mekanizması, arayan kişinin aradığı kişiye iddia ettiği kişi olduğunu kanıtlaması gerektiğinde arayan tarafından kullanılır (Glass ve diğ, 2000; Salgarelli ve diğ, 2003). Güvenli bir haberleşme için arayan kişi kimliğini aradığı kişiyle güvenli kanaldan paylaşmalıdır. Bu doğrulama işlemi hem cihaz hem de kişi bazında gerçekleşirse güvenlik unsurları arasında ilk adım bir bütün halinde sağlanmış olur.

VoIP altyapısında genel olarak iki standart protokol kullanılır, Oturum Başlatma Protokolü (SIP) ve Gerçek Zamanlı İletim Protokolü (RTP). SIP protokolü iki cihaz arasında bağlantıyı kişi, mesaj bilgisi (arama başlatma ve bitirme) ve aramayı etkileyecek önemli bilgiler ileterek oluşturur (Pecori ve Veltri, 2016). VoIP iletişim kurulumundaki ilk adım, gerçek zamanlı oturumları başlatan ve bitiren SIP protokolü ile sağlanır. Bununla birlikte, SIP protokolü kullanımı esnasında kullanılan temel SIP

kimlik doğrulama yöntemi, gizli dinlemeler (eavesdropping), kaba kuvvete dayalı bir yöntemle parola tahmini (brute force saldırısı) veya sunucu tabanlı sızdırma saldırılarına karşı savunmasızdır ve bu tür saldırılara kolayca maruz kalabilir (Zhang ve diğ, 2016). Bu açıdan SIP mesajları için yapılan kimlik doğrulama, VoIP kullanıcıları için yeterli bir kimlik doğrulama sağlamaz. SIP protokolü taraflar arasında bağlantıyı kurduktan sonra RTP protokolü ses ve video verisini taşımak için kullanılır (Porter ve CCNP, 2006). SIP ve RTP protokolleri standart olarak güvenlik önlemi alınmadan iletilirse büyük bir güvenlik sorunu oluşturur (Nikooghadam ve Amintoosi, 2020; Jan ve diğ, 2021). SIP mesajları ve RTP akışları (stream) temel ağ bilgisine sahip bir saldırgan tarafından kolaylıkla durdurulup dinlenebilir veya değiştirilebilir. Bu açıdan RTP ve SIP protokolleri belirli güvenlik protokolleriyle desteklenerek VoIP uygulamaları daha güvenli hale getirilmiştir. Birçok yeni protokol ve çalışma ile belirli teknolojilerin bir araya gelmesiyle kimlik doğrulama sağlanmaktadır. Ancak bu çalışmaların birçoğu esneklik ve ölçeklenebilirlik açısından bazı eksiklikler içermektedir. Ayrıca yine bu çalışmaların birçoğu temelde merkeziyetçi bir kimlik doğrulama modeli kullanır ve güvenilir üçüncü tarafları esas almaktadırlar. Bu durum gizlilik ve güvenilirlik açısından sorun oluşturmaktadır.

SIP mesajlarında kimlik doğrulama, gizlilik ve bütünlük genellikle Taşıma Katmanı Güvenliği (TLS) veya merkezi bir mimari modeli kullanan Güvenli/Çok Amaçlı İnternet Posta Uzantıları (S/MIME) gibi diğer güvenlik protokolleri ile birlikte kullanılarak gerçekleştirilir (Dhillon ve Kalra, 2019). Bu protokoller, Açık Anahtar Altyapısı (PKI) (Liao ve Wang, 2010) kullanılarak uçtan uca güvenli iletişimi sağlar. Yani TLS gibi geleneksel merkezi güvenlik yöntemleri, Güvenilir Üçüncü Taraf (TTP) veya Sertifika Yetkilisi (CA) üzerinden anahtar dağıtımı gerçekleştirerek kimlik doğrulaması sağlar. Bu nedenle, kimlik doğrulama tek sunucu mimarisine veya başka bir deyişle merkezi mimariye dayanmaktadır (K. Khacef ve Pujolle, 2019). Merkezi mimari mahremiyet konularında sıkıntılı ve anonimlikten yoksundur (Guo ve diğ, 2019; Lin ve diğ, 2019). Kimlik doğrulama süreci merkezileştirilirse sistem zayıf hata toleransı (low fault tolerance) ve tek nokta hatası (single point of failure) gibi potansiyel riskler içerir (Zhaofeng ve diğ, 2020). Ayrıca ölçeklenebilirlik (scalability), ağda çok önemli bir özellik olan büyüyen bir yapıyı yürütme yeteneğidir (Hammi ve diğ, 2018). Ancak, merkezi kimlik doğrulama ölçeklenebilirlik sorunlarına yatkındır ve mahremiyet (privacy) için uygun bir çözüm değildir (Khalid ve diğ, 2020). Ayrıca

TLS, medya oturumu için eşler arası şifreleme yapamaz, aksine cihazlar arası uçtan uca yani ağdaki cihazlar arasında şifreleme yaparak güvenlik unsurlarını sağlar. Bu şekilde eşler arası doğrudan güvenli görüşme gerçekleşmez. Güvenlik, mahremiyet ve kimlik doğrulama işlemi için TLS protokolünün tercih edilmesi durumunda, Oturum Açıklaması Protokol Güvenlik Açıklamaları (SDES) ve Multimedya İnternet Anahtarlama (MIKEY) gibi anahtar değişim protokolleri için hizmet esnasında veri değişikliği saldırı modelleri hala çok önemli bir tehdittir (Pecori ve Veltri, 2016).

Medya iletim katmanında (MTL), Güvenli Gerçek Zamanlı Taşıma Protokolü (SRTP), şifreli multimedya paketlerinin iletiminde en yaygın kullanılan protokollerden biridir. Ancak, simetrik şifreleme algoritması kullanan SRTP protokolü kullanımındaki en kritik sorun, güvenli ve güvenilir olmayan kimlik doğrulaması sonrası ortak anahtar dağıtımıdır. SIP protokolünden farklı olarak, RTP protokolü kullanan medya iletim katmanında güvenli iletim kanalı oluşturmak için Kısa Kimlik Doğrulama Dizini (SAS) kimlik doğrulaması kullanan Z ve Gerçek Zamanlı Aktarma İletişim Protokolü (ZRTP) protokolü güvenli anahtar dağıtımını merkezi olmayan bir mekanizma üzerinden sağlar. ZRTP protokolünde kullanılan SAS kimlik doğrulaması, VoIP kullanıcıları arasında bir sayının karşılıklı olarak yüksek sesle okunmasıyla doğrulanan bir yöntemdir. Ancak bu yöntem MITM saldırılarına veya sahtecilik (forgery) tehditlerine karşı etkisiz ve savunmasızdır (Perez-Botero ve Donoso, 2011). Bu nedenle, SRTP protokolünde güvenli anahtar dağıtımı sağlamak için bir aramadaki her iki kullanıcının da güvenli, sağlam ve merkezi olmayan bir platform tarafından doğrulanması gerekir. Bir VoIP haberleşmesinde meşru taraflar arasında anahtar dağıtımı ancak güvenliğin ilk adımı olan güvenilir kimlik doğrulaması ile sağlanabilir. Tam bu noktada blok zincir (blockchain) teknolojisi kimlik doğrulamaya yatkın dağıtık mimarisiyle merkeziyetçi yapıdan farklı şeffaf bir doğrulama için etkili bir çözümdür. Blok zincir teknolojisi, kimlik doğrulamada birçok tehdidin üstesinden gelen yenilikçi bir teknolojidir ve birçok alanda kimlik doğrulaması amacıyla kullanılmaktadır (Hammi ve diğ, 2018; Khalid ve diğ, 2020; Cui ve diğ, 2020). Eşler arası VoIP uygulamalarında bir güvenlik ilişkisinin kurulması, güvenli olmayan genel ağ (public channel) üzerinden medya iletişimini güvence altına almak için uygun bir ağ oluşturmaktadır. Ayrıca mahremiyet ve gizlilik açısından daha güvenli bir ortam sağlar.

Kimlik doğrulaması için eşler arasında istemci/sunucu veya tek sunuculu modeli kullanmayan bu tez çalışmasında, VoIP kullanıcıları arasında kimlik doğrulamasını sağlamak için VoIP uygulaması ve blok zincir platformu entegre edilmiştir. Blok zincir platformu şeffaflık, güvenlik, veri değişmezliği ve güvenilirlik gibi niteliklerinden dolayı tercih edilmektedir. VoIP bilginin doğru kişiye, gerçek zamanlı iletilmesini sağlarken, blok zincir asimetrik şifreleme algoritmasını ve zaman damgası teknolojisini kullanarak taraflar arasında bir güven mekanizması kurar. Böylece VoIP haberleşme sürecinde bilginin güncelliği, güvenliği ve izlenebilirliği sağlanır. Blok zincir, sağlam kriptografik şifreleme algoritmaları, kriptografik özet (hash) fonksiyonu, dijital imza, konsensüs algoritması (consensus algorithm) ve dağıtık defter (distributed ledger) kullanan merkezi olmayan bir teknolojidir (Zhaofeng ve diğ, 2020). Blok zincir kriptografik algoritmalarla ağda depolanan veriler için veri bütünlüğü ve inkâr edememe unsurları sağlar ve bu sayede kullanıcıların kayıtlı bilgileri için sahteciliğe ve veri üzerindeki kurcalamaya karşı güvenilir bir ortam sunar (Patwary ve diğ, 2020). Ayrıca, tek sunuculu kimlik doğrulama mimarisinden farklı olarak, merkezi olmayan kimlik doğrulama yüksek hata toleransı sağlar. Bu açıdan kayıt listesine sızılarak bilgiler üzerindeki değişiklik yapılmasına karşı dirençlidir. Bu tez çalışmasında, VoIP kullanıcıları arasında güvenli ve güvenilir doğrulamayı sağlayan Ethereum blok zincirini kullanan yeni bir merkezi olmayan kimlik doğrulama yöntemi geliştirilmiştir. Bu geliştirilen yöntem tek sunuculu kimlik doğrulama mimarisindeki hataların ve zayıflıkların önüne geçer. Ayrıca, güvenli olmayan internet ağı üzerinden VoIP kullanıcıları arasında karşılıklı kimlik doğrulama sağlanarak iletişim kurulmadan önce gereken güvenli iletişim altyapısını oluşturur.

Bu çalışmanın ana katkısı aşağıdaki şekilde özetlenerek listelenebilir;

- Bu tez, TTP ve CA yöntemleriyle anahtar dağıtımı sağlayarak yapılan kimlik doğrulama yerine merkezi mimarileri veya üçüncü tarafları ortadan kaldırarak VoIP ağı üzerinden yapılan bir çağrıda taraflar arasında güvenli kimlik doğrulamasını sağlar. Böylece VoIP kullanıcıları arasındaki iletişim için tek nokta hatası ortadan kalkar ve yüksek hata toleransı sağlanır. Ayrıca önerilen yöntemde, VoIP iletişiminde güvenlik unsuru olarak veri bütünlüğü ve inkâr edememe (non-repudiation) sağlanmaktadır.

- Önerilen merkezi olmayan kimlik doğrulama mekanizması, internet ortamında (genel ağda) olası saldırıları önler ve bir VoIP çağrısında taraflar arasında bu olası saldırılara karşı güvenilir bir kimlik doğrulamasını garanti eder.
- Önerilen yöntem, SIP protokolünün TLS ile kimlik doğrulama süreci gerçekleştirmesi ve literatürdeki temel SIP doğrulama şemaları gibi mevcut tek sunuculu mimari (istemci-sunucu modeli) yöntemleriyle zaman gecikmesi ve güvenlik açısından karşılaştırılmıştır. Ayrıca, uçtan uca güvenli arama performansı, zaman karmaşıklığı, hata toleransı, ortalama zaman gecikmesi ve güvenlik unsurları ile ilgili olarak literatürdeki blok zincir tabanlı kimlik doğrulama şemaları arasında kıyaslama yapılmış ve geliştirilen mekanizmanın güçlü yönleri ortaya konulmuştur.

1.1. Tezin Amacı

Bu tezde VoIP uygulamalarındaki IP tabanlı telefon görüşmeleri için ses verisi iletimi öncesinde doğrudan eşler arası kimlik doğrulaması yapılması amaçlanmaktadır. Oluşturulan mimari içerisinde merkezi olmayan ağ üzerinden tamamen güvenli VoIP haberleşmesi sağlayan blok zincir tabanlı bir arama ağı oluşturulmaktadır. Ayrıca yüksek düzeyde güvenlik sağlanırken hassas işlemler dağıtık yapı içerisinde şeffaf olarak uygulanmaktadır. Böylece güvenilir aracılara olan ihtiyaç (trusted third party) ortadan kalkmaktadır (Guo ve diğ, 2019). Sonuç olarak geliştirilen yöntem ile merkezi yapıda anahtar dağıtımı ile ortaya çıkan tek nokta hatasını önlenmekte ve yüksek hata toleransı sağlanmaktadır. Blok zincir platformu, tüm ağ düğümleri (node) tarafından erişilebilir durumdadır ve halihazırda yapılmış olan tüm işlemlerin kaydını tutar. Böylece görüşmelerdeki inkâr edememezlik (non-repudiation) özelliğini sağlayarak yapıyı daha güvenli ve güvenilir hale getirmektedir (Xu ve diğ, 2019). Genel olarak akıllı sözleşmeler (smart contract), konsensüs algoritmaları ve dağıtık modelleme teknolojilerini içeren blok zincir teknolojisi dijital sertifikaların üretilmesi, dağıtılması ve kimlik doğrulaması aşamasında kullanılabilmesi için gerekli dağıtık altyapıyı sağlayan güvenli bir kayıt listesidir.

Bu tezin amacı aşağıdaki şekilde özetlenmiştir:

- VoIP uygulamalarına tamamen merkezi olmayan ve sunucusuz bir mimari aracılığıyla kimlik doğrulaması yapmayı amaçlayan, blok zinciri tabanlı uçtan uca güvenli görüşme ortamı oluşturulmuştur. Önerilen yöntem maliyet

verimliliği ve güven özelliklerini somutlaştırarak VoIP uygulaması kullanıcılarının dijital deneyimini geliştiren yeni nesil bir kimlik doğrulama modeli sunmaktadır.

- Deney sonuçları ile elde edilen performans ölçümlerinin değerlendirilmesi adım adım ele alınmıştır. Tezde sunulan modelin blok zincir tabanlı olması sebebiyle finansal boyutu incelenmiştir. Uygulanan yöntemler ve elde edilen sonuçlar açısından, çalışmanın akademik literatüre katkısı karşılaştırmalar yapılarak gösterilmiştir. Önerilen şemanın gizlilik, bütünlük ve kimlik doğrulama unsurlarına ulaşabildiğini kanıtlamak için deneysel çalışmanın yanında AVISPA aracını kullanarak kapsamlı güvenlik analizi yapılmıştır.
- Bu çalışmadaki yöntemde, dağıtılmış hizmet reddi (DDoS) saldırısı, tekrarlama saldırısı (replay attack), kimlik hırsızlığı saldırısı (sybil attack), ortadaki adam saldırısı, ikame saldırısı (substitution attack) ve sahtecilik (spoofing) saldırısı dahil olmak üzere siber saldırılara karşı güvenliği analiz edilmiştir. Uçtan uca VoIP uygulamalarında merkeziyetçi mimari üzerinden kimlik doğrulamayı gerçekleştiren modellerle karşılaştırma yapılarak sunulan yöntemin üstün yanları ortaya konulmuştur.

1.2. Literatür Araştırması

İnternet kullanıcıları IP tabanlı iletişim hizmetlerini yaygın olarak kullandıklarından, VoIP ağında kullanıcılar arasında karşılıklı kimlik doğrulama önemli bir güvenlik unsurudur. VoIP uygulamalarının temel olarak kullandığı protokollerden biri olan SIP protokolü multimedya iletişim oturumlarını kontrol eden bir protokoldür ve VoIP uygulamalarında kimlik doğrulama genel olarak SIP protokolü üzerinden gerçekleştirilmektedir (Jiang ve Tian, 2015). SIP protokolü SIP sunucusuna ihtiyaç duyar. SIP metin tabanlı bir protokol olduğu için olası bir saldırgan tüm iletişimi rahatlıkla dinleyebilir ve içeriği değiştirebilir (Azrour ve diğ, 2017). Ancak bu duruma karşı SIP Sinyalleşme protokolü Temel Kimlik Doğrulaması (Basic Authentication), Özet Kimlik Doğrulaması (Digest Authentication), Oldukça İyi Gizlilik (PGP), S/MIME ve TLS benzeri yöntemler kullanmaktadır (Segeč ve diğ, 2017). Ancak sadece sinyalleşme fazındaki SIP protokolü üzerinden gerçekleştirilen şifreleme ve kimlik doğrulama yöntemleri tek başına yetersizdir. Kimlik doğrulama güvenilir bir anahtar değişim mekanizmasına ihtiyaç duymaktadır (Sureshkumar ve diğ., 2018).

SIP kimlik doğrulama şeması, ilk zamanlar IP telefon üzerinden karşılıklı telefon görüşmesinin hemen öncesinde temel (basic) ve özet (digest) kimlik doğrulama yöntemlerini kullanmıştır (Sureshkumar ve diğ, 2018). Ancak temel kimlik doğrulama düz metin olduğu için ele geçirilebilir veya değiştirilebilir. Özet kimlik doğrulama ise bütünlük ve gizlilik sağlamaz. Görüşme öncesi güvenli kanaldan paylaşılmış anahtar ihtiyacı vardır. Ayrıca çevrimdışı parola tahmin (off-line password guessing) saldırıları ve sahtekarlık (spoofing) saldırılarına karşı zafiyet içerirler (Yoon ve diğ, 2010). Kimlik doğrulama SIP protokolü üzerinden gerçekleşirse bu sunucuya yapılacak olası bir saldırı sistemi etkiler ve güvensiz bir haberleşme ortamı oluşturur. Bu durum sonucunda daha güvenli yöntemler oluşturmak için literatürde SIP protokolü için çok çeşitli kimlik doğrulama şemaları önerilmiştir (Nikooghadam ve Amintoosi, 2020; Irshad ve diğ, 2017; Kumari ve diğ, 2018; Zhang ve diğ, 2016; Qiu ve diğ, 2018). Bir diğer güvenlik protokolü olan S/MIME, SIP mesajının sadece Oturum Tanımlama Protokolü (SDP) içeriğini şifreler ve başlık kısmı şifrelenmeden aktarılır. Bu durum kimlik doğrulamayı tam anlamıyla güvenli hale getirmez. SIP protokolü üzerinden uygulanan S/MIME protokolü uçtan uca gizlilik, kimlik doğrulama ve bütünlük sağlar. Ancak Açık Anahtar Altyapısı (PKI) bağımlılığı vardır (Levi ve Güder, 2009; Omote, 2020).

Anahtar dağıtım yöntemlerinden ilk anahtar paylaşımı (pre-shared secret key) güvenli kanal üzerinden doğrudan cihazlara anahtar dağıtır. Ancak bu yöntem oldukça zahmetli ve zaman açısından kayıp oluşturur. Bunun yerine kullanılan TLS TCP/IP modeline göre taşıma katmanında çalışan ve kimlik doğrulama için kullanılan bir yöntemdir. Ancak TLS protokolü paket iletme esnasında iki uç arasında sürekli olarak cihazlar arası uçtan uca (hop by hop) bir güvenlik sağlar (Glissa ve Meddeb, 2019; D. Geneiatakis ve diğ, 2006). Bu durumda uçlardan herhangi birinde oluşan zafiyet TLS protokolünü ortadaki adam saldırısı benzeri açıklıklara karşı yetersiz bırakmaktadır. Doğrulama sürecini tamamen SIP protokolü üzerinden gerçekleştirmek için üçüncü bir taraf veya sertifika otoritesi kullanılarak anahtar dağıtımı sağlanır. Bu durum inkâr edememe özelliğinin sağlanamaması, düşük hata toleransının ortaya çıkması, mahremiyetin yok olması ve tek nokta hatasına sebebiyet vermesi açısından dezavantajlıdır.

Medya iletimi tarafında RTP protokolü üzerinden medya verisi aktarımı öncesi kullanılan MIKEY (Euchner, 2006), SDES ve ZRTP protokolleri de anahtar dağıtım protokolleri oldukları için kimlik doğrulama ihtiyacı duyarlar (Pecori and Veltri, 2016). Bu açıdan MIKEY ve SDES protokolleri TLS tabanlı kimlik doğrulama yöntemini kullanmaktadır. ZRTP protokolü ise daha farklı bir anahtar kimlik doğrulaması yöntemi olan Kısa Kimlik Doğrulama Dizisi (SAS) kullanır. SAS yöntemi Diffie-Hellman Anahtar Değişim (Diffie-Hellman Key Exchange) yöntemini doğrulamak için kullanılır (Gupta and Shmatikov, 2007). Arayan ve aranan eşlerin doğrudan birbirlerine sesli olarak bir özet değeri okuyarak gerçekleştirdiği bu yöntem birbirini hiç tanımayan iki kişi için ses taklidi saldırılarına (voice forgery attack) ortam oluşturur. Ayrıca MITM ataklarına karşı zafiyetler içerir (Zhang ve diğ., 2010).

Bilgisayar ağındaki iletişim güvenlik altyapısı kriptografik yöntemlerle sağlanır. Simetrik şifreleme günümüzde kullanılan en hızlı şifreleme yöntemlerinden biri olmasına rağmen, güvenli bir yöntem için bir tür asimetrik şifreleme gereklidir. VoIP uygulamasında ECC (Eliptik Eğri Şifreleme) algoritmaları, performans açısından simetrik şifrelemeye en yakın asimetrik eşdeğerini sunar. Eddine ve diğ. (2021) ECC'ye dayalı, gizliliği koruyan, geliştirilmiş bir kimlik doğrulama şeması önermektedir. Kayıtlanma esnasında oturum koruma işlemini yerine getirmek için SIP protokolünden yararlanan bu çalışmada anonimlik vurgulanan diğer bir noktadır. Dhillon ve Kalra (2019) VoIP iletişiminin performans verimliliğini artırmak için ECC kullanarak biyometrik tabanlı bir kimlik doğrulama modeli tasarlamıştır. Bu çalışma ECC yöntemi ile anahtar üzerinde daha hızlı anlaşma için karşılıklı kimlik doğrulama yapan çalışmalardan birisidir. ECC teknolojisinin hız performansından faydalanan bu çalışma zaman açısından sıkıntılıdır ancak güvenlik açısından etkili olan biyometrik kimlik doğrulama ile literatüre katkıda bulunmaktadır. Ayrıca son zamanlarda ECC ile kimlik doğrulama yöntemleri anahtar boyutu ve hız açısından ele alındığında oldukça popüler hale gelmektedir (Hammi ve diğ., 2018; Sureshkumar ve diğ., 2018). IP cihazlar arasında şifreleme için eliptik eğri kriptografisi (ECC) yöntemi kullanılmaktadır. ECC algoritmasının sağladığı güvenlik seviyesi, Rivest-Shamir-Adleman (RSA) ile aynı düzeydedir ancak ECC aynı güvenliği daha küçük bit uzunluğunda anahtar boyutu ile sağlar ve ayrık logaritma problemini çözmenin zorluğuna dayanır.

Blok zincir ağda kayıtlı verilerin bütünlüğünü ve yapılan işlemlerin inkâr edilemezliğini sağlayan şeffaf, güvenli ve güvenilir bir platformdur. Veri tabanlarından farklıdır çünkü blok zincirinde kayıtlı veriler silinemez veya değiştirilemez. Ayrıca akıllı sözleşmeler ile merkezi olmayan yapıyı destekler ve tarafların karşılıklı güvenini sağlar. Blok zincirin güvenli yapısını kullanan çalışmalardan biri olan Sheron ve diğ. (2020) doğrudan cihazlar arası merkezi olmayan kimlik doğrulama yöntemini cihaz doğrulama ve mesaj doğrulama olarak iki parçaya ayırarak Kablosuz Sensör Ağ (WSN) ve Nesnelerin İnterneti (IoT) yapısı içerisinde güvenliği sağlamaktadır. Ancak kayıtlanma fazında ürettiği kimlik (ID) bilgisini merkezi otorite (CA vb.) ile paylaşır. Yani tamamen merkezi olmayan bir yöntem sağlamamaktadır. Zhihua Cui ve diğ. (2020) ise hibrit bir blok zinciri kullanarak ağın yönetimini kolaylaştırmaktadır. Yine IoT tabanlı bir mimari için tasarlanan bu model tek nokta hatasını önlemek için ağı parçalara bölmektedir. Kumar ve Chouhan (2021) akıllı ev sisteminde güvenli bir kimliklendirme metodu sunmaktadır. Önceden belirlenen gizli bir anahtarı sisteme kaydolan kişinin kimlik bilgisi ile birlikte akıllı kartlara depolayarak ağa erişecek tüm aygıt sahipleri ile paylaşır. Ancak bu durumda merkezi kimlik doğrulama modeline hala ihtiyaç vardır. Benzer bir çalışmayı farklı bir alanda uygulayan Feng ve diğ. (2019) Araçsal Tasarsız Ağlar (VANET) yapısı içerisinde araçlara ilk üretim esnasında yüklenen değerler ile kayıtlanır ve önceden yüklenen değerler ile ilk anahtar dağıtımı için merkezi bir otoriteye ihtiyaç duyar. Dijital aygıtlar açık sistemler de herhangi bir kimlik doğrulaması olmadan ağa erişebilir. Bu yüzden akıllı şebekeler için kanıta dayalı, güvenli ve kimlik doğrulamalı anahtarsız yeni bir model öneren Zhang ve diğ (2019) anahtar yönetimi için blok zinciri teknolojisini kullanmaktadır. Blok zinciri ağı otonom bir çalışma yapısında olan akıllı sözleşmeler ve veri kurcalama saldırılarına dayanabilecek merkezi olmayan dağıtık defterler sağlar. Ayrıca benzer yapıda Patil ve diğ. (2020) mahremiyet korumalı bir mimari sunmaktadır. Bu çalışmalar dağıtık yapı üzerine kurulu olan blok zincir teknolojisi ile kullanılsalar da hala ilk etapta anahtar dağıtımı için merkezi bir yapıya ihtiyaç duymaktadır. Diğer taraftan, eşler arası ağlarda kimlik doğrulama son yıllarda güvenliği artıran önemli bir unsurdur. Bu açıdan Sunghyuck Hong (2020) IoT sensor düğümleri arasında uçtan uca kimlik doğrulamayı blok zinciri teknolojisi ile gerçekleştirmektedir. Blok zincirinde meydana gelen iş yükünü hafif (lightweight) protokol kullanarak azaltan bu çalışma daha güvenli bir mimari sunmaktadır. Ayrıca blok zinciri çalışmalarında genel bir inceleme yaparak temel mimarisinin kimlik

doğrulama teknolojisine yatkınlığını gösteren bazı çalışmalar da bulunmaktadır (Varshney ve diğ., 2019; Zhang ve Lee, 2020; Tanriverdi ve Üstündağ, 2019; Minoli ve Occhiogrosso, 2018).

Son yıllarda farklı bir bakış açısı olarak kimlik doğrulama yöntemi için bulut tabanlı çözüm önerileri getirilmeye başlanmıştır. Hızlı hesaplamalarla dağıtık yapıyı destekleyen çalışmalardan biri olan Guo ve diğ. (2019) blok zincir teknolojisini hesaplama ve veri depolamayı veri kaynaklarıyla birlikte kullanan dağıtık bir bilgi işlem modeli olan uç bilişim (edge computing) teknolojisi ile bir araya getirerek etkin bir model önermektedir. Gerçek zamanlı verinin iletimi esnasında hız ihtiyacı yüksek olan bir yapıya uygun model öneren Patwary ve diğ. (2020), sis bilişim cihazlarının blok zincir kullanarak bulut katmanında birbirlerini karşılıklı olarak doğrulayabildiği, güvenli merkezi olmayan konum tabanlı uçtan uca kimlik doğrulama modeli önermektedir. Bu çalışmalar enerji kısıtı olan cihazlara uygulandığı için enerji tüketiminde verimliliği artırır. Çünkü blok zincir platformu cihazların her seferinde merkezi bir yapıdan onay alması yerine cihazlar arası kimlik doğrulama yapısı oluşturmuştur. Temelde bu ve benzer çalışmaların amacı güvenliği sağlarken enerji tüketimini düşürmektir. Zhong ve diğ. (2020) bulut teknolojisi için anonim kimliğe dayalı bir yöntem geliştirmişlerdir. Verilerini depolamak için bulut teknolojisini kullanan cihazları güvenilir üçüncü taraf olarak kabul eden bu çalışmada enerji tüketimi bulut sistemler arasında iletim esnasında oldukça azalmaktadır. Ancak bu durum güvenlik ve mahremiyet açısından yeni zorluklar ortaya çıkartmaktadır. Bulut tabanlı çözüm önerileri ile kimlik doğrulamanın bulut sistemlerde yavaş kaldığı tespit edilmiştir.

Literatürdeki blok zincir tabanlı çalışmalar incelendiğinde dağıtık mimari içerisinde doğrudan cihazlar arası kimlik doğrulama gerçekleştirilebildiği görülmektedir. Ayrıca blok zincir mimarisinin anonim, şeffaf ve merkezi sistem ihtiyacını ortadan kaldıran bir platform olduğu anlaşılmaktadır. IoT, WSN ve akıllı şebekeler gibi teknolojilerde blok zincir gittikçe yaygınlaşmaktadır (Aste ve diğ., 2017; Dinh ve diğ., 2018; Yang ve diğ., 2018; Da Xu ve diğ., 2021). Literatür incelendiğinde VoIP uygulamalarında güvenli kimlik doğrulaması için blok zincir teknolojisi ile bütünleşmiş (entegre) kullanımı açısından henüz yapıcı bir çözüm getirilmemiştir.

1.3. Tez Organizasyonu

Bu tezin geri kalanı şu şekilde organize edilmiştir:

Bölüm 2'de bilgisayar ağlarında iletişim ve güvenlik konusunu üç ana başlık altında incelemektedir. Bunlar sırasıyla bilgisayar ağlarında iletişim, bilgisayar ağlarında güvenlik ve iletişimde güvenlik şeklinde kategorize edilmiştir. Veri şebekeleri üzerinden iletişim, bilgisayar ağ mimarileri, uçtan uca veri iletimi ve noktadan noktaya veri iletimi açıklanarak multimedya ağlarından biri olan VoIP teknolojisinin altyapısı ve bilgisayar ağlarındaki yeri açıkça belirtilmiştir. Güvenli veri iletiminin anlaşılması için güvenlik unsurları, kriptografik altyapı ve blok zincir teknolojisi sırasıyla açıklanmıştır. Bu tez çalışmasında blok zincir ve VoIP entegrasyonu ile kimlik doğrulama mekanizması sunulmuştur. Bu açıdan, VoIP mimarisinde merkezi sunucu kullanan geleneksel güvenlik mekanizmalarındaki yöntemler açıklanmış ve blok zincir teknolojisinin merkeziyetçi yapıdaki sorunları çözüm şekli belirtilmiştir.

Bölüm 3'te blok zincir teknolojisinin VoIP ağlarında uygulanabilirliğini göstermek için önerilen kimlik doğrulama mekanizması sunulmaktadır. Tezde sunulan mekanizmanın ana unsurları olan sistem bileşenleri ayrıntılı olarak açıklanmıştır. VoIP uygulamalarının temel çalışma yapısı, VoIP ve blok zincir entegrasyonu ve bu entegrasyonun güvenliğini sağlamak için ortaya konulan çözüm anlatılmaktadır. Blok zincir teknolojisinin güvenlik sorunlarına karşı sunduğu dağıtık yapısı ele alınmıştır. Sistem kimlik doğrulama mekanizması adım adım detaylandırılmıştır. Ayrıca VoIP ve blok zincir entegrasyonu göz önünde bulundurularak örnek bir Birleşik Modelleme Dili (UML) diyagramı üzerinden kimlik doğrulama şemasının genel akışı ile önerilen mekanizmanın çalışma yapısı adım adım anlatılmaktadır. Ardından, VoIP protokol yığını (protocol stack) ile VoIP ve blok zincir teknolojisinin çalışma detaylarını TCP/IP referans modeli üzerinden gösterilmektedir. Son olarak tercih edilen konsensüs algoritmasının hata toleransı ele alınmaktadır.

Bölüm 4'te tezde sunulan kimlik doğrulama mekanizmasının ağdaki farklı saldırılara karşı sağlamlığını ve güvenliğini resmi (formal) ve resmi olmayan (informal) yöntemlerle analiz edilmektedir. VoIP iletişim ortamının güvenliğini sağlamak için çok sayıda güvenlik unsuru bir arada karşılanmalıdır. Bu nedenle, bu bölümde güvenlik analizini ve VoIP iletişiminde tezde sunulan kimlik doğrulama mekanizmasının uygunluğunu değerlendirmek için güvenlik unsurları ele

alınmaktadır. Resmi olmayan güvenlik analizinde önerilen yöntemin erişilebilirlik, güvenilirlik, gizlilik, bütünlük, sürdürülebilirlik, inkâr edememe, kimlik doğrulama, kimlik teşhisi, ölçeklenebilirlik unsurları açısından incelenmiştir. Önerilen modelin kimlik hırsızlığı, sahtecilik, ikame, ortadaki adam, tekrarlama ve dağıtık hizmet aksatma saldırılarına karşı sağlamlığı detaylı şekilde açıklanmıştır. Ayrıca tezde sunulan mekanizmanın güvenli olduğu AVISPA aracıyla resmi olarak kanıtlanmaktadır.

Bölüm 5'te tezde sunulan kimlik doğrulama mekanizmasının uygulaması anlatılmış ve deneysel çalışma sonuçları değerlendirilmiştir. Deneyler sonucunda elde edilen performans ölçümleri adım adım açıklanmıştır. Ayrıca kimlik doğrulama mekanizmasının blok zincir tabanlı olması sebebiyle finansal maliyet ele alınarak detaylı incelenmiştir. Önerilen yöntem, literatürdeki benzer çalışmalarla karşılaştırılarak üstün yönleri ortaya konulmuştur.

Son olarak bölüm 6'da bu tez çalışmasında sunulan kimlik doğrulama mekanizmasının genel bir özeti sunularak üstünlükleri ve avantajlarından bahsedilmektedir. Blok zincir teknolojisinin VoIP alanında kullanımı tartışılmaktadır.

2. BİLGİSAYAR AĞLARINDA İLETİŞİM VE GÜVENLİK

Bu bölüm bilgisayar ağlarında iletişim ve güvenlik konusunu üç ana başlık altında incelemektedir. Bunlar sırasıyla bilgisayar ağlarında iletişim, bilgisayar ağlarında güvenlik ve iletişimde güvenlik şeklinde kategorize edilmiştir. Veri şebekeleri üzerinden iletişim, bilgisayar ağ mimarileri, uçtan uca veri iletimi ve noktadan noktaya veri iletimi açıklanarak multimedya ağlarından biri olan VoIP teknolojisinin altyapısı ve bilgisayar ağlarındaki yeri açıkça belirtilmiştir. Güvenli veri iletiminin anlaşılması için güvenlik unsurları, kriptografik altyapı ve blok zincir teknolojisi sırasıyla açıklanmıştır. Bu tez çalışmasında blok zincir ve VoIP entegrasyonu ile kimlik doğrulama mekanizması sunulması sebebiyle VoIP mimarisinde merkezi sunucu kullanan geleneksel güvenlik mekanizmalarındaki yöntemler açıklanmış ve blok zincir teknolojisinin merkeziyetçi yapıdaki sorunları çözüm şekli detaylı şekilde anlatılmıştır.

2.1. Bilgisayar Ağlarında İletişim

İkilik tabanda kodlanmış verinin bilgisayarlar arasındaki gerilim sayesinde aktarılmasını kapsayan iletişim türüne sayısal iletişim denmektedir. Bilginin sayısal olarak ifade edilmesi ise kodlama olarak adlandırılır ve bu terim sayısal bilgiye ait 1 ve 0'ların yeniden elde edilecek bir elektriksel işarete dönüştürülmesidir. Kısaca bilgilerin 1 ve 0'lar halinde tutulması için gerekli dönüşümdür.

Bilgisayar ağlarında veri iletişimi kablo gibi bir tür bağlantı yoluyla iki bilgisayar (düğüm) arasında gerçekleşir. İletim ancak gönderici (sender) ve alıcı (receiver) arasında kullanılacak olan veri formatları, hizmet işlevleri, işaretler ve temel aktarım birimlerinin değerlendirme yöntemleri üzerinde karşılıklı mutabakat sağlanarak gerçekleşir. Kurallar veya veri iletişimini yöneten bir dizi kural olan protokoller, veri formatlarının ve bilgi alışverişinin zamanlamasını düzenleyen kural dizisidir (Tanenbaum ve Wetherall, 2011). Başka bir ifadeyle, paketlerin gönderilmesinde ve alınmasında önemli işlevi olan kurallar dizinidir. Gönderim Kontrol Protokolü (TCP), Kullanıcı Veri Protokolü (UDP) ve IP benzeri protokoller bilgisayar ağlarında

haberleşmenin önemli yapı taşlarındandır. Aynı ağ içinde iki bilgisayar karşılıklı olarak iletişim kurabilmek için aynı protokolü kullanmak zorundadır. Ayrıca veri, hesaplama cihazları arasında seri ve paralel iletim şeklinde aktarılır.

İnternet milyonlarca cihazın bir araya gelerek oluşturduğu ağdır. Veri aktarımında genel olarak fiber optik, bakır, radyo veya uydu iletişim linki kullanır. Bu veri aktarımı esnasındaki bağlantı hızına bant genişliği (bandwidth) adı verilir ve sistem üzerindeki 1 saniyede ne kadarlık veri geçtiğini ölçen birimdir (Kurose ve Ross, 2012). Veri aktarımının kapasitesini ve hızını ölçmek için saniyede aktarılan Megabit cinsinden veri sayısı (Mbps) veya saniyede aktarılan Gigabit cinsinden veri sayısı (Gbps) benzeri ölçü birimleri kullanır. Bu veriler parçalara ayrılarak paketler haline getirilir ve internet ortamında yönlendirici ve anahtar cihazları kullanılarak paketlerin iletimi sağlanır. Bilgisayar ağlarında uç sistem ve uç sistemleri birbirine bağlayan haberleşme bağlantıları ile internet paketleri doğru lokasyona iletilir. Temelde bütün bilgisayar ağlarının aynı ortamda birleşmesi ile internet oluşmaktadır ve internet birbirine bağlanmış ISS'lerdir (Internet Servis Sağlayıcı) (Özbilen, 2006).

Bilgisayar ağlarının temel işlevi bilgi, kaynak ve uygulamaların paylaşımını gerçekleştirmektir. Evrensel bilgisayar ağı olan internet tüm bilgisayarları birbirine bağlar. İnternet ortamında iki tür bilgisayar bulunur. Bunlar sırasıyla; sunucu ve istemcidir. Bilgisayarlar birbirlerine Yıldız, Halka veya Mesh topolojisi benzeri bir ağ topolojisi ile bağlanırlar. Genel olarak topolojilerde 2 temel ifade kullanılır bunlar sırasıyla düğüm (node) ve paket (packet) tir. Düğüm topoloji içerisinde ağa bağlı herhangi bir cihazdır. Düğüm başka bir değişle iletişim sistemi içerisinde karşılıklı çalışma için gerekli protokolün tamamını veya bir kısmını içeren cihazdır. Paket ise düğümlerin birbirine gönderdiği mesajlar anlamına gelmektedir.

İletişim teknolojisinde OSI referans modeli teorik bir modelleme olarak bilgisayarlar arası iletişim şeklini göstermek için tasarlanmıştır (Tanenbaum ve Wetherall, 2011). Bilgisayar veri haberleşmesi süresince yapılması gereken işleri katmanlar düzeyinde tanımlayan referans bir modeldir. Bir düğümün iletişim sürecini çok katmanlı yapı şeklinde tanımlar. 7 katmandan oluşan OSI referans modeli Uygulama Katmanı (Application Layer), Sunum Katmanı (Presantation Layer), Oturum Katmanı (Session Layer), Taşıma Katmanı (Transport Layer), Ağ Katmanı (Network Layer), Veri Bağı Katmanı (DataLink Layer) ve Fiziksel Katman (Physical Layer) olarak sıralanır. Bu

katmanlı modelin tasarlanmasındaki amaç ağı daha iyi yönetebilmektir. Her katman bir servisle ilgilenir. Her alt katman üstteki katmana dayanır. Katmanlar birbirlerinin bilgilerine dayanarak ilerlerler. Ağ uygulamaları uygulama katmanı tarafından desteklenir. İşlem'den (process) işleme veri transferi taşıma katmanında gerçekleşir. Veri aktarım katmanı olarak taşıma katmanını kullanılır ve bu katman ağ üzerindeki iletişim kanallarının kurulması yönetilmesi ve sonlandırılmasından sorumludur. Kurulan iletişim altyapısı, tercih edilen protokole göre farklılık gösterir. TCP ve UDP protokolü kullanan taşıma katmanı TCP protokolü üzerinden bağlantı temelli (connection oriented) ve UDP protokolü üzerinden bağlantısız (connectionless) sanal iletişim kurarlar. Bu durumun temel sebebi TCP protokolü veri aktarımı öncesinde iki tarafın karşılıklı görüşmesini sağlar. Genel hatları ile TCP protokolü bir telefon görüşmesi yapar gibi görüşeceği tarafın müsaitlik durumunu sorgular. Bu açıdan TCP protokolü kullanan uygulamalar güvenilir bir iletişim sağlar. UDP protokolü ise iletilen paketlerin karşı tarafa ulaşacağının garantisini vermez. Hızlı bir şekilde paketleri iletilecek kişiye gönderir. Bu durum UDP protokolünü TCP protokolüne göre birçok açıdan eksik gibi gösterse bile internet ağı üzerinden gerçekleşen VoIP yani IP üzerinden ses, video veya mesaj gönderen gerçek zamanlı uygulamalar için daha uygundur (Özbilen, 2006).

Kaynaktan hedefe paketlerin hangi yoldan gideceği ağ katmanında belirlenirken komşu ağ elemanı ile veri transferinin nasıl gerçekleşeceğini veri bağı katmanı belirler. Fiziksel katman ise gerçek ortamda bit seviyesindeki verinin ilerlemesini ifade etmektedir.

2.1.1. Veri Şebekeleri Üzerinden İletişim

Ağ teknolojisi iletişim cihazlarının kurdukları bağlantı üzerinden veri ve ses aktarımı yapmaktadır. Ancak mesafelerin uzaması ve gelişen altyapının iletişim ihtiyaçlarını değiştirmesiyle zaman içerisinde uzak mesafe veri aktarımı ihtiyacı sonucu veri şebekeleri teknolojisi sürekli gelişmiştir. Gerçek zamanlı verilerin iletimi hız ve güvenilirlik gerektirir. Bu açıdan devre anahtarlamalı şebekeler sesin anlık iletimi için geliştirilmiştir. Devre anahtarlamalı şebekeler zaman içinde uzak mesafe görüşmelerinde ihtiyaç duyulan iletişim altyapısı ile veri iletimi alanında etkin olarak kullanılmaya başlanmıştır. Temel olarak 3 kategoriden oluşan devre anahtarlamalı

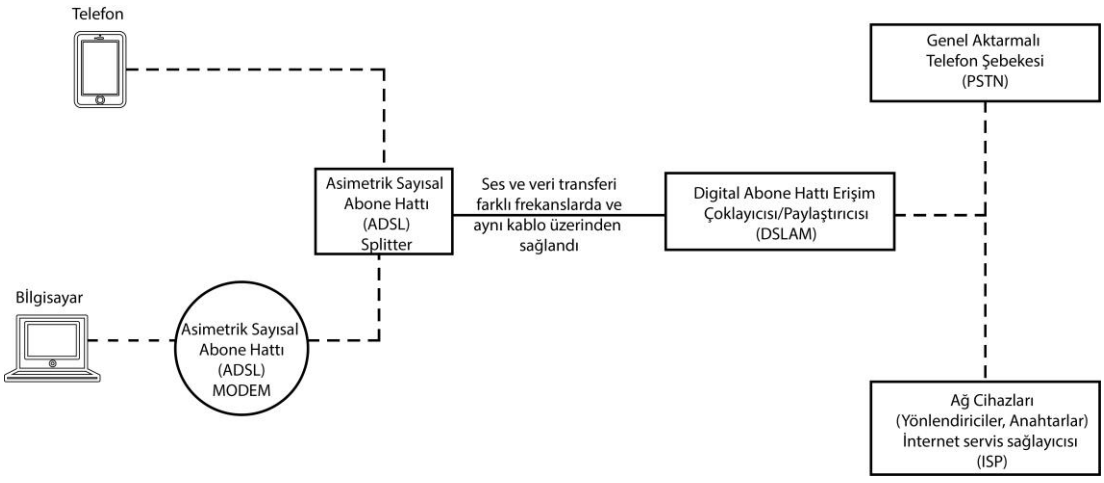
şebekeler sırasıyla; PSTN, Bütünleştirilmiş Sayısal Ağ Hizmetleri (ISDN) ve Zaman Bölmeli Çoğullama (TDM) teknolojileridir (Tanenbaum ve Wetherall, 2011).

Uzak mesafe veri iletimini hem ses olarak hem de veri olarak ileten bu devreler uç noktalar arasında görüşme sağlamaktadır. Ancak devre anahtarlamalı şebekeler maliyetli iletişim sunar. Gereksinime göre veri güvenliği, kaynak kullanımı vb. konularda duyulan ihtiyaç sonucu TDM şebekesi oldukça geliştirilmiştir. PSTN ise telefon santrallerinin birbirine bağlanarak oluşturduğu veri şebekesidir. Ortalama 64 Kbps bant genişliği üzerinden veri aktaran PSTN şebekesinin kısıtlı veri aktarımı sebebiyle ISDN teknolojisi geliştirilmiştir. Böylece veri şebekeleri analog iletişimden sayısal iletişime geçiş yaparak veri iletim hızını arttırmıştır. Ancak ISDN şebekesi noktadan noktaya ve sabit bant genişliğini gerçekleştirecek altyapıyı sağlayamamıştır. TDM ise her kanal için ayrı bir zaman ayırarak bit dizilerini iletir ve bu iletimi tek kanal üzerinden gerçekleştirir. Bu durumun sonucu olarak, TDM veri şebekesi geliştirilerek gerçek zamanlı veri ileten uygulamalar için daha etkin iletişim altyapısı oluşturulmuştur. Genel hatları ile devre anahtarlamalı şebekeler devrenin kurulması sonrası verinin iletilmesi ve iletimin sonlandırılması prensibiyle çalışmaktadır. Böylece veri iletimi daha güvenli hale getirilmiştir ve akış kontrolü sabit hatlarla iyileştirilmiştir. Veri iletiminde oluşturulan gecikmeler noktadan noktaya bağlantılar ile güvenli ve güvenilir hale getirilmiştir. Ancak devre anahtarlamalı sistemlerin olumlu yanlarına rağmen, yatırım maliyeti açısından pahalı bir teknoloji olması nedeniyle alternatif çözümler üretilmiştir (Çölkesen ve Örencik, 2003).

Paket anahtarlamalı şebekeler veriyi daha küçük boyutlara ayırarak ileten bir teknolojidir. Önceden belirli bir veri aktarım yolu kullanmaz. Günümüzde internet paket anahtarlama altyapısına göre veri aktarımı gerçekleştirmektedir. Paket anahtarlamalı şebekelerde yerel alan ağında veri iletim katmanı protokolü Ethernet kullanırken, geniş alan ağında Frame Relay protokolü kullanır. Bant genişliği konusunda iletişim altyapısı için daha esnek yapıya sahip olan paket anahtarlamalı şebekeler maliyet açısından daha ekonomiktir. Paket anahtarlamalı şebekelerde paketler uygun boyuttaki bloklar içerisinde veri aktarımı gerçekleştirir. Ağ iletim mekanizmasındaki karar algoritmaları ile anahtarlama lokasyonlarındaki veri iletilecek yere gönderilir. Her seferinde farklı yolları kullanan paketler hedef lokasyona ulaşır. Böylece ağda hataya duyarlılık artar. Örneğin Eş zamansız Aktarım

Modu (ATM) paket anahtarlama teknolojisine göre oluşturulmuş bir veri iletim altyapısıdır.

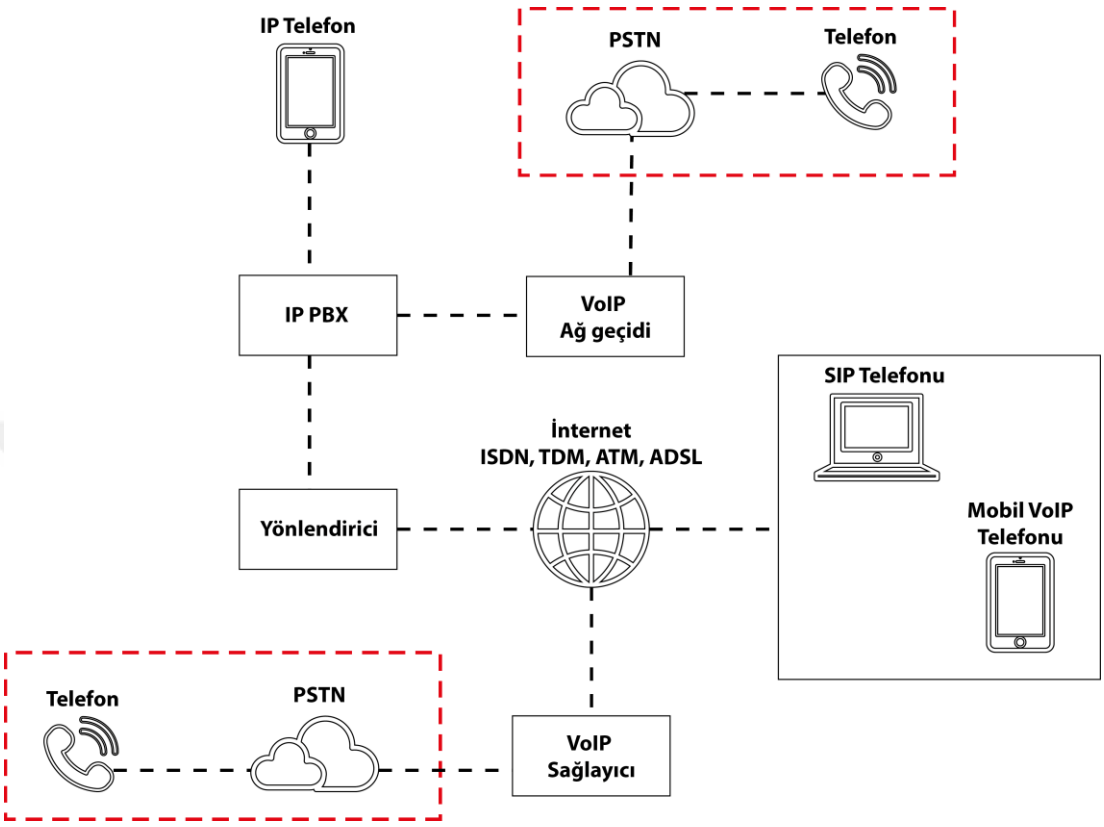
Gerçek zamanlı veri iletimi ile internet yüksek bant genişliğine ihtiyaç duymuştur. PSTN, ISDN, ATM ve Frame Relay teknolojileri yüksek maliyet gereksinimi sebebiyle son kullanıcılar için kullanışlı bir altyapı sunmamaktadır (Kolahi ve diğ, 2017). Örneğin, ISDN üzerinden gerçekleşecek bir arama için aradığınız numaranın da ISDN'ye sahip olması, veri iletişimi yapabilmesi ve hem sizin hem de aradığınız tarafın aynı iletişim protokolünü kullanması gerekiyordu. Diğer yandan Çevirmeli Ağ (Dial-up) sistemlerde telefon ile internet aynı anda kullanılamıyordu. Bu sebeple Dijital Abone Hattı (DSL) sistemi geliştirildi (Yen ve diğ., 2001; Özbilen 2006). Ardından veri iletimi çoğunlukla Asimetrik Sayısal Abone Hattı (ADSL) bağlantı hizmeti ile gerçekleşmeye başladı. Bu durum hem maliyet uygunluğu sağlamaktadır hem de yüksek bant genişliği ile multimedya ağ uygulamalarında internet ağını kullanışlı hale getirmektedir. Günümüzde bant genişliğinin yüksek kapasitelere ulaşması veri iletimi açısından son kullanıcılar için interneti daha kullanışlı kılmıştır. Ayrıca ADSL teknolojisi ses ve internet verisini birbirinden ayırarak analog sinyalle çalışan telefon kullanımını engellemez. Ağ Adresi Dönüştürme (NAT) ve Sanal Özel Ağ (VPN) benzeri teknolojileri destekleyerek hem güvenlik hem de iletişimde esneklik sağlar. Bu açıdan yüksek bant genişliği sağlayan ADSL teknolojisi iletişim alt yapısında kullanılarak sürdürülebilir bir iletişim sağlamaktadır.



Şekil 2.1: DSL Teknolojisi ile Aynı Anda Ses ve Veri İletimi.

Şekil (2.1)'de açıkça görüldüğü gibi veri DSL telefon hattı ile internet ağı üzerinden aktarılabilir. Ayrıca ihtiyaç duyulması durumunda ses telefon hattı ile telefon ağı olan

PSTN'e gönderilebilir. Böylece internet ve telefon hizmeti aynı anda kullanılabilir. Şekil (2.2)'de ise veri şebekesi üzerinden VoIP ağ altyapısı gösterilmiştir. Kırmızı ile işaretli PSTN ağı ücretli iletişim kısmını göstermektedir.



Şekil 2.2: Veri Şebekesi Üzerinden VoIP Ağ Altyapısı.

IP Telefon Santrali (IP PBX) cihazlarına kayıt olan IP telefonları VoIP servis sağlayıcılar vasıtasıyla IP tabanlı ağda, VoIP Ağ Geçidi (Gateway) vasıtasıyla ise diğer dijital ve analog taşıyıcılar üzerinden birbirleriyle iletişim kurar. Paket iletimi internet ortamında verinin iletileceği bilgisayara giderken kuyruklama gerçekleşir. Yönlendiricide kuyruğa giren paketler önceliklendirme protokolü ile iletilir. Ağda ses paketlerinin önceliği yüksektir. Bazı durumlarda paketlerde kayıplar da yaşanabilmektedir. Yönlendirici üzerinde bekleme alanı (buffer) dolu olma ihtimali ve paketin anlık kaybolma ihtimali bulunmaktadır. Bu durumda paket tekrar gönderilir veya ihmal edilir. Eğer paketlerin varış hızı yönlendiricinin çıkış hızından yüksekse kuyruklama gerçekleşir. Paketin büyük parçalar halinde iletimi ağda gecikmelere sebep olur. Bu durumda gerçek zamanlı veri iletiminde zorluklar yaşanabilir. Sunucu ve istemciler karşılıklı haberleşirken bir veriyi gönderecekleri zaman bu veri çok büyük olabilir. Bilgisayarlar bu veriyi paketlere ayırır (Kurose ve Ross, 2012). Paket

L bit uzunluğunda ise ve iletim hızını da *R* kabul edersek (link iletim hızından kasıt kapasite ve bant genişliği olarak ifade edilmektedir) bir bilgisayarın bir paketi ağ cihazı olan yönlendiriciye göndereceği paket iletim gecikme zamanı Denklem (2.1)'de gösterilmektedir.

$$\text{Paket İletim Gecikmesi} = \frac{\text{L(bits)}}{\text{R}\left(\frac{\text{bits}}{\text{saniye}}\right)} = \frac{1}{\text{saniye}} \quad \textbf{(2.1)}$$

2.1.2. Bilgisayar Ağ Mimarileri

Uygulama seviyesinde haberleşme sistemleri ağın nasıl çalıştığından veya mesajın hangi yolları kullanarak iletildiğinden ziyade her şeyin uygulama katmanında gerçekleştiği kabul edilir. Bu haberleşme sistemi içinde, ağa bağlı iki cihazın karşılıklı iletişim yöntemini ağ mimarisi belirler. Uygulama katmanında temelde kullanılan iki tür ağ mimarisi bulunmaktadır. Bunlar sırasıyla istemci-sunucu (client-server) mimarisi ve eşler arası (peer-to-peer) mimaridir (Granville, 2005). İstemci-sunucu mimarisinde sunucuların ağ hizmeti dışında başka bir işlevi bulunmaz. Sunucu her zaman çalışır durumdadır. IP adresi sabittir ve değişmez. Ağ altyapısına ölçeklenebilirlik sağlar. İstemci ise sunucu ile haberleşmeyi başlatır. Dinamik IP adresine sahiptir ve istemciler birbirleriyle doğrudan haberleşmezler.

Eşler arası ağ uygulamasında ise bir düğüm hem sunucu hem de istemci olarak kullanılabilir. Bu mimaride her zaman çevrimiçi olan bir sunucu yoktur. Farklı ve anlık olarak uç sistemler birbirleriyle doğrudan görüşür. İnternet aracılığıyla telefon görüşmesi yapılabilen uygulamalar (Skype, Viber vb.) veya IP TV sistemleri eşler arası mimariyi kullanır. Eşler arası mimaride servisi düğümler karşılıklı olarak birbirlerinden almaktadır. Bu mimaride talep durumunda ağdaki düğümlerden birine servis sunulmaktadır. Bu durum sonucu eşler arası mimari ağında ölçeklenebilirlik açısında sorunlar oluşabilmektedir. Kısaca eşler arası mimaride hem istemci hem de sunucu gibi davranan düğümler mevcuttur. Ancak ağ yönetimi oldukça zordur. Düğümler kendi aralarında haberleşir. Yukarı akım (Upstream) ve Aşağı akım (Downstream) açısından yüksek veri akışına sahiptir. Erişim ağları asimetrik yapıya sahiptir. Bu durumun sonucu olarak yukarı akım düşük ve aşağı akım yüksek bant genişliğine sahiptir. Eşler arası mimaride bu durum göz önüne alınmalıdır. Ayrıca güvenlik mekanizması istemci sunucu mimarisinde sunucu tabanlı olarak sağlanır. Ancak eşler arası ağlarda güvenlik ciddi sorunlar yaratabilir ve ağ güvenliği ciddi

önlemler gerektirir. Çünkü ağ herkese açık bir yapıda çalışır. Eşler arası ağlarda kimlik doğrulama veya yetkilendirme yoktur (Hong, 2020).

Ağ uygulamaları temel prensip olarak Veri Bütünlüğü (Data Integrity), İletim Zamanı (Transmit Time) ve Bant Genişliği kavramlarının bir arada sağlanmasına ihtiyaç duyar. Örneğin dosya transferi; veri bütünlüğü ve bant genişliğini önemserken zaman hassasiyeti taşımaz. Ancak gerçek zamanlı ses ve video uygulamaları veri bütünlüğü kavramından ziyade zaman hassasiyeti ve bant genişliğini öncelikli olarak konumlandırır.

Eşler arası (peer-to-peer) ve uçtan uca (end-to-end) kavramlarını incelediğimizde her ikisi de ağ iletişimi ile ilgili kavramlardır. Ancak bu kavramlar tamamen farklı seviyelerdedir. Uçtan uca kavramı, internet tasarımındaki ana ilkelerden biridir. İletişim, ağın uç noktaları arasında gerçekleştirilir. Mesajın iletileceği rotayı veya mesaj içeriğini önemsemez. Eşler arası kavramı ise, uygulama düzeyinde iletişim için bir kavramdır. Eşler Arası, iki uç düğüm cihazı arasında doğrudan iletişim kurmaktır. Uçtan uca ise ağdaki herhangi iki cihaz arasında gerçekleşen yöntemdir. İki cihazın son kullanıcı olması gerekmez. Yönlendiriciler, anahtarlar, sunucular veya güvenlik duvarları vb. bu cihazlara örnektir.

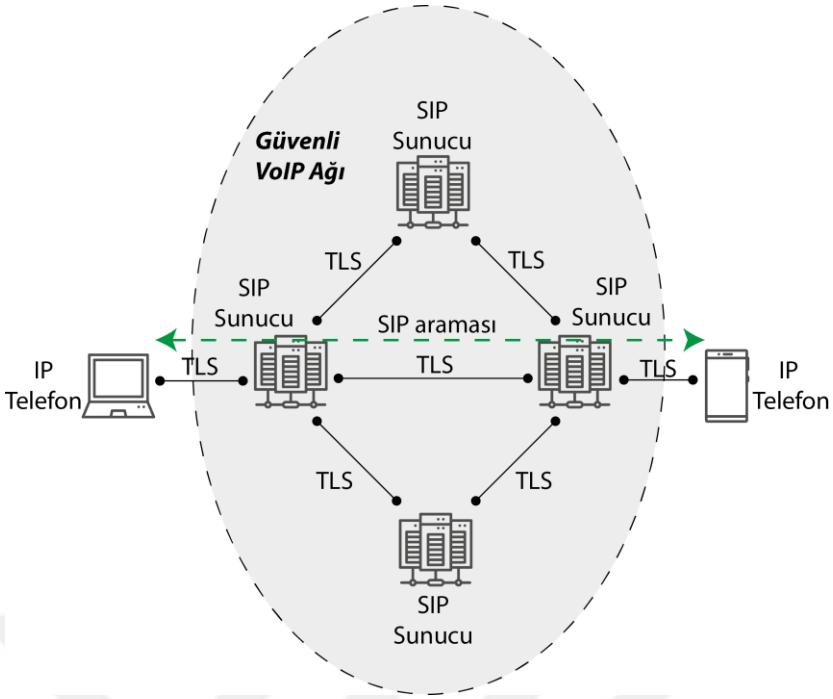
2.1.3. Uçtan Uca Veri İletimi

Taşıma katmanı iletişim kuracak iki cihaz arasında uçtan uca mantıksal bağlantı kurar. Mantıksal bağlantıdan kasıt fiziksel olarak hangi bitlerin gönderildiğinden ziyade karşı tarafa veri akışının sağlanıp sağlanmadığı anlamındadır. Taşıma katmanındaki TCP protokolü güvenilir iletişim sağlar. Mesajlaşma anında veri bütünlüğünü korur. Akışı kontrol eder. Gönderici cihaz alıcı cihaz tarafı bunaltmaz ve ağın fazla yüklenmesine engel olur. Ancak TCP servis modeli zaman hassasiyeti, bant genişliği garantisi ve güvenlik konusunda garanti vermez. Bağlantı merkezlidir ve önce alıcı cihaz ile bağlantı kurar daha sonra paket gönderimine başlar. UDP protokolü ise veri transferini güvenli şekilde gerçekleştirmez. Gönderilen mesajın yerine ulaştığını kontrol etmez. Akış kontrolü veya iletim hattındaki tıkanıklığı önemsemez. Ancak TCP servislerine göre daha hızlı servis sunar. Kısacası kaliteli paket gönderimi yapıp veri kaybını engellemek için TCP servisi kullanılır. Veri kaybını önemsemeden hızlı iletim UDP servisi ile gerçekleşir. Her iki protokolde İnternet Mühendisliği Görev Grubu (IETF) tarafından paket anahtarlamalı ağlarda son derece güvenilir bir iletişim bağlantısının

nasıl kurulacağını ve sürdürüleceğini belirleyen standartlar olarak tanımlanır. Ancak multimedya veri akışı ve internet üzerinde telefon kullanımlarında zaman hassasiyeti sebebiyle genellikle UDP servisleri kullanılır (Çölkesen ve Örencik, 2003; Yang ve Hanzo, 2021).

Gerek TCP gerek UDP servisleri şifreleme sunmamaktadır. Gelen paketleri internet üzerinden güvensiz şekilde transfer ederler. Güvenli Giriş Katmanı (SSL) veya TLS benzeri protokoller ile TCP bağlantılarının şifrelenmesi mümkündür. Böylece hem veri bütünlüğü sağlanır hem de son kullanıcı tarafında bir yetkilendirme söz konusu olur. SSL veya TLS protokolleri uygulama katmanında kullanılır. Böylece TCP servisleri şifreli veri aktarımı gerçekleştirir (Comer, 2009).

SIP RFC, gizli dinleme, mesaj kurcalama, mesajı tekrar iletme vb. saldırılara karşı gerekli korumayı sağlamak için TLS kullanılmasını önerir. Kullanıcılar bir arama yapmak ve belirli bir düzeyde gizlilik sağlamak istediklerinde TLS protokolünü kullanarak SIP sinyalleşmesini sağlayabilirler (Thermos ve Takanen, 2007). SIP mesajları TLS üzerinden iletilerek güvenli kanal oluşturulur. TLS, ortadaki adam saldırılarına karşı koruma sağlamak için üçüncü taraflardan sağlanan bir sertifika kullanarak karşılıklı kimlik doğrulama gerçekleştirir. Böylece VoIP cihazı hem kendini hem de SIP sunucusunu (veya SIP kaydedicisini) ağda doğrulayabilir. Hem simetrik şifreleme hem de özetleme fonksiyonlarıyla güvenliği belirli ölçüde sağlar. Ek olarak, SRTP protokolü için anahtar değişimi üzerinden oturum anahtarı üretilmesini sağlayan TLS taraflar arasında medya iletim şifrelemesini gerçekleştirir. TLS, iki uç nokta (istemci/sunucu ilişkisi) arasında gizlilik sağlamasına rağmen, ağ içerisinde aradaki SIP sunucular aracılığıyla güvenliği sağlar. SIP sunucular üzerinden bağlantı kuran iki kullanıcı arasında TLS uçtan uca (end-to-end) güvenlik sağlar ancak doğrudan eşler arası gizliliği desteklemez. Her segment için ayrı bir TLS bağlantısı kurar. Şekil (2.3) bu ilişkiyi göstermektedir.



Şekil 2.3: SIP Mesaj Koruması için Uçtan Uca TLS Kullanımı.

2.1.4. Noktadan Noktaya Veri İletimi

Ağ katmanı ulaşım katmanından gelen segment'i datagram haline getirir ve bu datagramın hangi ağ cihazları üzerinden gideceğine karar verir. Yönlendirme (routing) ve iletme (forwarding) işlemlerini gerçekleştirir. İletme yönlendiricinin girişine gelen paketin uygun çıkışa yönlendirilmesidir. Yönlendirme ise paketin kaynaktan hedefe hangi yoldan gideceğinin bulunmasıdır. Yönlendirme algoritmaları bu süreçte önemli işlevlere sahiptir.

Düğümler arası haberleşme kanalı bağlantı (link) olarak adlandırılır ve kablolu, kablosuz olarak 2 kategoriye ayrılır. Çerçeve (frame) veri bağlantı katmanında verinin ismidir. Bu katmanda işlev veriyi fiziksel katmanı iletmektir. Bu katmanda Ethernet ve Frame Relay protokolleri kullanılır. IPv4 ağ katmanında 32 bit ve IPv6 ağ katmanında 128 bit adrestir ve veri iletimi için kullanılırken MAC adresi çerçevelerin (frame) bir arayüzden diğerine iletimi için kullanılır ve 48 bittir (Tanenbaum ve Wetherall, 2011).

2.1.5. Multimedya Ağları

Multimedya ağlarında uygulamalar sesin veya videonun ağ üzerinden aktarımı şeklini ifade eder. VoIP veya gerçek zamanlı ses ve video iletimi bu ağdaki uygulamalara örnektir. Ses veya video verisi temelde analog sinyallerdir. Bu analog sinyaller dijital

sinyallere dönüştürülerek ağ içerisinde iletim gerçekleşir. Telefon için saniyede 8000 örnek alınarak veri aktarımı sağlanır. Çünkü insan sesini sayısallaştırmak için her örneğin 8 bitle örneklendiği varsayılarak bit hızı hesaplanır. İnsan sesi normal olarak 0 değerinden 4000 Hz'e (Hertz) kadar frekansları içerir. Telefon hatları için örnekleme hızı 4000 değerinin iki katı alınarak 8000 örnek/sn sonucu elde edilir. Bit hızı ise örnek başına düşen bit sayısı olan 8000 değerinin 8 ile çarpılması ile hesaplanır. Diğer bir ifade ile 1 saniyede aktarılan bit oranı için 256 seviyelendirme (quantized values) değerimiz varsa bu durumda her bir örnek için 8 bit veri kullanılacağı anlamına gelmektedir. Sonuç olarak 64000 bps (Bit/saniye) yani 64 kpbs (Kilobit/saniye) ses aktarımı gerçekleşir. Alıcı taraf aktarılan bitleri analog hale dönüştürür. Seviyelendirme yeterli seviyede yapılmadıysa ses verisinde kayıplar yaşanır. Saniyedeki bit sayısı ses kalitesinin önemli bir faktörüdür. Örneğin internet üzerinden ses aktarımı (IP telefonu, VoIP telefonu veya SIP telefonu benzeri bir cihazla) saniyede 5.3 kbps olarak gerçekleşir. Ses kalitesini artırmak için seviyelendirme artırılır. Ancak bu durumda her seviyelendirme bit kullanımındaki artış anlamına gelmektedir. Bu durum veri boyutunu artırır. Veri aktarımında denge sağlanmalıdır. Dengeyi sağlayıp ses kalitesini artırmak için bant genişliği artırılır. Bant genişliği arttıkça ses kalitesi de artar. Ayrıca video verisi ise sesten farklı olarak saniyede aktarılan görüntü sayısıdır (Kurose ve Ross, 2012).

Multimedya ağı temelde 3 uygulama türüne ayrılır ve bunlar sırasıyla; kaydedilmiş ses veya video aktarımı (streaming stored audio and video), VoIP, canlı ses veya video verisinin aktarımı (streaming live audio and video) şeklindedir.

Akış (stream); ses ve video kavramında kullanılan bir terimdir. Kaydedilmiş ses veya veri hızlıca indirilip daha sonra kullanılmaya başlar. Uygulama başlatıldığında sunucuya kaydedilen multimedya verisi daha sonra ilgili istemciye yönlendirilir. Bu uygulama türlerinde ağ gecikmesi değişkendir ve bu ağ gecikmesi terimi dalga bozulumu (jitter) olarak adlandırılmaktadır. Ağdaki gecikmelerin değişkenliği sebebiyle görüşmede ve video veri iletiminde bazı sıkıntılar yaşanabilir. Benzer durum canlı ses ve video aktarımlarında da gerçekleşebilir.

VoIP; ses paketlerinin IP üzerinden yani veri şebekesi üzerinden aktarılmasıdır (Thermos ve Takanen 2007). VoIP temelde iki fazdan oluşur. Bunlar sırasıyla sinyalleşme fazı (signaling layer) ve medya iletim fazıdır (media transport layer).

Sinyalleşme aşamasında çoklu ortam ya da ses oturumlarının başlatılması, değiştirilmesi ve sonlandırılması ile senkronize olan iki uç birim medya iletim fazı aşamasında ses ve video iletimi için gerçek zamanlı karşılıklı haberleşmeye başlamaktadır. Bu iki bileşenin kendine ait uygulama katmanı ve protokolleri vardır. Bunlardan ilki SIP protokolü sinyalleşme aşamasında kullanılan oldukça yaygın bir protokoldür. Genel olarak mevcut VoIP teknolojisinin medya aktarım oturumlarını başlatmak, değiştirmek veya sonlandırmak için kullandığı en önemli sinyalleşme protokolü, SIP olarak da bilinen Oturum Başlatma Protokolüdür (Rosenberg, 2002). RTP protokolü ise medya iletim protokolü olarak kullanılmaktadır. IP altyapısı üzerinden ses ve video gibi medya verisinin aktarımı RTP ile sağlanır (Schulzrinne ve diğ., 2003).

Paket anahtarlamalı bir teknoloji olan VoIP düşük maliyetli ve yüksek ölçeklenebilirlik için kullanılan bir iletişim sistemidir. Yeni nesil teknolojilerle kullanılabilirlik sağlar ve yeni servisleri geliştirme kolaylığı sunar. Bunların yanında, gelişmiş VoIP standartları ile Hizmet Kalitesi (QoS) sayesinde ses iletiminin yanında IP Multimedya servisleri, görüntülü konferans ve dilediğiniz zaman video izleme imkanı sağlayan Talep Üzerine Görüntü (VoD) servislerini de sunmaktadır (Geneiatakis ve diğ., 2008).

2.2. Bilgisayar Ağlarında Güvenlik

Son yıllarda bilgisayar ağlarının güvenilir, güvenli ve performanslı olması sağlanarak iletişim uygulamaları ve güvenilir veri iletimi için uygun altyapı oluşturulmaktadır. Ancak bu hedef ağ güvenlik unsurları bir arada sağlanarak oluşturulabilir ve bu güvenlik unsurları sırasıyla Gizlilik (Confidentiality), Bütünlük (Integrity), Erişilebilirlik (Availability), Kimlik doğrulama (Authentication), Yetkilendirme (Authorization) ve İnkar edememedir (Non-repudiation). Ayrıca, denetimli ve güçlü bir ağ sistemi için kriptografik yöntemler mevcuttur. Kriptografik algoritmalardan anahtar temelli simetrik şifreleme ve asimetrik şifreleme algoritmalarının yanı sıra özetleme fonksiyonları ve bir elektronik imza türü olan dijital imza rutin olarak kullanılan matematiksel algoritmalardır. Tez çalışmasında kullanılan yöntem olan blok zincir teknolojisi temelde dağıtık defter teknolojisidir. Dağıtık ağ içerisinde verileri dağıtık şekilde saklar. Dijital imza, özetleme algoritmaları ve asimetrik şifreleme algoritmaları ile verileri güvenli depolar. İşlemlerin merkezi olmayan şekilde

doğrulanmasını gerçekleştirerek maliyetten büyük ölçüde tasarruf eder ve böylece ucuz ve etkin şekilde ağ güvenliği sağlamlaşır. İletişim altyapısı için VoIP ağı içerisinde kimlik doğrulama blok zincir teknolojisi ile bütünleşmiş (entegre) şekilde gerçekleştirildiğinde güvenlik unsurlarının büyük bir kısmı sağlanmaktadır.

2.2.1. Güvenli Veri İletimi

Bir bilgisayar ağında sistem en zayıf halkası kadar güvenlidir. Bilgisayar ağlarında güvenli veri iletimi için yeterli güvenlik önleminin alınmaması durumunda saldırgan ağ üzerinden trafiği dinleyebilir, ağdaki anlık verileri (şifre vb.) ele geçirebilir, ağ bağlantısını sonlandırabilir ve bütün ağı çalışmaz duruma getirebilir. Bu durumda güvenli veri iletimi gerçekleşemez. Güvenli veri iletimi için güvenlik unsurlarının tamamı haberleşme öncesinde bilgisayar ağlarında sağlanmalıdır.

İletişim altyapısında kullanıcıların kimliklendirilebilmesi önemli bir problemdir. Kullanıcıların kimlik tespiti kolay bir işlem değildir. Ayrıca kişinin hangi lokasyondan hangi cihaz ile gerçekleştirdiği tespiti zor bir işlemdir. Çünkü kullanıcı bilgisayar ağına bağlanırken kullanıcıyı tanımlayan tek unsur IP adresidir. Cihazı tanımlayan tek değer ise MAC adresidir. Ancak IP adresi ve MAC adresi belirli yöntemlerle değiştirilebilir. Saldırgan rahatlıkla farklı bir kişi gibi sisteme sızabilir. Güvensiz bir haberleşme ortamında iletişim sağlanamaz. Bu açıdan bilgisayar ağlarında kullanıcı kimliklendirilmesi için bütün olası durumlar düşünülmeli ve sağlam bir kimlik doğrulama platformu üzerinden karşılıklı doğrulama ve anahtar dağıtımı gerçekleştirilmelidir.

2.2.2. Güvenlik Unsurları

Bilgisayar ağlarında veri korumasında güvenlik zaafiyeti oluşmaması için gizlilik, bütünlük ve erişilebilirlik unsurlarının sağlanmasının yanında mahremiyet, yetkilendirme, inkâr edememe ve kimlik doğrulama güvenli ve güvenilir şekilde gerçekleştirilmelidir (Gunduz ve Das., 2020).

Gizlilik, bilgilerin saldırgan kişi tarafından ele geçirilmesini engellemektir. Bütünlük yetkisiz kişi tarafından silinmesi veya değiştirilmesini önlemektir. Erişilebilirlik ise, bilgisayar ağının iletişim altyapısı için kesintisiz çalışır durumda olmasıdır. Cihazların yetkilendirilmesi öncesinde kimlik doğrulama gerekir (Kim ve Lee, 2017). Yetkilendirme, kaynaklara erişim haklarını belirleme işlevidir.

Şekil 2.4: Bilgi Güvenlik Unsurları.

Solomon ve Chapple (2004)'den uyarlanmıştır.

Kimlik doğrulama ise, bir kullanıcının tanımlama süreci ve yetkilendirme için bir ön koşuldur (Iqbal ve diğ., 2020). VoIP iletişiminde taraflar arasında güvenli bir iletişim kanalı oluşturmak için VoIP kullanıcılarının karşılıklı kimlik doğrulama gerçekleştirmesi gereklidir. Son olarak inkâr edememe unsuru işlemin herkes tarafından şeffaf şekilde bilinmesidir ve mesaj iletenin mesajın kendisine ait olduğunu reddedememesinin sağlanması durumudur. Şekil (2.4)'de bilgi güvenliği unsurları bir arada gösterilmektedir.

2.2.3. Kimlik Doğrulama

Kimlik doğrulama ağın donanımsal birimleri arasındaki haberleşme altyapısının güvenli ve doğru bir şekilde kurulmasına imkan sağlayan ve sistem kaynaklarını sadece meşru kullanıcılarının hizmetine sunan güvenlik unsurudur. Bilgi sistemlerinde güvenlik unsurlardan biri olan kimlik doğrulama, doğru kullanıcının doğru kimlikle doğru sisteme erişmesini sağlayarak bilgi sistem korumasında önemli bir rol oynar. Günümüzde kullanılan kimlik doğrulama türlerinden parola tabanlı kimlik doğrulama, sertifika tabanlı kimlik doğrulama ve yüz, parmak izi veya ses tanıma gibi insana ait biyolojik özelliklerden yararlanan biyometrik tabanlı kimlik doğrulama modelleri bulunmaktadır (Zhaofeng ve diğ, 2020). Ancak mevcut geleneksel kimlik doğrulama yöntemleri tek taraflı doğrulama yapan, zayıf hata toleransına sahip ve güvenilirliği düşük olan merkeziyetçi şemalardır. Örneğin, biyometrik bilgilerin toplanması zordur. Bilgiler şifrelenmemişse, özel bilgilerin sızmasına neden olabilir. Veri iletişiminin bilgisayar ağları üzerinden gerçekleşmesi kimlik doğrulama için daha güvenli ve

güvenilir yöntemlerin geliştirilmesi ihtiyacı ortaya çıkmaktadır. Özellikle günümüzde mobil haberleşme veya internet üzerinden iletişim en çok kullanılan ağ uygulamalarından biridir ve kullanıcılar arasındaki görüşme öncesinde yapılan kimlik doğrulama mahremiyet ve gizlilik açısından hayati önem taşımaktadır (Mukherjee ve diğ., 2014).

Tanımlama (identification) kimlik bazlı sisteme erişim verme işlemdir. Kullanıcının kim olduğunun sorusunun cevabıdır. Sisteme erişim talebinde bulunan her kullanıcıya kimlik bilgileri sorulmaktadır. Kullanıcı adı, şifre veya herhangi bir gizli bilgi kimlik tanımlama için örnek veri girişleridir. Meşru (legitimate) ve zararlı (malicious) kullanıcıların ayrımı bu şekilde yapılmaktadır. Ancak kimlik doğrulama sistemin kişinin kendisinin kim olduğunu kanıtlamasını isteme işlemidir (Bayat ve diğ., 2020). Kimlik doğrulama, mesajların güvenilirlik ve bütünlüğünü sağlar. Bir saldırganın mesajı değiştirmesini veya kimlikleri taklit ederek farklı bir mesajı göndermesini engeller. Bu nedenle, gizli bilgiye dayalı yaklaşımların yerini almak için alternatif kimlik doğrulama yöntemlerinin sürekli geliştirilmesi gereklidir. Çünkü geleneksel kimlik doğrulama modellerinde bazı sorunlar bulunmaktadır. Örneğin, kimlik doğrulama yöntemlerinden biri olan parola tabanlı kimlik doğrulama yönteminin elde edilmesi kolaydır ve kaba kuvvet saldırıları (brute-force attack) ve sözlük saldırısı (dictionary attack) gibi bazı ciddi güvenlik sorunları mevcuttur. Başka bir kimlik doğrulama yöntemi olan biyometrik tabanlı kimlik doğrulama ise, kullanıcının ne bildiğine veya ne tür doğrulama cihazı kullandığına değil, kullanıcının kim olduğuna ve bazı benzersiz kişiye özel parametrelere dayanır. Kişilerden biyometrik veri ile elde edilen çıktı doğrudan kişi ve cihaz doğrulamasını bir arada gerçekleştirmiştir ve bütün halinde güvenli doğrulama sağlayabilir. Diğer taraftan, biyometrik bilgilerin toplanması zordur. Bilgiler şifrelenmemişse, özel bilgilerin sızmasına neden olabilir (Zhaofeng ve diğ, 2020).

2.2.4. Kimlik Doğrulama Mekanizmasına Yönelik Tehdit Modeli

Kimlik doğrulama mekanizmasına yönelik saldırıların tespiti, VoIP ağında kullanıcıların doğrulanması sırasında olası her tehdidi tanımlamamızı sağlar (Rehman ve Abbasi, 2014). Tehdit modelini gerçekleştirirken olası saldırıları kategorize etmek ve olası yeteneklerini doğru bir şekilde analiz etmek gerekir. Bu çalışma, saldırganın önerilen sisteme karşı aşağıdaki saldırı modellerini yapabileceğini varsaymaktadır.

2.2.4.1. Hizmet Kesintisi

Bir sisteme yapılan dağıtılmış hizmet reddi saldırısı (DDoS), o sistemin kullanıcılarının hizmet kaybına neden olur. Bazı servisleri yavaşlatarak veya tamamen engelleyerek sürdürülebilirliği tehlikeye atan bir saldırı modelidir. Bu saldırı modelinde sertifika yetkilisine veya kimlik doğrulama sunucularına yapılan hizmet reddi saldırılarını önlemek zordur. Öte yandan, blok zincir ağının dağıtık yapısı, DDoS saldırısına karşı güvenli bir ortam sağlar (Guo ve diğ, 2019).

2.2.4.2. Hizmeti Ele Geçirme

MITM, kötü niyetli bir kullanıcının gizlice iki cihaz arasındaki bağlantıyı dinlemesi ve doğrudan iletişim kurduklarına inanan iki taraf arasındaki iletişimin içeriğiyle ilgili her türlü değişikliğin yapılabildiği bir siber saldırıdır (Patwary ve diğ., 2020). Tespiti oldukça zordur. Oturum anahtarı, kimliği doğrulanmış bir kanal aracılığıyla eşler arasında güvenli bir şekilde dağıtılmadığı sürece, tehlikeli bir saldırı modelidir. Gizlice dinleme (Eavesdropping), bir saldırganın iki veya daha fazla VoIP uç noktası arasındaki tüm sinyalleri ve akışı izleyebildiği ancak verilerin kendisini değiştiremediği bir yöntemi tanımlar. Ağ içindeki anomali tespiti veya trafiğin izlenmesi, temel bir siber güvenlik uygulamasıdır. Ancak, pasif bir saldırı modeli olan gizli dinleme anlaşılması oldukça zor bir saldırıdır. VoIP ağında S/MIME veya TLS benzeri protokollerle gelen ağ paketleri için bir tür kimlik doğrulama kullanarak iletişim öncesinde güvenli bir kanal oluşturulmaya çalışılır (Gunduz ve Das, 2020).

2.2.4.3. Hizmet Esnasında Veri Değişikliği

Hizmet esnasında veri değişikliği saldırıları bilginin bütünlüğüne yönelik bir saldırıdır. Saldırgan mesaj içeriğinde değişiklik, ekleme veya silme gibi işlemler gerçekleştirebilir. Saldırgan; Aldatma (Spoofing) saldırılarıyla verileri çalmak, kötü amaçlı yazılımları yaymak veya erişim kontrol sistemlerine erişmek için yetkili bir kullanıcının kimliğine bürünür. Bu saldırı özellikle iletişim sistemlerinde ve sesli mesaj gibi multimedya sistemlerinde yetkisiz erişime yönelik bir saldırı modelidir. Diğer taraftan, gönderilen mesajın içeriğinin saldırgan tarafından değiştirilmesi iletişim altyapısında veri bütünlüğünü yok eder. İçeriğin saldırgana göre değiştirilmesi, iletişim kanalının kullanılamaz hale gelmesine neden olur. Diğer bir saldırı şekli olan Sybil saldırıları, saldırganın sisteme yanlış bilgi göndermesi için orijinal kullanıcıları taklit ederek sahte kimlikler oluşturmaya dayalı bir saldırıdır.

Sistemi manipüle eder. Yetkilendirme tarafında yetkisiz erişim ile ciddi hasar oluşturur. Kimliğe Bürünme Saldırısı (Impersonation Attack) genellikle güvenilir bir kaynaktan geliyormuş gibi görünen bir mesajı içerir. Yeniden yönlendirme saldırılarından Tekrarlama Saldırısı (Replay Attack), saldırganın daha önce sistem içinde meşru bir kullanıcı tarafından kullanılan bir mesajı sisteme sızmak için kullandığı saldırı türüdür (Cui ve diğ., 2020). Bu saldırı modelinde, geçerli veri iletimi (sesli mesaj) kötü niyetli veya hileli olarak tekrarlanır.

Uçtan uca iletişim için hizmet esnasında veri değişikliği türündeki saldırılardan korunmak için parola tabanlı kimlik doğrulama ve biyometrik tabanlı kimlik doğrulama gibi çeşitli yöntemler halihazırda mevcuttur ancak yetersizdir (M. Zhaofeng ve diğ., 2020).

2.2.5. Kriptografik Altyapı

Gizli dünya anlamına gelen kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini güvenli şekilde gerçekleştirmesini sağlar. Temeli matematiksel zor problemlere dayanan teknik ve uygulamaların bütünüdür. Kriptoloji; kriptografi ve kripto analiz olarak iki yöntemin birleşimidir. Kriptografi bir verinin şifrelenmesi ve şifrenin çözülmesi için kullanılan yöntemlerken kripto analiz kriptografik mekanizmaların oluşturduğu sistemleri inceleyen ve bunları çözmeye çalışan bunun sonucunda zayıf ve kuvvetli yönleri bulan yöntemlerdir. Kriptografik altyapının genel konuları dijital imza, kimlik saptama, anahtar yönetimi, gizlilik paylaşımı (secret sharing) ve güvenlik protokolleridir (Trappe, 2006). Bu bölümde tezde kullanılan kriptografik yöntemler incelenmiştir.

2.2.5.1. Simetrik Şifreleme

İki VoIP kullanıcısı için taraflardan arayan kişinin IP telefonuna “Alice" ve aranan kişinin IP telefonuna "Bob" adını verelim. Alice ve Bob’u birbirine bağlayan şey, gizli bir değeri, bir "anahtarı" paylaşmalarıdır. Bu anahtarı simetrik şifreleme işlemlerini gerçekleştirmek için kullanırlar. Her iki taraf en başta gizli bir anahtarı asimetrik şifreleme yöntemi ile belirlemektedir. Alice’in Bob’a göndereceği bir *m* mesajı olduğunu varsayalım. Bu mesaj içerik olarak bir arama talebi veya bir sesli mesaj olabilir. Alice ve Bob, bir şifreleme anahtarına sahiptir. Alice, *m* mesajını şifrelemek için bu şifreleme anahtarını kullanarak bir simetrik şifreleme algoritması uygular ve Alice’in IP ağı üzerinden Bob’a gönderdiği bir şifreli metin üretir. Bob, şifreli metnin

şifresini çözmek için aynı şifreleme anahtarını kullanarak eşleşen bir simetrik şifre çözme algoritması uygulayarak orijinal m mesajını elde eder.

Alice ve Bob aynı zamanda bir kimlik doğrulama anahtarına sahiptir. Alice, bu anahtarı kullanarak şifreli metne bir Mesaj Doğrulama Kodu (MAC) uygular ve Alice'in internet üzerinden Bob'a gönderdiği ve anahtara erişimi olduğunu kanıtlayan bir kimlik doğrulama etiketi üretir. Bob, aynı anahtarı kullanarak aynı MAC'i uygulayarak hesaplamayı doğrular (Bernstein ve Lange, 2017). Simetrik şifreleme, IP ağında taraflar arasında iletilen verilerin gizliliğini sağlar. Bir saldırganın bir mesajın içeriğini görememesini sağlar. Simetrik şifreleme yöntemi hızlıdır ve bu yüzden çok büyük verileri şifrelerken simetrik şifreleme yöntemi kullanılmaktadır.

2.2.5.2. Asimetrik Şifreleme

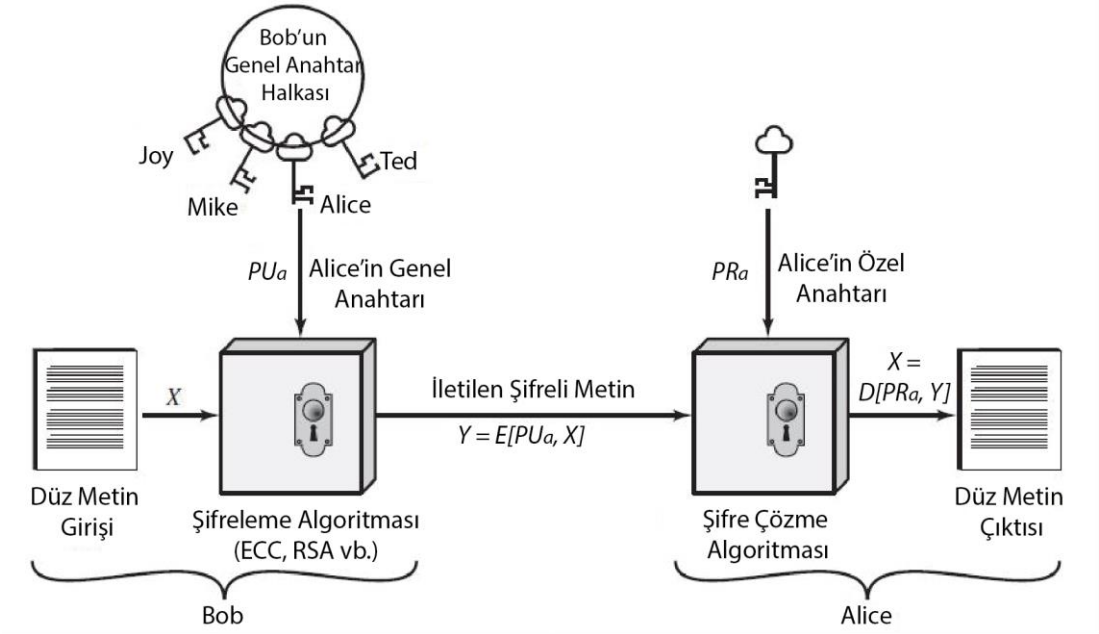
Bilgisayar ağ iletişimi, bilgi güvenliği sağlandığı sürece sürdürülebilir bir yapıdır. Veri transferini güvenli bir şekilde gerçekleştirmek için simetrik anahtar şifreleme yöntemi kullanılmaktadır. Ancak taraflar arasında aynı gizli anahtara sahip olması gerekir. Aynı veya gizli anahtarı karşılıklı değiştirmek için asimetrik şifreleme kullanılmaktadır. RSA, ECC veya Diffie-Hellman gibi algoritmalar asimetrik şifreleme algoritmalarına örnektir.

Asimetrik veya diğer adıyla açık anahtarlı şifrelemede her bir tarafın iki anahtarı bulunmaktadır. Bunlar sırasıyla genel anahtar ve özel anahtar (genel/özel anahtar çifti) olarak adlandırılmaktadır. Özel anahtarı yalnızca sahip olan taraf bilmektedir. Genel anahtar ise herkese açık hale getirilmektedir. Örneğin, Alice'in açık şifreleme anahtarı bilindiği zaman, herkes Alice'e göndereceği bir mesajı şifreleyebilir. Ancak gönderilen şifreyi çözmek için genel anahtara uygun özel anahtara yalnızca Alice sahiptir (Stinson ve Paterson, 2018).

Asimetrik şifrelemede tarafların (Alice ve Bob) anahtar çiftini (genel anahtar PU_k, özel anahtar PR_k) oluşturmak hesaplama açısından kolaydır. Alice'in genel anahtarını ve şifrelenecek mesajı bilen Bob için mesajı şifrelemek hızlı ve kolay bir işlemdir. Şifreli metin Y ve mesaj (düz metin) X ise $Y = E(PU_a, X)$ şeklinde mesaj için genel anahtar ile şifreleme (encryption) işlemi gerçekleştirilir. Alice alıcı taraf olarak şifreli mesajı çözmek için kendi özel anahtarını kullanır. Bu işlem oldukça kolay ve hızlı şekilde gerçekleşir. $X = D(PR_a, Y)$ işlemi ile şifreli metni deşifre eder (decryption). Saldırgan Alice'in genel anahtarını (PU_a) bilir ancak genel anahtar bilgisi ile Alice'in

özel anahtarını (PR_a) elde etmesi hesaplama açısından mümkün değildir. Genel anahtarı bilen ve şifreli metni ele geçiren bir saldırgan mesaj içeriğini anlamlı hale getiremez.

Şekil (2.5)'de ECC veya RSA gibi bir algoritma kullanarak asimetrik şifreleme yöntemi gösterilmektedir. Bob, Alice'e özel bir mesaj göndermek isterse, Bob, Alice'in genel anahtarını kullanarak mesajı şifreler. Buradaki mesaj genellikle simetrik şifrelemede kullanılacak anahtardır. Alice mesajı aldığında, özel anahtarını kullanarak mesajın şifresini çözer. Başka hiçbir alıcı mesajın şifresini çözemez çünkü sadece Alice kendi özel anahtarını bilir. Bu şifreleme şekli gizliliği sağlamaya yöneliktir. Süreci özetlersek: $PU_a(Şifrele) + PR_a(Şifre\ Çöz) = Gizlilik$. Genel anahtar verileri şifrelemek için kullanıldığında, verilerin şifresini çözmek için özel anahtar kullanılmalıdır. Yalnızca kullanıcının kendisi ilgili özel anahtara sahiptir; bu nedenle gizlilik sağlanır.



Şekil 2.5: Genel Anahtarla Asimetrik Şifreleme.

Stallings ve Brown (2018)'den uyarlanmıştır.

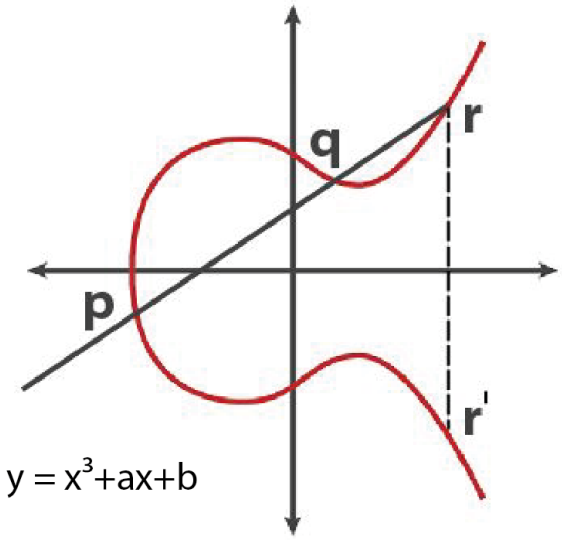
ECC yöntemi küçük anahtar boyutu ile güvenli olmasının yanı sıra zaman kısıtı konusunda da etkili bir çözüm sunmaktadır. Bu şifreleme teknolojisi zaman kısıtı olan VoIP benzeri iletişim uygulamalarında etkin ve güvenli bir ortam sağlar. ECC algoritması, saldırgan tarafından kırılması zor olan Eliptik Eğri Ayrık Logaritma Problemi (ECDLP) üzerinde çalışır. ECC daha küçük anahtar boyutu, daha az enerji

ihtiyacı ve toplam şifreleme de kullanılan parametre sayısı daha az olmasına rağmen diğer asimetrik şifreleme yöntemleriyle (RSA vb.) aynı güvenlik seviyesini sağlar (Amara ve Siad, 2011). 256 bit ECC yaklaşık 3072 bit RSA kadar güçlüdür. Anahtarı hızlı üretir ve anahtar boyutu küçüktür (Li ve diğ., 2018; Guo ve diğ., 2019). Bu perspektiften bakacak olduğumuz da ECC diğer algoritmalara göre önerilen yöntemde daha tercih edilebilir gözükmektedir.

Eliptik eğriler elipslerden oluşturulmaz. Elipsler kuadratik (örneğin: x^2) eliptik eğriler ise kübiktir (örneğin: x^3). Bitcoin ve Ethereum blok zincir platformlarında kullanılan ECC algoritması *secp256k1*'dir. *secp256k1* algoritmasında a değeri 0 ve b değeri 7 iken $y^2 = x^3 + 7$ denklemi elde edilir. Bu fonksiyon Bitcoin ve Ethereum blok zincirinde kullanılan eliptik eğri fonksiyonudur ve ECC fonksiyonu Denklem (2.2) ile gösterilmiştir.

$$y = x^3 + ax + b \tag{2.2}$$

Bütün asimetrik şifreleme altyapılarında olduğu gibi, ECC yöntemi de tek yönde hesaplanması basit, ancak işlemin tersine çevrilerek anahtarların elde edilmesi çok zor olan matematiksel denklemlerdir. Daha az parametre kullanarak asimetrik şifreleme yöntemleri arasında hem hız hem de güvenlik açısından iyi performans sergileyen ECC'yi şifreleme yöntemi olarak kullanmak sistem güvenliğine katkı sağlar.



Şekil 2.6: ECC Grafiği.

ECC temelde eliptik eğrilerin sonlu alanlar üzerinde cebirsel olarak nasıl yapılandırıldığına dayanır. Sonlu alanlar ve Fermat'ın Küçük Teoremi (Fermat's Little Teorem) ECC algoritmasında kullanılmaktadır. Sonlu alan kuralı ECC algoritmasında bölme işlemi yapmamıza olanak veren teoremdir. Eliptik eğri fonksiyonlarında nokta ekleme (addition), katlama (doubling) ve çarpma (multiplication) özellikleri bulunmaktadır. Eğri üzerinde iki nokta ($p\ ve\ q$) ile tanımlanan bir doğru eğride başka bir noktada (r) üçüncü kez kesişmektedir. $p\ ve\ q$ değerlerini birbirine eklemek demek üçüncü bir nokta olan r noktasının x-ekseninde simetrisini almak demektir. Kesişimin yani r noktasının x-eksenine göre simetrisi r' noktasıdır ve Şekil (2.6)'da sunulmuştur (Stinson ve Paterson, 2018).

$$P(x_1, y_1)\ ve\ Q(x_2, y_2) \quad \textbf{(2.3a)}$$

$$P + Q = R = (x_3, y_3) \quad \textbf{(2.3b)}$$

$$Eğim(\lambda) = \frac{y_2 - y_1}{x_2 - x_1} \quad \textbf{(2.3c)}$$

$$x_3 = \lambda^2 - x_1 - x_2 \quad \textbf{(2.3ç)}$$

$$y_3 = \lambda\ (x_1 - x_3) - y_1 \quad \textbf{(2.3d)}$$

$$r' = P + Q \quad \textbf{(2.3e)}$$

Denklem (2.3) eliptik eğride nokta ekleme (addition) özelliğini ifade etmektedir.

$$y^2 = x^3 + ax + b \quad \textbf{(2.4a)}$$

$$P = (x_1, y_1) \quad \textbf{(2.4b)}$$

$$R = (x_2, y_2) \quad \textbf{(2.4c)}$$

$$Eğim(\lambda) = \frac{3x_1^2 - a}{2y_1} \quad \textbf{(2.4ç)}$$

$$x_2 = \lambda^2\ - 2x_1 \quad \textbf{(2.4d)}$$

$$y_2 = \lambda \times (x_2 - x_1) - y_1 \quad \textbf{(2.4e)}$$

Eliptik eğri üzerindeki noktanın (p) tanjantını başka bir noktada (r) ikinci kez kestiği gerçeğinden yararlanılmaktadır. Bu özellik katlama (doubling) özelliğidir ve Denklem (2.4) adımları sırasıyla bu özelliği ifade etmektedir. (p) noktasını ikiye katlamak tanjantının kestiği noktanın x-ekseninde simetrisini ifade etmektedir. Diğer bir özellik ise eliptik eğride çarpma (multiplication) özelliğidir. Bazı eliptik eğrilerde noktaları çok daha büyük sonlu alanlar üzerinde çarpmak için 256 bit'lik değerler kullanmak

istersek bu adımı 2^{256} defa tekrarlamak gerekmektedir. Bu işlem günümüzde kullanılan en hızlı bilgisayarlarla bile yaklaşık 10^{64} yıl sürer. Bu süre çok uzun bir süredir ve bu sebepten ECC algoritmasında çarpma özelliği kullanılarak uygun parçalara bölünerek çarpılır.

Asimetrik şifreleme algoritması kullanan protokollerden biri olan Internet Anahtar Değişimi (IKE) IPsec VPN'lerin temel bir bileşenidir. IKE, IPsec güvenlik ilişkilerinin (security associations) kurulması, karşılıklı kimlik doğrulaması yapılması ve kriptografik anahtarların seçilmesi için varsayılan anahtar anlaşması protokolüdür (Yin ve Wang, 2007). Diğer bir algoritma ise Güvenli Giriş Katmanı (SSL) artık İnternet Mühendisliği Görev Gücü (IETF) standardı TLS olarak uygulanmaktadır. Güvenli Kabuk (SSH) protokolü, ağ cihazlarına güvenli bir uzaktan erişim bağlantısı sağlarken PGP protokolü kriptografik gizlilik ve kimlik doğrulama sağlar. Genellikle e-posta iletişimlerinin güvenliğini artırmak için kullanılır.

2.2.5.3. Özetleme Algoritmaları

Herhangi bir uzunluktaki verinin işlenip bu veriye özgü sabit uzunlukta bir değer üreten algoritmalardır. Belirli bir mesaj için sabit uzunlukta bir özet değeri oluşturur. $d = h(M)$ denkleminde d, h ve M sırasıyla özeti, özet fonksiyonunu ve giriş mesajını gösterir. Genellikle mesajın uzunluğu (M) mesajın özetinden çok daha büyüktür ($|M| \gg |d|$). Son yıllarda özetleme algoritması olarak çoğunlukla SHA-2 veya SHA-3 (*keccak* algoritması) kullanılmaktadır. Özetleme fonksiyonlarının kullanım amacı mesajın bütünlüğünün iletişim esnasında sağlanmasıdır (Trappe, 2006). Özet işlemi kazara meydana gelen değişiklikleri algılamak için kullanılabilir, ancak kasıtlı değişikliklere karşı koruma için kullanılamaz. Bu durum, doğru özet işlevine sahiplerse, herkesin herhangi bir veri için özet değeri hesaplayabileceği anlamına gelir. Bu nedenle, özetleme işlemi ortadaki adam saldırılarına karşı savunmasızdır ve iletilen verilere güvenlik sağlamaz. Bütünlük güvencesine kimlik doğrulaması eklemek için özet tabanlı mesaj doğrulama kodu (HMAC) kullanılır. Bir HMAC, şifreleme özet işlevini gizli bir anahtarla birleştirerek herhangi bir şifreleme algoritması kullanarak hesaplar. Yalnızca bu gizli anahtara erişimi olan taraflar bir HMAC işlevinin özetini hesaplayabilir. Böylece, ortadaki adam saldırılarına karşı yöntem güçlenir ve veri kaynağına kimlik doğrulaması sağlar.

Özetleme fonksiyonları bazı özelliklere sahiptir. Bunlar sırasıyla;

- Özetleme fonksiyonları hızlı ve etkin bir şekilde hesaplanır. Yani mesaj özeti hızlı bir şekilde gerçekleştirilmelidir. Çünkü mesajlar genelde çok büyük boyutludur ve sonuç hızlı bir şekilde elde edilmelidir.
- Özetleme algoritmaları tek yönlüdür. Özet değerinden tekrar mesaj elde edilemez (pre-image resistant). Özet değeri geri döndürülemez olmalıdır.
- Her mesajın özeti birbirinden farklıdır ve en ufak bir değişiklik özet değerini değiştirir.

2.2.5.4. Dijital İmza ve Anahtar Yönetimi

Anahtar yönetim mekanizmasında gizlilik açısından asimetrik şifreleme algoritmaları kullanılır ve asimetrik şifreleme kullanımının en az üç farklı yöntemi bulunmaktadır. Bunlar sırasıyla; genel anahtarın güvenli dağıtımı, güvenli oturum anahtarının (secret key) dağıtımı için genel anahtar şifrelemesi kullanmak ve geçici anahtarlar oluşturularak iletişimi güvenli hale getirmek için genel anahtar şifrelemesi kullanmak şeklindedir.

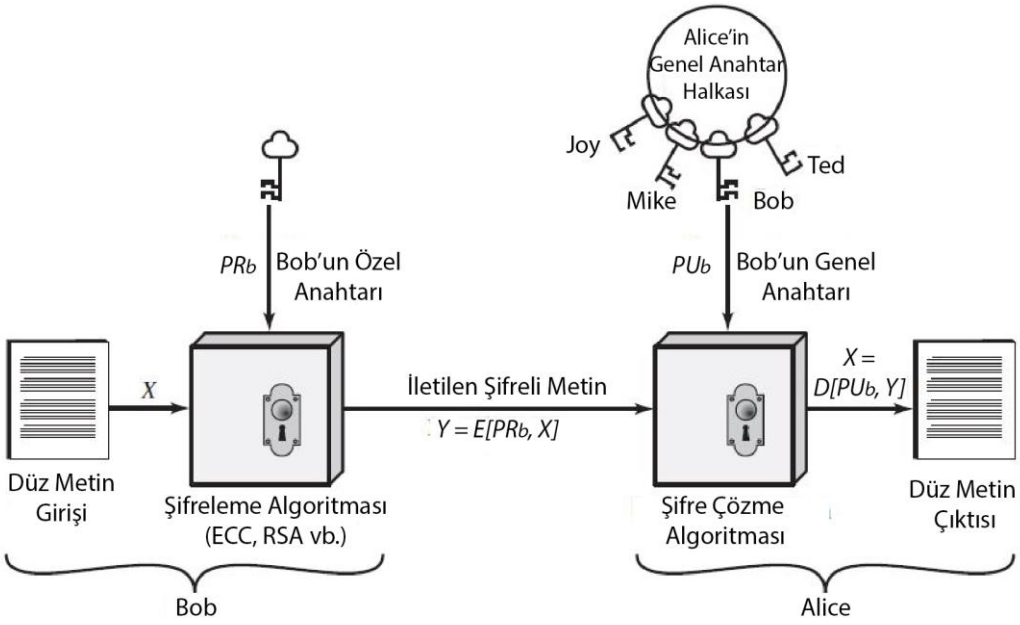
Diffie-Hellman anahtar değişimi yöntemiyle Bob ve Alice birlikte simetrik bir anahtar oluşturan hesaplamalar yapar. Diffie-Hellman, iki bilgisayarın daha önce iletişim kurmadan özdeş paylaşılan gizli bir anahtar oluşturduğu asimetrik matematiksel bir algoritmadır. Yeni paylaşılan anahtar, gönderen ve alıcı arasında hiçbir zaman değiştirilmez. Ancak bu durumda açık anahtar şifreleme kullanılmasına rağmen Bob'un, Alice tarafından sağlanan genel anahtarın gerçekten Alice'e ait olup olmadığını tespit etmesi gerekmektedir. Bu açıdan internet üzerinde güvenli sertifikalar bulunmaktadır. Bu sertifikaların indirilmesi ve doğrulanması üçüncü taraflar (third party) veya sertifika otoritesi (certificate authority) tarafından gerçekleştirilir. Bu durumda açık anahtarlı imzalar ile mesajların kimliğini doğrulayan açık anahtar şifrelemesi yani dijital imza gerçekleştirilir (Bernstein ve Lange, 2017).

Dijital imza matematiksel fonksiyonlarla desteklendiği için taklit edilemez. Mesajın ilgili kişiye ait olduğunu doğrular, verilerin içeriğini korur ve gönderici alıcı arasında kimlik tespiti yapar. Dijital imza 3 temel bileşenden oluşur; bu adımlar sırasıyla, Başlatma (Initialize), İmzalama (Signature) ve Doğrulama (Verification) işlemleridir (Kara ve diğ, 2021). Başlatma sürecinde dijital imzanın gerçekleşmesi için veriyi imzalayacak taraf asimetrik anahtar çiftini (genel/özel anahtar çifti) üretir. İmzalayacağı verinin tercih ettiği özetleme fonksiyonu ile özetini alır. Veri ses, video

veya blok zincir işlemi (transaction) vb. olabilir. Özet veriyi kendi özel anahtarı ile şifreler ve elde edilen şifreli veriye dijital imza adı verilmektedir.

Alıcı tarafta imzalı paket için doğrulama işlemi gerçekleştirilir. Doğrulama işleminin yapılması için gönderici taraf imzalanmış veri, gönderici imzası, kullanılan özetleme algoritması ve gönderici genel anahtarı iletilir. Alıcı taraf şifreli veriyi göndericinin yolladığı genel anahtar ile çözer ve gönderilen özet verisini elde eder. Daha sonra gönderilen imzalanmış veriyi gönderilen özetleme algoritması ile özetini alır. Gönderici tarafından gönderilen özet değer ile kendi ürettiği özet değeri karşılaştırır. Özet değerle aynı ise imza onaylanır.

Şekil (2.7)'de Bob kendi özel anahtarını kullanarak mesajı şifreler. Alice ise Bob'un genel anahtarı ile şifreli mesajı çözer. Bu işlem Şekil (2.4)'den farklı olarak kimlik doğrulama ve veri bütünlüğünü sağlamaya yöneliktir. Yapılan işlem açık anahtar şifrelemesiyle anahtar paylaşımı gerçekleştirilmesi sonrası dijital imza yönteminin uygulamasını anlatan bir örnektir. Asimetrik algoritmaların kimlik doğrulama amacı, özel anahtarla şifreleme işlemi uygulandığında başlatılır. Süreci özetlersek: $PR_b(Şifrele) + PU_b(Şifre\ Çöz) = Kimlik\ Doğrulama.$



Şekil 2.7: Dijital İmza için Şifreleme.

Stallings ve Brown (2018)'den uyarlanmıştır.

Tablo 2.1 asimetrik şifreleme algoritmalarını dijital imza, simetrik anahtar dağıtımı ve oturum anahtarlarının şifrelenmesi özellikleri üzerinden karşılaştırmaktadır.

Karşılaştırma sonuçlarına göre Dijital İmza Standardı (DSS) ve Diffie-Hellman yöntemlerinin aksine ECC ve RSA algoritmaları farklı alanlarda daha etkin kullanılmaktadır.

Tablo 2.1: Asimetrik Şifreleme Algoritmalarının Karşılaştırılması.

Algoritma	**Dijital İmza**	**Simetrik Anahtar Dağıtımı**	**Oturum Anahtarının Şifrelenmesi**
ECC	Evet	Evet	Evet
RSA	Evet	Evet	Evet
Diffie-Hellman	Hayır	Evet	Hayır
DSS	Evet	Hayır	Hayır

Stallings ve Brown (2018)'den uyarlanmıştır.

Dijital imza, veriyi imzalandığı iddia edilen kişi tarafından imzalandığını ve verinin imzadan bu yana değiştirilmediğini doğrulayabilir. Ayrıca, imzalayan imzayı reddedemez (Fang ve diğ, 2020). Dijital imza algoritmaları asimetrik şifreleme algoritmalarının kimlik doğrulama amacıyla kullanılmasıdır. İnkar edememe unsurunu sistem içerisinde sağlar (Migga Kizza, 2015). Sayısal (elektronik) imza yöntemlerinden biri olan dijital imza iki matematiksel modele dayanmaktadır. Biri modüler üs alma (modular exponentiation) işlemi diğeri ise ayrık logaritma problemidir (discrete logarithm problem). Çoğunlukla 3 çeşit dijital imza algoritması tercih edilmektedir.

- Dijital İmza Algoritması (DSA): Ayrık logaritmaların hesaplanmasının zorluğuna dayanan mesaj özetinin imzalanması işlemidir.
- RSA Dijital İmza Algoritması: RSA asimetrik şifreleme algoritmasını temel alır.
- Eliptik Eğri Dijital İmza Algoritması (ECDSA): Eliptik eğri kriptografisine dayalıdır (Stallings ve Brown, 2018).

Bu yöntemlerden küçük anahtar boyutuyla hızlı şifreleme işlemi gerçekleştiren ECDSA yöntemi blok zincir teknolojisinde kullanılmaktadır. ECDSA blok zincirinde hızlı ve güvenli işlemler (transaction) sağlar. (Xiong ve diğ, 2021; Hammi ve diğ, 2018).

Eliptik Eğri Dijital İmza Algoritması (ECDSA) algoritması DSA algoritmasının eliptik eğri üzerindeki eşdeğeridir. ECDSA algoritması için, p büyük bir asal sayı olsun ve ε, Z_p üzerinde tanımlanmış bir eliptik eğri olarak kabul edelim. A, ε üzerinde asal mertebesi q olan bir nokta olsun, öyle ki $< A >$ daki ayrık logaritma problemini hesaplamak oldukça zordur. $P = \{0,1\}^*, A = Z_q^* \; x \; Z_q^*$ olsun ve m değeri $0 \leq m \leq q - 1$ aralığındayken K değeri Denklem (2.5) ile gösterilmektedir.

$$K = \{(p, q, \varepsilon, A, m, B) : B = mA\} \quad \textbf{(2.5)}$$

$p, q, \varepsilon, A \; ve \; B$ değerleri genel anahtardır ve m değeri özel anahtardır.

$K = (p, 1, \varepsilon, A, m, B)$ için ve gizli bir rastgele sayi için $k, 1 \leq k \leq q - 1$ aralığında ise $\boldsymbol{imzala}_K(x, k) = (r, s)$ tanımlanır. Denklem (2.6)'deki işlemler sırasıyla gerçekleşir ve imza oluşturulur.

$$kA = (u, v) \quad \textbf{(2.6a)}$$

$$r = u \; mod \; q, ve \quad \textbf{(2.6b)}$$

$$s = k^{-1}(SHA3 - 224(x) + mr) \; mod \; q \quad \textbf{(2.6c)}$$

Eğer $r = 0$ veya $s = 0$ ise, yeni bir rastgele k değeri seçilmelidir. $x \in \{0,1\}^*$ ve $r, s \in Z_q^*$ için doğrulama (verification), Denklem (2.7)'deki hesaplamalar gerçekleştirilerek imza doğrulanmış olur. (Stinson ve Paterson, 2018).

$$w = s^{-1} \; mod \; q \quad \textbf{(2.7a)}$$

$$i = w \; \times \; SHA3 - 224(x) \; mod \; q \quad \textbf{(2.7b)}$$

$$j = wr \; mod \; q \quad \textbf{(2.7c)}$$

$$(u, v) = iA + jB \quad \textbf{(2.7ç)}$$

$$doğrula_K\big(x, (r, s)\big) = doğru \longleftrightarrow u \; mod \; q = r. \quad \textbf{(2.7d)}$$

RSA ve DSA ile karşılaştırıldığında, ECDSA bazı avantajlara sahiptir. ECDSA daha yüksek güvenlik performansı sağlar. Örneğin 160 bit ECDSA, 1024 bit RSA ve DSA ile aynı güvenlik gücüne sahiptir. Özel anahtarın (şifre çözme ve imzalama işlemi) işlem hızında ECDSA, RSA ve DSA'dan çok daha hızlıdır. ECDSA'nın sistem parametreleri RSA ve DSA'nınkinden çok daha küçüktür, dolayısıyla kullanılan depolama alanı çok daha küçüktür. Ayrıca düşük bant genişliği gereksinimi, ECDSA'nın yaygın olarak kullanılmasını sağlamaktadır (Fang ve diğ, 2020).

2.2.6. Blok Zincir Teknolojisi

Blok zinciri verilerin kalıcı bir şekilde depolanması ve yönetilmesini sağlayan dağıtık bir kayıt listesidir. Blok zincir doğrulama ve izlenebilirlik gerektiren çok adımlı işlemler için şeffaf ve merkezi olmayan bir çözüm yolu sunmaktadır (Di Pierro, 2017). Blok zincir ağ yapısında eşler arası iletişim akıllı sözleşmeler (smart contract) ve konsensüs algoritması (consensus algorithm) ile mutabakat yapısına ihtiyaç duyar. Veriler blok adı verilen yapılarda saklanır (Ahram ve diğ., 2017). İlk blok kaydı (genesis) gerçekleştikten sonra oluşturulan tüm bloklar birbirini takip eder. Bu yapı zincirin halkası gibi düzenli ve zaman damgasıyla sıralı şekilde ilerler. Oluşturulan zincir ne kadar uzun olursa blok zincir ağı veri bütünlüğü ve güvenilirlik açısından aynı oranda güçlenir. Ağdaki veriler bir sistem olarak bütün cihazlar üzerinden eşlenik bir kopya olarak tutulmaktadır (Salman ve diğ., 2018). Blok zincir mimarisinde saldırganlara karşı blokların içerdiği bilgilerin saklanması esas görev değildir. Blok zincir temelde bloklar içerisinde tutulan verilerin izinsiz ve gizlice değiştirilmesinin önlenmesini amaçlamaktadır. Blok zincir teknolojisi depoladığı verilerin bütünlüğünü dijital imza üzerinden sağlar. Blok zincir teknolojisini dışarıdan müdahale ile değiştirilemez yapan dijital imzadır. Bu açıdan kriptografik özetleme fonksiyonları kullanan blok zincir blok başlığı içinde zaman damgası ve nonce değeri üreterek inkâr edememe (non-reputation) unsurunu sağlar (Han ve Jang, 2017).

Blok zincir eşler arası karşılıklı iletişim kurma altyapısı sağlarken belirli kriptografik yöntemlerden yararlanmaktadır. Bu açıdan ağdaki cihazlar (düğüm) özel/genel anahtar çifti üreterek şifreli görüşmektedir. Herhangi bir cihaz özel anahtarı ile imzaladığı paketi karşı tarafa gönderdiğinde dijital olarak imzalanmış paketi gönderenin açık anahtarı ile açıp görebilmektedir. İmzalanan her işlem (transaction) ilgili cihaz tarafından diğer cihazlarla paylaşılmaktadır (broadcast). İşlem (transaction) onayı için işlemi oluşturan cihaz hariç blok zincirindeki tüm cihazların onayı alınmak zorundadır. Blok zincir ağında kullanılan konsensüs algoritması ile mutabakat mekanizması içerisinde onaylanmayan işlem yok edilir ve talep edilen işlem gerçekleşemez. Bu işleme blok zincirinde onaylama (verification) süreci denilmektedir. Konsensüs algoritması ile onaylanan işlemler bloklar içerisine zaman damgası ile birlikte kaydedilir. İlgili konsensüs algoritması üzerinden tek seferlik bir değer elde edilir ve bu değer ilgili blok ile ilişkilendirilir. Bu değeri ilk bulan cihaz diğer cihazlarla bilgiyi paylaşır (broadcast). Bu sürece madencilik (mining) denir. Ayrıca her blok bir önceki

bloğun özetini yapısında bulundurarak bir zincir oluşturur. Bu açıdan özet bağlı listeler veri yapısı mantığında çalışan blok zincir bu şekilde geriye dönük işlem değişikliklerini engellemektedir (Kfoury ve Khoury, 2018).

Blok zincirdeki akıllı sözleşmeler (smart contract) oluşturulan yapı içerisinde değiştirilemeyen yazılım kod parçalarıdır (Minoli ve Occhiogrosso, 2018). Bir kez oluşturulduktan sonra otonom olarak çalışırlar ve blok zincirindeki işlemleri işlem sırasında onaylar ve geçerlilik kontrolü yapar. Blok zincirindeki blok yapılarıyla etkileşimli olarak çalışır. Akıllı sözleşmeler için belirlenmiş kurallar, belirli bir koşul yerine getirildiğinde otomatik olarak uygulanmaktadır. Akıllı sözleşmeler, blok zincirlerin üzerine uygulanır. Onaylanan sözleşme maddeleri yürütülebilir bilgisayar programlarına dönüştürülür. Sözleşme maddeleri arasındaki mantıksal bağlantılar, programlardaki mantıksal akışlar biçiminde de korunmuştur. Herhangi bir sözleşme maddesinin blok zincir ağı içerisinde yürütülmesi, kayıt listesinde saklanan değişmez bir işlem olarak kaydedilir. Akıllı sözleşmeler, en başta belirlenen kurallar için uygun erişim kontrolü gerçekleştirir (Dai ve diğ, 2019). Belirlenen kuralların uygulanmasını garanti eder. Bu şekilde akıllı sözleşmeler sözleşme maddelerini uygularken deterministik bir yapıda çalışır. Akıllı bir sözleşmedeki herhangi bir koşul yerine getirildiğinde, tetiklenen ifade, karşılık gelen işlevi otomatik olarak öngörülebilir bir şekilde yürütür.

2.2.6.1. Blok Zincir Yapısı

Blok zincir ağında dijital imza işlemi üçüncü taraflara (güvenilir üçüncü taraf veya sertifika otoritesi vb.) ihtiyaç duymaz. Eşler arası ağ modelini kullanarak merkeziyetçi ağ modeline güvenilir bir alternatif üretilmiştir. Blok zincirinde kullanıcıların yaptığı her istek işlem olarak adlandırılır. İşlemler ağ içerisinde konsensüs algoritmalarıyla mutabakat sağlanarak bloklara kaydedilir. Bloklar arka arkaya sürekli zincire eklenerek uzar ve her blok bünyesinde barındırdığı bir önceki bloğun özet değeri, zaman damgası ve nonce (yalnızca bir kez kullanılabilen bir sayı) değeri ile kayıtlı verinin üzerinde değişikliği tespit eder.

Blok zincir ağı içerisinde oluşturulan en uzun zincir işlem sırasını ve düğümlerin (genellikle Merkezi İşlem Birimi (CPU) işlem gücü) fazla olduğu yapıyı göstermektedir. Blok zincirinde düğümlerin çoğunluğu saldırgan karşıtı olduğu sürece sistem güvenlidir. Tek sunuculu veya merkezi doğrulama sisteminde üçüncü taraflar

üzerinden anahtar dağıtımı veya kimlik doğrulama güvene dayalı bir sistem olmanın zayıflıklarını içerir. Üçüncü taraflara duyulan güven mekanizması yerine blok zincir yapısı kriptografik fonksiyonlarla sağlanan güvenilir sistem üzerinden matematiksel kanıtlarla taraflar arasında doğrudan veri iletimi (mesaj) gerçekleştiren bir mekanizma sağlamaktadır. Geri döndürülmesi mümkün olmayan depolama sistemiyle veri bütünlüğünü sağlayan mekanizma ağdaki olası saldırganlara karşı koruma sağlamaktadır.

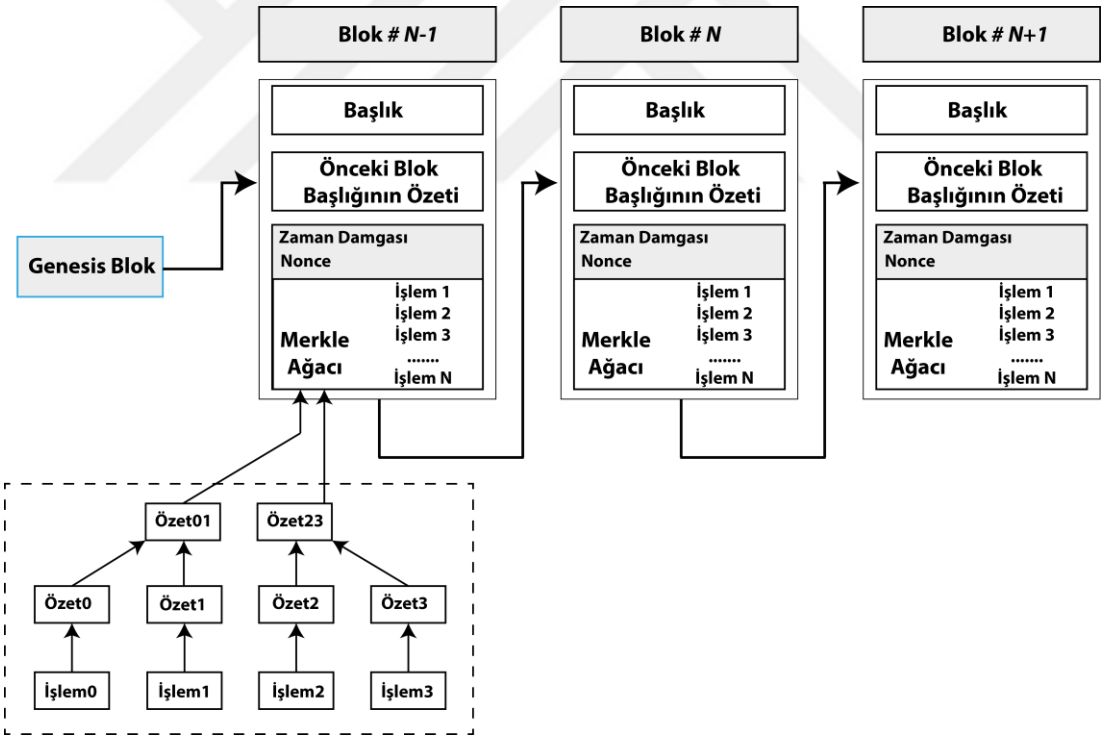
Blok zincire katılan düğümlerler arasında hesaplama gücünü elinde bulunduran grup (belirli konsensüs algoritmalarına göre değişkenlik gösterecek şekilde) çoğunluk ise sistem güvenlidir. Blok zincir, işlemler hakkında bilgi içeren dijital bir tablodur. Her işlem, farklı düğümler arasında veri aktarımı gerçekleştirmek içindir. Ağda bir işlem gerçekleşecekse dijital imza oluşturulur ve Denklem (2.8) ile bu dijital imzanın nihai yapısı gösterilmektir. PR_k gönderenin özel anahtarı, H özetleme fonksiyonu ve PU_k ise iletilen kişinin genel anahtarı olsun.

$$PR_k\big(\, H(\text{önceki işlem} \,||\, PU_k)\big) \tag{2.8}$$

Oluşturulan dijital imzaya mesaj eklenerek $(Dijital\ imza \,||\, mesaj)$ alıcı tarafa gönderilir. Alıcı taraf imzayı gönderici genel anahtarı ile doğrular. Alıcı tarafın mesaj içerisinde olası bir değişikliği kanıtlaması gerekmektedir. Bütün işlemler incelendikten sonra değişiklik tespiti yapılır. Bu tespit güvenilir bir taraf üzerinden gerçekleşmez. Bu açıdan, olası değişiklik işlemlerin blok zincir ağı içerisinde şeffaf şekilde gerçekleşmesiyle sağlanmaktadır. Ayrıca tüm düğümler işlemlerin gerçekleşme sırasını konsensüs algoritmalarıyla fikir birliği sağlayarak kanıtlamaktadır. İşlemi ileten kişinin blok zincir ağındaki düğümlerin çoğunluğu tarafından onaylanması gerekmektedir.

İşlem bloğunun özetleme fonksiyonu kullanılarak özeti alınır. Blok içerisine zaman damgası eklenerek ağ içerisinde yayınlanır. İletilen verinin özete girdiği yani sistemde yer aldığının kanıtı zaman damgalı işlemin ağ içerisinde yayınlanmasıyla gerçekleşir. Her blok bir önceki blokla ilişkilidir ve birlikte blok zinciri oluşturur. Blok zincir yapısında bloklar birbirine zaman damgası ve nonce değeri üretilerek sıralı şekilde bağlanmaktadır. Zincir uzadıkça sistem daha güvenli hale gelmektedir. Saldırgan bir bloğun işlemlerini değiştirmek isterse, özetler aracılığıyla bağlantılı oldukları için sonraki tüm bloklarda ilgili değişiklikleri yapmalıdır ve bu neredeyse imkansızdır.

Ayrıca Merkle Ağacı blok zincir ağına kayıtlı kullanıcının yeni talep edilen bir işlemin blok içerisine kayıt olmasını kontrol etmesi için kullanılmaktadır. Blok zincir ağı içerisinde gerçekleşen kayıtlı işlemlerin tamamını bir araya getirerek dijital bir imza oluşturur. Blok içerisindeki işlemlerin tamamının özetini alır. Tek bir özet değeri elde edene kadar iki işlemin özetini alarak işlemlerin tamamını bir özet değerinde bütünleştirir. En son elde edilen özet değeri Merkle Kökü (Merkle Root) olarak isimlendirilmektedir. Veri yapısı olarak Merkle Ağacı ikili şekilde yaprak düğüm oluşturarak aşağıdan yukarı işlemlerin özetini alır ve son özet değerini elde eder. Böylece blok zincir sistemi Merkle Ağacı kullanarak disk alanından tasarruf eder. Şekil (2.8) ağ üzerinde uygulanan blok zincirinin temel yapısını göstermektedir. Ayrıca Merkle Ağacı, Merkle Kök kullanarak veri bütünlüğü unsurunu da sağlar. Tüm işlemlerin özeti alınarak elde edilen kök özet değeri önceden gerçekleştirilen işlemlerdeki değişikliğin kontrolü için oluşturulur. Zincir içerisinde herhangi bir önceki oluşturulan blok değişikliği yeni bir Merkle Kök değeri oluşturur.



Şekil 2.8: Blok Zincir Yapısı.

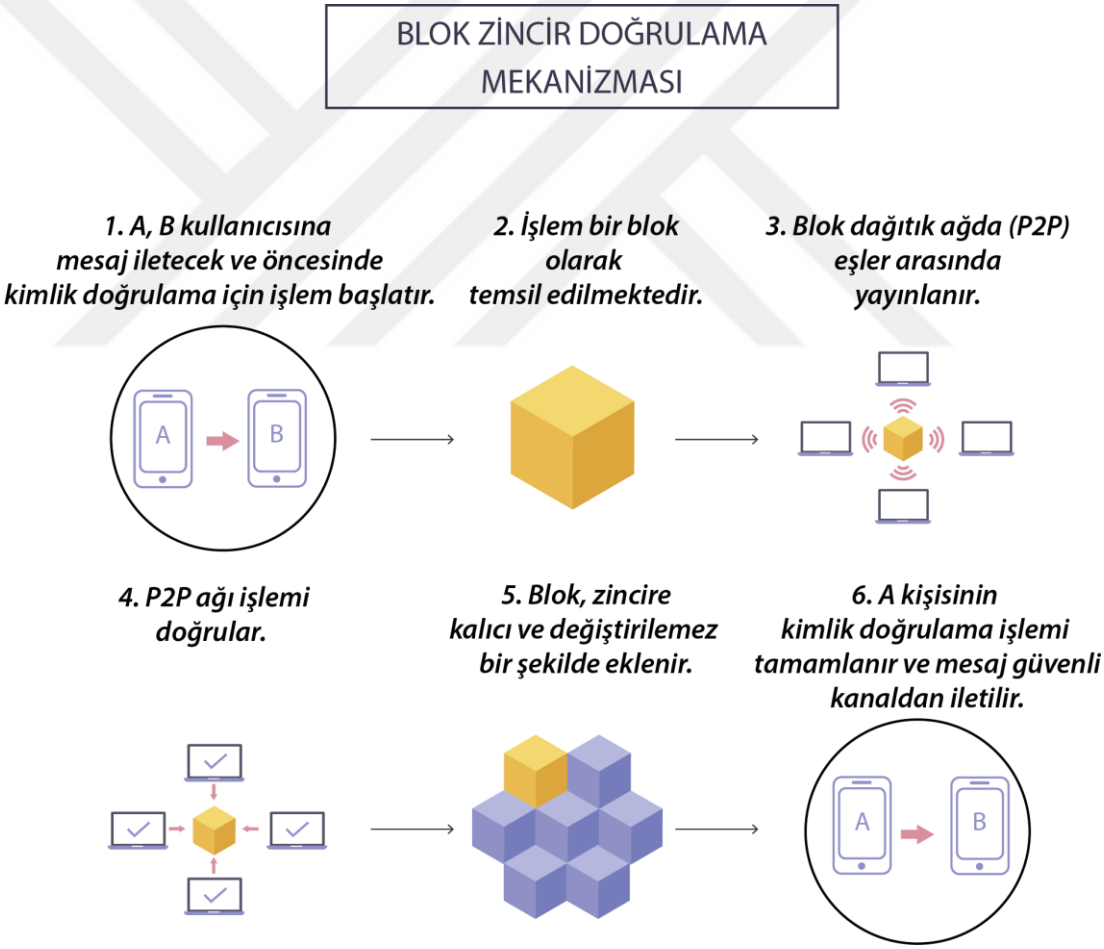
Blok zincir ağında cihazlar birbirlerine güvenmez. Güven mekanizması ancak konsensüs algoritması sayesinde sağlanmaktadır (Patwary ve diğ, 2020). Konsensüs algoritmaları kullanılarak güven oluşturulur ve tek sunuculu veya merkeziyetçi sistem ortadan kalkar. Blok zincir ağında her düğüm bir oy anlamına gelmektedir. En uzun

zincir konsorsiyum sağlandığını ve güvenli veri depolandığının kanıtıdır. Düğümler arasında çoğunluk saldırgan tarafından üretilmediyse gerçek zincir sahte zincirden daha uzun olacaktır. Böylece ağ içerisinde güvenlik ve güvenilirlik sağlanmış olacaktır.

Zincirdeki herhangi bir blok içeriğinin değişmesi için eklenen bloğun sonrasında eklenen tüm blokların saldırgan tarafından değiştirilmesi gerekmektedir. Ayrıca en uzun zincire alternatif bir zincir oluşturup gerçek zincir uzunluğunu geçmesi gerekmektedir. Blok zincir ağında sürekli blok ekleme işlemi gerçekleşir. Saldırgan en uzun zincire alternatif bir zincir oluşturmak için blok zincir ağındaki tüm düğümlerin gücünü yakalaması gerekmektedir. Bu güç İş Kanıtı (PoW) konsensüs algoritmasında Merkezi İşlem Birimi (CPU) işlem gücü anlamına gelirken diğer fikir birliği algoritmalarında farklı anlamlara gelebilmektedir. PoW algoritmasının sınırlarını ortadan kaldırmak için PoS algoritması önerilmiştir. PoW algoritmasından farklı olarak Hisse İspatı (PoS) algoritmasında sürece dahil olan madenciler yoktur. Yeni blokları doğrulayan, taklitçi (forger) adı verilen düğümler vardır. Taklitçiler, hesap bakiyelerinin büyüklüğüne göre seçilir. Daha büyük hisseye sahip olan düğümün, bir bloğu doğrulama ve onu genesis blok zincirine ekleme şansı daha yüksektir. Bunların dışında PFBT, Ripple ve RAFT benzeri birçok konsensüs algoritması bulunmaktadır. Bu konsensüs algoritmalarının uygulama içerisinde seçimi uygulama alanına, minimum kaynak gereksinimine, erişim kolaylığına, zaman gecikmesi, güvenilirlik, güvenlik ve mahremiyet gibi özelliklere bağlıdır (Khalid ve diğ, 2020; Jayasinghe ve diğ, 2019).

Blok zincir ağı içerisinde bir işlem her düğüme yayılır. Blok zincir ağına gönderilen işlem yeterli çoğunluğun oyuyla kabul edilirse düğümler işlemi blok içinde depolar. Düğümler kendi bloğu içerisinde konsensüs algoritması uygular ve sonucu ilk elde eden düğüm blok zincir ağı içerisinde diğer düğümlere sonucu yayınlar. Sonucu kontrol etmek için diğer düğümler blok kontrolü yapar. Eğer blok içerisindeki işlemler hatalı veya geçersiz değilse ilgili blok, zincir sistemine eklenir. Düğümler bu blok içerisine önceki blok özetini ekler. Bu işlem blok geçerliliğini ifade eder. Ayrıca yayınlanan blok herhangi bir düğüme ulaşmazsa daha sonraki blokta fark edilir ve ilgili düğüm ulaşmayan bloğu tekrar talep eder.

Şekil (2.9) ile blok zincir üzerinden doğrulanma isteği gösterilmektedir. Alice, Bob'a bir mesaj göndermek istiyor. İşlemi önce blok zincir cüzdanı aracılığıyla bir bilgisayarda başlatır. İşlem, gönderenin cüzdanı, alıcının adresi ve mesaj verisi gibi bilgileri içerir. İşlem esas olarak Alice'in özel anahtarı tarafından imzalanır ve daha sonra Alice'in genel anahtarı aracılığıyla diğer kullanıcılar tarafından erişilebilir ve doğrulanabilir. Ardından bilgisayar, başlatılan işlemi dağıtık ağda (P2P) diğer bilgisayarlara (veya düğümlere) yayınlar. Böylece her bilgisayar kendisi için konsensüs algoritmasını çalıştırır ve amaçlanan değeri ilk oluşturun bilgisayar P2P ağında sonuç değerini yayınlar ve blok oluşumu gerçekleşir. Oluşturulan blok zincire eklenir ve işlem blok içerisine kaydedilir. Son olarak, doğrulanmış işlem blok zincirine eklendiğinde her düğüm, güncellenmiş blok zincirinin bir kopyasını kaydeder.



Şekil 2.9: Blok Zincir Çalışma Mekanizması.

2.2.6.2. Blok Zincir Türleri

Üç tür blok zincir vardır. Bunlar sırasıyla genel (public), izinli(permissioned) ve özel (private) blok zinciridir. Bitcoin ve Ethereum genel blok zincir türüne örnektir. Genel

blok zincir platformunda herkes PoS veya PoW gibi tipik konsensüs mekanizmaları üzerine blok üretimine özgürce katılabilir veya blok oluşturmadan çıkabilir. PoW şemaları, bulmacayı (puzzle) çözmek için kapsamlı hesaplama gerektirir, bu durum yüksek enerji tüketimine neden olur. PoW'dan farklı olarak PoS, bir bloğun güvenilirliğini doğrulamak için Hisse Kanıtı gerektirir, çünkü daha fazla kripto para birimine (yani daha fazla hisseye (stake)) sahip kullanıcılar, daha az kripto para birimine sahip olanlardan daha güvenilirdir. (Dai ve diğ, 2019).

Pratik Bizans Hata Toleransı (PBFT) ve Yedekli Bizans Hata Toleransı (RBFT) gibi konsensüs algoritmalarının çalışma mekanizması farklıdır ve belirli bazı güvenilir düğümler tarafından korunur (Castro ve Liskov, 1999). PBFT algoritması, izinli blok zincirindeki en popüler algoritmadır. PBFT'de, mutabakat için eşit oy hakkına sahip olan her düğüm, oylama durumunu diğer düğümlere gönderecektir. Çok turlu oylama prosedüründen sonra fikir birliğine varılır. İzinli blok zincir türünde, konsensüs mekanizması önceden belirlenmiş bir grup tarafından yönetilir. Ağa katılan veya madencilik sürecinde bulunacak düğümler belirlenen grup tarafından kararlaştırılmaktadır (Lin ve diğ, 2019). Özel blok zincirler tek bir sistem tarafından kontrol edilen izinli blok zincirleridir. Özel blok zincir merkezi bir zincir yapısı kurar ancak zincirin kopyası her katılımcıda bulunur. Merkezi otorite ağ içerisinde kimin düğüm olabileceğini belirler ve bazı durumlarda blok zincir ağında her düğüm için eşit hak vermeyebilir. Özel blok zincirlere örnek olarak Ripple ve Hyperledger verilebilir.

2.3. İletişimde Güvenlik

Bu bölümde VoIP mimarisindeki güvenlik mekanizması, blok zincir teknolojisinin güvenlik altyapısı ve merkezi olmayan mimari üzerinden sağladığı güvenlik mekanizması açıklanacaktır.

2.3.1. VoIP Mimarisinde Güvenlik Mekanizması

Gerçek zamanlı çalışan bir teknoloji olan VoIP veri akışını internet (public channel) üzerinden sağladığı için ciddi saldırılara maruz kalmaktadır (Keromytis, 2010). Bu açıdan performans ve güvenlik yönünden klasik ağ uygulamalarına ilave tedbir gereksinimi de beraberinde getirmiştir. Sanal yerel alan ağları (VLAN) oluşturulması, QoS ile bazı paketlere öncelik verilmesi veya güvenlik duvarı gibi klasik tedbirlerin yanında Oturum Sınır Kontrolörü (SBC) gibi dinamik tedbirlerin kullanılması bunlara

örnek olarak gösterilebilir (Salsano ve diğ., 2002). Ayrıca bu tedbirlere ilave olarak VoIP teknolojisinin kullanımında alınabilecek en önemli güvenlik tedbirinden biri şifrelemedir. Söz konusu şifreleme için VPN teknolojisinin kullanımı hem performans yönünden hem de ihtiyacı tam olarak karşılamaması (terminalden terminale değil, ofisten ofise (site-to-site) şifreleme yapar) sebebiyle yeterli değildir. Bu sebeple ses haberleşmesine özel hem sinyalleşme hem de veri iletimi esnasındaki paketlerin iletimi için güvenlik protokolleri ve ayrı ayrı şifreleme teknikleri kullanılmaktadır.

2.3.1.1. VoIP Güvenlik Protokolleri

Sinyalleşme ve medya aktarım katmanlarındaki güvenlik yöntemleri farklı protokoller üzerinden sağlanmaktadır. Sinyalleşme katmanında SIP güvenliği belirli yöntemlerle sağlanırken medya aktarım katmanında medya güvenliği için güvenlik protokolleri geliştirilmektedir. SIP güvenliği Temel Kimlik Doğrulama (Basic Authentication) yöntemiyle kullanıcı adı ve parola üzerinden kimlik doğrulama gerçekleştirir. Yöntemde kullanılan içerik düz metin olduğu için ele geçirilebilir veya değiştirilebilir. Özet Kimlik Doğrulama (Digest Authentication) ise kullanıcı adı ve parola bilgisinin özet (hash) halini karşı tarafa gönderir. Zaman damgası (time stamp) kullanımı aynı paketin tekrar gönderilmesiyle yapılacak saldırılara karşı etkilidir. MITM ve tekrarlama saldırılarına karşı sınırlı ölçüde zafiyet içerir. Ancak bütünlük ve gizlilik sağlamaz. Paylaşılmış anahtar ihtiyacı vardır. (Zhang ve diğ., 2010; Franks ve diğ., 1999). Diğer bir yöntem olan PGP kriptografik özet fonksiyonu, veri sıkıştırma, simetrik ve asimetrik şifreleme algoritmalarını bir arada kullanan hibrit bir yapıya sahiptir. Gizlilik, kimlik doğrulama ve bütünlük sağlar. Tekrarlama saldırılarına karşı zafiyeti vardır. S/MIME kullanımıyla önemini yitirmiştir. (Khacef ve Pujolle, 2019). S/MIME, uçtan uca gizlilik, kimlik doğrulama ve bütünlük sağlar ancak tekrarlama saldırılarına karşı zafiyeti bulunmaktadır ve PKI bağımlılığı vardır. (Pecori ve Veltri, 2016; Gupta ve Shmatikov, 2007). TLS protokolü, sertifika otoritesi üzerinden X.509 sertifikalarını kullanarak anahtar dağıtımı sağlar. SIP mesajları da bu anahtar ile şifrelenerek iletilir. Gizlilik, kimlik doğrulama ve bütünlük sağlar. Varsayılan olarak 5061 numaralı portu kullanır. Cihazlar arasında uçtan uca (hop-by-hop) tekrar şifreleme yaparak güvenlik sağlar. (Salsano ve diğ., 2002; Zhang ve diğ., 2010).

Anahtar değişim protokolleri, güvensiz bir veri iletim ortamında iki veya daha fazla katılımcı arasında gizli oturum anahtarları oluşturmanın kriptografik olarak güvenli bir

yolunu sağlamayı amaçlar. Güvenli anahtar değişimi VoIP haberleşmesinde taraflar arasında güvenli oturum oluşturur. Medya aktarım katmanının güvenliği (gerçek ses paketlerinin iletildiği katman), oturum anahtarlarının gizliliğine ve oturum katılımcılarının kimlik doğrulamasına bağlıdır. Kimlik doğrulama, anahtar değişimi başarıyla tamamlandıktan sonra, taraflar arasında gönderilen ve alınan mesajlara ilişkin görüşlerinin eşleşmesini gerektirir. Oluşturulan gizli anahtar simetrik şifreleme yönteminde kullanılmaktadır. Çünkü ses paketleri hızlı veri iletimine ihtiyaç duymaktadır.

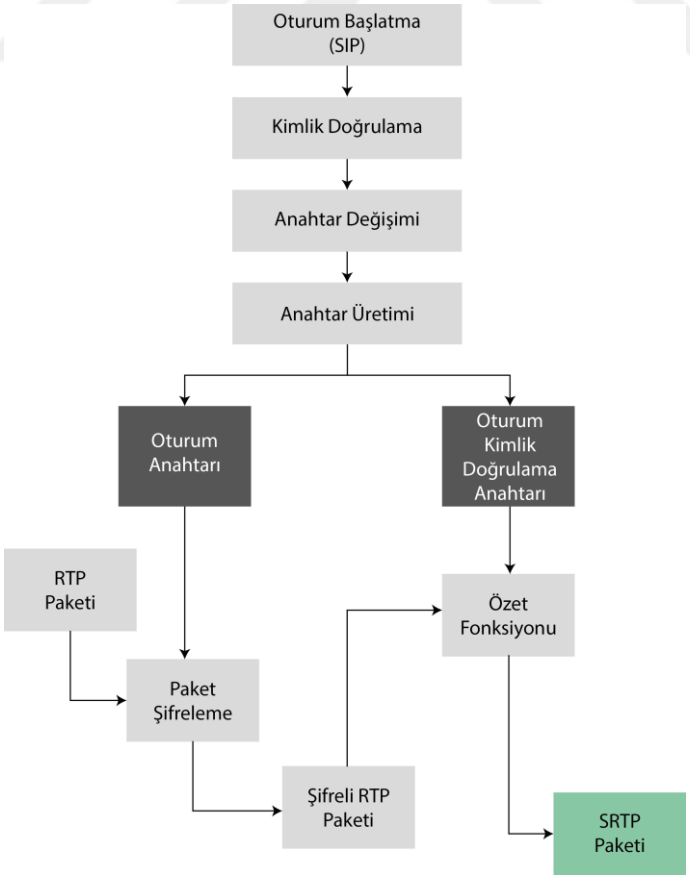
VoIP teknolojisi bağlantı tabanlı (connection-oriented) ve gerçek zamanlı bir haberleşme tipi olması sebebiyle internet üzerinden yapılan veri haberleşmesine göre farklılık göstermektedir. Bu sebeple kendine özgü güvenlik tedbirlerinin alınması gerekmektedir. Güvenli haberleşmedeki gizlilik gereksinimlerini karşılayan SRTP protokolü ise anahtar yönetim sistemini bünyesinde barındırmadığı için, anahtar dağıtımı ihtiyacının diğer protokoller tarafından karşılanması gerekmektedir. Buna yönelik literatürde TLS, MIKEY ve SDES gibi sinyalleşme veya DTLS ve ZRTP gibi medya aktarım sürecinde gerçekleşen çeşitli anahtar dağıtım yöntemleri olmakla birlikte, bunların da çeşitli zafiyetlere sahip oldukları bilinmektedir.

VoIP oturumunda medya güvenlik protokollerinden biri olan TLS veya Güvenli RTP (secure RTP) paketin veri bölümünü (başlıklar hariç) şifreleyerek güvenlik sağlamaktadır. Güvenli RTP gizlilik, kimlik doğrulama ve bütünlüğü sağlar. Simetrik şifreleme kullanmaktadır. Tekrarlama saldırılarına karşı dirençlidir. Ancak bu yöntemde anahtar dağıtım ihtiyacı ortaya çıkar ve dağıtılan anahtarın sonraki dağıtımda tekrarlanmayacağını varsayar (Hellwagner ve diğ., 2009). MIKEY anahtar dağıtım protokolünde ise anahtarlar SIP paketi içerisinde dağıtılır. Önceden paylaşılan anahtar (PSK) veya Diffie-Hellman yöntemleri ile genel anahtar dağıtımı gerçekleştirmektedir. Ancak Diffie-Hellman kullanımında anahtar gizliliği tam olarak sağlanamaz ve MITM benzeri saldırılara karşı zafiyet içermektedir (Pecori ve Veltri, 2016). SDES anahtar dağıtım yönteminde anahtarlar SIP paketleri içerisinde dağıtılmaktadır. Ancak SDES, S/MIME ve TLS zafiyetlerini üzerinde barındırır (Salsano ve diğ., 2002). Diğer bir anahtar dağıtım yöntemi olan ZRTP anahtar dağıtımı Açık Anahtar Altyapısı (PKI) bağımlılığı yoktur. Anahtar değişimi için MITM saldırılarına zafiyeti olan Diffie-Hellman yöntemine destek olarak SAS kimlik

doğrulama gerçekleştirir. Ancak her istek için hafızada yer açması sebebiyle DDoS ataklarına karşı zafiyeti barındırmaktadır. Ayrıca anahtarın kaybı veya aynı kişiyle birden fazla defa olan konuşmalarda aynı ZID ile kimlik doğrulama yaptığı için haberleşme kanalında zafiyet oluşturur (Mukherjee, 2015; Gupta ve Shmatikov, 2007).

2.3.1.2. Güvenli Medya Haberleşmesi

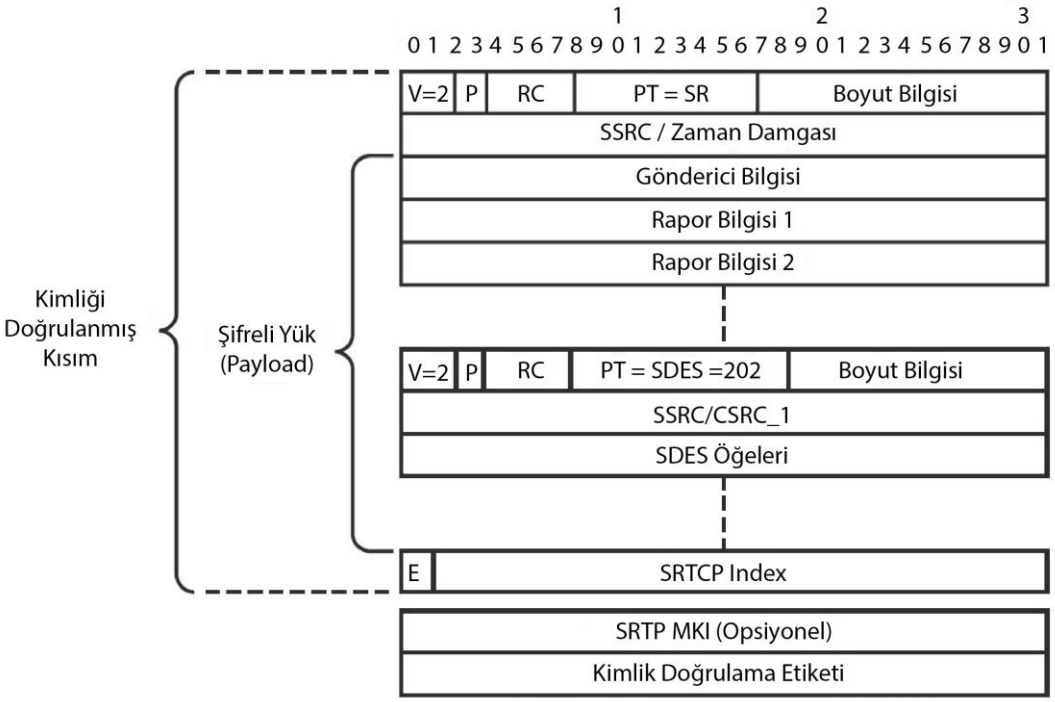
VoIP uygulamalarında oturum başlatma için kullanılan SIP ve oturumu tanımlama için kullanılan SDP'den farklı olarak, anahtar değişimi temel bir güvenlik mekanizmasıdır. Güvenli haberleşme sürecinde farklı protokollerin kullanımı arasındaki uyumsuzluklar ciddi güvenlik açıklarına sebep olacağı için, ilgili protokollerin hangi güvenlik tedbirini nasıl sağladığını anlamak önemlidir. Bu kapsamda SRTP haberleşme kanalını şifrelemek için varsayılan olarak AES simetrik şifrelemesini kullanır. Ancak simetrik şifreleme öncesinde kimliği doğrulanmış taraflar arasında anahtar değişimi gerçekleştirilmelidir. Güvenli medya haberleşmesinin ilk aşamasında da taraflar arasında oturum kurulması ve SRTP için kullanılacak ilk anahtarların değişimi Şekil (2.10) ile gösterilmektedir.



Şekil 2.10: Güvenli Medya Haberleşme Süreci.

İlk anahtarlar elde edildikten sonra her bir pakette kullanılacak oturum şifreleme ve kimlik denetimi anahtarları üretilerek işlem görmek üzere ilgili algoritmalara iletilir. Şifreleme anahtarı ile şifrelenen RTP paketlerinin sonuna oturum kimlik doğrulama anahtarı ile özet değeri alınan kimlik doğrulama etiketi eklenerek SRTP paketleri elde edilir ve alıcıya gönderilir. Alıcıda bu işlemlerin tersi yapılarak kimlik doğrulaması ve şifre çözme işlemleri yapılarak medya paketleri elde edilir.

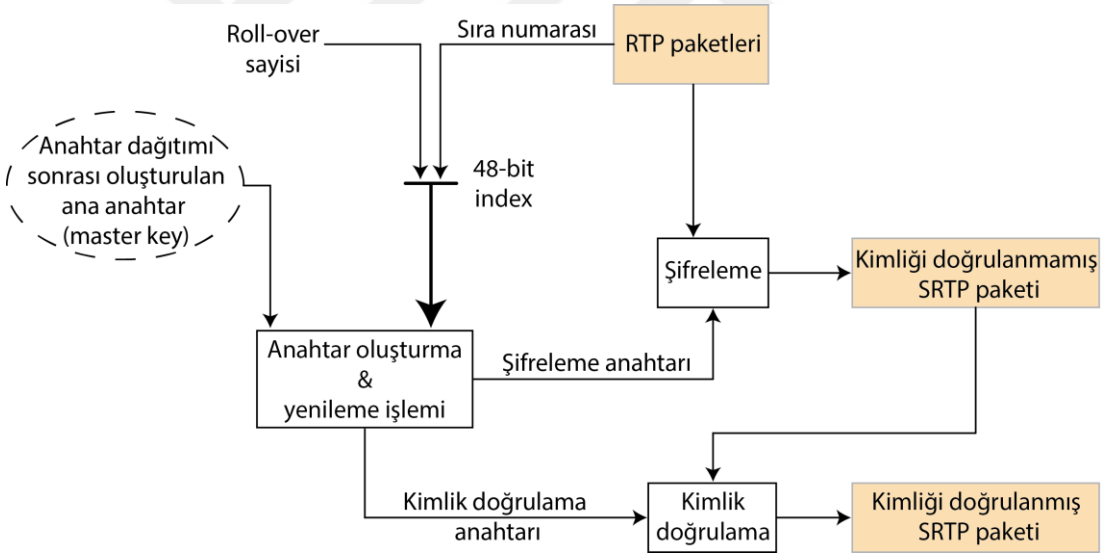
SRTP'nin güvenlik hedefleri, tekrarlama saldırılarına karşı koruma ile birlikte RTP ve Gerçek Zamanlı Aktarım Kontrol Protokolü (RTCP) yüklerinin (payload) gizliliğini ile tüm RTP ve RTCP paketlerinin bütünlüğünü sağlamaktır (Hercog, 2020). RTCP, RTP akışlarının çalışması için gerekli değildir. RTCP bağlantının kalitesi hakkında veri toplamak için faydalı olur. SRTP'nin işlevsel hedefi ise, yeni kriptografik dönüşümlerin kullanımına izin veren ve RTP başlık sıkıştırma verimliliğini koruyarak düşük bant genişliği gereksinimine imkan tanıyan bir çerçeve sağlamaktır (Baugher ve diğ, 2004; Thermos ve Takanen, 2007). Bu özellikleri sayesinde SRTP kablolu ve kablosuz ortamlarda etkin bir şekilde kullanılabilir. SRTP protokolüne ilişkin paket yapısı Şekil (2.11)'de sunulmuştur.



Şekil 2.11: SRTP Paket Yapısı.

Thermos ve Takanen (2007)'den uyarlanmıştır.

SRTP şifreleme ve mesaj kimlik doğrulama başlıkları ile güvenlik ve bütünlük sağlanmaktadır. Şifreleme safhasında sadece mesaj yükü için işlem yapılırken, kimlik doğrulama safhasında tüm başlık ve mesaj yükü için işlem gerçekleştirilir. SRTP ile RTP paketine Ana Anahtar Tanımlayıcısı (MKI) ve Kimlik Doğrulama Etiketi alanları eklenir. Eklenen MKI, kriptografik bağlam içerisinde şifreleme ve/veya kimlik doğrulama için ana anahtarı (master key) belirtmek için kullanılan isteğe bağlı alandır. Kimlik Doğrulama Etiketi (Authentication Tag) ise, RTP başlık ve mesaj yükü için mesaj doğrulama verisini tutan alandır. SRTP protokolü anahtar üretimi/yenileme sürecine ilişkin akış diyagramı Şekil (2.12)'de sunulmuştur. SRTP protokolü anahtar üretimi/yenileme sürecinde öncelikle RTP paketinin Roll-over sayısı ve sıra numarası parametrelerinin birleşimi ile elde edilen 48 bitlik indeks değeri ana (master) anahtar ile anahtar üretim/yenileme fonksiyonu girdi değeri oluşturur. Fonksiyonun çıkışında ise RTP paketlerinin şifrelendiği şifreleme anahtarı ile kimlik doğrulama aşamasında kullanılacak kimlik doğrulama anahtarı üretilir.



Şekil 2.12: SRTP Anahtar Üretim Süreci.

VoIP uygulamalarında, anahtarların dağıtımı için çeşitli anahtar yönetim mekanizmaları kullanılsa da (ZRTP, MIKEY vb.), SRTP, oturum anahtarlarını oluşturmak için kendi içinde bir anahtar oluşturma algoritması kullanır. RTP paketi içerisinde 16 bit sıra numarası (sequence number) bulunmaktadır. Roll-over sayısı ise 16 bitlik RTP sıra numarasının kaç defa 65.535 sayısını geçerek sıfırlandığını gösteren devir sayısıdır ve 32 bit boyutundadır. 32 bitlik Roll-over sayısı ve 16 bitlik sıra numarasının birleşiminden elde edilen değer 48 bit index değeridir. Burada

$index = 2^{16} \times Roll\ over\ sayisi + sıra\ numarası$ şeklinde formüle edilir. Anahtar dağıtımı sonrası oluşturulan ana anahtardan oturum anahtarı (şifreleme için) ve kimlik doğrulama anahtarı (kimlik doğrulama için) oluşturulur. Böylece şifreli ve kimliği doğrulanmış SRTP paketleri taraflar arasında iletilir ve güvenli medya haberleşmesi sağlanmış olur. Kimliği doğrulanmış taraflar arasındaki güvenli anahtar değişimi SRTP için oturum anahtarının güvenliğini sağlar. Böylece SRTP paketleri üzerinden iletilen ses verilerinin gizliliği, bütünlüğü ve kimlik doğrulaması sağlanmış olur. Hem RTP hem de RTCP için tekrarlama saldırılarına karşı koruma sağlar. SRTP kendi içinde anahtar üretim algoritması kullanarak harici bir anahtar yönetim mekanizması aracılığıyla kriptografik anahtarlar oluşturmak için hesaplama ve kaynak tüketimini en aza indirir.

2.3.2. Blok Zincir Teknolojisinde Güvenlik

Geleneksel VoIP mimarisinde kimlik doğrulama yöntemleri genellikle ilk anahtar dağıtımı veya merkezi otoriteye dayanan protokollerden (MIKEY, SDES ve TLS benzeri) oluşmaktadır. Bu protokoller güvenilir üçüncü taraf sunucusu üzerinden kimlik doğrulama gerçekleştirmektedir (Martin ve Hung, 2005). Bu durum tek nokta hatası (single point of failure) tehdidini ortaya çıkarmaktadır. Blok zincir merkezi olmayan ve üçüncü taraflara ihtiyaç duymayan bir teknolojidir. Çünkü blok zincir ağında düğüm adı verilen bilgisayarlarda dağıtık defterlerin bir kopyası bulunmaktadır. Blok zincir ağında gerçekleşen her işlem düğümler tarafından kendi defterlerinde zaman damgalı ve kayıtlı olarak tutulmaktadır. Kullanıcı tarafından doğrulanmak için blok zincire gönderilen bir işlem $[PU_{gönderen}, A, V, imza]$ şeklinde oluşturulur. $PU_{gönderen}$ işlemi oluşturan kullanıcının genel anahtarı, A alıcının adresi, V veri ve *imza* ise verinin özetleme fonksiyonu ile özeti alındıktan sonra özet halinin gönderen kullanıcının özel anahtarı ile imzalanmasıdır. Blok zincir ağına gönderilen işlem geçerli ise (genellikle konsensüs algoritmaları çalıştırılarak belirlenir) bloğa kaydedilir ve zincire eklenir. Blok zincirde madenci adı verilen düğümler arasında bir rekabet bulunmaktadır. Madenciler arasında işlemin kaydedileceği bloğu ilk oluşturan ve zincire ekleyen ilk düğüm ödül elde etmektedir. Özetleme fonksiyonları ve dijital imza gibi kriptografik altyapı kullanan blok zincir dağıtık bir mimari içerisinde eşler arasında mutabakat yapısı kurarak fikir birliği oluşturur ve PKI ihtiyacını ortadan kaldırır (Khacef ve Pujolle, 2019).

3. VoIP UYGULAMASINDA MERKEZİ OLMAYAN KİMLİK DOĞRULAMA MEKANİZMASI

VoIP, iletişimde daha düşük maliyet ve daha fazla esneklik sağlar ve haberleşme yükünü en aza indirir. VoIP haberleşme teknolojisi, sayısallaştırılmış ses verilerini bir IP ağı üzerinden iletir. Çağrı sisteminin tam işlevselliği, VoIP teknolojisi ile kullanıcıya IP ağına bağlı olan her yerde ölçeklenebilir, esnek ve uygun maliyetli bir iletişim altyapısı sağlar. Bununla birlikte, IP ağına bağlantı, internet ortamındaki güvenlik, gizlilik açıklarını ve kötü niyetli saldırıları ortaya çıkarır. Böylece gizlilik, bütünlük, erişilebilirlik, kimlik doğrulama ve inkâr edememe unsurlarının birlikte sağlanması güvenli iletişim için en yüksek öncelik haline gelmektedir. Ancak kimlik doğrulama, tüm bu güvenlik unsurlarının arasında ağ savunma mekanizmasının ilk hattıdır. Ancak, geleneksel yöntemlerde kimlik doğrulama mekanizması, üçüncü taraflara güvenerek gerçekleştirilmektedir ve böylece tek nokta hatası ve gizlilik sorunları gibi çeşitli güvenlik açıkları nedeniyle güvenli iletişim ortamı sağlayamamaktadır. Ayrıca, sertifika yetkilisi (CA) ve güvenilir üçüncü taraf (TTP) gibi anahtar dağıtım mekanizmaları, anahtarları merkezi sunucu üzerinden dağıtır ve bu nedenle güvenilir iletişim sağlanamaz. Bu tez çalışmasında, belirtilen dezavantajlara bir çözüm olarak VoIP için merkezi olmayan blok zincir tabanlı bir kimlik doğrulama mekanizması sunulmaktadır. Kimlik doğrulama mekanizması, VoIP uygulamalarında veri mahremiyeti ve güvenli iletişim sağlamak için blok zincir platformunun değişmezlik, şeffaflık ve hata toleransı gibi temel özelliklerini kullanır.

Kimlik doğrulama sertifikası sağlayan üçüncü taraflar yanlış türde sertifika yayınlayabilir ve bilgisayar korsanlığına, kimlik sahteciliğine veya dijital sertifikaların tahrif edilmesine karşı savunmasızdır. Merkezi doğrulama sistemlerinde, tüm yönetim hakları verilen önemli sorumluluk nedeniyle büyük bir risk taşıyan merkezi sunucularda toplanır. Bu nedenle güvenli iletişim gerçekleşemez. Kimlik doğrulama, VoIP kullanıcısının hangi görevleri yapabileceğini veya hangi dosyaları görebileceğini belirlemez. Kimlik doğrulama yalnızca kişinin veya sistemin kim olduğunu tanımlar ve doğrular (Barkadehi ve diğ, 2018). Bu açıdan bakıldığında güvenli VoIP görüşmesi

öncesinde taraflar arasında eşler arası (P2P) güvenli bağlantı için kimlik doğrulama gerçekleştirilmelidir. Böylece görüşme bazlı dinamik olarak oluşturulan ve taraflar arasında karşılıklı değiştirilen oturum anahtarı (session key) güvenli şekilde iletilebilir.

Literatür incelendiğinde, Feng ve Xu (2019) blok zincir teknolojisini mobil uydu iletişim ağına uygulayarak yeni bir güvenlik modeli sunmuştur. Blok zincir ağını mobil uydu iletişim ağı ile entegre ederek kritik uydu verilerini akıllı sözleşmelerde güvenilir şekilde depolanması ve verilerin uydu düğümleri tarafından düzenlenip korunarak güvenilir depolama, güvenli paylaşım üzerinden veri iletişim güvenliğini sağlanmıştır. Liu ve diğ. (2020), Mayıs 2017 ile Ocak 2020 arasında yayınlanan mevcut blok zinciri tabanlı kimlik yönetimi makaleleri ve patentlerin derinlemesine bir incelemesini sunmaktadır. Literatürün analizine dayanarak, potansiyel araştırma boşlukları ve fırsatları belirlenmiştir.

Kimlik doğrulama, meşru kullanıcıların tanımlanmasını sağlar ve IP ağında taraflar arasındaki iletişimi güvence altına alır. VoIP haberleşmesinin ölçeklenebilirlik, mahremiyet, güvenlik ve güvenilirlik ihtiyacının ses paketlerinin iletimini geciktirmeyecek şekilde bir arada sağlanması ihtiyacı geleneksel yöntemlere uygun değildir. Bu nedenle, VoIP çağrısı esnasında taraflar arasında düşük gecikme süresi ve iletişim yükü sağlayan güvenilir bir kimlik doğrulama mekanizmasına ihtiyaç duyulmaktadır. Literatürdeki çalışmalar incelendiğinde, SIP protokolünün en önemli rollerinden biri, güvenli bir kimlik doğrulama mekanizması sağlamaktır. VoIP kimlik doğrulaması yapan çalışmalar genellikle merkeziyetçi veya tek sunuculu kimlik doğrulama mekanizmalarıdır ve bir sunucu kullanıcı kimliğini doğrular (Nikooghadam ve Amintoosi, 2020; Zhang ve diğ, 2016; Gupta ve Prajapati, 2019; Farash, 2016). Bu tür kimlik doğrulama mekanizmaları IP ağındaki güvenlik tehditlerine, ölçeklenebilirlik sorularına ve tek nokta hatası zafiyetine oldukça yatkındır. Ayrıca, sertifika otoritesi veya güvenilir üçüncü taraflar olması durumunda, VoIP haberleşmesinde mahremiyet endişeleri artar ve bu da taraflar arasında veri paylaşımında daha az güvenilir bir ağ ortamı oluşturur.

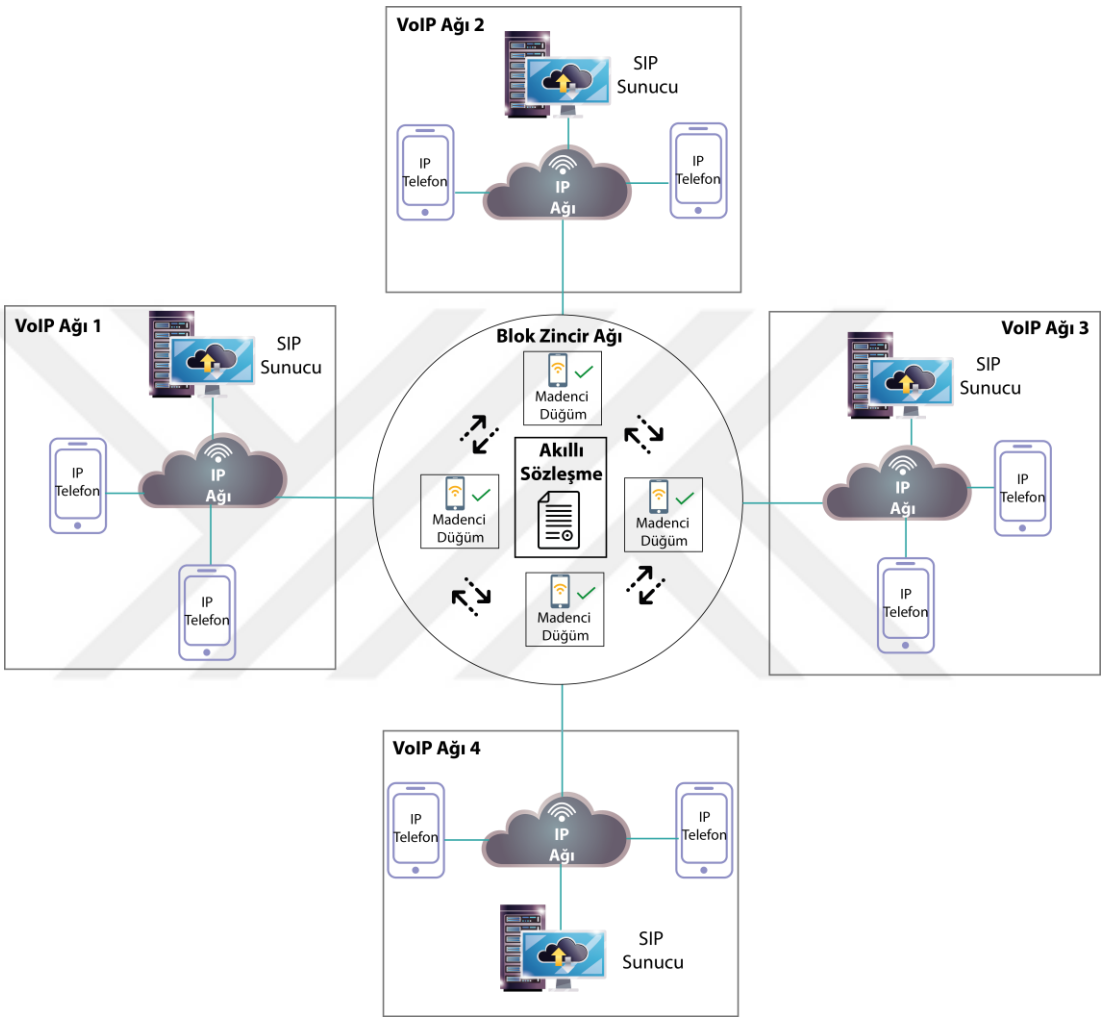
Uçtan uca kimlik doğrulama için VoIP ağıyla entegre blok zinciri kullanan Kfoury and Khoury (2018), blok zinciri kullanarak VoIP kullanıcılarının ortak anahtarını dağıtık defterlere kaydetmekte ve kayıtlı açık anahtarın güvenliğini şeffaf olarak sağlamaktadır. Ancak, her kimlik doğrulama işlemi için blok zincirinde yeni bir blok

oluşturur. Bu nedenle toplam çağrı kurulum süresi zaman gecikmesi açısından yüksektir. Chen ve diğ. (2021) arayanın gerçek kimliğinin tespiti için uçtan uca doğrulama sağlayan "*Callchain*" adı verilen bir çalışma sunmuştur. Bu çalışmada vekil (proxy) sunucuyu blok zincir ağında doğrulanacak şekilde dahil ederek bir kimlik doğrulama yöntemi önerilmiştir. Ancak, bu yaklaşım ortalama gecikme açısından oldukça yüksektir ve uçtan uca güvenli kimlik doğrulama ile anahtar değişim süreci yaklaşık 2 saniye sürer. Bu çağrı sırasında gerçekleşen bir süreç olarak yüksek bir değerdir. Çünkü internet bir telefon şebekesi için gereken tüm özellikleri sağlarken, beraberinde getirdiği bazı önemli sorunlar da vardır. İnternet ortamındaki hız ve performans sorunları bulunmaktadır. VoIP teknolojisinin PSTN'ye uygulanabilir bir alternatif olması için, yalnızca daha ucuz, dağıtımı ve bakımı daha kolay olmakla kalmamalı, aynı zamanda benzer veya daha iyi çağrı kalitesi sunarak son kullanıcıyı VoIP'e geçmeye motive etmelidir. Paket anahtarlama modelini kullanan internet ortamında güvenlik endişesi zaman maliyetini de ortaya çıkarmaktadır. Bu açıdan, VoIP için hem güvenli hem de performans açısından sorun oluşturmaması gereken bir güvenlik mekanizması sunulmalıdır. Çünkü internet ağında VoIP için gecikme (latency), paket kaybı (packet loss) ve dalga bozulumu (jitter) performans sorunları bulunmaktadır. Kara ve diğ. (2021) "*Bcvop2p"* adını verdiği çalışmada, VoIP uygulamaları için doğrudan eşler arası blok zincir tabanlı karşılıklı kimlik doğrulama şeması teorik olarak önerilmiştir. Bu tez çalışmasında, teorik olarak sunulan çalışma deneysel çalışmalarla desteklenmiştir. Sanal Ethereum platformu ve python dili kullanılarak gerçek bir uygulamaya benzetim yapılarak test edilmiştir. VoIP iletişimi için blok zincir tabanlı ve merkezi bir yapıya ihtiyaç duymayan kimlik doğrulama modeli tasarlanmıştır. Böylece, VoIP ağında ses veya anlık mesaj verilerin aktarımı öncesinde (RTP protokolü ile medya veri aktarımı gerçekleşmeden hemen önce sinyalleşme aşamasında) IP ağı üzerinden taraflar arasında (peer-to-peer) güvenli haberleşme yapısı kurulmuştur. İnternet ortamındaki performans sorunları yüksek verimlilik sağlanarak çözülmüştür.

3.1. Önerilen Kimlik Doğrulama Mekanizmasının Yapısı

Merkezi olmayan yani üçüncü taraflara ihtiyaç duymadan anahtar dağıtımı gerçekleştirilmesi VoIP uygulamasında taraflar arasında kimlik doğrulamasında kullanılmak üzere anahtar değişiminin (key exchange) güvenliğini ve güvenilirliğini

sağlamaktadır. Şekil (3.1)'de VoIP ağı ve blok zincir ağının entegrasyonu sunulmaktadır. Farklı veya aynı VoIP ağında taraflar arasında bir güvenli VoIP çağrısı gerçekleşmeden önce blok zincir ağına kayıtlı VoIP kullanıcıları arasında dağıtık olarak kimlik doğrulaması gerçekleşmektedir. Akıllı sözleşme ve madenci düğümler blok zincir ağında kimlik doğrulamasında rol alan önemli bileşenlerdir.



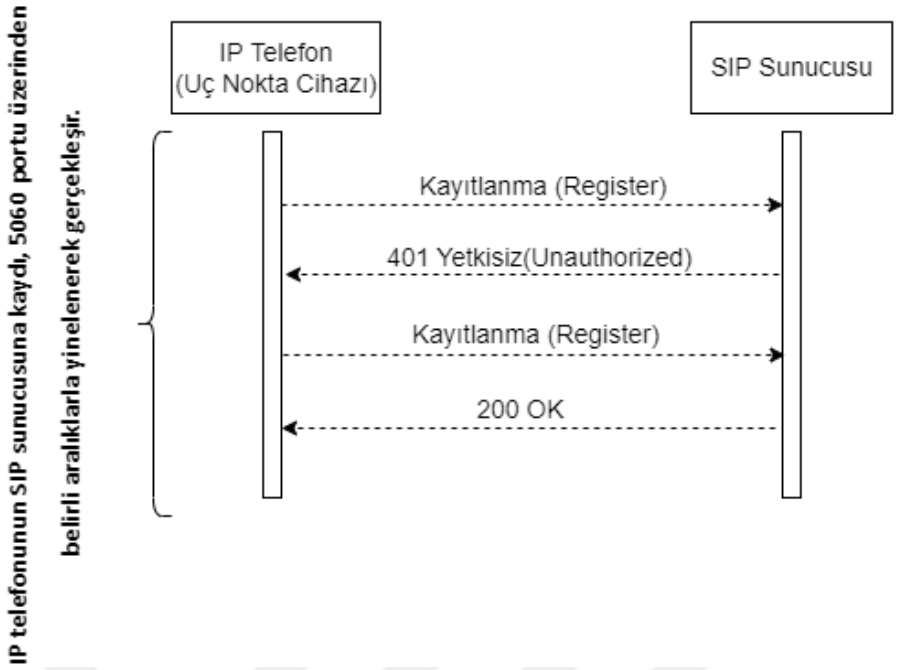
Şekil 3.1: VoIP Ağları ile Blok Zincir Ağının Entegrasyonu.

SIP, iki kişi arasında sesli arama veya bir ekip arasında video konferans şeklinde olabilen bir IP iletişim oturumunu başlatmakta ve sonlandırmaktadır. SIP mimarisinde ilk aşama, IP telefon cihazlarının SIP sunucusuna kayıt olmasıdır. VoIP kullanıcıları IP telefonlar üzerinden VoIP ağında arama yapabilmek için önce SIP sunucuna kayıt olur. SIP sunucusu, IP telefonu tespit etmek için adres olarak sırasıyla SIP adresi (SIP URI), iletişim adresi (contact address) ve medya adresi (media address) parametrelerini kullanır. VoIP kullanıcısının SIP adresi kullanıcıya ait numara ve kayıtlı olduğu sunucu IP adresini içermektedir. Buradaki SIP adresi bir e-posta

adresine benzemektedir ve örnek vermek gerekirse *numara@SIPadresi* şeklindedir. Buradaki numara bilgisi kullanıcıya ait numaradır ve SIP adresi ise kayıtlı olduğu SIP sunucunun adresidir.

SIP adresleri arasında veri paketleri şeklinde mesajlar iletilerek oturum kurulmaktadır. Her SIP adresi, fiziksel bir VoIP kullanıcısına yani bir IP telefona bağlıdır. İletişim adresi IP telefonun kimlik ve konum bilgisini kapsamaktadır. IP telefon SIP sunucusuna kayıt olması esnasında iletişim adresi kullanır. İletişim adresi VoIP kullanıcısı telefonunun IP adresini ifade etmektedir. Son olarak medya adresi medya verisinin (ses, video vb.) alınacağı konumdur ve genellikle VoIP kullanıcısının IP adresi ile aynı adres anlamına gelmektedir.

SIP sunucusuna kayıt olma işlemi VoIP sisteminde gerçekleştirilmesi gereken ilk adımdır. SIP kayıtlanma sunucusu, VoIP uygulamasındaki kullanıcı adlarını belirli bir ağ adresiyle ilişkilendirmesini sağlar ve bu süreç tezde sunulan blok zincir tabanlı eşler arasındaki kimlik doğrulama mekanizmasından tamamen bağımsızdır. SIP sunucu IP telefonun kimlik bilgilerini doğruladıktan sonra iletişim bilgilerini veri tabanına kaydeder. VoIP kullanıcısına 200 yanıt kodu gönderilir ve bu kod sürecin başarılı şekilde tamamlandığını ifade etmektedir. Böylece kayıtlanma süreci tamamlanır. VoIP ağında olası değişiklerin tespit edilmesi için IP telefon cihazının SIP sunucuya kayıtlanması periyodik olarak gerçekleşir. Bu periyodik süreç istek paketlerini (invite packet) iletecek olan SIP sunucuların ve iletişim kurulacak IP telefonların kayıtlanma durumunun kontrolü amacıyla gerçekleşir. Kimlik denetimli olarak yapılan kayıtlanma süreci Şekil (3.2)'de açıkça gösterilmektedir. IP telefonun SIP sunucusuna kayıtlanma talebi sonrası ilk olarak "401 Yetkisiz (401 Unauthorized)" cevabı dönmektedir. Bu mesaj kayıtlanma için gereken kimlik doğrulamasının yapılabilmesi için ilave bilgiye ihtiyacı olduğu anlamına gelmektedir. Kayıtlanma aşamasında isteğe bağlı olarak kullanılan bu kimlik doğrulama türü tamamen SIP kayıtlanma süreci için gerçekleşir. Önerilen kimlik doğrulamadan tamamen bağımsız ve farklı bir kimlik doğrulama sürecidir. İstemci taraf kimlik denetimine ilişkin bilgileri SIP sunucuya göndererek SIP kayıtlanma fazını başarılı şekilde tamamlamaktadır.



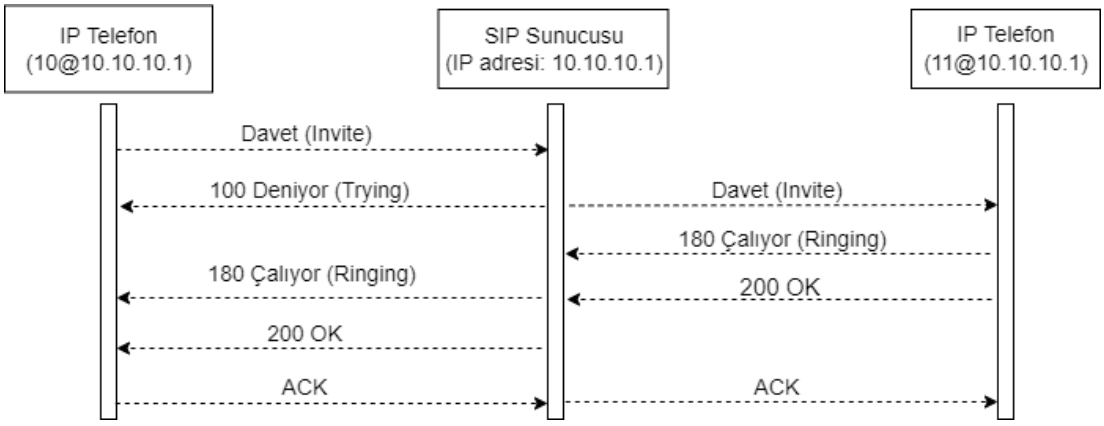
Şekil 3.2: SIP Kayıtlanma Fazı.

VoIP kullanıcıları tarafından güvenli ve merkezi olmayan kimlik doğrulamanın yapılabilmesi için blok zincir ağına kayıtlanma işlemi gerçekleşir. IP telefon güvenli kanaldan arama yapacaksa VoIP kullanıcısı SIP sunucusuna kayıtlanma sonrası blok zincir ağına kayıt olmalıdır. VoIP kullanıcılar için blok zincir tabanlı karşılıklı kimlik doğrulama işlemi üçüncü taraflara ihtiyaç duymadan doğrudan eşler arasında ve güvenli bir şekilde gerçekleşmektedir. Kimlik doğrulamanın güvenilir olması taraflar arasında anahtar dağıtımının güvenli ve güvenilir olmasını sağlamaktadır ve böylece ses, anlık mesaj veya video iletimi için güvenli medya oturumu kurulmuş olur. Bu sebeple, SIP kayıtlanma fazı gerçekleşmesi sonrası VoIP kullanıcısı IP telefonu için ikinci kayıtlanma aşaması olan blok zincir kayıtlanmasını gerçekleştirir.

SIP sunucusu istek-cevap (request–response) modeliyle çalışır. Bu sebepten dolayı, SIP sunucusu kendisine gelen görüşme isteklerini IP ağı üzerinden medya oturumunun kurulması için gerekli bilgilerin aktarımını sağlar. VoIP çağrılarında arama işlemi, doğrudan IP telefonları arasında gerçekleşemez. Ancak bir IP telefon kayıtlandığı SIP sunucusunun IP adresini bilmektedir. Arayan taraf, kayıtlı olduğu SIP sunucu üzerinden aranan taraf için Davet (invite) paketi göndererek aramayı başlatır. Arayan taraf aranan tarafın IP adresini SIP sunucusu aracılığıyla öğrenir (Sisalem ve diğ, 2008).

SIP arama akışının gerçekleşme süreci, arayan tarafından bir DAVET isteği göndermeyle başlar ve bu mesaj VoIP çağrısını başlatmak için aranan tarafa davet gönderme işlemidir. Davet fazı iki bölümden oluşur ve sırasıyla arayan tarafla SIP sunucusu arasında ve SIP sunucusu ile aranan taraf arasında gerçekleşir. Durum bilgisi olan bir SIP sunucusu arayan taraftan Davet talebini aldığında, arayan tarafa geçici bir mesaj, örneğin 100 veya 180 ile yanıt verir. 180 Çalıyor (ringing) yanıtı anlamına gelmektedir. Diğer taraftan sistem aranan cihazı bulma sürecinde 100 Deniyor (trying) mesajı gönderir. Aranan abone arayan tarafın SIP sunucusuna kayıtlı değilse Davet talebi aranan tarafın sunucusuna yönlendirilir. Davet hedef kullanıcıya ulaştığında arayan tarafa çalıyor mesajı iletilir. Çağrıyı kabul ettiğinde arayan tarafa kabul etme anlamında 200 OK yanıtı iletilir. Arayan taraftan aranan tarafa 200 OK paketini aldığına dair Onaylama (ACK) paketi gönderilir ve VoIP çağrı kurulumu tamamlanır.

DAVET istek paketinin içeriğinde, aranan IP telefon tarafından medya iletim fazında RTP veri akışı esnasında aradığı IP telefonun kendisine göndermesi için ihtiyaç duyacağı parametreleri (kodek, IP adresi, bağlantı noktası) sağlayan bir Oturum Açıklama Protokolü (SDP) mesajı taşır. SIP sunucusu gelen çağrı isteğine cevap verir ve bu isteğini hedef IP telefona gönderir. Gerçekleşen işlemlerin daha iyi anlaşılması açısından Şekil (3.3) ile SIP Davet fazı gösterilmektedir.



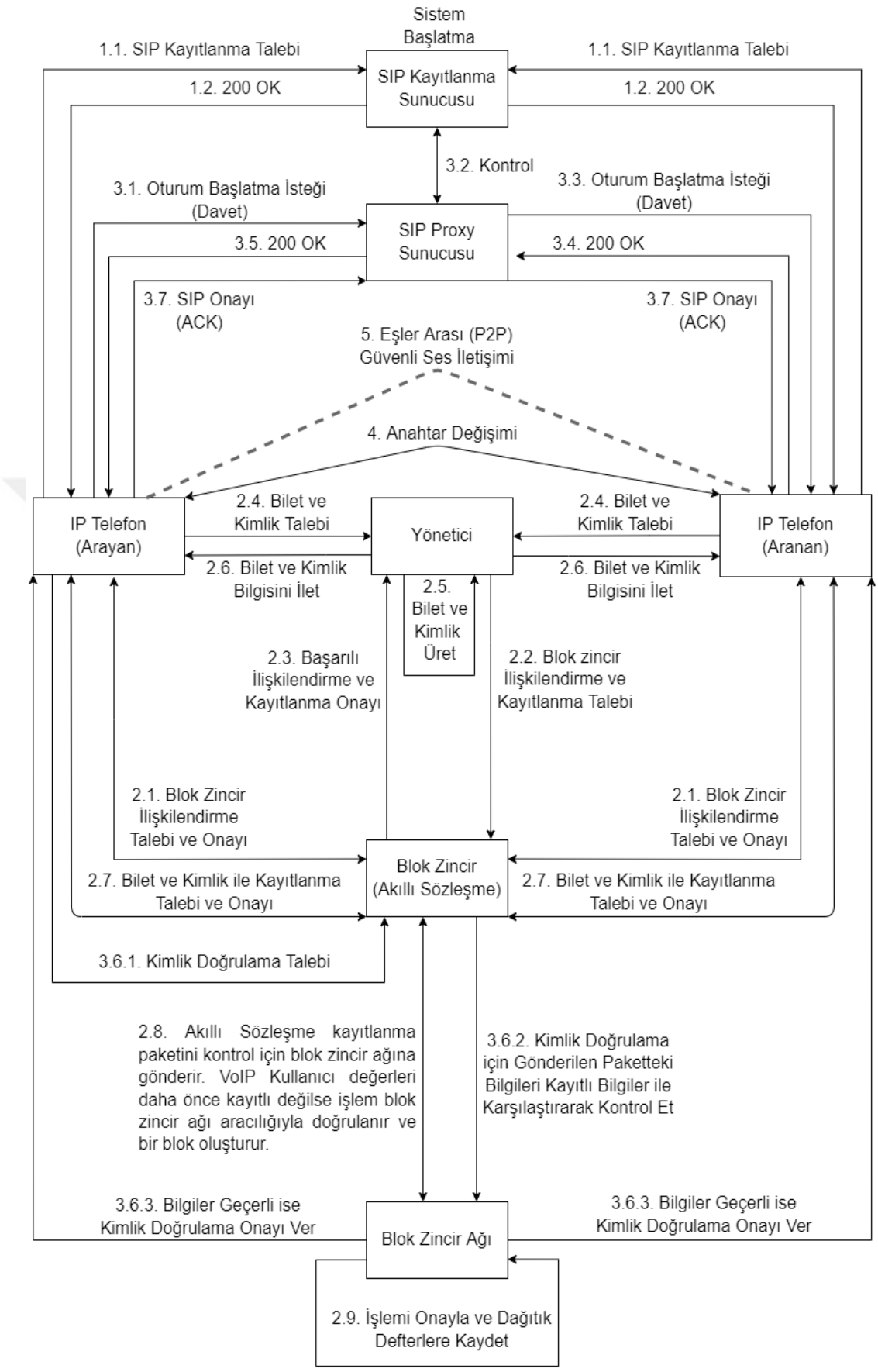
Şekil 3.3: SIP Davet Fazı.

RTP, ses ve video verileri gibi gerçek zamanlı verileri çok yöne veya tek yöne yayın servisleri üzerinden ileten uygulamalar için uçtan uca veri taşıma işlevi sağlar. Bir internet telefon bağlantısı sinyalizasyon ve çağrı esnasında ses verisinin karşılıklı iletildiği ve ses taşıma protokolü olarak RTP'nin kullanıldığı konuşma kanallarından oluşmaktadır. Bu açıdan, internet ağında gerçek zamanlı iletimi yönetmek için

kullanılan internet protokolüdür (Hercog, 2020). İletişim altyapısı doğrulandıktan sonra RTP protokolü ile ses verisi karşılıklı olarak iletilir.

SIP kayıtlanması, blok zincir kayıtlanması ve arama safhasının bütün adımlarının başarılı bir şekilde gerçekleşmesi sonrası medya iletim fazında RTP protokolü üzerinden VoIP görüşmesi başlaması için uygun ortam oluşmuş olur. Ancak IP telefonlar arasında medya iletim katmanında, ses paketlerinin taraflar arasında iletiminin hemen öncesinde blok zincir tabanlı merkezi olmayan kimlik doğrulama gerçekleşir. Kimlik doğrulama süreci sonrası şifreli veri iletimi için anahtar değişim mekanizması gerçekleştirilerek oturum anahtarı kullanıcılar tarafından oluşturulur.

Tez çalışmasında uygulanan blok zincir tabanlı güvenli merkezi olmayan kimlik doğrulama mekanizmasının bütün adımlarını özetleyen akış şeması Şekil (3.4)'de gösterilmiştir. Önerilen kimlik doğrulama mekanizmasında SIP protokolü, blok zincir ağından bağımsız olarak çalışır. SIP kayıtlanma aşaması tamamlandıktan sonra taraflar arasında çağrı, arayan tarafından başlatıldıktan ve aranan tarafından SIP Proxy sunucusu üzerinden 200 OK mesajı ile kabul edilir. Blok zincir üzerinden medya iletim aşamasında taraflar arasında görüşmeye başlamadan hemen önce kimlik doğrulama gerçekleşir. Kimlik doğrulama talebi başarıyla tamamlanırsa karşılıklı kimlik doğrulama tamamlanmış olur ve SIP onayı (SIP ACK) gerçekleştirilir. Böylece SIP üzerinden çağrı oturum kurulumu tamamlanır. Görüşme başlamadan hemen önce blok zincir üzerinden kimliği doğrulanmış taraflar RTP paketleri aracılığıyla gerçekleştirilen anahtar değişimine ihtiyaç duyar. Arayan, sır paylaşımı (shared secret) oluşturmak için arananın genel anahtarını ve arayanın özel anahtarını kullanır. Sır paylaşımı, taraflar arasında mesajı şifrelemek için Eliptik Eğri Diffie-Hellman Anahtar Değişimi (ECDH) kullanılarak oluşturulur. Kimlik doğrulama güvenli şekilde tamamlandığı için oturum anahtarı (session key) ortadaki adam saldırılarından etkilenmeden güvenli şekilde oluşturulur. Bu oturum anahtarı kullanılarak SRTP simetrik şifreleme protokolü ile çağrı esnasında iletilen mesajları (ses paketleri) şifreler. Bu tez çalışmasında güvenli ve güvenilir kimlik doğrulama sonrası oturum anahtarı taraflar arasında güvenli bir şekilde oluşturulmaktadır. Böylece üçüncü taraflara ihtiyaç duymadan IP ağı üzerinden taraflar arasında VoIP görüşmesi güvenli bir şekilde gerçekleştirilir.



Şekil 3.4: Önerilen Mekanizmanın Şematik Diyagramı.

3.2. Sistem Mimarisi

Bu bölüm, önerilen yöntemin temel unsurlarını, sistem bileşenlerini ve blok zincir tabanlı kimlik doğrulamasını sistem mimarisi üzerinden açıklamaktadır.

3.2.1. Sistem Bileşenleri

Tezde sunulan blok zincir tabanlı kimlik doğrulama mekanizması temel olarak yedi farklı bileşenden oluşur. Bunlar sırasıyla; VoIP Ağı, Yönetici, VoIP Kullanıcıları, Blok Zincir Ağı, Akıllı Sözleşme, Madenciler ve Konsensüs algoritmasıdır.

VoIP Ağı: Sesli mesajları veya multimedya paketlerini aktaran bir IP ağıdır. Üzerine VoIP uygulaması yüklüyse, herhangi bir bilgisayar, mobil cihaz veya akıllı telefon IP telefon (bazen SIP Telefonu veya VoIP telefonu olarak da adlandırılır) olarak kullanılabilir. VoIP uygulaması kullanıcıların VoIP ağı üzerinden IP telefon ile sesli arama yapmalarını sağlar.

Yönetici: Bir grup VoIP kullanıcısının blok zincirine güvenli bir şekilde kaydolması için bir kimlik (ID) ve bilet (Ticket) oluşturan yönetim cihazıdır. Sistem içerisinde blok zincir akıllı sözleşmesinin başlatılması ilişkilendirme için gereklidir ve bu işlem Yönetici tarafından gerçekleştirilir. Ayrıca Yönetici, VoIP Ağının bir üyesidir. VoIP ağında ilişkili VoIP kullanıcıları arasından bir Yönetici seçilir ve diğer kullanıcılara VoIP kullanıcıları adı verilmektedir. Yönetici kayıtlanma sürecinde gerekli olan güvenli ve güvenilir bilet ve ID üretir ve ilgili VoIP kullanıcısına iletir. Yöneticinin blok zincirindeki kimlik doğrulama sürecine rolü yoktur. Bu nedenle, Yönetici kesintiye uğradığında, yeni kullanıcılar için VoIP ağında kısa süreliğine kayıt işlemi durur ancak kimlik doğrulama işlemi etkilenmez ve tüm kayıtlı kullanıcılar için kimlik doğrulama süreci kesintisiz devam eder.

VoIP Kullanıcıları: Bir VoIP çağrısında kullanıcılar arayan veya aranan olabilir. VoIP kullanıcılarının temel amacı, bir IP ağı üzerinden güvenli kanal oluşturarak uçtan uca iletişim kurmaktır. VoIP ağı içerisinde IP telefonlar üzerinden etkileşim kurarlar. Kullanıcıların güvenli kimlik doğrulaması için blok zincir ağına kayıtlanması gerekir.

Blok Zinciri Ağı: Merkezi doğrulamaya dayanan geleneksel yöntemlerin aksine, blok zincir bir konsensüs algoritması aracılığıyla cihazları birbirine bağlayan merkezi olmayan bir eşler arası ağdır. Eşler arası yani P2P, ağdaki işlemlerin bir arada

onaylandığı ve tüm katılımcı düğümler (bilgisayarlar) arasında paylaşıldığı anlamına gelmektedir. Blok zincir ağları genel (public), özel (private) ve konsorsiyum (consortium) blok zincirleri olarak 3 şekilde kategorize edilebilir (Buterin, 2019). Bu tezde özel blok zincir tercih edilmiştir. Özel blok zincirler blok zincir ağındaki işlemleri hızlı gerçekleştirir çünkü genel blok zincir ağına göre daha küçük bir kullanıcı grubuna sahiptir. Öte yandan, özel blok zinciri, her kullanıcı tarafından okunabilen ancak yalnızca yetkili düğümler tarafından yazılan bir platformdur. Bu açıdan gerçekleştirilen bir işlemi doğrularken özel blok zincir ağında fikir birliğine varmak için daha az zaman harcanmaktadır. Özel blok zincirler her saniye binlerce işlemi işleyebilir ve kolayca ölçeklenebilir. Bu tez çalışmasında amaç gerçek senaryolarda blok zincir ağının VoIP ağında uygulanabilirliğini göstermektir. Çünkü VoIP haberleşme herkese açık, esnek ve ölçeklenebilir bir şekilde kullanılmalıdır. Kimlik doğrulama işlemi blok zincir ile şeffaf bir şekilde gerçekleştiği için akış kontrolü sağlanarak güvenli ve inkâr edilemeyen bir haberleşme altyapısı sağlanmış olur.

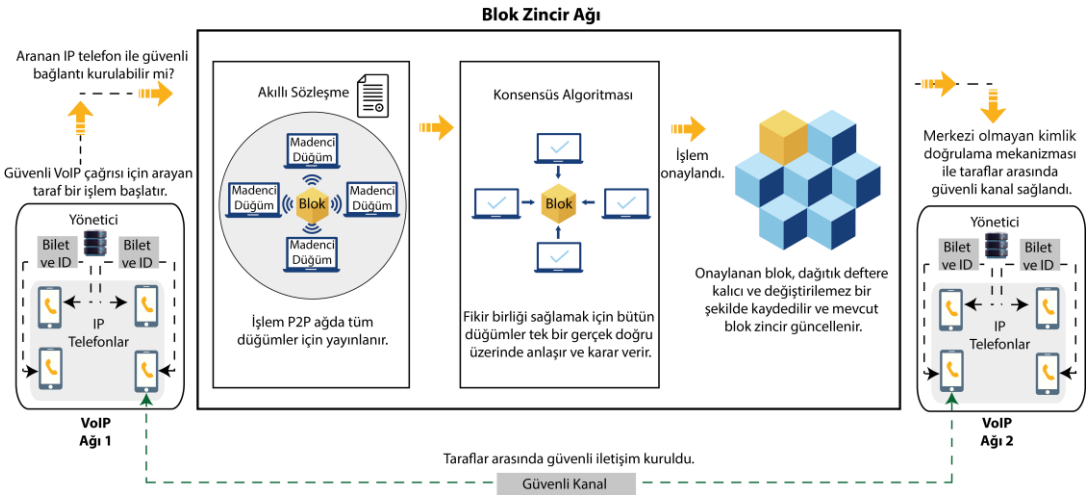
Akıllı Sözleşme: Blok zinciri merkezi olmayan uygulamalar için bir ağ hale getiren akıllı sözleşme adı verilen kod parçasıdır. Önerilen sistemde akıllı sözleşmelerin kullanılması, VoIP hizmetlerinin ve kaynaklarının paylaşımını kolaylaştırır. Sistem içerisindeki iş akışında mevcut olan ve zaman alıcı kriptografik işlemleri otonom hale getirir. Akıllı sözleşmelerin blok zincir tarafından etkinleştirilmesiyle, ağ içerisinde belirli bir koşul yerine getirildiğinde en başta belirlenen sözleşme kuralları otomatik olarak yürütülür. Akıllı sözleşme sayesinde blok zincir bir kere çalıştırıldığında VoIP kullanıcıları ile otonom şekilde etkileşim gerçekleştirebilmektedir. Akıllı sözleşme, VoIP kullanıcısı tarafından gönderilen kayıtlanma talep mesajının doğruluğunu ve meşruluğunu kontrol ettikten sonra, VoIP kullanıcısının blok zincire işlem göndermesine izin verecektir.

Madenci Düğüm: Blok zincir ağlarındaki madenciler, işlemleri onaylayarak ve blok zincirinin kopyalarını saklayarak sistemin güvenliğini ve veri değişmezliğinin sağlar. Madenciler, kayıtlı VoIP kullanıcılarının kimlik doğrulama kurallarını saklamak ve herkese açık olarak erişmek için blok zincir arayüzünü kullanır. Blok zincir ağındaki madenciler aracılığıyla veriler tamamen merkezi olmayan bir ağda değiştirilemez şekilde dağıtık defterlerde saklanır ve güvenilirdir. Dağıtık defterler sayesinde

geçmişteki işlemlerin bir kopyası bütün katılımcılarda mevcuttur. Bu açıdan blok zincirinde madenciler dağıtık defter kullanması sistem içerisinde güvenilirlik sağlar.

Konsensüs Algoritması: Madenciler mutabakat sağlamak için konsensüs algoritması kullanır. Konsensüs algoritması ile bazı madenciler başarısız (fail) olsa bile, sistemdeki tüm madenciler tek bir doğru kaynak üzerinde uzlaşır ve böylece hata toleransı sağlanır. Blok zincirin güvenliği, özetleme algoritması ve konsensüs algoritmalarının yaratıcı kullanımından gelir. Konsensüs algoritması sunulan tezdeki kimlik doğrulama mekanizmasında VoIP kullanıcılarının dağıtık bir ortamda koordine olmasını sağlayan mekanizmadır. Böylece, bir konsensüs mekanizması, bir blokta (veri depolama alanı) kurcalamayı önler ve diğer blokların tüm özet değerlerini yeniden hesaplar. Blokların dürüst bir şekilde doğrulandığını kanıtlamak için çok sayıda mekanizma mevcuttur. En çok kullanılanlar İş Kanıtı (PoW) ve Hisse İspatı (PoS) mekanizmalarıdır. Konsensüs algoritmaları sunulan yöntemde, yalnızca meşru kullanıcıların kayıtlanmasına izin vererek haberleşme sistemini güvende tutar. Diğer taraftan, PoW ve PoS arasındaki en büyük fark, enerji kullanımlarıdır. PoW, madencilerin karmaşık matematik problemlerini çözmek için rekabet etmesini gerektirir. Sorunu çözen ilk madenci, bir işlem bloğu ekler ve ödül kazanır. Bu durum, blok zincir ağındaki tüm madencilik cihazlarının aynı problemi hesaplamasına ve yüksek miktarda enerji kullanımı ve zaman kaybına neden olur. PoS mekanizması ise, tüm karmaşık denklemleri çözmek için madenci değil doğrulayıcılar (validators) kullanır ve blok zincir ağındaki işlemleri doğrulamak için daha az enerji harcar. Enerji verimliliği daha fazla ölçeklenebilirlik sağlar. VoIP gerçek zamanlı ses verisi iletimi için kullanılmaktadır. Bu açıdan, önerilen yaklaşımda PoS konsensüs algoritması kullanımı daha uygundur.

Bu tez çalışmasında, konsensüs mekanizması, dağıtık defter ve akıllı sözleşme gibi blok zincir bileşenleri, güvenli bir VoIP çağrısı oluşturmak için kimlik doğrulamada kullanılmaktadır. Şekil (3.5); önerilen blok zincir tabanlı merkezi olmayan kimlik doğrulama mekanizmasının sistem mimarisini göstermektedir.



Şekil 3.5: VoIP'te Merkezi Olmayan Kimlik Doğrulama Sistem Mimarisi.

Önerilen yöntemde, VoIP kullanıcıları kimlik doğrulama gerçekleştirebilmek için blok zincirine bir kayıt talebi gönderir. Blok zincir platformu, akıllı sözleşme kullanarak kullanıcı bilgilerini doğrular ve özet değerini güvenli şekilde saklar. Dağıtık defter ise, VoIP kullanıcı bilgilerini kalıcı ve değiştirilemez bir şekilde depolamak için kullanılır. Ardından, VoIP ağı içerisindeki her meşru VoIP kullanıcısı için imzalı bir sertifika oluşturulur. Bilet olarak adlandırılan bu sertifika blok zincirinde kayıtlanma esnasında kullanıcı bilgilerini doğrular. Tüm VoIP kullanıcıları, sisteme kaydolmak için ilgili bileti Yönetici'den talep eder. Yönetici, her yeni VoIP kullanıcısı için yeni bir benzersiz kimlik bilgisi üretir. Daha sonra VoIP kullanıcısının kimliği ve genel anahtarını kullanarak ilgili bir bilet oluşturur. Bu bilet, ECDSA kullanılarak Yönetici özel anahtarıyla imzalanır ve ilgili VoIP kullanıcısına gönderilir. VoIP kullanıcısı, akıllı sözleşme aracılığıyla blok zincir platformuna kaydolmak için bilet ve kimlik bilgisini özel anahtarıyla imzalar ve genel anahtarı ile birlikte blok zincir ağına gönderir.

Blok zincir ağındaki akıllı sözleşme tarafından kimlik ve bilet doğrulama (validation) süreci gerçekleştirilir. Genel anahtarın ve imzanın gönderilmesi sonrası blok zincir ağındaki madenciler işlemi (transaction) doğrulayabilir ve işlemi geçerli olarak kabul edebilir. Bilet onaylanırsa, yeni kullanıcı bilgileri güvenilir listeye (trusted list) eklenir ve işlem raporunu blok zincire eklemek için yeni bir blok oluşturulur. Tüm bu adımlar başarıyla tamamlanırsa, yeni VoIP kullanıcısı blok zinciri ağına kaydedilir. Böylece taraflar arasında güvenli kanal üzerinden anahtar değişimi gerçekleştirilerek güvenilir VoIP çağrısı oluşturulur.

3.2.2. Varsayımlar

Önerilen modeli açıklamadan önce bazı varsayımları derinlemesine incelemek faydalı olacaktır. Bu varsayımlar sırasıyla;

- VoIP ağındaki bir VoIP kullanıcısı, Yönetici olarak tasarlanmıştır. Ayrıca herhangi bir kullanıcı ağda Yönetici olarak aday gösterilebilir.
- Yönetici güvenilir ve meşru kabul edilmektedir.
- Yönetici ile akıllı sözleşme arasındaki haberleşme öncesinde, Yönetici tarafından oluşturulan imza, akıllı sözleşme ile güvenli bir şekilde paylaşılır.

3.3. Sistem Kimlik Doğrulama Süreci

Tezde sunulan kimlik doğrulama mekanizması temel olarak dört ana fazdan oluşur. Bu dört faz sırasıyla (1) Blok Zincir İlişkilendirme Süreci, (2) Sistemi Başlatma, (3) Sisteme Kayıtlanma ve (4) Kimlik Doğrulamadır.

Blok zincir ağındaki düğümler, belirli bir işlemi tekrarlayarak eşler arası merkezi olmayan bir ağ oluşturur. İlk adım için düğümler, bir çift özel/genel anahtar aracılığıyla blok zincir ağı ile etkileşime (ilişkilendirme) girer. VoIP kullanıcısının kayıtlanma ve kimlik doğrulama işlemlerini yapabilmesi için öncesinde blok zincir ağına ilişkilendirme sürecinin tamamlanması ve Yönetici tarafından akıllı sözleşmenin başlatılması gerekmektedir. Özel anahtarlarını kendi işlemlerini dijital olarak imzalamak için kullanırlar ve açık anahtarları aracılığıyla ağ üzerinde adreslenebilirler. İmzalanan her işlem, işlemi oluşturan bir düğüm tarafından yayınlanır. İkinci adım ise blok zincir ağındaki işlemi oluşturan düğüm dışındaki tüm düğümler tarafından doğrulanması sürecidir. Bu adımda geçersiz işlemler yok edilir. Bu sürece doğrulama (validation) denir. Sonraki adımda, her düğüm belirli bir zamanda doğrulanmış işlemleri bir bloğa toplar ve blok için yalnızca bir kez kullanılan bir sayı (nonce) değeri oluşturarak konsensüs algoritmasını (Hisse İspatı (PoS) veya İş Kanıtı (PoW) benzeri) uygular. Bir düğüm nonce değeri oluşturduğunda, bloğu tüm düğümlere yayınlar. Bu sürece madencilik denir. Son olarak tüm düğümler ilk kez yayınlanan bloğu seçer ve bloğun geçerli işlemler içerdiğini ve zincirlerinde (chain) önceki bloğun özet değerini ve doğru referanslar içerdiğini onaylar. Bu durumda, bloğu zincirlerine ekler ve blok zincirinde güncelleme gerçekleştirirler. Aksi halde, önerilen blok kabul edilmez ve zincire eklenmez.

Tezde sunulan yöntem için, Şekil (3.6) birbiriyle iletişim kuran VoIP kullanıcıları için işlemleri yöneten kontrol fonksiyonlarını ve parametreleri açıklar.

Parametre ve Fonksiyon Açıklamaları

//Parametreler ve fonksiyonların tanımı.
Parametreler:

Admin: Nesne (Object) *// Blok zincirin Yönetici nesne gösterimi*
Obj: Nesne
Arayan*:* Nesne
Aranan*:* Nesne
Ids: Eşleme, Haritalama (mapping) (***Adres***=>integer) *// Adres tablosunu kullanıcı kimliğine (ID) eşleme (güvenilir liste - trusted list)*
Güvenilir Üye: Eşleme (integer=>adres) *// Kullanıcı kimliğini adrese haritalama (mapping) tablosu*
MsgBox: Eşleme (integer=>string) *// ID tablosunu mesaja eşleme (VoIP kullanıcısının gelen kutusu)*

Fonksiyonlar:

1. ***Fonksiyon*:** BcAdminInit(Object Yönetici) *// Blok zincir Yönetici nesnesi tarafından Başlatma (initialization) işlemi gerçekleştirme*
2. ***Fonksiyon*:** ObjIdExists(Integer objId) *// NesneID değerini blok zincirde kullanılıp kullanılmadığını kontrol etme*
3. ***Fonksiyon*:** ObjAddrExists(address objAddr) *// Nesnenin genel anahtarının blok zincirde kullanılıp kullanılmadığını kontrol etme*
4. ***Fonksiyon*:** ControlofTrust(object arayan, object aranan) *// Arayan ve aranan tarafın güvenilir listede olup olmadığını kontrol etme*
5. ***Fonksiyon*:** TicketVerify(object obj, integer Bilet) *// Biletin geçerli olup olmadığını kontrol etme*
6. ***Fonksiyon*:** AddTrustedObject (Object obj) *// Güvenilir listeye yeni nesne (VoIP kullanıcı) ekleme işlemi*
7. ***Fonksiyon*:** sendMSG (object arayan, object aranan, text msg)
   // Mesajı alıcının mesaj kutusuna gönderin
8. ***Fonksiyon*:** readMSG(Object caller) // readMSG(Object arayan)
   // İlgili güvenilir kullanıcıdan gelen mesajı oku
9. ***Fonksiyon*:** Error (string Err) *// Bir hata mesajı döndürür*

Şekil 3.6: Sistemdeki İşlemleri Yöneten Kontrol Fonksiyonları ve Parametreler.

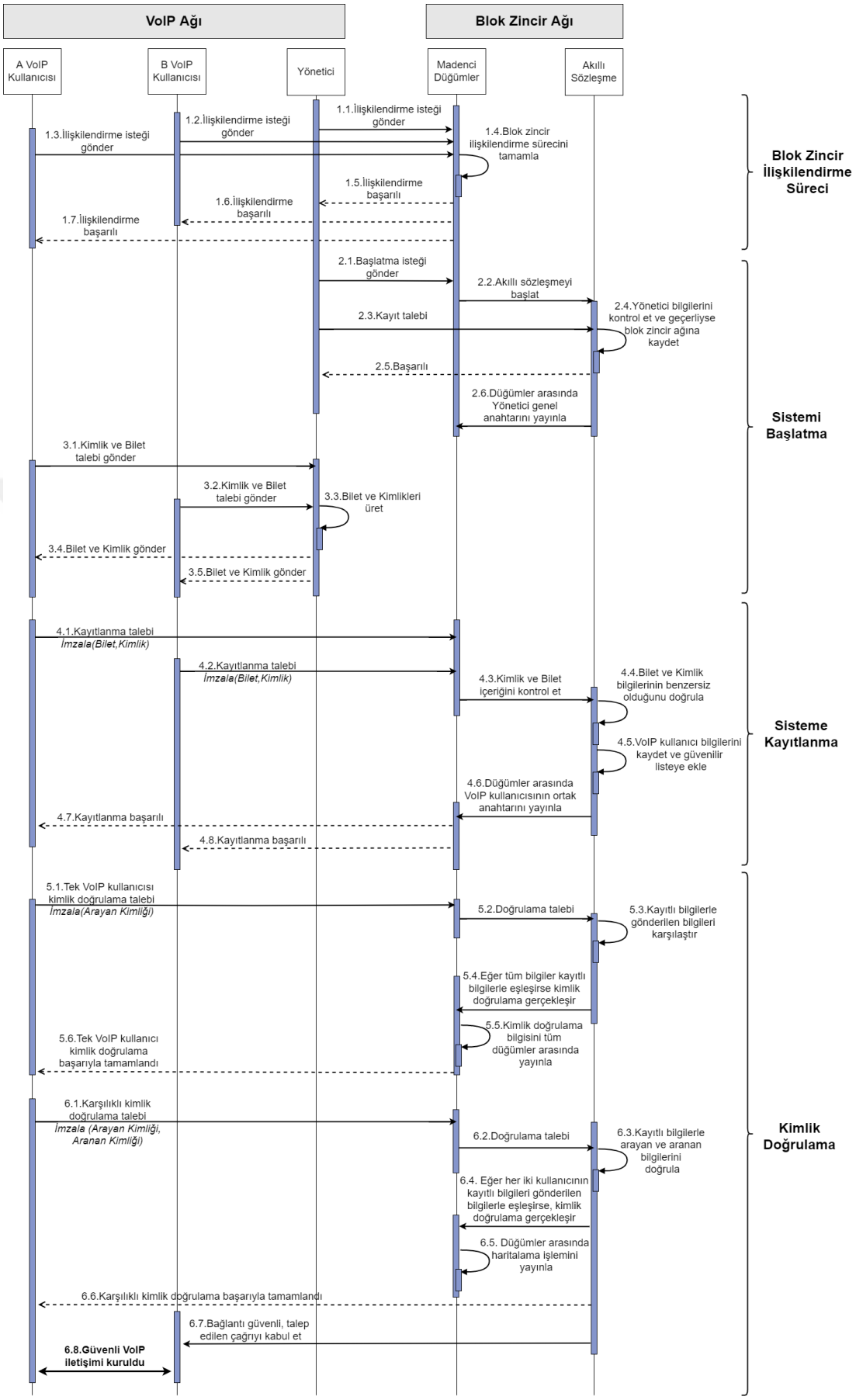
Bu tezde, VoIP uygulama kullanıcılarının kimlik doğrulaması için tipik bir akıllı sözleşme, gerekli tüm işlevler ve merkezi olmayan kimlik doğrulama sisteminin uygulanması için haritalama listeleri (depolama için güvenli listeler) tasarlanmıştır. Bu açıdan akıllı sözleşme, güvenilir listedeki bilgileri kontrol ederek VoIP kullanıcısının kimlik doğrulama sürecini yönetir. Böylece her kimlik doğrulamada madencilik yaparak yeni bir blok oluşturulmasına gerek yoktur. Yani hızlı bir kimlik doğrulama süreci gerçekleştirilir.

3.3.1. Önerilen Kimlik Doğrulama Yönteminin Çalışma Mekanizması

Bu bölümün amacı, VoIP kullanıcıları arasında uçtan uca güvenli ve güvenilir kimlik doğrulaması sağlayan yöntemin şemasının tüm adımlarını detaylı olarak açıklamaktır. UML sıralama (sequence) diyagramı oluşturularak tezde sunulan kimlik doğrulama mekanizmasının 4 ana faz halinde tüm adımları ve nesne etkileşimleri ayrıntılı olarak Şekil (3.7)'de sunulmuştur.

Tüm VoIP kullanıcıları için (1) Blok zincir ilişkilendirme sürecinin gerçekleştirilmesi bir adımdan, (2) Sistemi Başlatma fazı, blok zincirin akıllı sözleşmesinin başlatılması ve VoIP kullanıcı kayıtlanma bilgilerinin Yönetici tarafından gönderilmesi olmak üzere iki adımdan, (3) Sisteme Kayıtlanma fazı, VoIP kullanıcıların kayıtlanması olarak bir adımdan ve (4) Kimlik Doğrulama fazı, ise mesaj kutusundan sesli mesaj dinlemek ve karşılıklı VoIP görüşmesi yapmak üzere iki farklı kimlik doğrulama adımından oluşmaktadır. IP ağındaki VoIP kullanıcıları arasında güvenli kimlik doğrulamayı sağlayan ve toplamda 6 adımdan oluşan bu 4 ana aşama sırasıyla adım adım aşağıda sunulmuştur.

Adım 1: SIP, ses ve anlık mesaj iletişimi için IP telefonlar aracılığıyla medya haberleşme oturumlarının sinyalizasyonunu ve yönetimini gerçekleştirir. VoIP ağında kullanıcıların SIP kayıtlanması tamamlandıktan sonra, sisteme kayıtlı VoIP kullanıcıları blok zincir ilişkilendirme talebi gönderir. Ayrıca, blok zincir platformuyla ilişkili tüm VoIP kullanıcıları, Eliptik Eğri Dijital İmza Algoritması (ECDSA) kullanarak genel/özel anahtar çiftleri oluşturur.



Şekil 3.7: Önerilen Kimlik Doğrulama Şemasının Genel Akışı.

Adım 2: Blok zincir ilişkilendirme aşaması başarılı bir şekilde tamamlandıktan sonra başlatma (initialization) aşaması işlemleri gerçekleşir. İlk olarak Yönetici, akıllı sözleşmeye bir başlatma talebi gönderir. İşlemler akıllı sözleşme işlevlerini çağırabilir. Akıllı sözleşmeler, esneklik sağlayarak kullanıcılar arasındaki işlemleri ve sözleşmeleri güvenilir ve tutarlı bir şekilde yürütür. Ek olarak, sistemin otomatik olarak çalışmasını (execution) kontrol eder.

Blok zincir ağındaki işlemler, tüm blok zinciri madenci düğümleri tarafından şeffaf olarak izlenebilir ve blok zincir ağında gerçekleşen bir işlem kayıt altına alınır. Bir saldırganın herhangi bir işlemi değiştirmesi girişimi başarısız olacaktır. Çünkü blok zincir özet işaretçisi (hash pointer) adı verilen bir kriptografik teknik kullanmaktadır ve verilerin yerini işaret ederken kriptografik özetleme (hash) fonksiyonu ile özetleyerek gösterir. Ayrıca blok zincir ağında her madenci düğümde blok zincirin bir kopyası vardır (public ledger) ve bir saldırganın ağdaki tüm kopyaları değiştirmesi çok zordur. Madenci düğümleri, tanımlanmış kurallara uygun olarak blok içindeki işlemlerin doğrulanmasını yönetir. Madenci düğümleri, eklenen bloğu doğrulamak için konsensüs mekanizmasını kullanır. Akıllı sözleşmeyi başlattıktan sonra Yönetici blok zincire bir kayıt talebi gönderir. İstek kabul edilirse, akıllı sözleşme, blok zincir düğümleri arasında Yönetici'nin genel anahtarını yayınlar.

Adım 3: Bu adımda artık Yönetici, blok zincirine ilişkilendirilmiş ve kayıtlı olduğundan güvenli bir cihaz olarak kabul edilmektedir. Blok zincire kayıtlanmak isteyen tüm VoIP kullanıcıları Yönetici'ye Bilet ve Kimlik isteği gönderir. Yönetici, her yeni VoIP kullanıcısı için benzersiz bir kimlik oluşturur, ardından VoIP kullanıcısının yeni kimliğine ve genel anahtarına dayalı olarak ilgili bir benzersiz Bilet oluşturur. Bilet ve ID değerini ilgili VoIP kullanıcısına gönderir.

Adım 4: Bilet ve ID değerine sahip her VoIP kullanıcısı blok zincirine kayıtlanmak için imzalı bir işlem (transaction) oluşturur. VoIP kullanıcı bilgilerinin tamamı blok zincirin kullandığı güçlü kriptografik algoritmalarla şifrelenir ve blok zincirindeki dağıtık defterlerde saklanır. Blok zincir, akıllı sözleşme aracılığıyla gerçekleştirilen özetleme algoritmalarından elde edilen özet veriyi kullanır. Kayıtlanma için, bir VoIP kullanıcısı blok zincir ağına bir Bilet ve Kimlik bilgisi gönderir ve bunları dijital imza ile imzalar. Ardından, blok zincirdeki madenciler, doğrulama talebi için VoIP kullanıcı kimlik bilgilerini akıllı sözleşmeye gönderir. Akıllı sözleşme, VoIP kullanıcısının daha

önce kayıtlı olup olmadığını kontrol etmek için imzayı doğrular ve kimlik bilgilerini kontrol eder. VoIP kullanıcı bilgilerinin doğrulanması başarılı olursa, ilgili kullanıcının bilgileri güvenilir listeye eklenir ve güvenli şekilde depolanır. Yani işlem geçerlidir ve dağıtık defterlerde kayıt altına alınır. Kayıtlanma tamamlandıktan sonra, VoIP kullanıcısının açık anahtarı blok zincir ağında isimsiz tutularak (anonim) gizlilik ve mahremiyet sağlanır. Böylece blok zincir ağında iki kişinin görüşme yaptığı şeffaf olarak bilinir ancak VoIP kullanıcılarının kimlik bilgisi ağda paylaşılmaz.

Adım 5: Kayıtlanma sonrası her VoIP kullanıcısı blok zincir ağında meşrudur ve kimlik doğrulama gerçekleştirebilir. Önerilen şemada iki tür kimlik doğrulama vardır. Birincisi, tek kullanıcı kimlik doğrulama modelidir. VoIP kullanıcısı, sesli mesajlarını okumak için blok zincir ağına dijital bir anahtarla imzalanmış arayan kimliği ile tek kullanıcı kimlik doğrulama isteği gönderir. Blok zincirindeki akıllı sözleşme, gönderilen bilgileri kontrol eder ve doğrular. Eğer VoIP kullanıcı tarafından gönderilen işlem bilgileri güvenilir listedeki kayıtlı verilerle eşleşirse kimlik doğrulama gerçekleştirilir. Gerçekleşen doğrulama işleminden sonra, kimlik doğrulama bilgileri madenci düğümleri arasında yayınlanır.

Adım 6: Arayan tarafından internet gibi açık ve güvensiz ağ üzerinden arama yapılmasına karar verilmesi durumunda, arama öncesinde VoIP kullanıcıları arasında karşılıklı kimlik doğrulama (mutual authentication) yapılmalıdır. İlk olarak arayan, kendisinin ve aranan kişinin kimliğini özel anahtarıyla imzalanmış olarak gönderir. Ardından, akıllı sözleşme arayan ve aranan bilgilerini kayıtlı bilgilerle doğrular. Kimlik doğrulama başarılı olursa, güvenilir listede haritalama (mapping) işlemi gerçekleşir. Böylece sonraki aramalarda kimlik doğrulama daha hızlı gerçekleşir. Çünkü eşleşme haritasından kontrol hızlıca yapılabilir. Ayrıca madenciler arasında haritalama şeffaf bir şekilde yayınlanır. Son olarak karşılıklı kimlik doğrulaması onaylanır ve aranan kişi çağrıyı kabul ederse güvenli iletişim kurulur.

Daha kolay anlaşılması açısından genel hatları ile altı adımda özetlenen tezde sunulan kimlik doğrulama mekanizmasının dört ana aşamada ayrıntılı açıklaması aşağıda sunulmuştur. Bu dört ana aşama sırasıyla (1) Blok Zincir İlişkilendirme Süreci, (2) Sistemi Başlatma, (3) Sisteme Kayıtlanma ve (4) Kimlik Doğrulamadır. Aşamalar tezde sunulan yöntemin teknik altyapısını ayrıntılı olarak ele almaktadır.

Aşama 1: Blok Zincir İlişkilendirme Süreci

Sinyalleşme katmanı, bir veya daha fazla katılımcıyla VoIP oturumlarını oluşturmak, değiştirmek ve sonlandırmak için kullanılan bir uygulama katmanı kontrol sistemidir. Bu katman, oturum işlemi için genellikle SIP protokolünü kullanır. Sunulan tezde ilk olarak VoIP ağı kurulur. Arama işlevleri sağlamak için tüm VoIP telefon cihazlarının SIP sunucusuna kayıtlı olması gerekir. Arayan SIP sunucusuna bir çağrı talebi ilettiğinde SIP protokolü oturumu başlatır ve VoIP kullanıcıları arasında bağlantı kurar. Bu tez çalışmasında önerilen kimlik doğrulama, medya veri aktarımı (ses paketlerinin konuşma esnasında iletimi) başlamadan hemen önce ve sinyalleşme katmanında SIP sunucusu üzerinden taraflar arasında çağrı kurulması esnasında ara bir katman olarak blok zincir ağında gerçekleştirilir.

Sunulan kimlik doğrulama mekanizmanın TCP/IP protokolündeki yeri taşıma katmanı ile uygulama katmanı arasındadır. Bunlar medya aktarım katmanı ve sinyalleşme katmanı olarak iki alt katmandan oluşmaktadır. Kimlik doğrulama işlemi, SIP protokolü kullanılarak VoIP uygulamasında taraflar arasında bağlantı kurduktan sonra blok zincir ağı üzerinden gerçekleştirilir. Böylece oturum anahtarı oluşumu için anahtar değişim mekanizması güvenli şekilde gerçekleştirilebilir. VoIP Protokol Yığını (Protocol Stack) olarak adlandırılan tüm bu süreç Şekil (3.8)'de açıkça gösterilmektedir.

Şekil 3.8: VoIP Protokol Yığını.

Bu çalışmada önerilen mekanizma, kullanıcılar arasında güvenli gizli bir anahtar oluşturmak için Eliptik Eğri Diffie-Hellman Anahtar Değişimi (ECDH) algoritmasını tercih eder. ECDH algoritmasının seçilmesinin temel nedeni, hem bellek kullanımı ve yürütme sürelerinde Diffie-Hellman gibi diğer algoritmalardan süre olarak daha iyi performans göstermesi ve hem de daha güçlü şifreleme sağlamasıdır. Anahtar değişimi sonrası simetrik şifreleme algoritması kullanan SRTP, medya aktarım katmanında uçtan uca güvenli iletişim için oturum anahtarı oluşturur. SRTP genellikle AES simetrik şifreleme algoritmasını tercih eder. Çağrı işlemi sırasında mesajlar RTP protokolü üzerinden güvenli bir şekilde iletilir.

Her VoIP kullanıcısı, öncelikle blok zincir ağıyla ilişkilendirme sürecini başlatır ve blok zinciri ağına bir işlem (ilişkilendirme talebi) gönderir. İlişkilendirme talebi öncesinde tüm VoIP kullanıcıları ve Yönetici, genel/özel anahtar çiftini ECDSA kullanarak üretir. ECDSA, imza süresi (şifreleme) kısadır ve aynı güvenlik seviyesini anahtar boyutu açısından RSA gibi geleneksel imza algoritmalarına göre daha küçük boyutlu şifreleme anahtarları ile sağlar. ECDSA, eliptik eğri üzerinde kullanılan bir dijital imza algoritması türüdür ve VoIP kullanıcıları arasında mesajları imzalamak için anahtar üretir. Böylece, güvenli veri aktarımı için ECDSA ile, ağda düğümler arasındaki haberleşmede iletilen mesajların şifrelenmesi sağlanır ve mesaj verisinin içeriğinin saldırgan tarafından ele geçirilmesi önlenir.

ECC algoritması, etki alanı parametrelerine dayanmaktadır. P, eğrinin tanımlandığı bir alandır, $a\ ve\ b$ eğrinin değerleridir, G üretici noktasıdır ve n, G'nin asal mertebesidir. O halde, $n \times G = 0$. Ayrıca özel anahtar (P_{rk}), hesaplanabilen rastgele bir değerdir ve Denklem (3.1) ile verilmiştir.

$$1 \leq P_{rk} \leq n - 1 \quad \textbf{(3.1)}$$

Denklem (3.2) ile özel anahtarın ve üretici noktasının eliptik eğri nokta çarpımı olan genel anahtar (P_{uk}) ifadesi gösterilmiştir.

$$P_{uk} = P_{rk} * G \quad \textbf{(3.2)}$$

Genel/özel eliptik eğri anahtar çifti oluşturulduktan sonra kayıtlanma ve kimlik doğrulamada işlemi imzalayarak blok zincire iletme VoIP kullanıcıları tarafından gerçekleştirilebilir.

Yönetici ECDSA kullanarak genel anahtarını (A_{puk}) ve özel anahtarını (A_{prk}) üretir. Genel anahtarının ilk 5 basamak değerini kullanarak kimlik (ID_{admin}) değerini oluşturur. Yönetici özel anahtarını güvenli şekilde saklar. Kayıtlanmak için genel anahtarını ve kimlik bilgisini imzalayarak blok zincirine iletir. Blok zincir genel anahtar ve kimlik bilgisini akıllı sözleşme üzerinden kontrol eder ve onaylar veya reddeder. Yönetici genel anahtarı için ilişkili bir zaman damgası (timestamp) üretir. Yönetici özel anahtarını kullanarak genel anahtar ve zaman damgasını imzalar. Ardından oluşturulan imza ve kimlik bilgisini birlikte imzalar. Oluşturulan imzalı işlem blok zincire gönderilir. Denklem (3.3) ile Yöneticinin kayıtlanmak için oluşturduğu imzalı işlem sunulmuştur.

$$Imza_{A_{prk}}(ID_{admin},\ Imza_{A_{prk}}(A_{puk}, zaman\ damgası)) \quad \textbf{(3.3)}$$

İşlem blok zincire iletildiğinde, Yönetici'nin özel anahtarıyla imzalanmış işlem madenciler tarafından doğrulanır ve bütünlüğü kontrol edilir. Denklem (3.4) ile Yönetici genel anahtarı kullanılarak imzalı işlem doğrulanmaktadır ve bütünlük kontrolü gerçekleştirilmektedir.

$$A_{puk}(ID_{admin},\ Imza_{A_{prk}}(A_{puk}, zaman\ damgası)) \quad \textbf{(3.4)}$$

Madenciler, blok içindeki işlemlerin tanımlanmış kurallara uyduğunu doğrular. Madenciler, eklenen bloğu doğrulamak için konsensüs mekanizması kullanır ve ID_{admin} değerinin blok zincire daha önce kayıtlanmadığını kontrol eder. ID_{admin} değeri daha önce blok zincire kaydedilmemişse işlem doğrulanır. Böylece Yönetici'nin bilgileri ($ID_{admin}, A_{puk}\ ve\ zaman\ damgası$) blok zincir ağına depolanır ve Yönetici ilişkilendirme ve kayıtlanma işlemi tamamlanmış olur.

Aşama 2: Sistemi Başlatma

Tezde sunulan mekanizma, çok sayıda VoIP kullanıcısı için uygulanabilir. Ancak, öncesinde bazı adımların gerçekleştirilmesi gerekmektedir. Bu adımlar sırasıyla;

I. Başarılı bir blok zincir ilişkilendirme sürecinden sonra Yönetici, akıllı sözleşmeyi başlatır. Akıllı sözleşme, Yönetici bilgilerini blok zincirindeki dağıtık defterlerde saklar. Ayrıca blok zincir ağındaki madenciler arasında Yönetici ortak anahtarı bir işlem oluşturularak yayınlanır.

II. Blok zincir ağında asimetrik kriptografi dijital imzalar üretmek için kullanılmaktadır. Blok zincire gönderilen her işleme özel sayısal bir imza üretilir. Bu imza yalnızca özel anahtarı bilen ilgili VoIP kullanıcı tarafından

üretilebilir. Ancak, genel anahtara sahip olan herkes, imzayı doğrulayabilir. Asimetrik kriptografinin bu kullanışlı özelliği, herkesin her işlemde her imzayı doğrulamasını mümkün kılarken, yalnızca özel anahtar sahiplerinin geçerli imzalar üretebilmesini sağlar.

III. Başlatma aşamasında, Yönetici'den bilet talep eden ve sisteme uygun görülen her VoIP kullanıcısı, blok zincir üzerindeki akıllı sözleşme ile iletişim kurarak blok zincir ağına kaydolabilir. Kayıtlanmak isteyen VoIP kullanıcısı genel anahtarını, ID değerini ve biletini kullanarak özel anahtarıyla imzalı bir işlem oluşturur ve blok zincire gönderir. VoIP kullanıcıları blok zincirindeki akıllı sözleşme aracılığıyla doğrulanarak blok zincire kayıtlanır.

IV. Kayıtlı VoIP kullanıcılarının genel anahtarları güvenilir listede saklanır. Akıllı sözleşme, güvenilir listenin veri değişmezliği için bir dizi kural içerir. Bu sayede blok zincir ağında depolanan veriler için bütünlük sağlanmış olur. Akıllı sözleşmenin güvenilir listeyi yönetmesi içeriğine müdahale edebilip değiştirebilmesi anlamına gelmez. Tüm kullanıcılar için güvenilir listeyi şeffaf hale getirir ve bir arayüz oluşturarak kullanıma sunar.

VoIP ağında akıllı sözleşmeyi başlatan Yönetici tarafından akıllı sözleşme başlatma kuralları Şekil (3.9) ile verilen algoritma üzerinden açıklanmıştır. Bu kurallar akıllı sözleşme için başlatıldıktan sonra Yönetici belirlenir ve bu andan itibaren diğer kullanıcılar Yönetici olamaz veya sistem içerisinde herhangi bir kural değiştirilemez. Ayrıca algoritma ile belirtilen adres (address) ifadesi, genel anahtar anlamına gelir.

Algoritma: Akıllı Sözleşme için Başlatma Kuralları

```
Başla
    if (BcAdmin.address = 0) then
        BcAdminInit(Yönetici)
    else
        return Error ("Blok zincirinin Yöneticisi zaten başlatıldı")
Bitir
```

Şekil 3.9: Akıllı Sözleşme için Başlatma Kuralları.

Aşama 3: Sisteme Kayıtlanma

Başlatma aşamasında belirtildiği gibi, Yönetici güvenli bir şekilde belirlenir ve kaydedilir. Yönetici kaydından sonra VoIP kullanıcıları kayıt işlemlerine başlar. İlk olarak, her VoIP kullanıcısı kendi genel anahtarını kullanarak Yöneticiden bir bilet talep eder. Yönetici tarafından VoIP kullanıcıları için bilet ECDSA kullanılarak oluşturulur. Ardından Yönetici, talepte bulunan ilgili VoIP kullanıcısı için benzersiz bir kimlik (ID_u) oluşturur. Denklem (3.5) ile benzersiz bir kimlik (ID) tanımlamak için kullanılan yöntem gösterilmektedir.

$$ID_u = universally\ unique\ ID \tag{3.5}$$

Evrensel Tekil Tanımlama Numarası (UUID) kimlik numarası için kullandığımız 128 bitlik bir alfanümerik değer üretme yöntemidir. Genelde cihazın MAC adresine, IP adresine ve sistem tarihine göre bir değer üretir. Kullanılan bu yöntemde ID standart yöntemler üzerinden üretilir ise değerlerin yineleme olasılığı neredeyse imkansızdır. Bu yöntem üzerinden tezdeki çalışma her kullanıcı için farklı bir ID değeri üretir (Leach ve diğ, 2005). Merkezi bir yapıdan bağımsız olarak değer oluşturmaktadır.

Bilet üretimi için Yönetici, ilgili VoIP kullanıcısının genel anahtarını ve kimliğini birleştirir. Ardından, SHA-256 algoritmasını kullanarak birleştirmeyi özetler (hash). P_{uk_u} ilgili VoIP kullanıcısının genel anahtarıdır ve A_{prk} Yönetici'nin özel anahtarıdır. Yönetici kendi özel anahtarı ile özet değerini imzalar, özet ECDSA algoritması kullanılarak imzalanır. Her bilet benzersizdir ve ilgili VoIP kullanıcısına özel üretilir. Denklem (3.6) ile Bilet üretmek için kullanılan kriptografik işlem sunulmuştur.

$$Bilet = Imza_{A_{prk}}\left(h(P_{uk_u} || ID_u)\right) \tag{3.6}$$

Bilet üretimi sonrası VoIP kullanıcısı Yönetici'den bileti ve kimliği alır ve blok zincirindeki akıllı sözleşmeye göndererek kayıt talebi için bir işlem başlatır. Akıllı sözleşme, VoIP kullanıcısının genel anahtarının ve kimliğinin daha önce kaydedilip kaydedilmediğini kontrol eder. Kayıtlı değilse, akıllı sözleşme, Yönetici genel anahtarı ile imzayı doğrular ve bileti kontrol eder. Ardından, bilet geçerliyse akıllı sözleşme VoIP kullanıcısını güvenilir listeye ekler. Ayrıca, ilgili VoIP kullanıcısına kayıt onayı hakkında bilgi vermek için bir yanıt mesajı gönderilir. Son olarak, VoIP kullanıcısı blok zincir ağına kaydedilir. Şekil (3.10) ile gösterilen algoritma, tezde sunulan kimlik doğrulama mekanizması için akıllı sözleşme ilişkilendirme kurallarını açıklamaktadır

ve akıllı sözleşmenin parametreler üzerinden kayıtlanma için kontrol işlemini sunmaktadır. Blok zincirdeki akıllı sözleşme yeni VoIP kullanıcı adresinin (genel anahtar) ve kimliğinin daha önce başka bir VoIP kullanıcısı tarafından kullanılmadığını veya kayıt olup kayıt olmadığını denetlemektedir. Son olarak kullanıcıları güvenilir listeye eklemek için VoIP kullanıcısının biletinin geçerliliğini kontrol eder.

Algoritma: Akıllı Sözleşme için İlişkilendirme (Association) Kuralları

Başla

if (BcAdmin.address = 0) ***then***

return Error ("Yönetici nesnesi başlatılmadı")

if (ObjIdExists (obj.id) = true) ***then***

return Error ("object id kullanılıyor")// Kimlik ataması daha önce zaten yapılmış

if ObjAddrExists (obj.address) ***then***

return Error ("object adresi kullanılıyor")//genel adres ataması zaten yapılmış

if (TicketVerify(obj.id, obj.ticket) = failed) ***then//*** bilet "*ticket"* olarak tanımlanmaktadır.

return Error ("Bilet geçersiz")

AddTrustedObject(obj) // Hata görüntülenmezse yeni kişi güvenilir kabul edilir

Bitir *// İlişkilendirme başarıyla tamamlandı*

Şekil 3.10: Akıllı Sözleşme ile İlişkilendirme Süreci.

VoIP kullanıcılar, işlemlerine güvenilir bir alanda depolanan gizli bir özel anahtar ile erişirler. Anahtarın blok zincir dahil başka bir yerde bir kopyası yoktur. Bir VoIP kullanıcısı anahtarını kaybederse blok zincir ağında depoladıkları veya kaydettikleri her şeye erişimi kaybederler. Bu durumda ilgili VoIP kullanıcısı için kayıtlanmanın tekrarlanması gerekmektedir.

Aşama 4: Kimlik Doğrulama

Bir VoIP çağrısındaki taraflar arasında merkezi olmayan uçtan uca kimlik doğrulamasını güvenli bir şekilde sağlamak için bazı işlemler gerçekleştirilir. Bu tez çalışmasında iki tür kimlik doğrulama sağlanmaktadır. Bunlar sırasıyla tek VoIP kullanıcısı için gerçekleştirilen kimlik doğrulaması ve karşılıklı kimlik doğrulamasıdır.

Tek VoIP kullanıcısı kimlik doğrulama yöntemi, sesli mesajları (voicemail messages) okumak için blok zincir platformu aracılığıyla tek taraflı bir kimlik doğrulamadır. VoIP kullanıcısı sesli mesaj aldığında mesajı okumadan önce blok zincir tabanlı akıllı sözleşme, sesli mesaj sahibinin kimliğini doğrular. Bu kimlik doğrulama türünde, VoIP kullanıcısı genel anahtarını (P_{uk_u}) ve ID_u olarak belirtilen kimliğini imzalar ve blok zincirine gönderir. Ardından akıllı sözleşme imzayı doğruladıktan sonra, güvenilenler listesindeki VoIP kullanıcı kimliğini ve genel anahtarı kontrol eder. Sonuç olarak, T güvenilir liste olarak kabul edilir ve kimlik doğrulama (Authentication) işleminin sonucu için Denklem (3.7) ile gösterilen yöntemle karar verilmektedir. Akıllı sözleşme, kimlik doğrulama sonucuna göre VoIP kullanıcısına yanıt vermektedir. Akıllı sözleşme tarafından gönderilen cevap mesajı kabul veya kabul etmeme (ret) şeklinde olabilmektedir.

$$Auth\left(P_{uk_u}, ID_u\right) = \begin{cases} 1, & Eğer\ P_{uk_u}\ ve\ ID_u \in T \\ 0, & Aksi\ durumda \end{cases} \quad \textbf{(3.7)}$$

İkinci kimlik doğrulama türü, karşılıklı kimlik doğrulamadır. Karşılıklı kimlik doğrulama veya iki yönlü kimlik doğrulama, bir bağlantının her iki tarafı da birbirinin kimliğini doğruladığında gerçekleşir. Güvenli bir VoIP çağrısı oluşturmak için arayan ve arananın kimlik bilgileri, blok zincirinde doğrulanmalıdır. İlk olarak, arayan taraf, kendi özel anahtarını kullanarak kendi kimliğini ve aranan tarafın kimliğini ECDSA ile imzalayarak bir işlem oluşturur ve bu işlem üzerinden blok zincirine bir kimlik doğrulama isteği gönderir. Akıllı sözleşme, gönderilen kimlik bilgilerini ve ilgili genel anahtarlarını güvenilir listede kontrol eder. Görüşme yapmak isteyen taraflar blok zincirinde kayıtlı ise, karşılıklı kimlik doğrulama sağlanır.

Çağrı sürecinin başında, arayan, arananın genel anahtarını bilmez. VoIP kullanıcılarının tüm açık anahtarları, sağlam ve değişmez bir depolama ortamı olan blok zincirinde saklanır. Böylece merkezi olmayan blok zincir üzerinden güvenli anahtar dağıtımı sağlanır. Kimlik doğrulamadan sonra, blok zincir onay doğrulama isteği için bir yanıt mesajı oluşturur ve mesaj ile birlikte aranan kişinin ortak anahtarını arayan kişiye sunar. Böylece kimlik doğrulama için genel anahtar dağıtımı güvenli şekilde gerçekleşir.

Şekil (3.11) ile gösterilen algoritma, önerilen kimlik doğrulama için akıllı sözleşme üzerinden güvenli iletişim kurallarını açıklamaktadır. Bu algoritma, taraflar arasındaki güvenli haberleşme kanalının kurulumu öncesinde blok zincirdeki akıllı sözleşme kontrol sürecini ifade etmektedir. Akıllı sözleşme kontrol için güvenilir listeden aranan ve arayan kişinin kimlik bilgisini ve ilgili genel anahtarlarını kontrol eder.

Algoritma: Akıllı Sözleşme Güvenli İletişim Kuralları

Başla

if (ObjAddrExists (caller.address) = True AND ObjIdExists (caller.id) = True AND (ObjIdExists (callee.id) = True) ***then***
sendMSG(caller, callee, msg)

else

return Error ("Mesaj Gönderme Hatası")

if (ObjAddrExists (callee.address) = True AND ObjIdExists (callee.id) = True) then
readMSG(callee)

else

return Error ("Mesaj Okuma Hatası")

Bitir

Şekil 3.11: Akıllı Sözleşme İçin İletişim Kuralları.

3.3.2. Önerilen Yöntemin Hata Toleransı

Merkezi yani tek sunuculu mimariden farklı olarak, veriler blok zincir ağında bir blok içinde depolanır. Blok zincir dağıtık bir veri tabanıdır, yani merkezi bir işlemcide depolama yapmaz. Bunun yerine, işlemleri gerçekleştirmek ve doğrulamak için kullanılan her bilgisayarda (düğüm) bir kopyası vardır. Bir işlem eklendiğinde, tüm kopyalar aynı anda değişir. Zincirdeki her bloğun bir zaman damgası vardır, böylece ağdaki herkes ilgili işlemin ne zaman eklendiğini görebilir. Ayrıca, bloğu belirli bir uzunlukta bit dizisine çevirerek şifreleyen "özet" adı verilen kriptografik imza içerir. Ancak günümüzde bilgisayarlar saniyeler içerisinde yüz binlerce özetleme (hashing) işlemini hesaplayabilir. Bu nedenle, herhangi bir saldırgan bir bloğu kurcalayabilir veya diğer blokların tüm özetleme işlemini yeniden hesaplayabilir. Blok zincir ağı, konsensüs algoritmalarını kullanarak bloğun kurcalanmasını veya yeniden hesaplanma ihtimalini oldukça azaltır. Çünkü konsensüs algoritması, bir grup bilgisayarın neyin en doğru olduğu konusunda aralarında anlaşmak için kullandığı bir stratejidir. Kullanılan

algoritmalar açısından anlaşmanın ne kadar güvenli olduğu ve kimin neye oy vereceği açısından her birinin farklı özellikleri olan farklı türde konsensüs algoritmaları bulunmaktadır. Ancak genel olarak, konsensüs algoritmasının amacı, ağdaki katılımcılardan belirli bir kısmının tüm katılımcıların takip ettiği ve üzerinde anlaştığı işlemin gerçekliğini belirlemesini yönetmektir. Böylece verilerin depolandığı blok güvenliği sağlanmış olur. Ethereum blok zincir madenci düğümleri arasında fikir birliği sağlamak için PoS konsensüs algoritmasını tercih etmektedir. PoS algoritması, ağı daha dağıtık (merkezi olmayan) ve güvenli hale getiren düğümler kurar. Konsensüs yani fikir birliği süreci, tek bir veri değeri için düğümler arasında bir anlaşmaya ihtiyaç duyar. Bu düğümlerden bazıları başarısız olabilir veya başka şekillerde güvenilmez olabilir, bu nedenle konsensüs protokolleri hataya dayanıklı olmalıdır. Fikir birliği sürecinde her aracı düğüm bir şekilde aday değerlerini ortaya koymalı, eşler arası iletişim kurulmalı ve tek bir fikir birliği değeri üzerinde anlaşmaya varılmalıdır. Bu sürece göre, önerilen şemanın güvenliği, güvenilirliğini ve ölçeklenebilirliğini anlamak için hata toleransı hesaplanmalıdır. Sunulan tezde, toplam düğüm (n) ve hata düğümleri (f) arasında ilişki blok zincir ağının güvenilirliği için belirli bir değer aralığında olmalıdır. Denklem (3.8) ile Hata Toleransı hesaplaması yapılmıştır.

$$f \leq \frac{n-1}{2} \tag{3.8}$$

Blok zincir ağında kullanılan PoS konsensüs algoritmasında, bloğa veri eklenmesi için ağın çoğunluğu tarafından onaylanması gerekir. Verileri bozmak veya manipüle etmek isteyen kötü niyetli kişiler, ağın çoğuna sahip olmalıdır. Bu nedenle kimlik hırsızlığı (sybil) saldırı türünde %51 saldırısı gibi yöntemler teorik olarak neredeyse imkansızdır. Saldırı toleransını ele alırsak PoW algoritmasında CPU hesaplama gücü olarak veya PoS algoritmasında hisse (stake) olarak toplam düğümdeki dürüst düğüm oranı %50'den büyük olmak zorundadır. Denklem (3.8) ile belirtilen konsensüs algoritmasının hata toleransı, sunulan tezdeki mekanizmanın manipülasyona karşı güvenli olduğunu göstermektedir. Ek olarak, PoW ve PoS tipik olarak önce doğrulanmış bloğu zincire kaydeder ve ardından tüm düğümlerin fikir birliğini arar. Bir başka konsensüs algoritması olan PBFT ise önce bloğa onay verir ve ardından doğrulanmış bloğu zincire kaydeder. Ancak PBFT algoritmasının hata toleransı yüksek olmasına karşın zaman karmaşıklığı (time comlexity) oldukça yüksektir. Bu durum ses verisi gibi hızlı veri iletimi ihtiyacı duyan uygulamalarda uygun değildir.

4. ÖNERİLEN KİMLİK DOĞRULAMA MEKANİZMASININ GÜVENLİK ANALİZİ

Bu bölümde, tezde sunulan kimlik doğrulama mekanizması güvenlik unsurları açısından ele alınmaktadır. Tezde sunulan çalışmanın farklı saldırılara karşı güvenlik unsurları üzerinden sağlamlığı incelenecek ve güvenilirlik açısından analiz edilecektir. Saldırı türlerine karşı dayanıklılığı detaylı olarak açıklandıktan sonra önerilen modelin güvenli olduğu AVISPA aracıyla kanıtlanacaktır.

4.1. Güvenlik Analizi

VoIP ağında IP telefonlar sistem içerisindeki zafiyet noktalarıdır çünkü IP telefon üzerinden gerçekleştirilen VoIP aramaları ve sesli posta mesajları, internet ortamındaki saldırılara açık verilerdir. VoIP iletişim kanalındaki güvenlik analizi için güvenilirlik, erişilebilirlik, gizlilik, bütünlük, sürdürülebilirlik, kimlik doğrulama, inkâr edememe, kimlik teşhisi ve ölçeklenebilirlik unsurları incelenerek tezde sunulan çalışmanın güvenilir bir ortam sağladığı detaylı olarak anlatılmaktadır. Ayrıca, önerilen yöntemin IP ağındaki görüşme esnasında olası kimlik hırsızlığı (sybil), sahtecilik (spoofing), ikame (substitution), ortadaki adam (man-in-the-middle), tekrarlama (replay) ve dağıtık hizmet aksatma (DDoS) saldırılarına karşı güvenliği analiz edilerek güçlü yönleri ortaya konmaktadır.

4.1.1. Güvenilirlik

Bir VoIP iletişim ağından beklenen güvenilir yapı belirli bir zaman aralığında, belirli koşullar altında hatasız olarak performans göstermesidir. Tezde sunulan mekanizma, veri iletimi sırasında veri bütünlüğünü korur. Yönetici ilk kayıtlanma esnasında genel anahtarından ürettiği benzersiz kimlik bilgisine genel anahtar ve zaman damgasını birleştirerek kendi özel anahtarı ile imzalanmış halini ekler. İlgili mesajı ECDSA yöntemi ile imzalayarak blok zincire gönderir. Bu yöntemle Yönetici ile akıllı sözleşme arasında güvenli bir haberleşme sağlanır. Güvenliği sağlanmış Yönetici bilet

ve ID üretimi yaparak istekte bulunan ilgili VoIP kullanıcılarına iletir. Bu şekilde sistem içerisinde güvenli bir yapı oluşturulur. Ayrıca yöntem VoIP kullanıcıları için blok zincir ağı içerisinde güvenilir depolama sağlar. Blok zincir ağında sağlanan bütünlük, inkâr edememe ve güvenilir depolama unsurları sayesinde veri üzerinde saldırgan tarafından yapılan değişiklik tespit edilir. Blok zincirinde kriptografik yöntemlerle dağıtık kayıt defteri özelliğinin bir arada kullanılması üçüncü tarafları ortadan kaldırarak iletişim ortamındaki güvenilirlik unsurunu daha güçlü hale getirmektedir (Zhang ve Lee, 2020). Son olarak, blok zincirde akıllı sözleşmeler bir kez çalıştığında en başta belirlenen kurallar değiştirilemez ve belirlendiği şekilde yürütülür. Saldırganlar tarafından müdahale edilemez.

4.1.2. Erişilebilirlik

Güvenilirlik, sistemin önemli bir ölçüsüydü. Ancak erişilebilirlik, bir şeyin ne kadar güvenilir olabileceğinin ötesine geçer ve bir sistemin veya hizmetin gerektiğinde işlevini yerine getirmeye hazır olduğunun bir ölçüsüdür. Bir platformun veya sistemin istendiğinde çalıştırılabileceği süre olan erişilebilirlik unsuru dağıtık bir veri yapısına ve eşler arası bir iletişim ağına dayanan blok zincir teknolojisiyle sağlanmaktadır (Carrara ve diğ, 2020). Bir blok zincir ağdaki her bir düğüm için tüm geçmiş ve güncel işlemlerin yedeğini alarak kayıtlı üyelere şeffaf şekilde veri erişilebilirlik unsuru sağlar. Ayrıca akıllı sözleşmeler sayesinde her an erişim sağlanan kayıtlı veriler için merkezi olmayan ve otonom bir çalışma mekanizması sunulmuştur. İlgili VoIP kullanıcıları internet bağlantısı olan her noktadan talep edilen her an kimlik doğrulama yaparak güvenli VoIP görüşmesi gerçekleştirebilirler.

4.1.3. Gizlilik

Gizlilik; VoIP uygulamalarında cihazlara ve iletişim esnasında aktarılan ses verisi içeriğine yetkisiz erişimin engellenmesiyle sağlanır. Tezdeki çalışmada, her VoIP kullanıcı ECC tabanlı genel/özel anahtar çiftini üretir. VoIP ağı içerisinde talepte bulunan her kullanıcı için Yönetici tarafından imzalı bir sertifika (bilet) üretilir. Ayrıca VoIP ağında medya veri aktarımının hemen öncesinde kimliği doğrulanmış taraflar arasında güvenli anahtar dağıtımı gerçekleştirilmiş ve gizli ortak bir anahtar oluşturulmuştur. Taraflar arasında kimlik doğrulama sonrası ve görüşme öncesinde ECDH algoritması ile anahtar değişimi gerçekleştirilmiştir. Anahtar değişimi ile

sağlanan ana (master) anahtar elde edilmiştir. Böylece SRTP protokolü AES simetrik şifreleme için anahtar oluşumu gerçekleştirebilmektedir.

Diğer taraftan, blok zincirinde depolanan tüm VoIP kullanıcı bilgileri şifrelenir veya anlaşılmayacak şekilde tutularak gizlenir. Bu açıdan kullandığımız tüm kriptografik algoritmalar güvenliyse, veri gizliliği iyi korunacaktır. Sunulan tezde anahtar dağıtımı için tek nokta hatası ve mahremiyet konularında yetersiz bir çözüm olan PKI kullanımına gerek kalmaz. Yapılan işlemler şeffaftır ancak anonim bir şekilde gerçekleşir. Ağdaki işlemler herkes tarafından görülür ancak işlemi kimin yaptığı sadece taraflar arasında bilinir. Ağda işlemi kimin yaptığına dair bilgi paylaşılmaz. Blok zincirdeki güvenilir listede depolanan genel anahtarlar bir kere ağda yayınlanıp madenciler tarafından doğrulandığında bir daha değiştirilemez. Ayrıca tüm genel anahtarlar isimsiz depolanarak mahremiyet ve gizlilik sağlanır.

4.1.4. Bütünlük

Veri aktarımı sırasında bütünlük unsuru için blok zincir platformunda özetleme fonksiyonları ve dijital imzalar kullanılmaktadır. Blok zincir işlemleri güvenli dijital imzayı (örneğin, Bitcoin ve Ethereum'da ECDSA) kullanır (Zhang ve Lee, 2020). Dolayısıyla işlem iletimi sırasında bütünlük garanti edilir. Sunulan yöntemde kayıt için önce Yönetici tarafından bilet oluşturma süreci gerçekleşir. Ardından Yönetici özel anahtarı ile imzaladığı bileti ECDSA algoritması kullanarak iletir. Kayıtlanma işleminde ilgili VoIP kullanıcısı bu mesajın kendisine ait olduğunu ispatlar. VoIP çağrısı öncesi anahtar dağıtımı için sertifika otoritesi gibi üçüncü taraflara ihtiyaç yoktur ve blok zincir genel anahtar dağıtımını güvenli şekilde gerçekleştirdiği için dijital imza güvenli şekilde gerçekleşir ve mesaj bütünlüğü korunur.

Ayrıca blok zincir ağında bağlı liste veri yapısıyla özetlenmiş işlemler bloklar aracılığıyla birbirine bağlanır. Merkle ağacı yöntemi ile verileri doğrulamanın basit bir matematiksel yolu sağlanmaktadır. Merkle ağacı eşler arası bir ağdaki eşler arasında geçen veri bloklarının eksiksiz, hasarsız ve değiştirilmemiş olduğundan emin olmak için Merkle Kökü kullanır. Blok zincirindeki her bloğun benzersiz bir özet numarası ve önceki bloğun veya ana bloğun özet numarası vardır. Böylece bir verideki değişiklik bütün verileri etkiler ve saldırgan tespit edilir. Bu açıdan özetleme fonksiyonları sayesinde internet benzeri güvensiz kanaldan gönderilen bilgilerin bütünlüğü sağlanmış olur.

4.1.5. Sürdürülebilirlik

Sürdürülebilirlik VoIP ağındaki meşru kullanıcıların (legitimate user) VoIP sistemine kolaylıkla erişebilmesi anlamına gelmektedir. DDoS benzeri saldırılara karşı dağıtık bir mimari kullanarak yapının sürdürülebilirliği sağlanmıştır. Ayrıca dağıtık mimari kullanımı sayesinde tek nokta hatası ortadan kalkmaktadır.

Bu tez çalışmasında sunulan yöntem izlenebilirlik, güvenilirlik, senkronize işlem süreci ve maliyet verimliliği unsurlarını bünyesinde barındırmaktadır (Saberi ve diğ, 2019; Park ve Li, 2021). Böylece önerilen güvenli VoIP iletişim sistemiyle taraflar arasındaki çağrı süreci PSTN benzeri geleneksel telefon şebekelerine göre daha sürdürülebilir ve uygun bir alternatif haline dönüşmektedir.

4.1.6. Kimlik Doğrulama

Kimlik (ID) ve Bilet (Ticket) parametreleri VoIP kullanıcıları tarafından kayıtlanma esnasında blok zincire gönderilir ve akıllı sözleşme tarafından doğrulanma sonrası benzersiz olduğu tespit edilirse blok zincir ağında güvenilir listede depolanır. Ardından kimlik doğrulama esnasında kayıtlı bilgiler ilgili VoIP kullanıcısı için blok zincir ağında doğrulanır. Bu durumda blok zincir ağının güvenliği kritiktir. Çünkü bütün yapı blok zincir ağının depoladığı bilgi için kırılmaz bir veri saklama alanı sağlayacağı kabul edilerek geliştirilmiştir. Blok zincir ağındaki zincirin sağlamlığı test edilerek verilerin değiştirilemez şekilde ağa kayıtlandığının ispatı için blok zincir ağındaki orijinal zincire alternatif zincir sağlayarak ele geçirmek isteyen bir saldırgan olduğunu varsayalım. Saldırgan orijinal zincire alternatif zincir oluştursa bile bu durum ağdaki verilerin değiştirilmesi için yeterli değildir. Çünkü düğümler geçersiz bir işlemi onaylamaz ve meşru düğümler geçersiz işlemleri içeren blokları reddeder. Saldırgan blok zincir ağında doğrulandıktan sonra kayıtlanmış veriler için oluşturulan bir işlemi değiştirmek isteyebilir. Orijinal zincir ile saldırganın oluşturmak istediği alternatif zincir arasındaki rekabeti *Rastgele Binom Yürüyüşü* modeli ile ele alalım. İlgili modelde, başarılı olma durumu orijinal zincirin bir blok uzamasıdır ve böylece bir birim öne geçtiğini kabul edilmektedir. Başarısız olma durumu ise saldırganın alternatif zincirinin bir blok uzamasıdır ve aradaki farkı bir birim azaltır. Saldırganın alternatif zinciri oluşturma ihtimalini *Kumarbazın İflası* problemine benzeterek sınırsız hakkı olduğunu kabul edelim (Nakamoto, 2008). Bu durumda sonsuz sayıda deneme yaparak orijinal zinciri yakalama olasılığını aşağıdaki şekilde hesaplanır:

p = meşru düğümün sıradaki bloğu bulma olasılığı

q = saldırganın sıradaki bloğu bulma olasılığı

q_z = saldırganın z blok geriden gelerek orijinal düğümü yakalama olasılığı olsun. Bu durumda "$\boldsymbol{q_z}$" ifadesi Denklem (4.1) ile belirtilen şekilde sunulmuştur.

$$q_z = \begin{cases} 1 & ,p \leq q \\ (q/p)^z & ,p > q \end{cases} \quad \textbf{(4.1)}$$

$p > q$ ihtimalinde blok sayısı arttıkça saldırganın orijinal düğümü yakalama olasılığı üssel olarak azalır.

Taraflar arasında IP ağı üzerinden gerçekleştirilen bir arama işleminde saldırgan blok zincire ağındaki kayıtlı veriler üzerinde değişiklik yapmak isteyebilir. Aranan taraf yeni bir çift anahtar üreterek genel anahtarını imzalamaz ve arayan tarafa iletir. Alternatif zincir oluşumu bu yolla engellenir. İşlem gönderiminde saldırgan işlemin içeriğini değiştirerek alternatif zincir üretebilir. Taraflardan aranan işlemin bir bloğa eklenmesini ve bloğa *z blok* daha bağlanmasını bekler. Meşru bloklar blok zincir platformunda ortalama bir süreye sahiptir ve o süre içerisinde üretildiği için saldırganın potansiyel ilerleme miktarı beklenen değere göre *Poisson dağılımının* matematiksel modeli Denklem (4.2) ile gösterilmiştir.

$$\lambda = z\frac{q}{p} \quad \textbf{(4.2)}$$

Denklem (4.3) ile saldırganın orijinal zincire alternatif üretme ihtimali hesaplanır. İlerleme oranı, Poisson yoğunluğunun bu noktadan itibaren yakalama olasılığı ile çarparak hesaplanır.

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} f(x) = \begin{cases} (q/p)^{(z-k)}, & k \leq z \\ 1, & k > z \end{cases} \quad \textbf{(4.3)}$$

Sonsuz dağılım kuyruğunun toplam değerini alarak yeniden matematiksel olarak formüle edersek Denklem (4.3) Denklem (4.4) haline dönüşür (Nakamoto, 2008).

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} (1 - ((q/p)^{(z-k)}) \quad \textbf{(4.4)}$$

Bu formüllerin sözde kodu Şekil (4.1)'deki algoritma ile açıklanmaktadır.

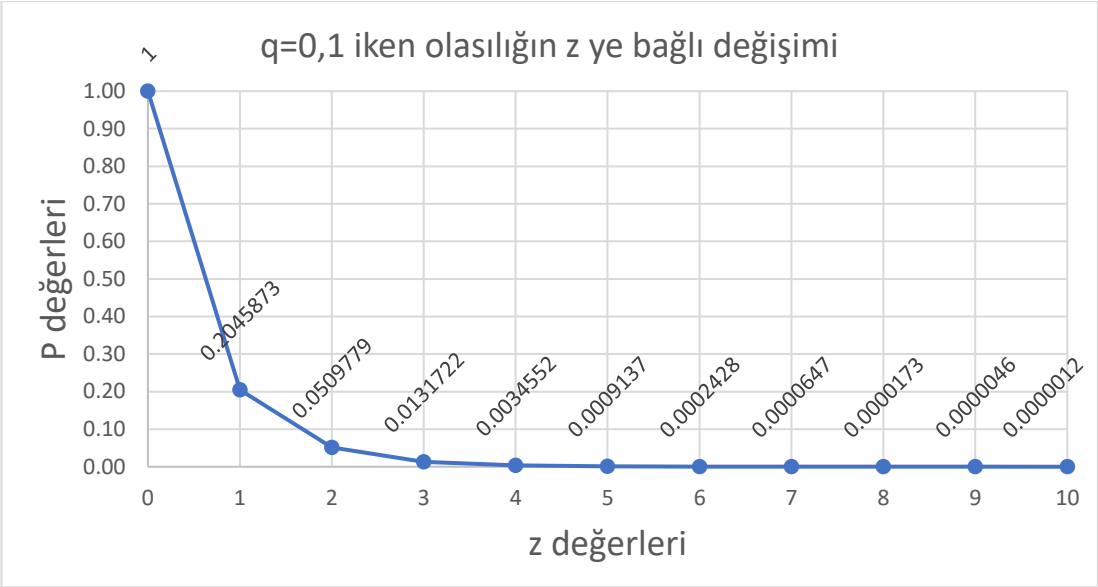
Algoritma: Blok Zincir Ağının Saldırgana Karşı Başarı Olasılığı

```
//Değişkenleri tanımlama
Değişkenler:
double p // meşru düğümün sıradaki bloğu bulma olasılığının değişkeni
double q // saldırganın sıradaki bloğu bulma olasılığı değişkeni
double z // bloğa z blok daha bağlanması durumunu ifade eden değişken
double lambda // Poisson dağılımı ifadesi değişkeni
double toplam // Sonuç değeri değişkeni
int i,k // Döngü değişkenleri
double poisson // Poisson değişkeni

Fonksiyon: double SaldirganBasariOlasiligi(double q, int z)

Başla
    p = 1.0 - q;
    lambda = z * (q / p);
    toplam = 1.0;
    for k in 0 to z
        do poisson = exp(-lambda);
        for i in 1 to k
            poisson =  poisson * (lambda / i);
            toplam = toplam – ( poisson * (1 - pow(q / p, z - k)));
        endfor
    endfor
    return toplam;
Bitir
```

Şekil 4.1: Blok Zincir Ağının Saldırgana Karşı Başarı Olasılığı.

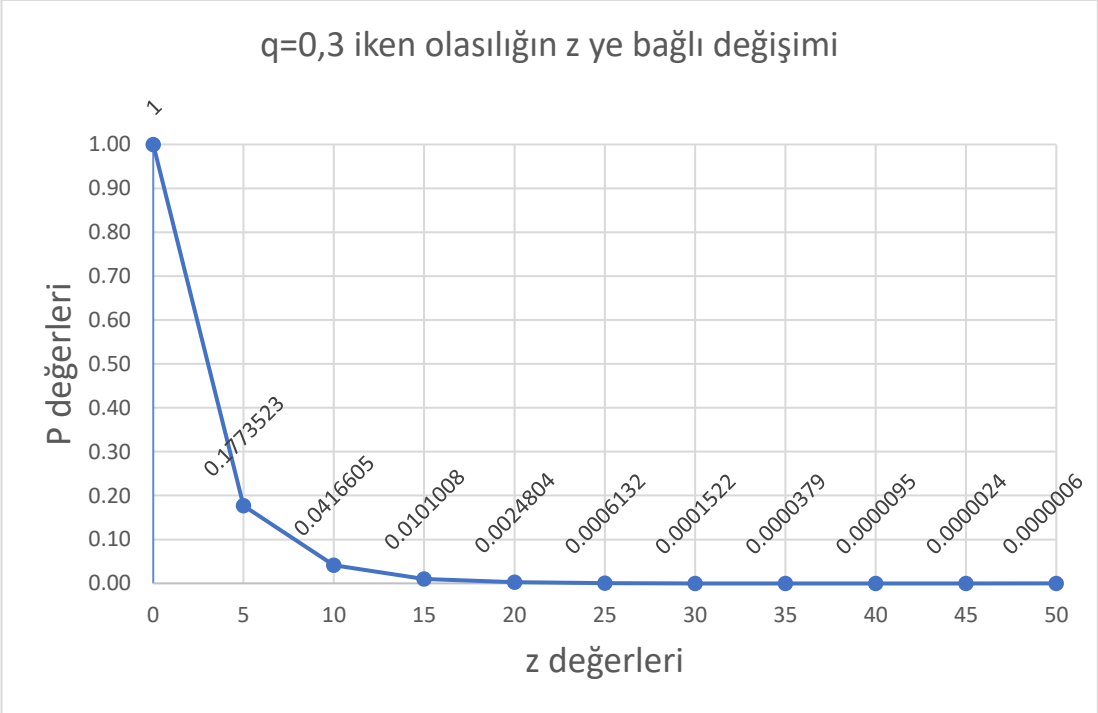
Nakamoto (2008)'den uyarlanmıştır.

Blok zincir ağının saldırgana karşı başarı olasılığı için oluşturulan algoritmada gösterilen kod parçası çalıştırılarak Şekil (4.2) ve Şekil (4.3) elde edilmiştir. Bu iki şekil, saldırganın sıradaki bloğu bulma olasılığı yani "**q**" değerine farklı sayısal değerler verilerek çeşitli denemeler yapılması sonucu elde edilen grafiği göstermektedir.



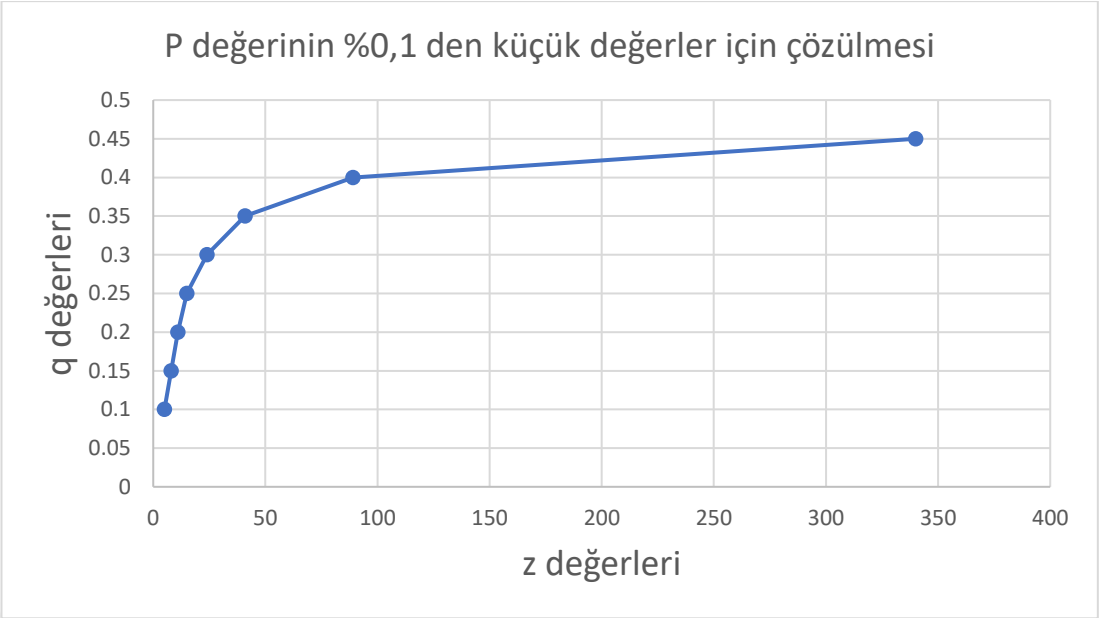
Şekil 4.2: q=0,1 iken Blok Zincir Ağının Saldırı Stresi Altında Kırılma Durumu.

Bu denemelerin sonucunda olasılığın "**z**" değerine bağlı olarak üstel artış göstererek azaldığı görülmüştür.



Şekil 4.3: q=0,3 iken Blok Zincir Ağının Saldırı Stresi Altında Kırılma Durumu.

P değeri %0,1 den daha küçük sayılar ile ele alındığında ise Şekil (4.4)'deki grafik elde edilmektedir.



Şekil 4.4: P < 0,001 iken Çözdüğümüzde Elde Edilen Sonuç Grafiği.

Sonuçlar göstermektedir ki blok zincir ağında işlemler kalıcı ve değiştirilemez şekilde depolanır. Blok zincir ağı saldırganlara karşı ilişkilendirilmiş zincir modeliyle güçlü şekilde direnç sağlar ve böylece üçüncü taraflara ihtiyaç duymadan otonom ve dağıtık şekilde kimlik doğrulama gerçekleştirir. Ayrıca dağıtık defterlere kayıt olan işlemler şeffaftır. Her blok kendisinden önceki blok ile bağlantılı şekilde zincir oluşturulur. Blok zincir ağında geçersiz bir işlem (transaction) kabul edilmez ve blok zincire eklenemez.

4.1.7. İnkâr Edememe

Blok zincir, verilerin bütünlüğünü ve reddedilmemesini sağlayan dağıtık bir depolama sistemidir (Axin ve diğ, 2019). Blok zincirde depolanan veriler üzerinde değişiklik yapılamaz. Blok zincirindeki işlemler, tüm blok zincir madencileri tarafından şeffaf olarak izlenebilir. Blok zincir ağında gerçekleşen bir işlem kayıt altına alınır ve değiştirilmesi oldukça zordur. Önerilen modelde uç nokta IP telefon ve blok zincir arasında güvenli anahtar değişimi üzerinden kullanılan dijital imza yöntemi sayesinde kullanıcılar yaptığı işlemi inkâr edemez. Ayrıca blok zincir ağında kayıtlanma aşamasında güvenilir liste kullanılmaktadır. Kontrol edilen her işlem blok zincir içerisinde VoIP kullanıcı bilgilerinin benzersiz olduğunun doğrulanmasıyla onaylanır ve gerçekleşen işlem blok zinciri ağında güvenilir listeye değiştirilemez şekilde kaydedilir. Bir defa blok oluşturulup işlem ağ içerisinde onaylandığında ve dağıtık defterlere (distributed ledger) yazıldığında artık defterler üzerinde değişiklik yapılsa

bile yüzde 50 artı 1 oranında düğüm sayısı tek kişi tarafından ele geçirilmediği sürece bu saldırı bir anlam ifade etmez. Yani gönderilen sesli mesaj veya yapılan VoIP çağrısı ağ içerisinde şeffaf bir şekilde yayınlanır ve hiçbir zaman inkâr edilemez.

4.1.8. Kimlik Teşhisi

Her VoIP kullanıcısı benzersiz bir ID değeri ile sisteme kayıtlanır. VoIP kullanıcı ID değeri, blok zincire iletilmeden önce ilgili bilet ile birleştirilir ve imzalanır. Oluşturulan imzalı işlem kayıtlanma için blok zincire gönderilir. Kayıtlanma mesajı için güvensiz kanaldan iletim bu şekilde gerçekleşir. Akıllı sözleşmeler bilet onayı sonrası blok zincir ağında VoIP kullanıcısının ID değerini kontrol eder. ID daha önce kayıtlanmadıysa ve benzersizse gönderilen ID değeri ilgili VoIP kullanıcısının genel anahtar ile birlikte sisteme kayıtlanır. Tezde sunulan yöntemde güvenli bir VoIP çağrısı oluşturmak için arayan ve arananın kimlik bilgileri, blok zincirinde doğrulanmalıdır. Kimlik doğrulama fazında VoIP kullanıcısı akıllı sözleşme tarafından güvenilir listedeki kayıtlı ID değeri üzerinden kolayca doğrulanır.

4.1.9. Ölçeklenebilirlik

Ölçeklenebilirlik, bir sistemin kullanıcılarının aynı anda bir işlemi yapmak istemeleri durumunda bu isteklerini gerçekleştirebilmesidir. Yüksek işlem hacmi ve gelecekteki büyümeyi destekleme yeteneğini ifade eder. Ölçeklenebilir bir ağ tasarlanırsa kullanıcılar, bilgisayar (düğüm) sayısı veya veri miktarından etkilenmez. Ağ performansı düşmez. Tezde sunulan çalışmada, VoIP iletişim ağı eşler arası (P2P) bir ağ olan özel blok zincir ile entegre edilmektedir. Merkezi sisteme göre eşler arası ağlar, ölçeklenebilirliği karşılamak için daha etkin bir çözümdür (Hammi ve diğ, 2018).

Ölçeklenebilirlik sorunu verim (throughput), depolama (storage) ve ağ (network) oluşturma özelliklerinin birleşimidir (Xie ve diğ, 2019). Verim olarak blok zincir platformunun verimi, her bloktaki işlem sayısı ve blok aralığı süresi ile ilgilidir. Ethereum blok zincir ağında blok işleme ve doğrulama süresi ortalama 12 saniye civarındadır ve Bitcoin için bu süre yaklaşık 10 dakikadır. Ancak tezdeki çalışmada blok işleme ve doğrulama süresi ortalama 1422 milisaniye (ms) olarak hesaplanmıştır. Bu süre oldukça düşük bir zaman aralığında gerçekleşir ve gerçek zamanlı iletişim altyapısı için uygundur. Ayrıca, blok zincir disk alanından tasarruf eder. Depolama alanı işlemleri özet fonksiyonlarını kullanan Merkle ağacı yapısında saklar. Bir blok başlığı ortalama 80 bayt uzunluğundadır (Nakamoto, 2008). Bitcoin her 10 dakikada

bir blok üretir ve bu bloklar hafıza içerisinde yaklaşık olarak senede 4.2 MB (8*6*24*365) yer kaplar. Bu oran depolama alanları için önemsenmeyecek kadar küçük bir değerdir. Blok zincir dağıtık bir sistemdir ve eşler arası ağlarda ağa yük binmesi açısından bir sorun oluşmaz. Ancak birden çok eşin aynı anda işlem talep etmesi ağa yük bindirir ve tezde sunulan kimlik doğrulama mekanizmasında ağı etkilemeyecek kadar olsa da az miktarda bir yük oluşturur. Blok zincir ağında her işlem tüm düğümlere iki kez iletilir. Bu durum hem ağ kaynaklarını tüketir hem de oluşturulan blok için yayılım gecikmesine sebep olabilir. Ancak tezde sunulan mekanizma bu durumun önüne geçecek şekilde tasarlanmış ve deneylerle ispatı sağlanmıştır.

4.1.10. Kimlik Hırsızlığı Saldırısı

Saldırgan tarafından sayısız sahte kimlik oluşturan kimlik hırsızlığı saldırısı geleneksel yöntemlerde güvenilir bir otorite tarafından verilen doğrulanmış kimlikler ile çözülmektedir. Başarılı kimlik hırsızlığı saldırısı, ağda etkileşimler başlatarak bazı düğümlerin itibarını arttırır veya bazılarının itibarını düşürür (Otte ve diğ, 2020). Böylece saldırgan ağı kontrol etme girişimini gerçekleştirebilir.

Tezde sunulan yöntemde, her VoIP kullanıcısının yalnızca bir kimliği (ID) olabilir ve her kimliğin belirli bir zamanda yalnızca bir anahtar çifti olabilir. Blok zincirinde her işlem, bu kimlikle ilişkili özel anahtar tarafından imzalanır. Ayrıca, tüm kimliklerin Yönetici tarafından dağıtıldıktan sonra VoIP kullanıcısı tarafından blok zincir ağına kayıtlanması ve akıllı sözleşme sistemi tarafından onaylanması gerekir, bu nedenle tezde sunulan yöntemde bir saldırgan sahte kimlik kullanamaz.

4.1.11. Sahtecilik Saldırısı

Saldırgan tarafından kimliğiniz taklit edilerek sisteminize kendisini tanıtan ve fayda elde etmek için ağa giriş yapan saldırı modeline sahtecilik saldırısı denir (Hammi ve diğ., 2018). VoIP çağrısı öncesinde karşılıklı kimlik doğrulama gerçekleştirilerek taraflar arasında bilgiler merkezi olmayan blok zincir ağında doğrulanır. Blok zincire kayıtlanmış her VoIP kullanıcısı meşru kabul edilir. Güvenilir listede değişmez şekilde depolanan VoIP kullanıcı bilgisi sahtecilik saldırını önlemektedir. Sahtecilik saldırısı sunulan kimlik doğrulama mekanizmasında ancak özel anahtar ele geçirilirse gerçekleşebilir. Kısaca saldırgan mesajı imzalayanın özel anahtarını elde edemediği sürece sunulan mekanizma sahtecilik saldırısına karşı dayanıklıdır. Diğer taraftan

kullanıcıların güvenli olarak çevrimdışı depoladığı ve güvensiz ağda iletmediği özel anahtarın saldırgan tarafından ele geçirilmesi oldukça zordur.

4.1.12. İkame Saldırısı

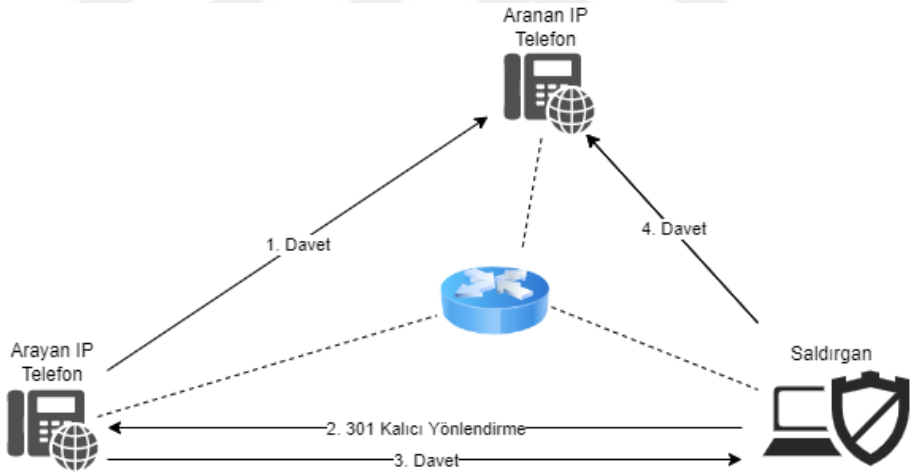
Saldırgan bu saldırı türünde, açık ağda gönderilen mesajları tespit eder ve yakalayabilir. Taraflar arasındaki ağı dinler ve iletilen mesajların içeriğini meşru kullanıcı tarafından gönderilmiş gibi değiştirir (Cui ve diğ., 2020). Tezde sunulan mekanizmada tüm işlemler dijital imzalı olduğundan, bir saldırgan bir mesajı değiştirirse, bunu geçerli bir özel anahtarla imzalaması gerekir. Ancak, başlatma aşamasında Yönetici tarafından yalnızca güvenilen VoIP kullanıcılarına Bilet sertifikası verilmiştir. Yönetici kayıtlanma esnasında ürettiği eliptik eğri anahtar çiftinin genel anahtarını kullanarak ID değeri üretmektedir. Ardından genel anahtarı ve zaman damgası değeri oluşturarak özel anahtarı ile bu değerleri imzalar. Daha sonra ID değeri ve imza değerini birleştirip tekrar imzalar. Bu şekilde blok zincirdeki akıllı sözleşme ilgili imzalanmış işlemi doğrular. Karşılıklı veri iletiminde zaman damgası ile desteklenen tezde sunulan çalışmada iletilen mesajın değiştirilip kullanılması engellenir. Özetle, Yönetici'nin güvenli şekilde kayıtlanması sonrası Yönetici tarafından güvenli kanaldan sağlanan Bilet ve ID üzerinden VoIP kullanıcıları blok zincire doğrudan kayıtlanma isteği gönderir. VoIP kullanıcıları VoIP ağında ve blok zincir ilişkilendirmesi esnasında mesaj iletimi sürecinde mesajlara ikame saldırısı olasılığı yoktur.

4.1.13. Ortadaki Adam Saldırısı

Ortadaki adam saldırısı, saldırganın araya girip tüm konuşmayı kontrol ettiği gizli bir dinleme türüdür. Saldırgan kimlik doğrulama sürecinde kimlik doğrulama mesajını engellemek isteyebilir, taraflar arasında VoIP çağrısı esnasında pasif dinleme yaparak verileri ele geçirebilir veya mesaj içeriğini değiştirebilir. Bu saldırı modelinde saldırganın hedef VoIP kullanıcısının kimliğini taklit etmesi gerekmektedir.

Tezde sunulan yöntem, MITM saldırılarını neredeyse imkansız hale getirdi. VoIP kullanıcıları blok zincir ağında bir işlem başlatarak blok zincirine açık anahtarlarla birlikte kayıtlandığında, kullanıcı bilgisi blok zincir ağındaki madenciler tarafından dağıtık deftere depolanarak bloğa eklenir. İlgili blok özetleme algoritmalarıyla önceki bloklara bağlanır. Böylece saldırgan tüm blokları değiştirmek zorunda kaldığı için geçerli bir blok işlemi sağlayamaz.

VoIP çağrısında SIP protokolü kullanılarak taraflar arasında bağlantı kurulur. Bu sebepten SIP mesajında çok sayıda gizli bilgi bulunmaktadır (SIP adresleri, bağlantı bilgileri vb.). Ancak bu bağlantı SIP sunucusuna kayıtlanma sonrası gerçekleşir. SIP kayıtlanması esnasında VoIP kullanıcı istek (request) mesajı içeriğinin değiştirilerek başkasının adına sahte kayıt oluşturulması olası bir MITM saldırısıdır. Bu saldırı esnasında 3XX yönlendirme mesajları (301 Kalıcı yönlendirme, 302 geçici taşıma vb.) kullanılarak tekrar yönlendirme yapılır. Saldırgan VoIP kullanıcısına 3xx cevabı gönderir ve SIP bileşenlerinden birinin yerine geçerek hedef veriyi elde eder. Davet isteği gönderen VoIP kullanıcı sahte 3xx mesajı aldığı zaman ses paketlerini saldırgan üzerinden göndermeye başlar. Şekil (4.5) olası kayıt bilgilerini değiştirme veya 3xx mesajlarını kullanarak aramayı saldırgan üzerine yönlendirme senaryosunu göstermektedir. Tezdeki çalışma, SIP sinyalleşme esnasında blok zincir üzerinden kimlik doğrulama gerçekleştirir. Böylece SIP kimlik doğrulamanın zayıflıklarından etkilenmez ve SIP kurulumu sonrası taraflar arasında doğrudan eşler arası blok zincir tabanlı kimlik doğrulama sağlar.



Şekil 4.5: Sinyalleşme Katmanında Ortadaki Adam Saldırı Senaryosu.

VoIP kullanıcıları genel anahtarlarını anonim isimlerle blok zincir ağında güvenilir listede depolar. Böylece VoIP çağrısı öncesinde anahtar dağıtımı akıllı sözleşmeler tarafından taraflar güvenli şekilde doğrulanarak sağlanır. Anahtar dağıtımı sonrası oturum anahtarını güvenli şekilde oluşturulur. Kimlik doğrulama sonrası anahtar değişim işlemi güvenli şekilde tamamlanır. Tezde sunulan çalışmada, VoIP iletişimi için taraflar arasında ortak gizli bir anahtar oluşturmak için Eliptik-Eğri Diffie–Hellman (ECDH) ve dijital imza için Eliptik Eğri Dijital İmza Algoritması (ECDSA)

algoritması kullanılır. Böylece taraflar arasında mesaj iletimi esnasında VoIP kullanıcıları taklit edilemez. Bu yöntem ortadaki adam saldırılarından telekulak (evasdropping) ve kimliğe bürünme (impersonation) saldırılarına karşı oldukça etkilidir.

4.1.14. Tekrarlama Saldırısı

Tekrarlama saldırısı veri iletiminin saldırgan tarafından kendi amaçları doğrultusunda tekrarlanması veya geciktirilmesidir (Kshetri, 2017). VoIP kullanıcısının kimlik bilgisi yani ID değeri blok zincirinde bir kez kayıt olabilir. Blok zincirinde kayıtlandıktan sonra işlem değiştirilemez. Çünkü blok zincir ağında her işlem bir zaman damgasına sahiptir ve konsensüs süreciyle geçerli hale gelmektedir. Zaman damgası kullanımı tekrarlama senaryolarını önlemek için güçlü bir yöntemdir ve saldırgan tarafından tekrarlanan mesaj için oluşturulan işlem blok zincir ağında konsensüs sağlanamadığından reddedilir.

4.1.15. Dağıtık Hizmet Aksatma Saldırısı

Dağıtık mimari üzerinden doğrudan eşler arası kimlik doğrulama merkezi bir sunucuya ihtiyacı ortadan kaldırmaktadır. Böylece kimlik doğrulama sistemindeki tek nokta hatası zafiyeti ortadan kaldırılır. Tezde sunulan çalışma anahtar dağıtımı için tek sunuculu merkezi mimari kullanmaz ve kimlik doğrulaması merkezi olmayan mimaride gerçekleştirilerek hizmet aksatma saldırılarına karşı etkili bir yöntem ortaya konulmaktadır. VoIP ağında tek noktadaki cihaza yapılacak olan DDoS bu tez çalışmasının kapsamında değildir ve sadece kimlik doğrulama mekanizmasına yapılacak olası DDoS saldırıları önlenebilecektir.

4.2. Resmi Güvenlik Doğrulaması

Resmi olmayan doğrulamaya ek olarak, önerilen yöntem AVISPA kullanılarak resmi olarak doğrulandı. AVISPA, güvenlik protokollerinin modellerini analiz etmeye yönelik bir uygulama paketidir. Analiz edilecek bu protokoller High Level Protocol Specification Language (HLPSL) ile yazılır (Von Oheimb, 2021). Önerilen algoritmanın güvenlik testi için AVISPA'nın OFMC uzantısı (backend) altındaki uygulaması seçilmiştir. Bunun nedeni, OFMC'nin saldırıları tespit etmenin yanı sıra protokollerin doğrulanmasında etkili olmasıdır.

AVISPA çıktısının sonucu için bazı ayrıntıların anlamları aşağıda sırasıyla açıklanmaktadır.

- *Özet* (Summary): Bu bölüm, önerilen şemanın güvenli olup olmadığını anlatır.
- *Ayrıntılar* (Details): Bu bölüm, önerilen şemanın hangi koşullar altında güvenli olarak sonuçlandığını, bir saldırı bulunduğunu veya sonucun neden sonuçsuz olduğunu anlatır.
- *Şema, Hedef ve Arka uç* (Scheme, Goal, and Backend): Bu bölümler sırasıyla şema adını, analizin amacını ve kullanılan arka ucu belirtir (Dhillon ve Kalra, 2019).

OFMC, tezde sunulan sistemin tekrarlama saldırısı ve ortadaki adam saldırısı benzeri hizmet esnasında veri değişikliği yapan saldırıları önleyip önlemediğini kontrol eder. Örneğin AVISPA üzerinden SAS kimlik doğrulama yöntemini kullanan ZRTP protokolünün siber saldırılara karşı zafiyet içerdiğini tespit eden çalışmalar bulunmaktadır (Gupta ve Shmatikov, 2007).

AVISPA aracı kullanılarak elde edilen sonuçlar, tez çalışmasında sunulan kimlik doğrulama mekanizmasının aktif ve pasif saldırılara karşı güvenli olduğunu göstermektedir. Şekil (4.6), önerilen şemanın güvenlik analizinin AVISPA çıktısını göstermektedir. Şekil üzerinde gösterilen sonuçlar, önerilen kimlik doğrulama mekanizmasının hem IP telefon cihazı ve blok zincir ağı arasındaki iletişimi hem de blok zincir ağı içerisindeki düğümler arasındaki iletişimin OFMC arka ucunda (back-end) güvenli olduğunu açıkça göstermektedir.

IP telefon cihazı ve blok zincir ağı arasındaki iletişim güvenliği

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/M2.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.01s
  visitedNodes: 2 nodes
  depth: 1 plies
```

Blok zincir ağında düğümler arasındaki iletişim güvenliği

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/BC_test.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.32s
  visitedNodes: 162 nodes
  depth: 9 plies
```

Şekil 4.6: Tezde Sunulan Kimlik Doğrulama Mekanizmasının OFMC Kullanılarak Yapılan Analiz Simülasyon Sonucu.

5. BLOK ZİNCİR TABANLI GÜVENLİ VoIP İLETİŞİMİ İÇİN TEST ORTAMININ KURULMASI ve TEST EDİLMESİ

Bu bölümde, tezde sunulan kimlik doğrulama mekanizmasının uygulaması açıklanacaktır. Deneysel kurulum anlatılacak ve deney sonuçları ile elde edilen performans ölçümlerinin değerlendirilmesi adım adım ele alınacaktır. Tezde sunulan modelin blok zincir tabanlı olması sebebiyle finansal boyutu incelenecektir. Uygulanan yöntemler ve elde edilen sonuçlar açısından, çalışmanın akademik literatüre katkısı karşılaştırmalar yapılarak gösterilecektir.

5.1. Uygulama

Önerilen blok zincir tabanlı merkezi olmayan kimlik doğrulama şemasının uygulaması bu bölümde açıklanacaktır. VoIP uygulamalarının üçüncü taraflara gerek duymadan doğrudan taraflar arasında gerçekleşen kimlik doğrulama mekanizmasının uygulanabilirliğini göstermek için bir Kavram Kanıtı (PoC) ele alınmış ve deneysel çalışmalarla desteklenmiştir. PoC, önerilen bir yöntemin gerçek hayatta uygulanabilirliğini kanıtlama durumudur. Sunulan mekanizmanın uygulanabilir olduğunu göstermek yani PoC süreci için tercih edilen teknoloji, Ethereum blok zinciridir (Wood, 2014). Deneysel sonuçlar ve performans, Bölüm 5.2'de ayrıntılı olarak gösterilmektedir.

Tezde sunulan kimlik doğrulama mekanizması, Ganache olarak adlandırılan özel bir platformda geliştirildi. Ganache, sanal hesaplar oluşturan sanal bir blok zincir uygulamasıdır ve gerçek hayat senaryosunu simüle eden bir Ethereum ortamı sağlar (Khalid ve diğ., 2020). Başka bir deyişle, bu uygulamanın amacı, blok zincir ağının gerçek ortamda VoIP uygulamaları ile erişilebilirliğini göstermektir. VoIP uygulamasındaki taraflar arasında (blok zincir ağı içerisinde bu kişiler anonimdir) işlemleri ve kuralları güvenli ve güvenilir şekilde otonom hale getiren akıllı sözleşme, Solidity programlama dili kullanılarak tasarlanmış ve geliştirilmiştir. Akıllı sözleşmeyi derlemek ve uygulamak için, derleyicisinin son sürümünü destekleyen Truffle üzerinden kodlama ile benzetimi yapılmıştır. Node.Js ise, javascript kodunu

bir web tarayıcısı dışında çalıştırabilen, iletişim sürecinde ve VoIP kullanıcıları arasında veri aktarımı yapabilen arka uç çalışma zamanı (back-end runtime) ortamı sağlamak için kullanılmıştır. Ek olarak, düğümlerin Uzaktan Yordam Çağrısı (RPC) aracılığıyla başka bir Ethereum düğümü ile etkileşime girmesine izin veren Web3 kütüphanesi kullanıldı. Diğer taraftan, RPC teknolojisi düğümler ve blok zincir arasındaki iletişimin gerçekleştirilmesi için tercih edildi. Bağımsız bir iletişim platformu ve veri formatı sağlamak için Jason API seçilmiştir. Node.js Express üzerinden, Node.js için web sunucu çatısı (sistemin arka kısmı, back-end) oluşturuldu. Böylece sistemin verimli ve etkin çalışması sağlandı.

5.2. Değerlendirme

Bu bölüm, tezde sunulan kimlik doğrulama mekanizması için deneysel kurulum ve deney sonuçlarıyla elde edilen performans ölçümlerini sunmaktadır. Değerlendirme kapsamında tezde sunulan mekanizmanın adımları olan bilet oluşturma, kayıtlanma ve kimlik doğrulama aşamaları sırasıyla değerlendirildi. Değerlendirme simüle edilmiş bir senaryoda deneysel olarak gerçekleştirildi. Tezde sunulan mekanizma, literatürdeki hem tek sunuculu merkezi mimari hem de VoIP ağında blok zincir kullanan farklı kimlik doğrulama çalışmaları ile ortalama zaman gecikmesi açısından karşılaştırıldı. Deneyler sonucunda ortalama zaman gecikmesinin, test bileşenlerinin Rastgele Erişim Belleği (RAM) boyutu ve test ortamının ağ hızı ile doğrudan ilgili olduğu tespit edilmiştir. Bu sebeple, gerçek hayat senaryolarında önerilen mekanizmanın halka açık blok zincirine uygunluğunu anlamak için uygun test ortamı sağlanmıştır. Deney, her durum için 100 farklı kez çalıştırılarak oluşturulan deney platformunda test edilmiştir.

5.2.1. Deneysel Kurulum

Deneyler, 3GB Bellek ve Intel(R) Core (TM)2 Duo CPU T6600 @2.20 GHz ile Windows 10 Pro 64-bit işletim sistemi üzerinde uygulandı. Tezde sunulan yöntem Ganache-GUI'de simüle ve test edildi. Ganache, sanal ETH hesapları oluşturmak için kullanılan bir Ethereum platformudur. Ganache platformu, geliştirme sırasında akıllı sözleşmeleri test etmek için kullanıldı. Ethereum geliştirme için özel bir blok zincir ortamı oluşturur ve böylece sözleşmeleri dağıtmak, uygulamalar geliştirmek ve testler yapmak için kullanılabilir (Ch ve diğ, 2020). Ayrıca Ganache, yerleşik bir blok gezgini ve gelişmiş madencilik kontrolleri gibi uygun araçlar sağlamaktadır. Truffle ise akıllı

sözleşmelerin test edilmesini sağlayan bir geliştirme platformudur. Ganache platformunda varsayılan hesap sayısı 10'dur. Öte yandan, oluşturulabilecek maksimum hesap sayısı 100'dür. Bu açıdan, ortalama süreleri ve gecikmeleri göstermek için birbirinden farklı 100 hesap oluşturuldu ve test ortamı uygulandı. Remix IDE, Ethereum benzeri blok zincir platformları için akıllı sözleşmelerin geliştirilmesine, dağıtılmasına ve yönetilmesine izin verir. Ayrıca, VoIP kullanıcıları arasındaki ve blok zincir platformundaki performans değerlendirme testlerinin sonuçlarını göstermek için Python dili kullanıldı. Tablo 5.1'de deneyde kullanılan araçların genel bir açıklaması yapılmaktadır.

Tablo 5.1: Deneyde Kullanılan Araçların Açıklaması.

Ganache-cli	Ethereum Emülatörü
1. Visual Studio-Solidity supports	Python'da VoIP kullanıcısı ve düğüm arabiriminin geliştirilmesi için IDE
2. Truffle	Akıllı sözleşmenin derlenmesi ve çalıştırılması için
3. JsonRPC	Düğüm ve blok zincir arasındaki iletişimin gerçekleştirilmesi için
4. Remix	Akıllı sözleşmenin geliştirilmesi için IDE

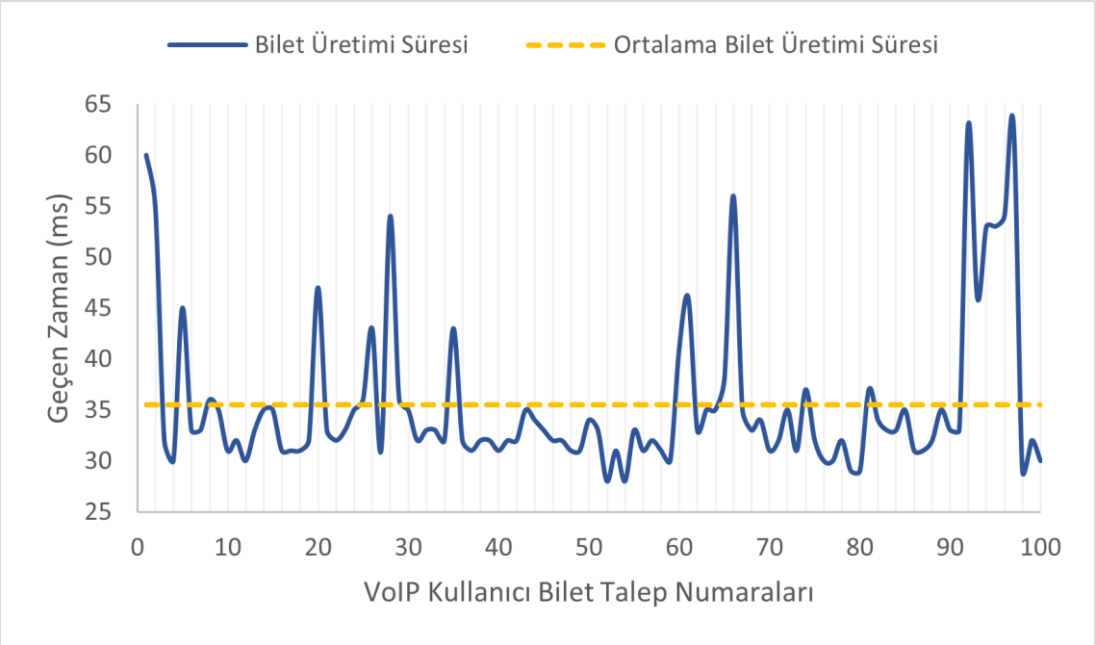
5.2.2. Performans Değerlendirmesi

Tezdeki çalışma, VoIP kullanıcılarının kimlik doğrulama için bilet oluşturma, kayıtlanma ve kimlik doğrulama aşamalarına göre değerlendirmektedir. Önerilen kimlik doğrulama mekanizması, merkezi yapıyı kullanan SIP-TLS süreci ve SIP kimlik doğrulama yöntemini kullanan mevcut şemalarla karşılaştırılmıştır. Ayrıca önerilen mekanizmanın güvenilirliği ve hızlı kimlik doğrulama süreci, blok zincir kullanarak VoIP uygulamalarında merkezi olmayan kimlik doğrulama gerçekleştiren literatürdeki çalışmalarla karşılaştırılarak gösterilmektedir.

5.2.2.1. Bilet Oluşturma Süreci

VoIP uygulamasındaki yeni bir VoIP kullanıcısı, Yönetici'den bir kayıtlanma bileti talep eder ve bu bilet, özetleme işlemi yapılan kullanıcının adresinin (genel anahtar) ve VoIP kullanıcısının bilgilerinin imzalı (özel anahtarla şifrelenmiş) bir biçimidir. Bilet oluşturma, tek yönlü özetleme algoritması ve ECDSA kullanan hızlı, etkin ve güvenilir bir işlemdir. Bu işlem sürecinde, özetleme algoritması olarak SHA-256 algoritmasını kullanılır ve bileti Yönetici'nin özel anahtarıyla imzalamak için ECDSA

kullanılır. Bu açıdan, bilet üretimi blok zincir ağının bir parçası değildir ve blok zincirinin dışında gerçekleşmektedir. Ayrıca bilet üretimi herhangi Ethereum Gas birimine (Ethereum Gas fee) mal olmaz. Çünkü bu işlem blok zincir ağında yeni bir bloğa ihtiyaç duymaz, bu durum 0 Gas maliyeti anlamına gelir. Biletin talep edilmesi ve üretilmesi için deney esnasında 100 farklı VoIP kullanıcısı için testler gerçekleştirilmiş ve bilet üretim süresi sırasıyla hesaplanmıştır. Her bir VoIP kullanıcısı için bilet talebinde geçen üretim süresi test edikten sonra hesaplanan ortalama bilet üretim süresi Şekil (5.1)'de gösterilmektedir.



Şekil 5.1: Bilet Üretimi için Önerilen Yöntemin Deneysel Sonucu.

Bilet oluşturma işleminin her VoIP kullanıcısı için ortalama süresi 36 ms civarındadır. Bilet oluşturma süresi, önerilen şemadaki tüm diğer işlemlere göre daha kısadır. Bu durum tezde sunulan mekanizmanın VoIP ağındaki gerçek zamanlı uygulamalar açısından uygun olduğu anlamına gelmektedir.

5.2.2.2. Kayıtlanma Süreci

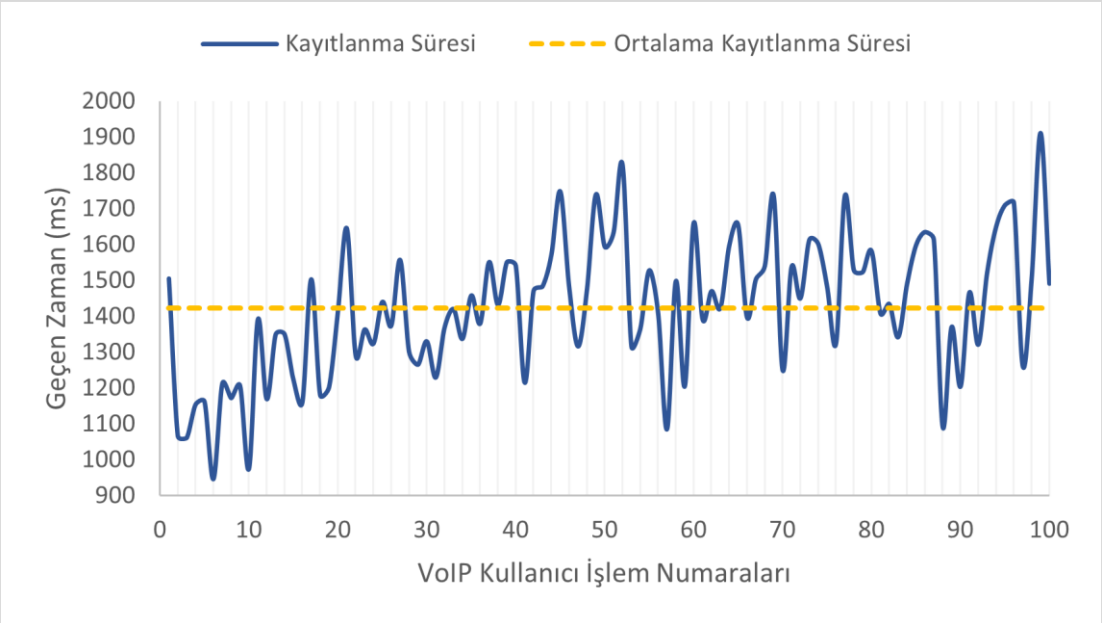
Blok zincir platformunda, ağ üzerinde gerçekleşen her işlem süreci için yaklaşık bir maliyet oluşur. Blok zincire yapılan bir talep akıllı sözleşmeyi tetikler. Blok zincir içindeki akıllı sözleşmeler ile ağda karşılıklı mesaj alış-verişi başladığında artan veri trafiği ve yapılan hesaplamaların maliyeti, blok zincir platformuna kayıtlanma talebini gerçekleştiren VoIP kullanıcıları tarafından ödeme yöntemi ile gerçekleşir.

Gas ölçü birimi, Ethereum platformunda kullanıcılar tarafından talep edilen işlemlerin yapılabilmesi için maliyetlerin hesaplanmasında kullanılır. VoIP kullanıcıları, bir defa gerçekleşecek olan Ethereum blok zincir platformuna kayıtlanma işlemi için talepte bulunur. İşlem talebini blok zincir ağına göndermeden önce, Gas adı verilen birim ile işlem maliyetini karşılar. Çünkü madenciler arasında konsensüs algoritması ile uzlaşı sağlamak ve talep edilen işlemi gerçekleştirmek için sistemde Gas maliyeti ortaya çıkar. Etherum blok zincirine kayıtlanmak isteyen VoIP kullanıcıları, Gas maliyetini ödemeleri gerekmektedir. Blok zincirine kayıtlanma sırasında her VoIP kullanıcısı için kayıt maliyeti 73381 Gas'dır. Bölüm 5.2.2.4'de finansal maliyet olarak Gas biriminin para birimi karşılığı detaylı olarak hesaplanmaktadır.

Tezde sunulan mekanizmanın bilet üretimi veya kimlik doğrulama işlemi gibi diğer aşamalarıyla karşılaştırıldığında, her kullanıcı talebinde ayrı bir işlem (transaction) gerekir. Ayrı bir işlem blok zincir madenciliğine dayandığından kayıt işlemi daha fazla zaman gerektirir. Öte yandan, blok zincirinin dağıtık ve güvenli depolama ortamı sayesinde VoIP kullanıcı kayıt verileri, değişmez ve güvenli bir şekilde blok zinciri ağında saklanır. Her yeni VoIP kullanıcısı bir kez kayıtlanır ve sistem içinde kayıtlı kullanıcılar için tekrar kayıt işlemine izin verilmez. Diğer taraftan, arama işlemi sırasında kayıt işlemi gerçekleşmez ve kayıtlanma süreci arama sürecinden bağımsızdır. Bu nedenle kayıtlanma süreci IP ağı üzerinden gerçekleşen çağrılarda arama süresini etkilenmediğinden kayıt işlemi için gereken süre VoIP uygulamaları için kabul edilebilir bir seviyededir. Gerçek hayat senaryolarında tezde sunulan mekanizma merkezi olmayan kimlik doğrulaması sağlamak için kayıt işlemini Bitcoin sisteminde gerçekleştirilebilir. Ancak, Bitcoin ortalama her 10 dakikada bir blok işleme ve doğrulama kapasitesine sahiptir. Her blok kendisinden önce gelen tüm işlemlerin kaydını içeren, sırayla listelenen ve yeni işlemle biten bir dosyadır. Bitcoin PoW konsensüs mekanizması kullanır. Ethereum blok zincirinde ise blok işleme ve doğrulama süresi ortalama 12-14 saniye aralığındadır. Bitcoin veya Ethereum'da gerçek hayat senaryoları için tezde sunulan mekanizma ile kimlik doğrulama gerçekleştirilebilir. Önerilen yaklaşımın kimlik doğrulama esnasında gerçek hayat senaryolarında herhangi bir zaman sınırlaması bulunmamaktadır ve tezde sunulan kimlik doğrulama mekanizmamıza ek bir gecikme süresi eklemez. Sadece kayıtlanma işlemi için blok işleme ve doğrulama süreci daha geç sağlanır. Yani bu zaman gecikmesi sadece kayıtlanma aşaması için geçerlidir. Gerçek hayatta kayıtlanma

aşamasındaki bu gecikme Ethereum blok zincirinde kullanılan PoW konsensüs mekanizmasından kaynaklanmaktadır. Ancak, hesaplama açısından yoğun olmayan diğer alternatif konsensüs algoritmalarının (PoS, Ripple, vb.) kullanılması zaman alıcı faktörü iyileştirebilir. Diğer taraftan, sadece kayıtlanma aşamasında gecikme oluşacağı için bir VoIP çağrısında kimlik doğrulama esnasında iletişim gecikmeleri oluşmaz.

Şekil (5.2)'de, blok zincir ağındaki her bir VoIP kullanıcısının kayıtlanma işlemi (transaction) için deneysel sonuçları gösterilmiştir.



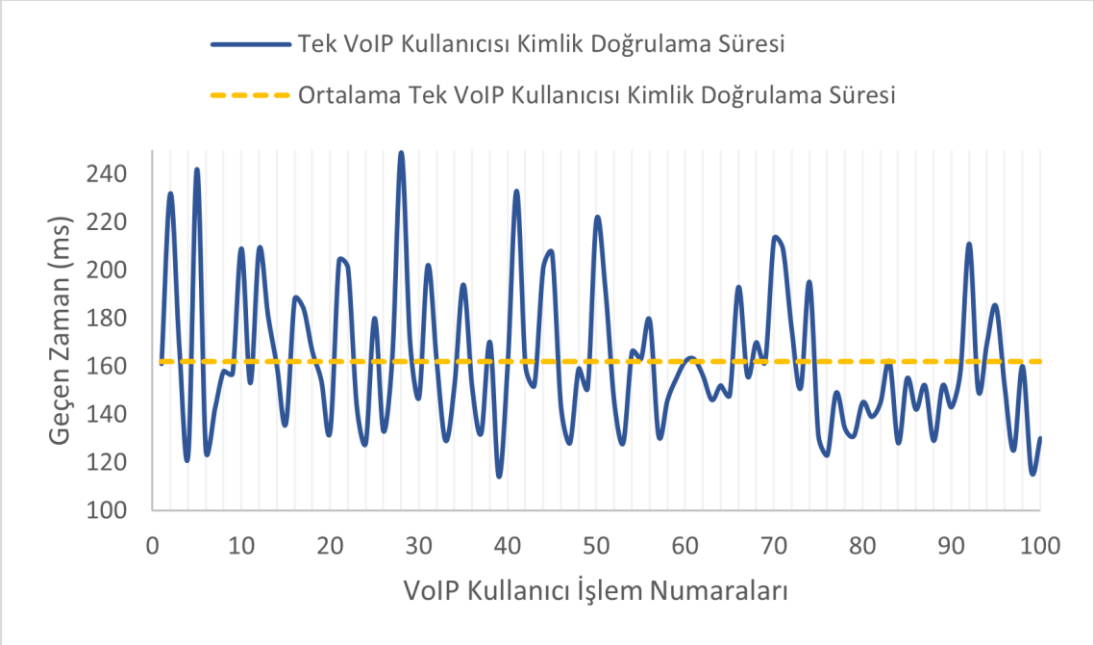
Şekil 5.2: Kayıtlanma Süreci için Önerilen Yöntemin Deneysel Sonucu.

Kayıtlanma sürecini test etmek için 100 farklı VoIP kullanıcısı üzerinden deney gerçekleştirilmiştir. Ortalama geçen zaman değerleri 1000 ms ile 1900 ms arasında değişmektedir. Tezde sunulan çalışmada güvenilir bir kimlik doğrulama sağlanması açısından bir VoIP kullanıcısı için blok zincirine ortalama kayıtlanma süresi yaklaşık 1422 ms'dir.

5.2.2.3. Kimlik Doğrulama Süreci

Tek VoIP kullanıcısı kimlik doğrulaması, sesli mesajları (voicemail) okumak için kullanıcı tarafından yapılan taleptir. Blok zincir platformu aracılığıyla tek taraflı bir kimlik doğrulaması gerçekleşir. Herhangi bir VoIP kullanıcısı sesli mesaj aldığında blok zincir ağında kimlik doğrulaması gerçekleştirerek mesajın içeriğine ulaşabilir. Şekil (5.3)'de, 1'den 100'e kadar değişen birbirinden farklı VoIP kullanıcıları ile

geçen zamanın anlık değişimi ve ortalama kimlik doğrulama süresi gösterilmektedir. Tek VoIP kullanıcısı tarafından talep edilen kimlik doğrulama süreci için ortalama süre hesaplaması, 100 yineleme üzerinden 100 farklı VoIP kullanıcısı ile test edilmiştir. Tezde sunulan yöntemde tek VoIP kullanıcısı için kimlik doğrulamasında, gerçekleşen işlem bilgileri blok zincir ağında bir blok içinde saklamadığı için herhangi bir finansal Gas maliyeti oluşmaz. Yani kayıtlanma işlemi gibi dağıtık defterde depolanacak işlemler oluşturup konsensüs süreci için gereken bir maliyet yoktur.

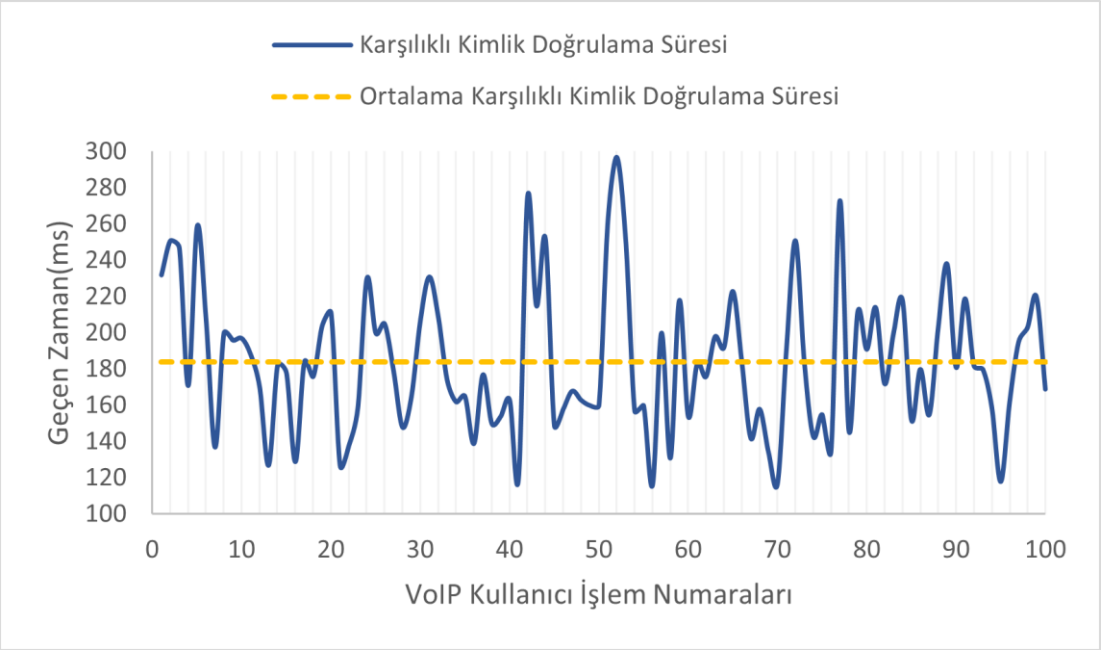


Şekil 5.3: Önerilen Yöntemin Tek VoIP Kullanıcısı için Kimlik Doğrulama Sonuçları.

VoIP kullanıcısının oluşturduğu işlem sonrasında kimlik doğrulama süreci için, kayıtlanma aşamasında blok zincir ağında güvenilir listede depolanan VoIP kullanıcısının kayıtlı bilgileri kontrol edilir. Kontrol işlemini blok zincir akıllı sözleşmesi sağlar. Tek VoIP kullanıcı kimlik doğrulaması için ortalama süre yaklaşık 162 ms'dir. Ayrıca VoIP kullanıcısı sisteme bir kez kayıt olarak sürekli kimlik doğrulaması yapabilmektedir. Her kimlik doğrulama sürecinde ayrı bir kayıtlanma sürecine ihtiyaç yoktur.

İkinci kimlik doğrulama türü, arayan ve aranan arasında gerçekleştirilen karşılıklı kimlik doğrulamadır. Karşılıklı kimlik doğrulama için geçen zamanın anlık değişimi ve ortalama kimlik doğrulama süre testi 100 farklı kullanıcı için 100 yineleme üzerinden hesaplanmış ve sonuç Şekil (5.4)'de açıkça gösterilmiştir. Arayan ile aranan

arasındaki ortalama kimlik doğrulama süresi yaklaşık 184 ms'dir. Tek VoIP kullanıcı kimlik doğrulaması ile karşılaştırıldığında, karşılıklı kimlik doğrulama daha fazla zaman alır. 100 farklı kullanıcı üzerinden yapılan karşılıklı kimlik doğrulama deney sonuçları tek VoIP kullanıcı doğrulaması ile karşılaştırılmış ve artışın yaklaşık %13,5 oranında gerçekleştiği tespit edilmiştir. Çünkü blok zincir ağında VoIP çağrısını gerçekleştirecek tarafların kayıtlı bilgileri sırasıyla kontrol edilir. Öte yandan, her iki kimlik doğrulama türünde de standart sapma düşüktür ve bu da hesaplamaların kararlılığına tanıklık eder.



Şekil 5.4: Önerilen Yöntemin Karşılıklı Kimlik Doğrulama Sonuçları.

Ayrıca önerilen yöntem aynı anda birden çok kullanıcıya ve birden çok bağlantıya eş zamanlı hizmet etmektedir. Karşılıklı kimlik doğrulama işlemi VoIP uygulaması üzerinden taraflar arasındaki IP telefonunda anlık gerçekleşip sonuçlanan bir durumdur. VoIP gerçek zamanlı bir uygulamadır ve kullanıcı sayısının artışından ağdaki trafik artabilir. Günümüz IP telefon cihazında yeterli RAM, CPU olduğunda ve uygun internet bant genişliği sağlandığında taraflar arasında VoIP çağrısında herhangi bir aksaklık oluşmayacaktır.

Şekil (5.2), (5.3) ve (5.4)'de tezde sunulan çalışmadaki farklı süreçler (kayıtlanma ve kimlik doğrulama) için geçen test süresi ile VoIP kullanıcı işlem numaraları arasındaki ilişki değerlendirilmiştir. Ancak geçen süre ile VoIP kullanıcı sayısındaki artış ilişkisi değerlendirilmemiştir. Çünkü eşler arası (peer-to-peer) mimari sistem kullanıcı

sayısından bağımsızdır. Tezde sunulan yöntemde, VoIP kullanıcılarının sayısı arttıkça kimlik doğrulama süresi aynı oranda doğrusal olarak artmaz. Çünkü önerilen kimlik doğrulama, eşler arası (peer-to-peer) bir kimlik doğrulama mekanizmasıdır. Bu sebepten dolayı önerilen yöntem aynı anda birden çok VoIP kullanıcısına ve birden çok bağlantıya gerçek zamanlı veri iletiminde süre gecikmesi oluşturmadan hizmet eder.

5.2.2.4. Finansal Maliyet

Gas birimi, Ethereum ağındaki işlem (transaction) ücretlerini ifade eder. Gas ücretleri, Ethereum blok zincirindeki işlemleri doğrulamak için ve gereken işlem enerjisini telafi etmek için kullanıcılar tarafından yapılan ödemelerdir. Önerilen şema, ağ üzerinde gerçekleştirilen tüm depolama amaçlı hesaplamalar için bir ücret talep ederek ödül sistemi üzerinden kötü niyetli kullanıcıların ağda değişiklik yapmasını (mesela ID sahtekarlığı) engeller. Kısaca, Gas ücretleri blok zincir ağ güvenliğine katkıda bulunur ve finansal maliyet sistemi, VoIP kullanıcılarını blok zincirinde güvenilir ve meşru tutmak içindir. Kayıtlanma sürecinde her bir VoIP kullanıcısı için işlemin maliyeti Şekil (5.5) ile gösterilen algoritma kullanılarak hesaplanmıştır.

Algoritma: Önerilen Yöntemin Maliyet Hesaplaması

```
const registration_cost = 73381     // gas
const gas_in_Eth = 0.000000001      // gas
const Eth_in_Dollar = 1.170,92      // ETH

Fonksiyon: FinancialCost (double transaction_number)
    Başla
        return ((transaction_number * registration_cost) * gas_in_Eth * Eth_in_Dollar)
    Bitir
```

Şekil 5.5: Finansal Maliyet Hesaplaması.

Ethereum Ether (ETH) adında bir para birimine sahiptir. Ethereum blok zincir ortamında, Gas ücretleri ETH ile ödenir. Gas fiyatları, ETH'nin bir birimi olan Gwei cinsinden belirtilir. Her Gwei, 0.000000001 ETH'ye (10^{-9} ETH) eşittir. Gerçek maliyet, ETH biriminin gerçek değerinin para birimine çevrilmesiyle dolar cinsinden hesaplanır. Tezde sunulan kimlik doğrulama mekanizması için kayıtlanma sürecinin

işlem maliyeti, ETH cinsinden 73381 Gas'dır ve hesaplanma şekli Denklem (5.1) ile verilmiştir.

$$Eth = gwei * 10^{-9} \quad \textbf{(5.1a)}$$

$$Eth = 73381 * 10^{-9} \quad \textbf{(5.1b)}$$

Dolar cinsinden ETH'nin (Eth = 0.000073381) 20.06.2022 yılındaki mevcut fiyatına göre, her VoIP kullanıcı kaydı için dolar para birimi cinsinden yaklaşık maliyet 8 Cent olarak hesaplanmaktadır. Öte yandan, bu ücret sadece bir defaya mahsus ve VoIP kullanıcısının kayıtlanma işlemi içindir. Kimlik doğrulamanın maliyeti ise 0 Gas'dır. Çünkü kimlik doğrulama sonrasında blok zincir ağında veri depolamak için işlem blokları oluşturulmaz.

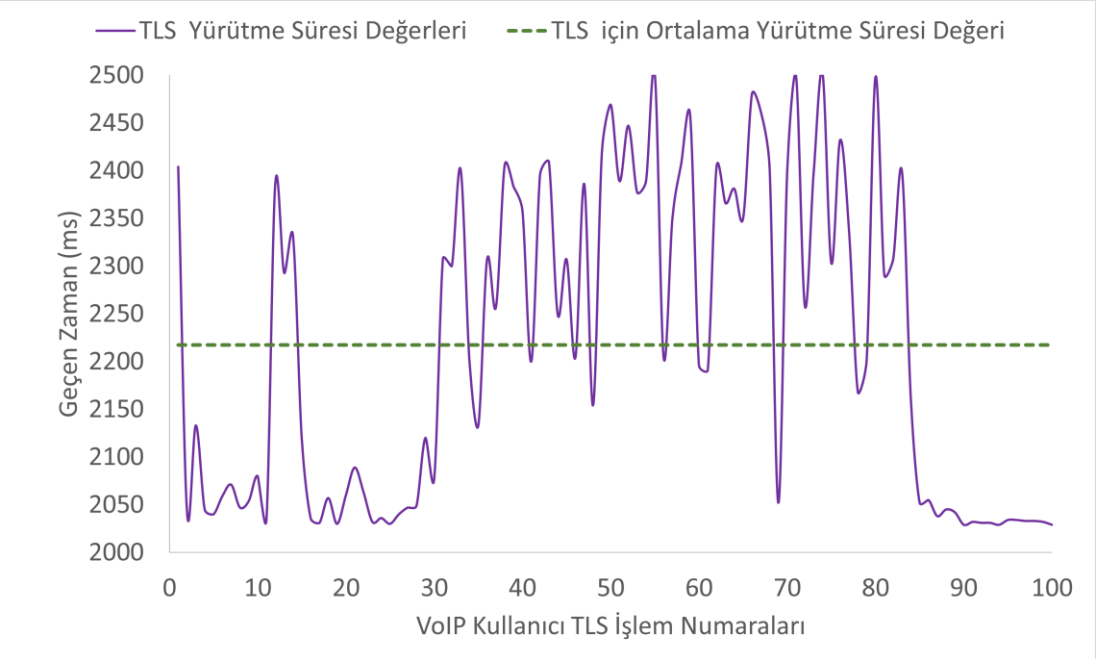
5.2.3. Karşılaştırma

Bu bölüm, tezde sunulan kimlik doğrulama mekanizmasını ortalama zaman gecikmesine göre literatürdeki diğer şemalarla karşılaştırmaktadır. Önerilen yöntem, SIP protokolünün TLS ile kimlik doğrulama süreci gerçekleştirmesi ve literatürdeki temel SIP doğrulama şemaları gibi mevcut tek sunuculu mimari (istemci-sunucu modeli) yöntemleriyle zaman gecikmesi ve güvenlik açısından karşılaştırılmıştır. Ayrıca, uçtan uca güvenli arama performansı, ortalama zaman gecikmesi ve güvenlik unsurları ile ilgili olarak literatürdeki blok zincir tabanlı kimlik doğrulama şemaları arasında kıyaslama yapılmış ve geliştirilen mekanizmanın güçlü yönleri ortaya konulmuştur.

5.2.3.1. Sunucu Tabanlı Yöntemlerle Karşılaştırma

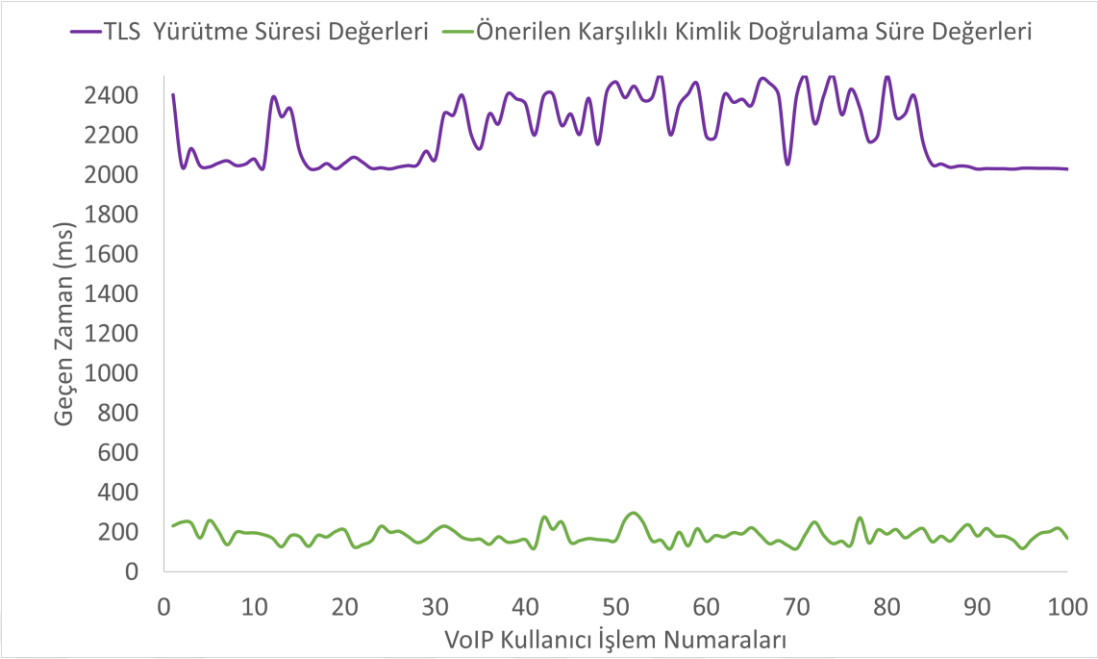
VoIP uygulaması kullanılarak bir IP ağı üzerinden gerçekleştirilen bir VoIP çağrısında kimlik verilerinin değiştirilmediğini ve yok edilmediğini doğrulamak için en iyi seçeneklerden biri TLS protokolüdür. Karşılıklı kimlik doğrulama, TLS sürecinin bir parçasıdır. Bu deneyde, VoIP kullanıcı cihazına kurulabilecek en yüksek TLS sertifikası olan TLS v.1.3 kullanılmıştır. Yapılan deneyler TLS sertifika doğrulaması için TLS v.1.3 ortalama gecikme süresinin yaklaşık 2056 ms olarak sonuç verdiğini göstermiştir. Ayrıca TLS protokolünde kayıtlanma süreci her arama için tekrar gerçekleşir. Her çağrıda gerçekleşen kayıtlanma süreci, gerçek zamanlı veri ileten VoIP uygulamalarında zaman gecikmesine neden olur. Şekil (5.6), IP ağı üzerinden

VoIP çağrısı gerçekleştiren VoIP kullanıcıları için TLS işlemi ortalama süresinin deneysel sonucu göstermektedir. Taraflar arasındaki VoIP çağrısının TLS üzerinden yapılması sonucu geçen sürenin 2050 ms ile 2450 ms aralığında gerçekleştiği görülmüştür. Ayrıca, TLS işleminin kimlik doğrulama ortalama gecikme süre hesaplaması için kullanılan farklı 100 düğüm üzerinden elde edilen değer yaklaşık 2217 ms olduğu görülmüştür.



Şekil 5.6: Karşılıklı Kimlik Doğrulama için TLS Protokolü Deneysel Sonucu.

Şekil (5.7), TLS süreci ile tezde sunulan yöntem arasındaki kimlik doğrulama süreci karşılaştırmasının deneysel sonucunu göstermektedir. Deneysel sonuçlara göre tezde sunulan yöntemin TLS kimlik doğrulama sürecine göre ortalama zaman gecikmesi açısından yaklaşık 10 kat daha hızlı olduğunu görülmektedir. Bölüm 5.2.2.2'de bahsedildiği gibi tezde sunulan mekanizmanın ortalama kayıtlanma süresi yaklaşık 1422 ms'dir ve kimlik doğrulama işlemi için kayıtlanma sadece bir kez gerçekleşir. Yani kayıtlanma süresi VoIP çağrısı esnasındaki taraflar arasında kimlik doğrulama sürecine dahil değildir. Bu nedenle kayıt ve doğrulama işlemleri TLS'den daha hızlıdır. TLS protokolü ile kullanılan merkezi yapı nedeniyle artan hata toleransı ve güvenilir olmayan yapıya ek olarak, TLS işleminde kimlik doğrulama süreci için ortalama geçen süre önerilen kimlik doğrulama mekanizmasına göre oldukça fazladır.

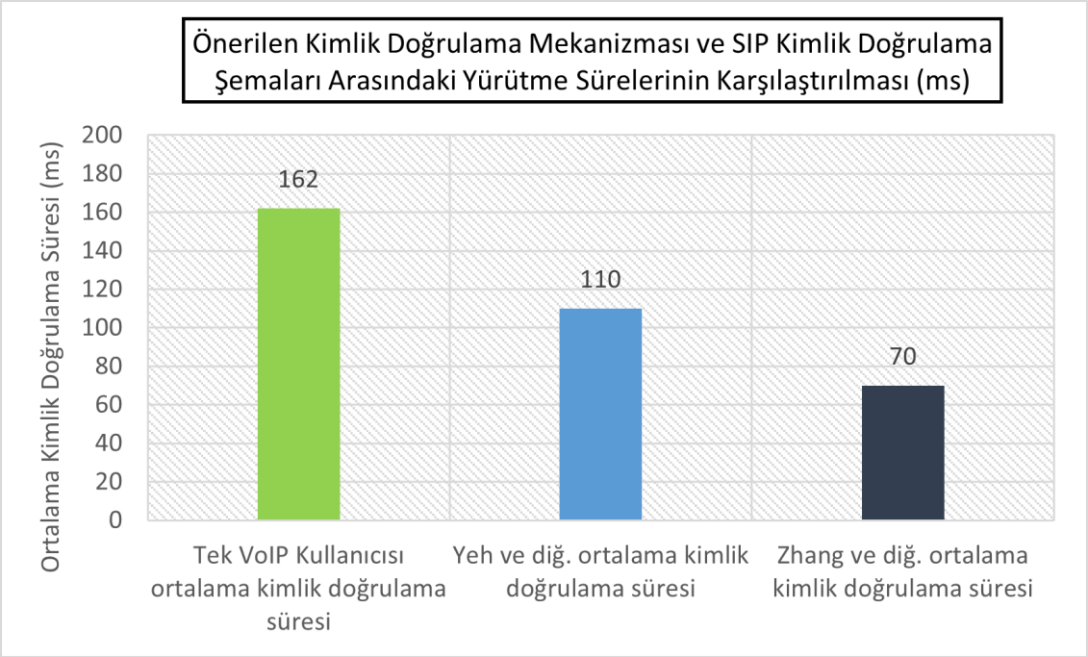


Şekil 5.7: Karşılıklı Kimlik Doğrulama için TLS Protokolü ve Önerilen Kimlik Doğrulama Yönteminin Performans Karşılaştırması.

TLS protokolü iki kısımdan oluşur ve bunlar sırasıyla TLS Kayıt bölümü (Record) ve El Sıkışma bölümüdür (three-way handshake). TLS iki kısımdan oluşur ve kayıt kısmı şifreleme için, üçlü el sıkışma kısmı ise kimlik doğrulama için kullanılır. Tezde sunulan mekanizmanın TLS kimlik doğrulama sürecine göre ortalama zaman gecikmesi açısından yaklaşık 10 kat daha hızlı olmasının temel sebebi, el sıkışma bölümünün şifre paketi (cipher suite) (genel anahtar için), blok şifreleme (block cipher encryption), özetleme (hashing) ve sıkıştırma yöntemlerini gerçekleştirmesidir. Ayrıca, Kayıt bölümünde, veri sıkıştırma için ZIP, Özet Tabanlı Mesaj Doğrulama Kodu (HMAC) ile özetleme ve blok şifrelemenin Şifre Blok Zincirleme (CBC) modunu yerine getirerek gerçekleşen işlemler en yüksek zaman gecikmesine sebep olur. Ayrıca TLS, karşılıklı kimlik doğrulama için merkezi yapıdaki bir sunucudan alınan sertifikaları (X.509 sertifikası) kullanır. Diğer taraftan tezde sunulan mekanizma, TLS protokolünün SIP güvenliğini sağlarken barındırdığı açıklıkları ve üçüncü taraflar (CA veya TTP) sorunlarını ortadan kaldırır.

TLS, uçtan uca (end-to-end) bir güvenlik kanalı sağlar ve bir dizi şifreleme işlevini birleştirir. Ancak bu, TLS'nin eşler arası (peer-to-peer) güvenlik sağladığı anlamına gelmez. TLS tercih edilirse, MITM saldırısı hala bir problemdir. Çünkü veri aktarımı ağda iki cihaz arasında tekrar tekrar şifrelenerek iletilir. Böylece VoIP çağrısında ses paketleri için haberleşme kanalında tam anlamıyla eşler arası gizlilik sağlamaz.

Şekil (5.8)'de açıkça gösterildiği gibi, literatürdeki SIP kimlik doğrulaması kullanan yöntemlerle karşılaştırıldığında, Yeh ve diğ. (2013) önerdiği yöntemde kimlik doğrulama yaklaşık 110 ms'dir. Yine benzer bir yöntem kullanan Zhang ve diğ. (2016) şeması kimlik doğrulama ortalama süresi olarak yaklaşık 70 ms'dir. Ancak, tezdeki çalışmada tek VoIP kullanıcı kimlik doğrulaması için ortalama süre yaklaşık 162 ms'dir. Bu sonuçlara göre, Zhang ve diğ. (2016)'nın sunduğu yöntem, kimlik doğrulama işlemi sırasında yalnızca tek yönlü özetleme işlemi (one-way hash function) ve özel veya işlemleri (exclusive-or operations) kullanarak en iyi performansı elde etmektedir.

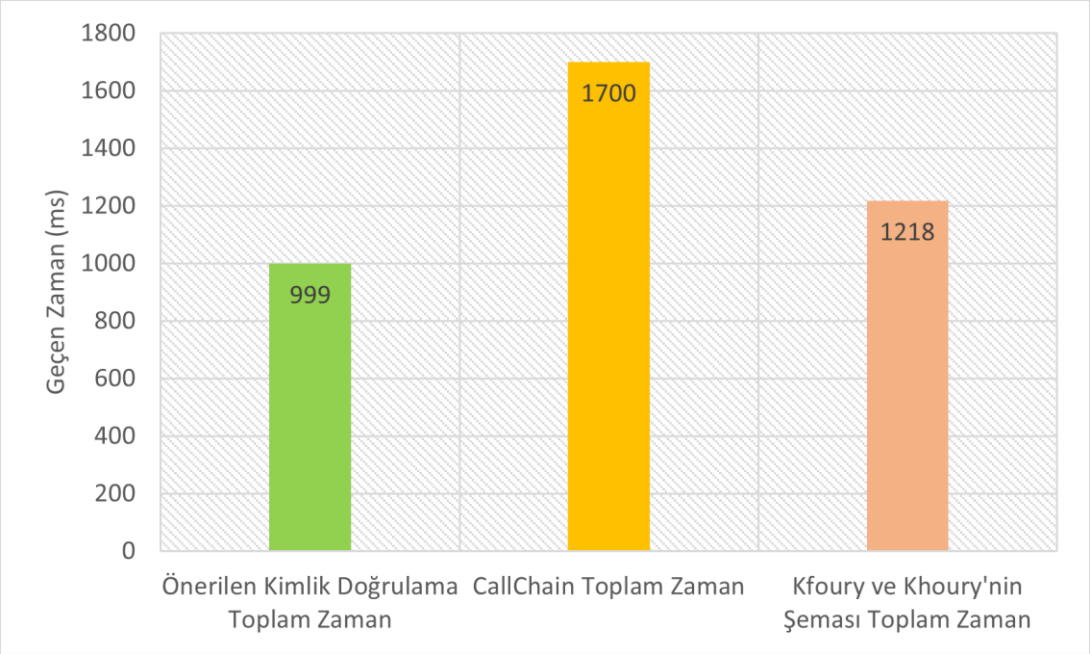


Şekil 5.8: Mevcut SIP Kimlik Doğrulama Şemaları ile Önerilen Mekanizmanın Karşılaştırılması.

Her ne kadar Yeh ve diğ. (2013) ve Zhang ve diğ. (2016) ortalama kimlik doğrulama süresini önemli ölçüde azaltsa da, önerdikleri yöntem güvenlik açısından oldukça zayıftır. Sadece bu yöntemle kimlik doğrulama gerçekleştirmek VoIP ağımızda tek nokta hatası (single point of failure), zayıf hata toleransı (low fault tolerance), anahtar dağıtımında güvensizlik ve mahremiyet (privacy) sorunları gibi bazı güvenlik zayıflıkları barındırır. Bütün bunların yanında, karşılaştırılan SIP tabanlı kimlik doğrulama yapan şemalara göre daha yavaş kimlik doğrulama süresine sahip olan tezdeki çalışma, çok daha güvenli ve güvenilir kimlik doğrulama sürecinin yanında IP ağı üzerinden yapılan işlem sürecinde kabul edilebilir bir zaman gecikmesi ortaya koymaktadır.

5.2.3.2. Blok Zincir Tabanlı Yöntemlerle Karşılaştırma

VoIP ağında blok zinciri kullanarak kimlik doğrulaması yapan şemalar ve tezde sunulan kimlik doğrulama mekanizmasının karşılaştırılması Şekil (5.9)'da sunulmuştur. Kfoury ve Khoury (2018) önerdiği yöntemde VoIP kullanıcıları arasında uçtan uca güvenli bir çağrı süreci kurmak için gereken toplam ortalama süre 1218 ms olarak hesaplanmıştır. Çünkü uçtan uca güvenli bir çağrı kurulumu esnasında, blok zinciri üzerinden anahtar dağıtımı, asimetrik şifreleme (ortak anahtarla şifreleme ve özel anahtarla şifre çözme), SIP sinyalizasyonu, simetrik anahtar üretimi ve SRTP protokolü için simetrik anahtar üretimi sırasıyla adım adım gerçekleştirilir. Ethereum kullanan CallChain (Chen ve diğ., 2021) şemasının toplam çağrı kurulum süresi ise tezde sunulan çalışmaya ve Kfoury ve Khoury (2018) önerdiği yönteme göre daha yüksektir. 4G ve Wi-Fi üzerinden iki farklı şekilde bant genişliği üzerinden IP telefon cihazlarını test ederek deneysel sonuçlar elde edilmiştir. CallChain şemasında taraflar arasında uçtan uca güvenli bir çağrı kurmak 4G üzerinden ortalama 1700 ms ve Wi-Fi üzerinden ortalama 1600 ms'dir.



Şekil 5.9: Blok Zincir Kullanan Kimlik Doğrulama Şemaları İle Ortalama Çağrı Kurma Süresi Karşılaştırması.

Belirtilen şemaların gecikme süresini esas olarak blok zincir ağındaki işlemler, VoIP uygulamasının blok zincir ağına entegre edilme yöntemi ve sırasının yanı sıra kullanılan kriptografik yöntemler etkilemektedir. Ayrıca madenci düğümleri

tarafından bir blok zincir ağında işlem üreterek yeni bir blok oluşturmak zaman alır ve tüm süreçleri yavaşlatır. Bu açıdan VoIP ağı ve blok zincir ağının etkileşimi, çağrı sürecindeki kimlik doğrulama, anahtar dağıtımı ve SIP sinyalizasyonu benzeri süreçlerin doğru sırada kullanılması önemlidir. Bir VoIP uygulaması, kimlik doğrulamayı blok zincir tabanlı kullanarak gerçekleştiriyorsa sinyal katmanı bileşenlerinin çalışma sırası zaman gecikmesi ve güvenli çağrı oluşturma süreci için önemlidir. Tezde sunulan yöntemde VoIP kullanıcı oturumlarını başlatıp yöneten SIP sinyalizasyonu, blok zincir ağından bağımsız olarak çalışır. IP ağı üzerinden gerçekleşen VoIP çağrısı, arayan tarafından başlatıldıktan ve aranan tarafından kabul edildikten sonra, kimlik doğrulama medya aktarım aşamasından hemen önce gerçekleşir. Ayrıca her kimlik doğrulama işlemi için yeni bir blok oluşturup zincire eklenmez. Yalnızca kayıt işlemi esnasında, zincire yeni bir blok eklenir ve dağıtık defterlere ilgili veriyi depolamak için işlemler üretilir. Böylece tezdeki çalışma maliyet açısından uygun ve hızlı bir kimlik doğrulama şeması sunmaktadır. Tezde sunulan kimlik doğrulama mekanizması için uçtan uca toplam çağrı kurulum süresi diğer blok zinciri kullanan şemalara göre daha hızlı, güvenli ve güvenilir performans göstermektedir.

IP cihazları arasındaki çağrı kurulumu, VoIP ağında sinyal katmanında iki bölümden oluşur. İlk kısım SIP Daveti (SIP Invite) aşamasıdır ve ardından aranan kişi arama talebini kabul eder. Bundan sonra ikinci kısma geçilir. Böylece VoIP kullanıcıları arasında OK (onay) mesajları ve ACK (bilgi) mesajları karşılıklı iletilerek bir çağrı süreci kurulmuş olur. Ancak tüm bu süreçlerin gerçekleşmesi için bir SIP sunucusuna ihtiyaç vardır. Deneysel sonuçlara göre, VoIP kullanıcıları arasında IP ağı üzerinden uçtan uca güvenli bir arama yapmak için tezde sunulan kimlik doğrulama mekanizmasında ortalama toplam çağrı kurulum süresi yaklaşık 999 ms olarak hesaplanmaktadır. SIP Davet mesajının gönderilmesinden yapılan aramayı kabul etme sürecine kadar ortalama süre yaklaşık 295 ms ve OK mesajından ACK mesajına kadar geçen ortalama süre SIP sinyalleşme katmanında yaklaşık 350 ms'dir. Arayan ve aranan arasındaki ortalama kimlik doğrulama süresi, blok zinciri ağında yaklaşık 184 ms'dir. Son olarak anahtar değişimi için ECDH algoritmasının ortalama süresi yaklaşık 170 ms olarak belirlenmiştir.

Sonuç olarak, tezde sunulan yöntemde toplam ortalama süre, VoIP arama kurulumu için zaman gecikmesi olarak Kfoury ve Khoury (2018)'in şemasından yaklaşık %28 daha hızlıdır. Benzer şekilde CallChain, tezde sunulan mekanizmadan yaklaşık %70 daha yavaştır. Diğer taraftan çağrı kurulum süresindeki %70 oranındaki artış VoIP benzeri gerçek zamanlı uygulamalarda son kullanıcı tarafından hissedilebilir. VoIP gibi gerçek zamanlı uygulamaların kullanılabilirlik unsuru, internet bant genişliğine ve RAM boyutuna bağlıdır. Bu nedenle VoIP uygulamalarında kimlik doğrulama gibi güvenlik yöntemleri olabilecek en hızlı ve güvenli şekilde gerçekleşmelidir.

Tablo 5.2: Önerilen Şemanın Literatürdeki Şemalarla Karşılaştırılması.

Özellikler	Yeh ve diğ. (2013)	Zhang ve diğ. (2016)	Call-Chain (2021)	Kfoury ve Khoury (2018)	Önerilen Yöntem
Merkezi veya Merkezi Olmayan	Merkezi	Merkezi	Merkezi Olmayan	Merkezi Olmayan	Merkezi Olmayan
Enerji Tüketimi	Düşük	Düşük	Orta	Yüksek	Düşük
Karar Stratejisi veya Konsensüs Mekanizması	Tek Sunuculu	Tek Sunuculu	RBFT	PoW	PoS
Hata Toleransı	1	1	$3f + 1 \leq n$	$2f + 1 \leq n$	$2f + 1 \leq n$
Zaman Karmaşıklığı	$O(1)$	$O(1)$	$O(n^2)$	$O(n)$	$O(n)$
Güvenlik/Güvenilirlik ve Hız	Düşük ve Hızlı	Düşük ve Hızlı	Yüksek ve Yavaş	Orta ve Yavaş	Yüksek ve Hızlı

Literatürdeki şemalarla tez çalışmasında sunulan kimlik doğrulama mekanizması karşılaştırıldığında, karar alma mekanizması tek sunuculu olan yani merkezi sistemlere göre zaman karmaşıklığı daha yüksektir ancak sağlam, hata toleransı yüksek, güvenli ve güvenilir bir sistem sunmaktadır. Tezde sunulan merkezi olmayan

blok zincir tabanlı kimlik doğrulama mekanizmasının birçok açıdan üstün yönleri bulunmaktadır ve avantajlara sahip olduğu kanıtlanmıştır. Bu avantajlar sırasıyla dağıtık yapı içerisinde iş birliğine dayalı kimlik doğrulama, yüksek hata toleransı, hızlı karar alma sistemi, merkezden yönetilmeme, güvenilirlik ve üst düzey güvenlik sağlamaktır. Bu çalışma blok zincir tabanlı benzer çalışmalarla karşılaştırıldığında fikir birliği algoritması olarak PoS konsensüs mekanizması önermektedir. Çünkü, hata toleransı Pratik Bizans Hata Toleransı (PBFT) ve PBFT tarafından geliştirilen Yedekli Bizans Hata Toleransı (RBFT) benzeri algoritmalar kadar yüksek olmasa da bu algoritmalara göre oldukça hızlıdır. Ayrıca PBFT algoritması ağdaki düğüm sayısı az olduğunda sağlam ve güvenli bir algoritmadır ancak büyük ağ yapılarında güvenilirlik açısından yetersiz bir algoritmadır. Bunun nedeni, her düğümün ağı güvenli tutmak için diğer tüm düğümlerle konuşması yani iletişim kurması gerekmektedir. Bu durum, düğüm sayısı arttıkça hızla büyük bir iletişim maliyetine dönüşebilir.

Enerji tüketimi açısından PoS, PoW ile karşılaştırıldığında ağı korumak için son derece düşük miktarda bilgisayar üzerinden hesaplama işlem gücü kullanır. Güvenlik açısından ise, azaltılmış %51 kimlik hırsızlığı (sybil) saldırı olasılığına sahiptir. Yani saldırganın PoS sisteminde aynı piyasa değerine sahip bir PoW sistemine göre %51 saldırısı başlatması daha zordur. Böylece bu tez çalışmasında önerilen yöntem, IP ağında VoIP iletişimi için daha yüksek güvenlik gereksinimleri olan uygulama senaryoları için daha uygundur. Ayrıntılı sonuçlar Tablo 5.2'de gösterilmektedir.

6. SONUÇLAR

VoIP uygulamaları hızla günlük hayatımızın bir parçası haline gelmektedir. Daha uygun iletişim maliyeti, daha uygun donanım ve yazılım, aynı anda birden fazla kişiyle telefon görüşmesi yapabilme imkanı ve geleneksel telefon sistemlerinden daha fazla özellik sunması internet tabanlı telefon uygulamalarına artan talebin başlıca nedenleridir. Ancak IP ağı üzerinden gerçekleşen VoIP teknolojisinin kullanım oranındaki artış bu alandaki gizlilik, mahremiyet ve güvenlik ihtiyacını artırmaktadır.

VoIP uygulamalarındaki geleneksel kimlik doğrulama yöntemlerinin merkeziyetçi modellere dayanması sonucu kimlik doğrulaması esnasında ortaya çıkan hataları ve zafiyetleri ortadan kaldırmak, güvenli ve güvenilir bir kimlik doğrulama ortamı sağlamak ve bu güvenilir ortamın gerçekleştirilmesi için blok zincir tabanlı merkezi olmayan bir model oluşturarak güvenlik unsurlarını bir arada sağlamak bu tez çalışmasının temel amacını oluşturmaktadır. Bu amaçla, güvenli ses iletişimi için merkezi olmayan blok zincir tabanlı kimlik doğrulama mekanizması geliştirilmiş ve geliştirilen mekanizma deneysel çalışmalarla sınanmıştır. VoIP ağına Ethereum blok zincir entegre edilerek hızlı, düşük maliyetli ve merkezi olmayan bir kimlik doğrulama modeli önerilmiştir.

Kimlik doğrulama, günümüze kadar IP ağı üzerinden telefon görüşmelerinde önemli sorunlardan biri olmuştur. Bu sebepten dolayı internet ortamında güvenli ses paketleri ileterek görüşmeler gerçekleştiren yazılım ve/veya donanım çözümlerinin sayısı giderek artmaktadır. Tüm bu çözümler, SIP ve RTP protokolleri üzerinden veri akışının iki uç nokta arasında şifreli bir iletişim kanalı kurulmasıyla çalışmaktadır. IP telefon uygulamaları arasında veri güvenliğini sağlamak isteyen çalışmaların genellikle iki ana alternatifi vardır. Birincisi uygulama katmanı üzerinde güvenlik protokolü geliştirmek ikincisi ise uygulama protokolünü güvenli bir taşıma katmanı üzerinden uçtan uca sağlamaktır. Tipik olarak, uygulama katmanı güvenlik protokolleri üstün güvenlik özellikleri sağlasa da günümüzdeki saldırı modellerine karşı güvenilir ve güvenli sistem mimarileri gerekmektedir. IP telefonlar üzerinden

gerçekleştirilen VoIP çağrısında sürece katılan tarafların gerçek kimliklerinin doğrulanması, bir dinleyicinin içeriğe erişme olasılığının engellenmesi için çok faydalı olmaktadır. Bir VoIP haberleşmesinin tüm adımlarını sırasıyla açıklayan tezdeki çalışma, şema içerisinde kimlik doğrulama modelini bir bütün halinde sunmaktadır. VoIP uygulamaları genellikle sesli aramalar için kullanılır. Aramaya ek olarak, bir VoIP uygulamasındaki herhangi bir kullanıcı sesli mesaj da alabilir. Bu tez çalışmasında iki tür kimlik doğrulama yöntemi sunulmuştur. Birincisi, mesaj kutusundaki sesli mesajı dinlemek için kullanıcıların kimliğini doğrulamaktan sorumlu olan Tek VoIP Kullanıcı kimlik doğrulaması yöntemidir. İkincisi ise, görüşmenin hemen öncesinde taraflar arasında gerçekleşen Karşılıklı kimlik doğrulamasıdır. Tez sunulan çalışmada eşler arası kimlik doğrulama, sinyalleşme katmanındaki işlemler ile eş zamanlı olarak gerçekleşir. Böylece medya iletim katmanından hemen önce (konuşma öncesinde) iletişim kurmak isteyen VoIP kullanıcıları arasında şeffaf ve güvenli şekilde kimlik doğrulama sağlanmaktadır. Kimlik doğrulama sonrası VoIP çağrısında doğrudan taraflar arasında güvenilir kanal üzerinden anahtar değişimi yapılmaktadır. Ayrıca VoIP gibi gerçek zamanlı iletişim sistemleri saniyeler içerisinde binlerce işlem kapasitesine ihtiyaç duymaktadır. Bu açıdan, önerilen mekanizma ölçeklenebilir ve hata toleransı yüksek kimlik doğrulama modeli sunmaktadır. Ayrıca merkeziyetçi yapı ortadan kaldırılarak konsensüs algoritmalarıyla kayıtlanma sürecinde doğrulama işlemi merkezi olmayan güvenli bir ağ ortamında gerçekleştirilmiştir. Blok zincirin temel özellikleri olan akıllı sözleşmeler, fikir birliği için kullanılan konsensüs algoritmaları, inkâr edememe özelliği sağlayan dağıtık defterler ve kriptografik algoritmalar kullanılarak, internette bilinen tehditlere karşı VoIP iletişimi esnasında sağlam bir kimlik doğrulama modeli sunulmuştur. Önerilen yöntem, tek sunuculu kimlik doğrulama yöntemleri ve blok zincir tabanlı yöntemlerle karşılaştırılmıştır. Deneysel sonuçlara göre, tezde sunulan mekanizma merkezi kimlik doğrulama modellerine göre daha esnek ve saldırılara karşı daha dirençlidir.

Zaman gecikmesi ve hata toleransı, güvenli bir çağrı kurulumunda etkili parametrelerdir. Önerilen yöntem, zaman gecikmesi açısından blok zincir kullanan benzer yöntemlerden daha başarılıdır çünkü zaman karmaşıklığından ödün vermeden hata toleransını azaltır. Diğer taraftan güvenli haberleşme altyapısına dahil olmak isteyen herhangi bir IP telefon cihazı genel (public) blok zincirine kısıtlama olmadan

katılabilmektedir. Bu durum merkezi yapıda ortaya çıkan tek nokta hatası ortadan kaldırılmıştır.

IP telefon sistemleri, önemli ölçüde minimum gecikme gereksinimi ile çalışır. Gizlilik ve mahremiyet konusunda güvenliği sağlamak tek başına yeterli olmaz. Bu sebepten önerilen model tüm doğrulamaları gerçek zamanlı iletişim başlamadan ses verisinin aktarımının hemen öncesinde gerçekleştirir. Böylece, blok zincirin oluşturduğu dağıtık bir ağ üzerinden sertifika üreterek güvenilir bir sistem sağlanmasının yanında dağıtık model üzerinden sisteme erişimde gecikmeler oldukça azaltılmıştır.

Bu tez çalışmasında, güvenli bir haberleşme ağında gereken güvenlik unsurlarını tanımlanmış ve bir tehdit modeli oluşturulmuştur. Güvenlik ve performans analizleri yapılarak modelin güvenli ve gerçek zamanlı ses paketleri için verimli çalıştığı kanıtlanmıştır. AVISPA aracını kullanarak resmi güvenlik analizi ve resmi güvenlik doğrulaması gerçekleştirilmiştir. Böylece önerilen şemanın diğer ilgili şemalara kıyasla daha güvenli bir haberleşme kanalı sağladığı kanıtlanmıştır.

Kimlik doğrulamada güvenlik mekanizmasının sağlanması açısından önerilen yöntemde tüm kayıtlı kullanıcılar için referans olarak blok zincir ağındaki güvenilir liste esas alınmıştır. Kimlik doğrulama amaçlı bir işlem blok zincirinde yayınlandığında bilgisayarlar (düğümler) tarafından sağlam ve değişmez güvenilir listeler kullanılır ve bilgisayarlar işlem bilgilerini kontrol eder. Güvenilir liste, kayıtlanma aşamasında konsensüs mekanizması kullanılarak düğümler arasında mutabakat sağlandıktan sonra oluşturulur. Böylece her bilgisayarın dağıtık defterlerinde kayıtların bir kopyası güvenli şekilde saklanır. Diğer taraftan, VoIP kullanıcıları arasındaki her çağrıda taraflar arasında gerçekleşen kimlik doğrulanma işlemi (transaction) için blok zincirinde depolama ihtiyacı yoktur. Böylece, VoIP uygulamasında daha hızlı kimlik doğrulama işlemi gerçekleştirilmiştir.

VoIP haberleşmesindeki güvenlik ihtiyacı blok zincir entegrasyonu ile kimlik doğrulamada önemli bir basamak oluşturmaktadır. Blok zincir teknolojisini güvenli hale getiren dağıtık yapısı, inkâr edememe özelliği, şeffaflık, veri değişmezliği, izlenebilirlik, güvenilirlik, kriptografik yöntemleri bünyesinde barındırması, konsensüs algoritmalarının bir arada kullanımı ve otonom etkileşim sağlamasıdır. Akıllı sözleşme, bir blok zincirinde depolanan ve yürütülen kod parçacığıdır ve

taraflara dağıtılıp bir kez çalıştırıldıktan sonra, katılımcılar bunu değiştiremez. Akıllı sözleşme sayesinde kullanıcı, alıcı tarafın adresine bir işlem gönderebilir ve işlem yürütülür. Akıllı sözleşmeyle yapılan her etkileşim, blok zincirinde bir işlem olarak kabul edilir ve bloklar içerisine kaydedilmektedir. Blok zincir doğrulama gerektiren işlemleri genellikle akıllı sözleşmeler üzerinden gerçekleştirir. Akıllı sözleşmeler geleneksel bir sözleşmenin yaptığı gibi yalnızca bir anlaşmanın etrafındaki kuralları ve cezaları tanımlamazlar, aynı zamanda bu yükümlülükleri otomatik olarak uygularlar. Dağıtık defterlerdeki kullanıcı bilgilerini kontrol eden ve blok zincirinde dağıtık defterde depolanan veriler için arayüz oluşturan akıllı sözleşmedir. Dağıtık defterler, merkezi olmayan ve akıllı sözleşmelerle otonom etkileşim kuran kayıt listeleridir. Bu açıdan, blok zincir taraflar arasında gerçekleştirilen işlemleri ağ içerisinde herkes tarafından içeriği bilinen dağıtık defterlere kaydetmektedir. Böylece veri bütünlüğü ve inkâr edememe özellikleri ağ içerisinde sağlamaktadır. VoIP ağındanki katılımcılar tarafından talep edilen her kayıtlanma işlemi düğümlerin çoğunluğunun konsensüs algoritmasını kullanarak mutabakat sağlamasıyla dağıtık defterlere kaydedilmektedir.

Geleneksel kimlik doğrulama yöntemlerinde VoIP haberleşmesinde merkezi bir yapı aracılığıyla kimlik doğrulama ve anahtar dağıtımı gerçekleştirilmektedir. Bu durum ekstra maliyet, performans açısından darboğaz ve tek nokta hatası oluşturur. Blok zincir dağıtık bir teknoloji olduğundan arada üçüncü taraf olmadan doğrudan iki eş arasında merkezi olmayan doğrulamayı sağlar. VoIP kullanıcıları birbirleriyle daha önce iletişim kurduklarını inkâr edebilir ancak bu durumda dijital imza yöntemini kullanan blok zincir hatayı tespit eder. Blok zincir her işlemi kriptografik yöntemlerle imzalar ve işlemi gerçekleştiren VoIP kullanıcıları tarafından reddedilemez. Böylece ağ içerisinde inkâr edememe unsuru sağlanmış olur.

Blok zincirindeki herhangi bir düğüm veya VoIP kullanıcısının güvenliği ihlal edilirse ağ içerisinde güvenlik riski oluşur. Blok zincirinde (Bitcoin, Ethereum vb.) her kullanıcının blok zincirindeki erişim hakkı ve önemi eşittir. Örneğin, Bitcoin PoW konsensüs mekanizmasını kullanır ve her CPU bir oy anlamına gelmektedir. Kullanıcı tarafından yapılan her işlem onaylanır ve blok zinciri ağına kaydedilir. Kayıtlanma sonrası kullanıcılar blok zincir verilerini şeffaf bir şekilde görebilir. Sisteme kayıtlanma sonrası veriler (kriptografik anahtar vb.) depolanır ancak saldırgan

tarafından değiştirilmek istenebilir. Blok zincirine depolanan veriler bağlı liste veri yapısı modeliyle blokları bir önceki bloğun özetini alarak ardışık olarak bağlı bir blok zincir oluşturur. Bir blokta yapılan değişiklik blok oluşturulduktan sonra oluşturulan tüm blokları geçersiz kılar. Böylece iletişim sistemi içerisinde veri bütünlük unsuru sağlanmış olur. VoIP ağındaki kullanıcıların veri takibi güvenlik açısından izlenebilir olmalıdır. Blok zincir her işlemi zaman damgası ile depolar. Böylece her kullanıcı işlem verisi kolayca doğrulanır ve izlenebilir. Ancak VoIP ağındaki kişi bilgileri blok zincir içerisinde anonim şekilde saklanır ve şifreleme yapılarak güvenlik ve gizlilik sağlanmaktadır. Bu tez çalışmasında, merkezi yapıya ihtiyaç duymayan kimlik doğrulama işlemi VoIP ağının blok zincir ağı ile entegre edilmesiyle sağlanmaktadır. Böylece kimlik doğrulama esnek ve ölçeklenebilir hale gelir. Blok zincir ağında kayıtlı olmayan herhangi bir VoIP kullanıcısı, önerilen mekanizmada kötü niyetli olarak kabul edilir. VoIP ağının çok farklı unsurları bulunmaktadır ve değerlendirme esnasında hassas ölçümler gerekmektedir. Önerilen yöntemde, VoIP güvenlik altyapında deneysel sonuçları değerlendirmek için özel blok zincir (private blockchain) kullanılmıştır. Veri değişikliğine ve kimlik tahrifatına karşı sağlam yapısı nedeniyle Ethereum blok zincir platformu tercih edilmiştir.

Deneysel sonuçlar, önerilen şemanın VoIP iletişim sisteminde merkezi olmayan bir kimlik doğrulama sistemi sağlayarak çağrı süreci için verimli ve uygun maliyetli bir çözüm olduğunu göstermektedir. Ayrıca, uçtan uca güvenli arama performansı, ortalama zaman gecikmesi açısından mevcut blok zincir tabanlı kimlik doğrulama çalışmalarına göre %30-%70 oranında daha iyi performans göstermektedir. Çalışma sonucu elde edilen veriler taraflar arasında kimlik doğrulaması yapmak için sunulan yöntemin TLS protokolünden neredeyse on kat daha hızlı olduğu görülmüştür. Temel SIP kimlik doğrulaması gibi oldukça hızlı gerçekleşen yöntemler üzerinden yapılan karşılaştırmada elde edilen verilere göre sunulan yöntemin çağrı sürecinde kabul edilebilir bir aralıkta gecikme süresi vardır. VoIP uygulamaları gibi gerçek zamanlı bir uygulama da kimlik doğrulama hızlı ve güvenli gerçekleşmelidir. Blok zincir benzeri yapılar kullandığı konsensüs algoritmalarına göre farklı süreler içerisinde blok oluşturmaktadır. Bu sebepten dolayı kullanılan uygulamaya (VoIP, IoT, WSN vb.) uygun olarak bir blok zincir platformu seçilmelidir. Bu tez çalışmasında, Ethereum blok zincir tespiti gerçekleştirilmiş ve sorun çözülmüştür.

KAYNAKÇA

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain technology innovations. *In 2017 IEEE technology & engineering management conference (TEMSCON)*, (pp. 137-141). IEEE.

Alqassem, I., & Svetinovic, D. (2014). A taxonomy of security and privacy requirements for the Internet of Things (IoT). *In 2014 IEEE International Conference on Industrial Engineering and Engineering Management*, (pp. 1244-1248), IEEE.

Amara, M., & Siad, A. (2011). Elliptic curve cryptography and its applications. *In International workshop on systems, signal processing and their applications, WOSSPA*, (pp. 247-250). IEEE.

Aste, T., Tasca, P., & Di Matteo, T. (2017). Blockchain technologies: The foreseeable impact on society and industry. computer, 50(9), 18-28.

Azrour, M., Ouanan, M., & Farhaoui, Y. (2017). A new efficient SIP authentication and key agreement protocol based on chaotic maps and using smart card. *In Proceedings of the 2nd International Conference on Computing and Wireless Communication Systems* (pp. 1-8).

Barkadehi, M. H., Nilashi, M., Ibrahim, O., Fardi, A. Z., & Samad, S. (2018). Authentication systems: A literature review and classification. *Telematics and Informatics*, 35(5), 1491-1511.

Bayat, M., Pournaghi, M., Rahimi, M., & Barmshoory, M. (2020). NERA: A new and efficient RSU based authentication scheme for VANETs. *Wireless Networks*, 26(5), 3083-3098.

Baugher, M., McGrew, D., Naslund, M., Carrara, E., & Norrman, K. (2004). The secure real-time transport protocol (SRTP) (No. rfc3711).

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188-194.

Buterin, V. On public and private blockchains, Ethereum blog, 2015, https://blog. ethereum.org/2015/08/07/on-public-and-private-blockchains/, Alındığı Tarih: 14 Nisan 2022.

Carrara, G. R., Burle, L. M., Medeiros, D. S., de Albuquerque, C. V. N., & Mattos, D. M. (2020). Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. *Annals of Telecommunications*, 75(3), 163-174.

Castro, M., ve Liskov, B. (1999). Practical byzantine fault tolerance. *In Proc. 3rd USENIX Symp. Oper. Syst. Design Implement*. (OSDI), New Orleans, LA, USA, Feb. 1999, pp. 173–186.

Ch, R., Srivastava, G., Gadekallu, T. R., Maddikunta, P. K. R., & Bhattacharya, S. (2020). Security and privacy of UAV data using blockchain technology. *Journal of Information Security and Applications*, 55, 102670.

Chen, Y., Wang, Y., Wang, Y., Li, M., Dong, G., & Liu, C. (2021). CallChain: Identity Authentication Based on Blockchain for Telephony Networks. *In 2021 IEEE 24th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, (pp. 416-421). IEEE.

Comer, D. (2009). Computer networks and internets. Upper Saddle River, NJ: Pearson/Prentice Hall.

Cui, Z., Fei, X. U. E., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid blockchain-based identity authentication scheme for multi-WSN. *IEEE Transactions on Services Computing*, 13(2), 241-251.

Çölkesen, R., & Örencik, B. (2003). Bilgisayar haberleşmesi ve ağ teknolojileri. Papatya Yayıncılık.

Da Xu, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal, 8(13), 10452-10473.

Dai, H. N., Zheng, Z., & Zhang, Y. (2019). Blockchain for Internet of Things: A survey. *IEEE Internet of Things Journal*, 6(5), 8076-8094.

Dantu, R., Fahmy, S., Schulzrinne, H., & Cangussu, J. (2009). Issues and challenges in securing VoIP. *Computers & Security*, 28(8), 743-753.

Dhillon, P. K., & Kalra, S. (2019). Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things. *Multimedia Tools and Applications*, 78(16), 22199-22222.

Di Pierro, M. (2017). What is the blockchain?. Computing in Science & Engineering, vol. 19, no. 5, pp. 92–95, 2017, doi: 10.1109/MCSE.2017.3421554.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. IEEE transactions on knowledge and data engineering, 30(7), 1366-1385.

Eddine, M. S., Ferrag, M. A., Friha, O., & Maglaras, L. (2021). EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles. *Journal of Information Security and Applications*, 59, 102802.

Euchner, M. (2006). HMAC-Authenticated Diffie-Hellman for Multimedia Internet KEYing (MIKEY). RFC 4650, Eylül 2006.

Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. EURASIP Journal on Wireless Communications and Networking, 2020(1), 1-15.

Farash, M. S. (2016). Security analysis and enhancements of an improved authentication for session initiation protocol with provable security. *Peer-to-Peer Networking and Applications*, 9(1), 82-91.

Feng, M., & Xu, H. (2019). Msnet-blockchain: A new framework for securing mobile satellite communication network. *In 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, (pp. 1-9). IEEE.

Feng, Q., He, D., Zeadally, S., & Liang, K. (2019). BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks. *IEEE Transactions on Industrial Informatics*, 16(6), 4146-4155., doi: 10.1109/TII.2019.2948053.

Ferrag, M. A., Maglaras, L., Derhab, A., & Janicke, H. (2020). Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. *Telecommunication Systems*, 73(2), 317-348.

Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., & Stewart, L. (1999). RFC2617: HTTP authentication: basic and digest access authentication. Adres: http://www.rfc-editor.org/rfc/pdfrfc/rfc4648.txt.pdf.

Geneiatakis, D., Dagiuklas, T., Kambourakis, G., Lambrinoudakis, C., Gritzalis, S., Ehlert, K. S., & Sisalem, D. (2006). Survey of security vulnerabilities in session initiation protocol. *IEEE Communications Surveys & Tutorials*, 8(3), 68-81.

Geneiatakis, D., Lambrinoudakis, C., & Kambourakis, G. (2008). An ontology based-policy for deploying secure sip-based VoIP services. *Computer and Security*, 27(7–8), 285–297.

Glass, S., Hiller, T., Jacobs, S., & Perkins, C. (2000). Mobile IP authentication, authorization, and accounting requirements. *Work in Progress*. Erişim: https://www.hjp.at/doc/rfc/rfc2977.html.

Glissa, G., & Meddeb, A. (2019). 6LowPSec: An end-to-end security protocol for 6LoWPAN. *Ad Hoc Networks*, 82, 100-112.

Granville, L. Z., da Rosa, D. M., Panisson, A., Melchiors, C., Almeida, M. J. B., & Tarouco, L. M. R. (2005). Managing computer networks using peer-to-peer technologies. *IEEE Communications Magazine*, 43(10), 62-68.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, 169, 107094.

Guo, S., Hu, X., Guo, S., Qiu, X., & Qi, F. (2019). Blockchain meets edge computing: A distributed and trusted authentication system. *IEEE Transactions on Industrial Informatics*, 16(3), 1972-1983..

Gupta, B. B., & Prajapati, V. (2019). Secure and efficient session initiation protocol authentication scheme for VoIP communications. *In 2019 International Conference on Communication and Electronics Systems (ICCES)*, (pp. 866-871). IEEE.

Gupta, P., & Shmatikov, V. (2007). Security analysis of voice-over-ip protocols. *In 20th IEEE Computer Security Foundations Symposium (CSF'07) (pp. 49-63)*. IEEE.

Hammi, M. T., Bellot, P., & Serhrouchni, A. (2018). BCTrust: A decentralized authentication blockchain-based mechanism. *In 2018 IEEE wireless communications and networking conference (WCNC)*, (pp. 1-6), IEEE.

Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, 78, 126-142.

Han, D., Kim, H., & Jang, J. (2017). Blockchain based smart door lock system. *In 2017 International conference on information and communication technology convergence (ICTC)*, (pp. 1165-1167). IEEE.

Hellwagner, H., Kuschnig, R., Stütz, T., & Uhl, A. (2009). Efficient in-network adaptation of encrypted H. 264/SVC content. *Signal Processing: Image Communication*, 24(9), 740-758.

Hercog, D. (2020). Protocols RTP/RTCP. *In Communication Protocols* (pp. 343-344). Springer, Cham.

Hong, S. (2020). P2P networking based internet of things (IoT) sensor node authentication by Blockchain. *Peer-to-Peer Networking and Applications*, 13(2), 579-589.

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., & Bangash, Y. A. (2020). An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet of Things Journal*, 7(10), 10250-10276.

Irshad, A., Kumari, S., Li, X., Wu, F., Chaudhry, S. A., & Arshad, H. (2017). An improved SIP authentication scheme based on server-oriented biometric verification. *Wireless Personal Communications*, 97(2), 2145-2166.

Jan, M. A., Cai, J., Gao, X. C., Khan, F., Mastorakis, S., Usman, M., ... & Watters, P. (2021). Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges and future directions. *Journal of Network and Computer Applications*, 175, 102918.

Jayasinghe, U., Lee, G. M., MacDermott, Á., & Rhee, W. S. (2019). TrustChain: A privacy preserving blockchain with edge computing. *Wireless Communications and Mobile Computing*, 2019.

Jiang, Q., Ma, J., & Tian, Y. (2015). Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol of Zhang et al. *International Journal of Communication Systems*, 28(7), 1340-1351.

Kara, M., Aydin, M. A., & Balik, H. H. (2021). Bcvop2p: Decentralized Blockchain-Based Authentication Scheme for Secure Voice Communication. *Intelligent Automation and Soft Computing*, 31(3), 1901-1918.

Kara, M., Şanlıöz, Ş. G., Merzeh, H. R., Aydın, M. A., & Balık, H. H. (2021). Blockchain Based Mutual Authentication for VoIP Applications with Biometric Signatures. *In 2021 6th International Conference on Computer Science and Engineering (UBMK)*, (pp. 133-138). IEEE.

Keromytis, A. D. (2010). Voice-over-IP security: Research and practice. *IEEE Security & Privacy*, 8(2), 76-78.

Kfoury, E. F., & Khoury, D. J. (2018). Secure End-to-End VoIP System Based on Ethereum Blockchain. *Journal of Communication*, 13(8), 450-455., doi: 10.12720/jcm.13.8.450-455.

Khacef, K., & Pujolle, G. (2019). Secure Peer-to-Peer communication based on Blockchain. *In Workshops of the International Conference on Advanced Information Networking and Applications*, (pp. 662-672). Springer, Cham.

Khalid, U., Asim, M., Baker, T., Hung, P. C., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, 23(3), 2067-2087.

Kim, H., & Lee, E. A. (2017). Authentication and Authorization for the Internet of Things. *IT Professional*, 19(5), 27-33.

Kolahi, S. S., Mudaliar, K., Zhang, C., & Gu, Z. (2017). Impact of IPSec security on VoIP in different environments. *In 2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, (pp. 979-982). IEEE.

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10), 1027-1038.

Kumar, P., & Chouhan, L. (2021). A secure authentication scheme for IoT application in smart home. *Peer-to-Peer Networking and Applications*, 14(1), 420-438.

Kumari, S., Karuppiah, M., Das, A. K., Li, X., Wu, F., & Gupta, V. (2018). Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography. *Journal of Ambient Intelligence and Humanized Computing*, 9(3), 643-653.

Kurose, J. F., & Ross, K. W. (2012). Computer Networking: A Top-Down Approach, sixth ed., Addison-Wesley Educational Publishers, Boston.

Leach, P.; Mealling, M.; Salz, R. (2005). A Universally Unique IDentifier (UUID) URN Namespace. Internet Engineering Task Force. doi:10.17487/RFC4122. RFC 4122. Erişim: 17.01.2017.

Levi, A., & Güder, C. B. (2009). Understanding the limitations of S/MIME digital signatures for e-mails: A GUI based approach. *Computers & Security*, 28(3-4), 105-120.

Li, X., Niu, J., Bhuiyan, M. Z. A., Wu, F., Karuppiah, M., & Kumari, S. (2018). A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things. *IEEE Transactions on Industrial Informatics*, 14(8), 3599-3609.

Liao, Y. P., & Wang, S. S. (2010). A new secure password authenticated key agreement scheme for SIP using self-certified public keys on elliptic curves. *Computer Communications*, 33(3), 372-380.

Lin, C., He, D., Kumar, N., Huang, X., Vijayakumar, P., & Choo, K. K. R. (2019). HomeChain: A blockchain-based secure mutual authentication system for smart homes. *IEEE Internet of Things Journal*, 7(2), 818-829.

Liu, Y., He, D., Obaidat, M. S., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Blockchain-based identity management systems: A review. Journal of network and computer applications, 166, 102731.

Martin, M. V., & Hung, P. C. (2005). Towards a security policy for VoIP applications. *In Canadian Conference on Electrical and Computer Engineering*, 2005. (pp. 65-68). IEEE.

Migga Kizza, J. (2015). Guide to Computer Network Security. Springer London.

Minoli, D., & Occhiogrosso, B. (2018). Blockchain mechanisms for IoT security. *Internet of Things*, vol. 1–2, pp. 1–13, doi: 10.1016/j.iot.2018.05.002.

Mukherjee, A. (2015). Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE*, 103(10), 1747-1761.

Mukherjee, A., Fakoorian, S. A. A., Huang, J., & Swindlehurst, A. L. (2014). Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys & Tutorials*, 16(3), 1550-1573.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. D*ecentralized Business Review*, 21260.

Nikooghadam, M., & Amintoosi, H. (2020). A secure and robust elliptic curve cryptography-based mutual authentication scheme for session initiation protocol. *Security and Privacy*, 3(1), e92.

Ntantogian, C., Veroni, E., Karopoulos, G., & Xenakis, C. (2019). A survey of voice and communication protection solutions against wiretapping. *Computers & Electrical Engineering*, 77, 163-178.

Omote, K. (2020). A Decentralized Secure Email System based on Conventional RSA Signature. *In 2020 International Symposium on Information Theory and Its Applications (ISITA)*, (pp. 494-498). IEEE.

Otte, P., de Vos, M., & Pouwelse, J. (2020). TrustChain: A Sybil-resistant scalable blockchain. *Future Generation Computer Systems*, 107, 770-780.

Özbilen, A. (2006). Bilgisayar ağları ve güvenliği. Pusula yayınevi.

Park, A., & Li, H. (2021). The effect of blockchain technology on supply chain sustainability performances. *Sustainability*, 13(4), 1726. Erişim: https://doi.org/10.3390/su13041726

Patil, A. S., Hamza, R., Hassan, A., Jiang, N., Yan, H., & Li, J. (2020). Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. *Computers & Security*, 97, 101958.

Patwary, A. A. N., Fu, A., Battula, S. K., Naha, R. K., Garg, S., & Mahanti, A. (2020). FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain. *Computer Communications*, 162, 212-224.

Pecori, R., & Veltri, L. (2016). 3AKEP: Triple-authenticated key exchange protocol for peer-to-peer VoIP applications. *Computer Communications*, 85, 28-40.

Perez-Botero, D., & Donoso, Y. (2011). VoIP eavesdropping: A comprehensive evaluation of cryptographic countermeasures. *In 2011 Second International*

Conference on Networking and Distributed Computing (pp. 192-196). IEEE, doi: 10.1109/ICNDC.2011.46.

Qiu, S., Xu, G., Ahmad, H., & Guo, Y. (2018). An enhanced password authentication scheme for session initiation protocol with perfect forward secrecy. *PloS one*, 13(3), e0194072.

Rehman, U. U., & Abbasi, A. G. (2014). Security analysis of VoIP architecture for identifying SIP vulnerabilities. *In 2014 International Conference on Emerging Technologies (ICET)*, (pp. 87-93). IEEE.

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., et al. (2002). SIP: Session initiation protocol Internet Engineering Task Force, RFC 3261.

Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117-2135.

Salgarelli, L., Buddhikot, M., Garay, J., Patel, S., & Miller, S. (2003). Efficient authentication and key distribution in wireless IP networks. *IEEE Wireless Communications*, 10(6), 52-61.

Salman, T., Zolanvari, M., Erbad, A., Jain, R., & Samaka, M. (2018). Security services using blockchains: A state of the art survey. *IEEE Communications Surveys & Tutorials*, 21(1), 858-880.

Salsano, S., Veltri, L., & Papalilo, D. (2002). SIP security issues: the SIP authentication procedure and its processing load. *IEEE Network*, 16(6), 38-44.

Schulzrinne, H., Casmer, S., Frederick, R., & Jacobson, V. (2003). RTP: A transport protocol for real-time applications. *Internet Engineering Task Force*, RFC 3550.

Segeč, P., Moravčík, M., Hrabovský, J., Papán, J., & Uramová, J. (2017). Securing SIP infrastructures with PKI—The analysis. *In 2017 15th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, (pp. 1-8). IEEE.

Sheron, P. F., Sridhar, K. P., Baskar, S., & Shakeel, P. M. (2020). A decentralized scalable security framework for end-to-end authentication of future IoT communication. *Transactions on Emerging Telecommunications Technologies*, 31(12), e3815.

Singh, H. P., Singh, S., Singh, J., & Khan, S. A. (2014). VoIP: State of art for global connectivity—A critical review. *Journal of Network and Computer Applications*, 37, 365-379.

Sisalem, D., Liisberg, M., & Rebahi, Y. (2008). A Theoretical Model of the Effects of Losses and Delays on the Performance of SIP. *In IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference*, (pp. 1-6), IEEE.

Solomon, M. G., & Chapple, M. (2004). *Information Security Illuminated*. Jones & Bartlett Publishers.

Stallings, W. & Brown, L. (2018). Computer security: principles and practice. Upper Saddle River: 4th Edition, Pearson Education.

Stinson, D. R. & Paterson, M. (2018). Cryptography: Theory and Practice, *Fourth Edition*. Chapman and Hall/CRC.

Sukma, N., & Chokngamwong, R. (2017). One time key issuing for verification and detecting caller id spoofing attacks. *In 2017 14th International Joint Conference on Computer Science and Software Engineering (JCSSE)*, (pp. 1-4). IEEE.

Sureshkumar, V., Amin, R., & Anitha, R. (2018). A robust mutual authentication scheme for session initiation protocol with key establishment. *Peer-to-Peer Networking and Applications*, 11(5), 900-916.

Tanenbaum, A. S., & Wetherall, D. J. (2011). Computer networks fifth edition. In Pearson Education, Inc.. Prentice Hall.

Tanrıverdi, M., Uysal, M., & Üstündağ, M. T. (2019). Blokzinciri teknolojisi nedir? ne değildir?: alanyazın incelemesi. *Bilişim Teknolojileri Dergisi*, 12(3), 203-217.

Thermos, P., & Takanen, A. (2007). Securing VoIP networks: threats, vulnerabilities, and countermeasures. Pearson Education.

Trappe, W. (2006). Introduction to cryptography with coding theory. *Pearson Education India*.

Varshney, T., Sharma, N., Kaushik, I., & Bhushan, B. (2019). Authentication & encryption based security services in blockchain technology. *In 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, (pp. 63-68). IEEE.

Von Oheimb, D. (2005). The high-level protocol specification language HLPSL developed in the EU project AVISPA. *In Proceedings of APPSEM 2005 workshop* (pp. 1-17). Erişim: 01.06.2021, adres: http://www.davoh.de/cs/talks/AVISPA-HLPSL.pdf.

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014), 1-32.

Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., & Liu, Y. (2019). A survey on the scalability of blockchain systems. *IEEE Network*, 33(5), 166-173.

Xiong, H., Jin, C., Alazab, M., Yeh, K. H., Wang, H., Gadekallu, T. R. R., ... & Su, C. (2021). On the design of blockchain-based ECDSA with fault-tolerant batch verication protocol for blockchain-enabled IoMT. *IEEE Journal of Biomedical and Health Informatics*.

Xu, Y., Ren, J., Wang, G., Zhang, C., Yang, J., & Zhang, Y. (2019). A blockchain-based nonrepudiation network computing service scheme for industrial IoT. *IEEE Transactions on Industrial Informatics*, 15(6), 3632-3641.

Yang, Y., & Hanzo, L. (2021). Permutation-based TCP and UDP transmissions to improve goodput and latency in the Internet of Things. *IEEE Internet of Things Journal*, 8(18), 14276-14286.

Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. (2018). Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 6(2), 1495-1505.

Yeh, H. L., Chen, T. H., & Shih, W. K. (2013). Robust smart card secured authentication scheme on SIP using elliptic curve cryptography. *Computer Standards & Interfaces*, 36(2), 397-402.

Yen, D. C., Chou, D. C., & Wang, J. C. (2001). DSL: the promising standard for new Internet era. *Computer Standards & Interfaces*, 23(1), 29-37.

Yin, H., & Wang, H. (2007). Building an application-aware IPsec policy system. IEEE/ACM transactions on networking, 15(6), 1502-1513.

Yoon, E. J., Yoo, K. Y., Kim, C., Hong, Y. S., Jo, M., & Chen, H. H. (2010). A secure and efficient SIP authentication scheme for converged VoIP networks. *Computer Communications*, 33(14), 1674-1681.

Zhang, C., Zhu, L., Xu, C., Zhang, C., Sharif, K., Wu, H., & Westermann, H. (2020). BSFP: blockchain-enabled smart parking with fairness, reliability and privacy protection. *IEEE Transactions on Vehicular Technology*, 69(6), 6578-6591.

Zhang, H., Wang, J., & Ding, Y. (2019). Blockchain-based decentralized and secure keyless signature scheme for smart grid. *Energy*, 180, 955-967.

Zhang, L., Tang, S., & Zhu, S. (2016). An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks. *Journal of Network and Computer Applications*, 59, 126-133.

Zhang, R., Wang, X., Yang, X., & Jiang, X. (2010). On the billing vulnerabilities of SIP-based VoIP systems. *Computer Networks*, 54(11), 1837-1847.

Zhang, S., & Lee, J. H. (2020). Analysis of the main consensus protocols of blockchain. *ICT Express*, 6(2), 93-97.

Zhaofeng, M., Jialin, M., Jihui, W., & Zhiguang, S. (2020). Blockchain-based decentralized authentication modeling scheme in edge and IoT environment. *IEEE Internet of Things Journal*, 8(4), 2116-2123.

Zhong, H., Zhang, C., Xu, Y., & Liu, L. (2020). Authentication and Key Agreement Based on Anonymous Identity for Peer-to-Peer Cloud. *IEEE Transactions on Cloud Computing*.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : KARA Mustafa
Uyruğu : T.C.

Yayınlar

Kara, M., & Furat, M. (2016). Security threats for industrial control systems and a solution with DMZ. *In 1 st International Mediterranean Science and Engineering Congress*, (pp. 26-28).

Kara, M., & Furat, M. (2017). A New Intrusion Detection System Instead of Encryption for IoT Device Communication, *International Advanced Researches Engineering Congress-2017*, (pp. 1257-1263).

Tunuz, A., Kara, M., Furat, M. (2017). Challenges And Solutions for IoT Applications in the Iron and Steel. *International Conference on Engineering Technologies. Selçuk University.*

Kara, M. & Furat, M. (2018). Client-Server Based Authentication Against MITM Attack via Fast Communication for IIoT Devices. *Balkan Journal of Electrical and Computer Engineering*, 6(2), 88-93.

Şanlıöz, Ş., G., Kara, M., Aydın, M., A., Balık, H., H. (2019). Attack Detection of Web Phishing With Machine Learning Methods. *In 2019 International Conference on Information Security and Cryptology (ISC Turkey)*. IEEE.

Eksim, A., & Kara, M. (2019) Açık Kaynak İstihbaratı Üzerinden Siber Saldırı Tespiti Yöntemleri. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 7(1), 577-593.

Kara, M., Şanlıöz, Ş. G., Merzeh, H. R., Aydın, M. A., & Balık, H. H. (2021, September). Blockchain Based Mutual Authentication for VoIP Applications with Biometric Signatures. *In 2021 6th International Conference on Computer Science and Engineering (UBMK)*, (pp. 133-138). IEEE.

Merzeh, H. R. J., Kara, M., Aydın, M. A., & Balık, H. H. (2022). Secure Mutual Authentication Scheme for IoT Smart Home Environment using Biometric and Group Signature Verification Methods. 4th International Conference on Artificial

Intelligence and Applied Mathematics in Engineering (ICAIAME 2022), Azerbaijan Technical University.

Kara, M., Aydin, M. A., & Balik, H. H. (2021). Bcvop2p: Decentralized Blockchain-Based Authentication Scheme for Secure Voice Communication. *Intelligent Automation and Soft Computing*, 31(3), 1901-1918.

Merzeh, H. R. J., Kara, M., Aydin, M. A., & Balik, H. H. (2021). GDPR Compliance IoT Authentication Model for Smart Home Environment. *Intelligent Automation and Soft Computing*, 31(3), 1953-1970.

Proje

"Nesnelerin İnterneti Ekosistemi Güvenlik Test ve Değerlendirme", İstanbul Kalkınma Ajansı, İstanbul Üniversitesi-Cerrahpaşa Proje ve Teknoloji Ofisi, *Araştırmacı*, 2021.

Tezden Türetilen Yayınları/Sunumları

Kara, M., Şanlıöz, Ş. G., Merzeh, H. R., Aydın, M. A., & Balık, H. H. (2021, September). Blockchain Based Mutual Authentication for VoIP Applications with Biometric Signatures. In 2021 6th International Conference on Computer Science and Engineering (UBMK) (pp. 133-138). IEEE.

Kara, M., Aydin, M. A., & Balik, H. H. (2021). Bcvop2p: Decentralized Blockchain-Based Authentication Scheme for Secure Voice Communication. Intelligent Automation and Soft Computing, 31(3), 1901-1918.