Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2022.021309
Article

Tech Science Press

Bcvop2p: Decentralized Blockchain-Based Authentication Scheme for Secure Voice Communication

Mustafa Kara[1,*], Muhammed Ali Aydın[1,2] and Hasan Hüseyin Balık[1]

[1]Hezarfen ASTIN Computer Engineering Department, National Defense University, Istanbul, 34000, Turkey
[2] Faculty of Engineering, Istanbul University-Cerrahpasa, Istanbul, 34320, Turkey
*Corresponding Author: Mustafa Kara. Email: mkara@hho.msu.edu.tr
Received: 28 June 2021; Accepted: 29 July 2021

Abstract: Peer-to-peer VoIP applications are exposed to threats in the Internet environment as they carry out conversations over the Internet, which is an electronic communication line, and its security has always been largely a matter of concern. Authentication of the caller is the first line of defense among the security principles and is an important principle to provide security in VoIP application. Authentication methods in VoIP applications are usually based on trusted third parties or through centralized architecture. This situation creates problems in terms of single point of failure and privacy in call security over IP based communications. However, blockchain technology with a distributed architecture offers an innovative solution to multimedia communication authentication model. In this paper, a blockchain-based mutual authentication scheme for VoIP applications is proposed. In addition, the model's having a comprehensive security structure against various threats is explained via security and communication cost analysis. The proposed schema shows better performance than the methods that make a verification through the centralized architecture in the literature. The proposed model has been formally verified using the AVISPA tool, and it has been proven that the model is safe against potential threats.

Keywords: Blockchain; secure voice communication; authentication; VoIP

1 Introduction

Thanks to the routing function of the Internet Protocol (IP), this protocol is widely used in security systems, camera systems, communication systems and many other system infrastructures. Voice over Internet Protocol (VoIP), built on the IP protocol infrastructure, is a technology that has increased rapidly in recent years and basically allows phone calls. The most important reason for this increase is that VoIP applications provide high performance and their cost efficiency and low cost, besides scalability. VoIP technology is an important part of the communication infrastructure. Phone calls can be made over any internet-connected device, phone or computer, on which the relevant software has been installed thanks to VoIP technology. This system, on which VoIP software is installed in the VoIP application, is called an IP phone and is a telephone service provided entirely over the internet protocol infrastructure [1]. Compared

to traditional telephone systems such as Public Switched telephone network (PSTN), VoIP offers an infrastructure that offers low-cost, flexible, scalable and comfortable communication technology. However, since the VoIP system makes calls over the internet, which is an electronic communication line, all possible attack models in the internet environment are valid for VoIP [2].

Confidentiality, integrity, availability, non-repudiation, access control and authentication should be provided as a whole for secure conversation [3]. However, authentication and authorization are the first requirements in this security system. In Internet Multimedia Communication systems, including VoIP, user and device authentication is required before authorization. Because caller ID information can be spoofed in a call and used as an attack on VoIP communication infrastructure. If the identity of the caller and the callee is not authenticated, their identity can be spoofed [4]. This situation causes issues such as managing, changing and cancelling communication through attacks such as replay attack and Man in the middle attack (MITM). In this respect, the security of the layer where the real audio data is transmitted (media session) mainly depends on the secrecy of the session keys and the authentication of the session participants [5]. Authentication is used by the caller when the caller needs to know that the caller is the person they claim to be [6]. For a secure communication, both the caller and the IP phone device at the endpoint must share their identity with the caller over a secure channel. If this verification process takes place on the basis of both the device and the person, the first line of security is provided as a whole.

Two standard protocols are generally used in VoIP infrastructure. Session Initiation Protocol (SIP) protocol establishes the connection between two devices by transmitting contact, message information (call initiation and ending) and important information that will affect the call [7]. This can be from phone to phone or from phone to a device in the VoIP system. After the SIP protocol establishes the peer-to-peer connection, Real time Transport Protocol (RTP) protocol is used to transport audio and video data. However, if SIP and RTP protocols are transmitted as standard without security measures, it creates a major security problem [4,8]. SIP messages and RTP streams can be listened or changed by being intercepted easily by an attacker with basic network knowledge. In this respect, VoIP applications have been made more secure by supporting RTP and SIP protocols with certain protocols. Authentication is provided by the combination of many new protocols and working specific technologies. However, many of these studies contain deficiencies at certain points in terms of flexibility and scalability. In addition, many of these studies are basically based on a centralized and reliable third party. At this point, blockchain technology is promising in terms of transparent verification, which is different from the centralized structure with its distributed architecture that is prone to authentication. Blockchain technology is an innovative technology that overcomes many threats in authentication and is used for authentication in many areas [9,10]. Establishing a security relationship in P2P VoIP applications creates a suitable network for securing media communication over an unsecured public channel. It also provides a safer environment in terms of privacy and confidentiality.

In the proposed architecture, the verification of the IP phone devices at the endpoints is carried out over the blockchain network. In this study, it is aimed to make direct peer-to-peer (P2P) authentication before voice data transmission for IP-based phone calls in VoIP applications. Within the created architecture, a blockchain-based search network is created that provides completely secure VoIP communication over the decentralized network. It also implements sensitive transactions transparently in a distributed structure while providing a high level of security. This method eliminates the need for trusted intermediaries (trusted third party) [11]. This prevents the single-point failure error that occurs with key distribution in the central structure (certified authority). The blockchain is accessible to all network nodes and keeps track of all transactions that have already been made. Thus, it provides the non-repudiation feature in the interviews, making the structure more secure and reliable [12,13]. It is a database that will establish the necessary environment for the blockchain technology Public Key Infrastructure (PKI) infrastructure, which includes Smart Contracts, Consensus Algorithms and distributed modeling technologies in general.

The aim of this study presents a mutual authentication scheme over the blockchain network for secure key distribution just before the multimedia communication of P2P VoIP applications. The main contributions of the study are summarized as follows:

1. It creates a blockchain-based peer-to-peer secure communication environment that aims to authenticate VoIP applications through a completely decentralized architecture. A compatible environment for secure voice communication is created by providing decentralized blockchain-based authentication.
2. Among the devices in the proposed scheme, Elliptic Curve Cryptography (ECC) asymmetric encryption algorithm is used to generate key pairs to gain speed and key size. In addition, including Distributed Denial of Service (DDoS) attack, replay attack, sybil attack, man-in-the-middle attack, substitution attack and spoofing attack, robustness against cyber-attacks is analyzed. In P2P VoIP application, the study presented the model's superiorities by comparing with the models that perform authentication over the centralized architecture.
3. The proposed model is a new generation authentication model that enhances the digital experience of VoIP application users by embodying cost efficiency, convenience and trust. The study is provided a comprehensive security analysis using the AVISPA tool to prove that the proposed scheme achieves privacy, integrity and sustainability.

2 Related Works

Since Internet users widely use IP-based communication services, mutual authentication between users is an important issue. SIP, one of the protocols basically used by VoIP applications, is a protocol that controls multimedia communication sessions, and authentication in VoIP applications is generally performed over the SIP protocol [14]. SIP protocol needs SIP server. Since SIP is a text-based protocol, a potential attacker can easily listen to all communication and change the content. However, SIP Signaling protocol uses methods like Basic Authentication, Digest Authentication, Pretty Good Privacy (PGP), Secure/Multipurpose Internet Mail Extensions (S/MIME) and SIP Secure (TLS) [15]. However, these methods, which take place only over the SIP protocol, are insufficient on their own.

The SIP authentication scheme initially used basic and digest authentication methods just before the mutual telephone conversation over the IP phone. However, since basic authentication is plain text, it can be intercepted or modified. Digest authentication does not provide integrity and confidentiality. It needs a shared key over the previously secure channel. They are also vulnerable to offline password guessing attacks and server spoofing attacks [16]. If authentication takes place over the SIP protocol, a possible attack on this server will affect the system and create an insecure communication environment. As a result of this situation, various authentication schemes for SIP protocol are suggested in the literature to create more secure methods [4,17,18]. Another method, S/MIME, encrypts only the Session Description Protocol (SDP) content of the SIP message and the header is transmitted unencrypted. This does not make authentication completely secure. The S/MIME protocol implemented over the SIP protocol provides end-to-end confidentiality, authentication and integrity. However, there is a dependency on PKI [19].

Authentication methods in traditional VoIP architecture usually consist of first key distribution (pre-shared secret key) or protocols based on central authority. However, this method is quite laborious and time-consuming. Instead, Transport Layer Security (TLS) is used for authentication, which works in the transport layer. However, TLS protocol provides a continuous end-to-end (hop by hop) security between two ends during packet forwarding [20]. In this case, the weakness in any of the hops or the fact that it does not use the TLS infrastructure makes the TLS protocol insufficient. Performing the verification

process entirely over the SIP protocol is provided by a third party or by key distribution with the certificate authority. This situation causes non-repudiation feature, loss of privacy and single point of failure.

MIKEY, SDES and ZRTP protocols, which are used before media data transfer via RTP protocol on the media transmission side, also need authentication since they are key distribution protocols [7]. In this respect, MIKEY and SDES protocols use TLS-based authentication method. The ZRTP protocol, on the other hand, uses a different key authentication method, the Short Authentication String (SAS). The SAS method is used to validate the Diffie-Hellman Key Exchange method [5]. This method, which is carried out by the caller and the called spouses, by reading a hash value directly to each other, creates an environment for voice forgery attacks for two people who do not know each other at all. It also contains vulnerabilities against MITM attacks [21].

In general, the use of blockchain is an ever-growing distributed list of records in blocks that connect devices on the network using cryptographic infrastructure and provide transparent security. It supports decentralized structure with smart contracts. For example [9,11] simplifies the authentication of the network by using a blockchain network.

In summary, when the blockchain-based studies in the literature are examined, it is seen that it is an anonymous, transparent and distributed architecture that eliminates the need for a centralized system. Studies using blockchain technology bring specific solutions for end-to-end security. Considering the studies examined, blockchain is becoming more and more common in technologies such as Internet of Things (IoT), Wireless Sensor Networks (WSN) and Smart Grid [22]. However, most systems still basically start with a centralized approach and propose regionally distributed and decentralized structures. When the literature is examined, a constructive solution has not yet been brought to the blockchain technology for secure authentication in VoIP applications.

3 System Architecture

In this study, a blockchain-based authentication architecture is designed without the need for centralized model. With this decentralized authentication and authorization mechanism, an end-to-end secure communication structure is established over the IP network before multimedia data transfer.

Authentication does not determine what tasks a person can do or what files they can see. Authentication only identifies and verifies who the person or system is. In this respect, the recommended system is to authenticate before the end-to-end connection for VoIP call security. Thus, encrypted keys that change dynamically on a conversation basis can be obtained. Any device that is not registered to the blockchain in the proposed system architecture is considered a malicious device. In addition, end-to-end authentication is carried out over smart contracts using the public blockchain within the architecture. Instead of using the private blockchain, the public blockchain is preferred to ensure scalability of the system. For VoIP communication, the structure can be used in an open, flexible and scalable manner. The verification process is carried out transparently with the blockchain, and flow control is ensured, thus providing a secure and undeniable communication structure.

The process, which is called a transaction, must be verified by the blockchain for each conversation that is desired to be made. For example, if caller wants to have a conversation with callee, he or she must make a request to the blockchain with the token certificate given to her by the blockchain structure during his/her registration to the blockchain. If the blockchain network verifies the contents of the certificate, the transaction is validated. In conclusion VoIP calling takes place over the IP network. Fig. 1 presents the system architecture by showing the whole structure together.

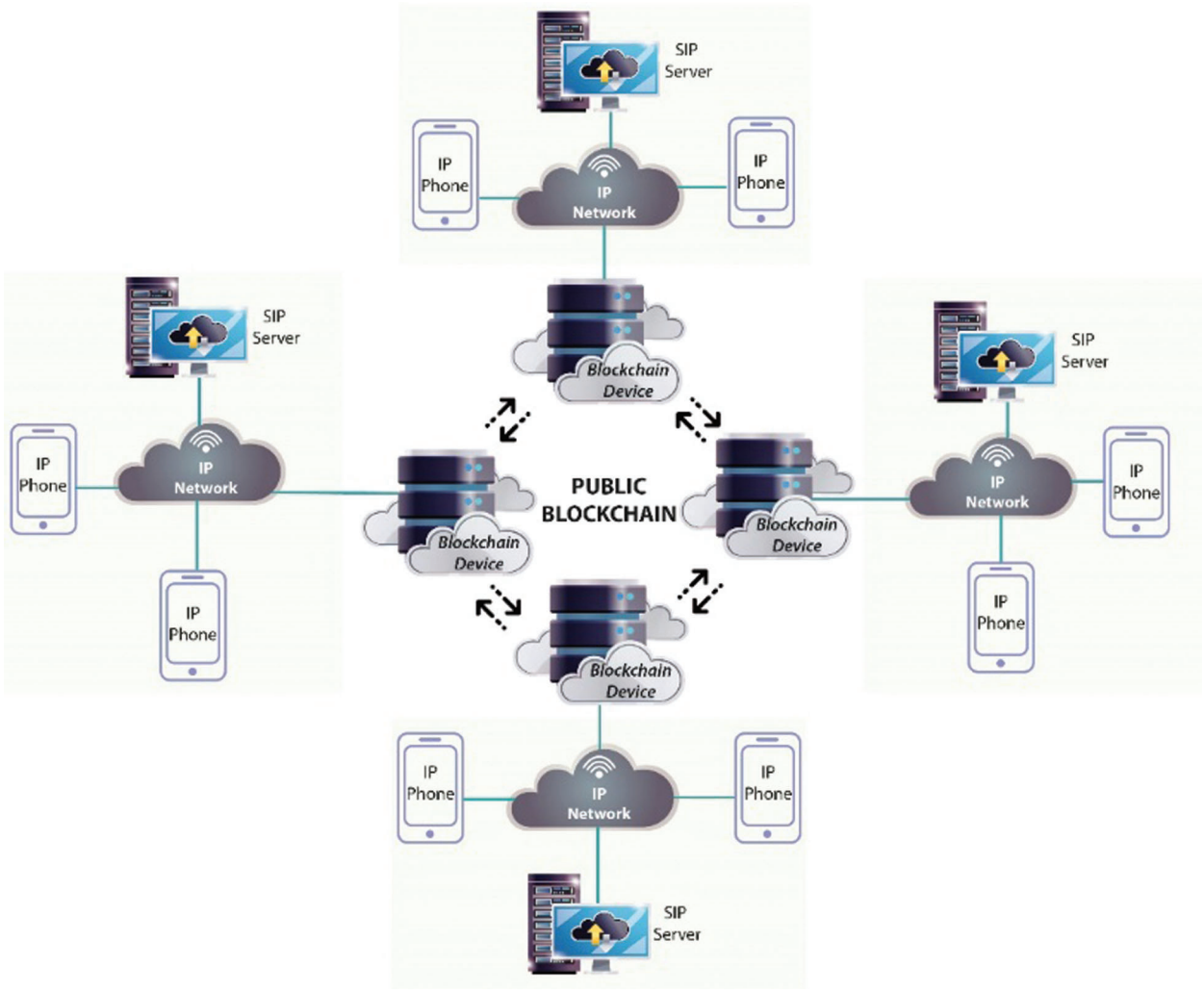

Figure 1: System architecture

4 The Proposed Scheme

The overall process of the proposed scheme for secure communication can be classified into four stages. In the first step, all registration processes are explained in detail. After SIP registration, the devices register to the blockchain network and blockchain-based endpoint device verification will take place. Next, the steps consist of SIP Invite phase over SIP Server, authentication phase over Blockchain, and Peer-to-Peer Media Session Phase.

4.1 System's Functioning

SIP registration is the first step of the phone call in VoIP application. After the SIP server authenticates the IP phone, it saves the contact information in the database. A 200 OK response containing the contact addresses of other devices is sent to the user and the registration process is completed. The authentication here is used entirely for the SIP registration process and is completely independent of the structure in the proposed model. Registration of the IP phone device to the SIP server over port 5060 takes place periodically. This periodic process takes place in order to check the registration status of the SIP servers

that will transmit Invite Packets and the endpoint IP Phones to be contacted. The registration process is generally as shown in Fig. 2.

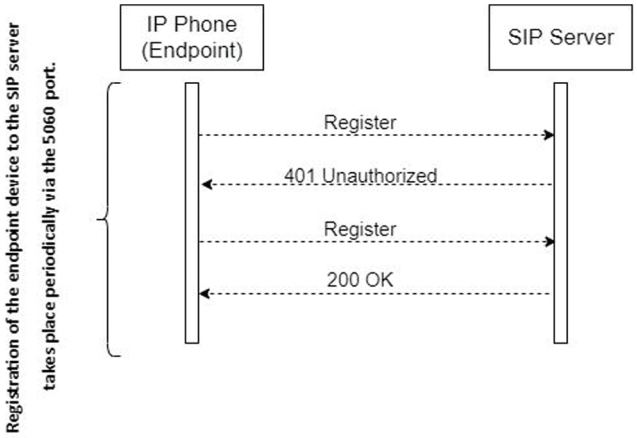

Figure 2: SIP registration phase

Authentication, which is the first step of the security infrastructure, must be performed so that the IP phone at the endpoint can communicate securely from end to end. In this respect, the 5 steps in the proposed architecture for end-to-end communication should be applied in the Media Session Phase. After the SIP registration, the IP phone at the endpoint performs the second registration stage, the blockchain registration. If the IP phone is going to make calls over the secure channel, it must be registered with the SIP server and the blockchain network beforehand. During the blockchain registration, the certificate named Token is generated by the blockchain device and sent to the IP phone. The IP phone will perform pre-call authentication with this token certificate. This scenario is explained in detail in Section 4.2.2.

SIP server works on request-response model. For this reason, the SIP server establishes and manages the incoming call requests and media sessions over IP. In VoIP architecture, the call process cannot initiate directly between two endpoint IP telephony devices. The Caller initiates the call by sending to the Callee an Invite packet. Assuming that a user with phone number 10 as the caller is calling a person with IP phone number 11, IP phone 10 does not know the IP address of phone 11. However, it knows the IP address of the SIP server it is registered with. The Caller IP phone will request a call to the SIP server for the number to call. When sending the call request, the called IP phone @ SIP server IP address (similar to 11@10.10.10.1) creates a SIP URI header. The body of the Invitation request carries an SDP message that provides the parameters (codec, IP address, port) the called party will need to send the RTP stream to the caller. The SIP server answers and sends the call invitation request to the target phone. Fig. 3 illustrates the SIP Invite phase.

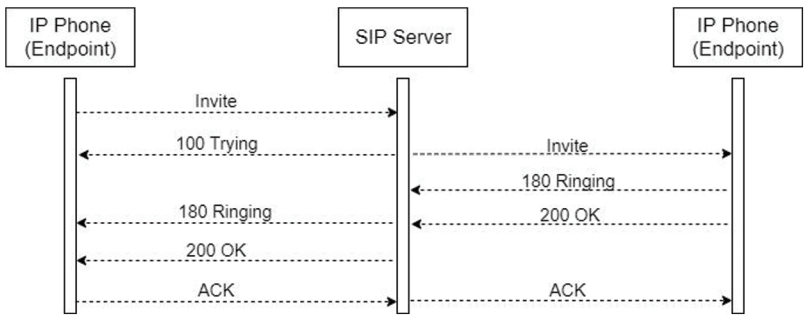

Figure 3: SIP invite phase

After SIP registration, Blockchain registration and SIP Invite realization, a suitable environment is created for starting a conversation over the RTP protocol. However, just before the meeting, a decentralized authentication is carried out over the blockchain in the proposed architecture. The schematic diagram of the proposed model, where all the steps are explained in this section, is shown in detail in Fig. 4.

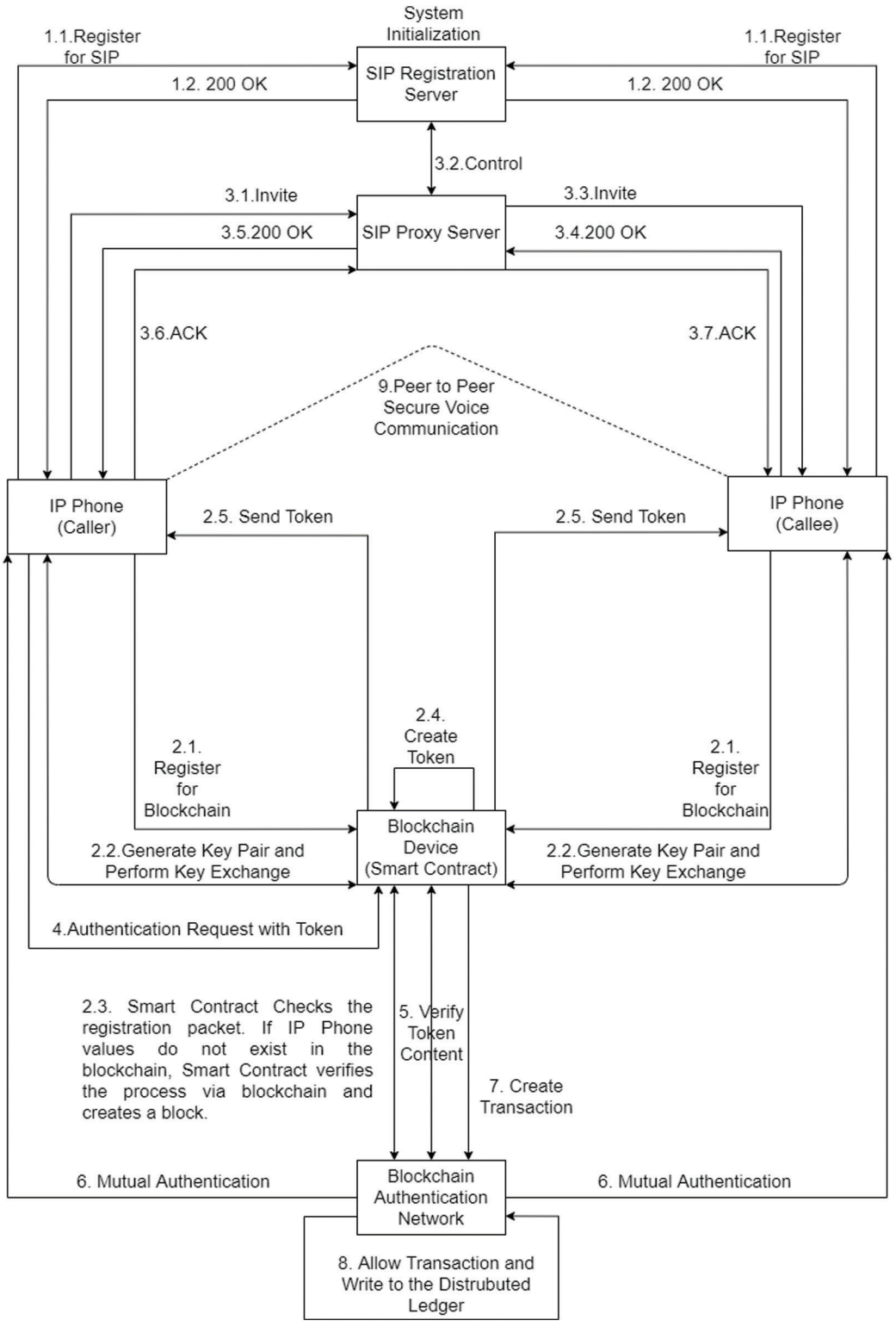

Figure 4: Schematic diagram of the proposed model

After completing the registration phases on both the blockchain side and the SIP server side, the endpoint IP phone device that sends the call request to the relevant phone over the IP network has to perform the authentication in the blockchain infrastructure. During the blockchain registration, the IP phone sends the Token certificate sent to it by the blockchain device to the relevant blockchain device. The blockchain device that signs this Token certificate with its private key validates the Token Certificate by making the necessary value comparisons. However, the authentication of the content in the Token Certificate takes place in a decentralized model by the blockchain network. This scenario is explained in detail in Section 4.2.3.

RTP is an internet protocol used to manage real-time transmission over unidirectional and multicast services. After the communication infrastructure is verified, the voice data is transmitted mutually with the RTP protocol. The SRTP protocol encrypts conversations with AES symmetric encryption. The session key is shared with each other when the authentication is completed. For this reason, conversations are carried out securely during the conversation.

4.2 Endpoint Device Authentication

In this section, the registration of the endpoint device in VoIP Application to the blockchain network and the decentralized authentication phase of the proposed architecture are explained in detail.

4.2.1 Assumptions

Before moving on to the proposed mechanism, it is necessary to explain some assumptions in items:

Each IP phone has a Global System for Mobile Communications (GSM) number to be used in sending Short Message Service (SMS).

The study accepts that blockchain devices are legitimate and non-aggressive.

The working mechanism of the proposed scheme starts when the blockchain device receives a request for registration. Once the received request is broadcasted and approved on the blockchain network, the necessary procedures are completed.

4.2.2 Blockchain Registration Phase

If the IP phone is going to make calls from the authenticated channel, it has to be registered in the blockchain system. Devices that are not registered to the blockchain network cannot be authorized within this network. In short, IP phones cannot communicate securely with any IP phone that is not registered in the blockchain.

Step 1: ID Generation

The endpoint IP telephony device first generates a unique ID value (UID). For generated unique ID values, the study uses UUID version 5 in accordance with RFC 4122 using Universally Unique ID (UUID) with 128-bit Length [23].

Step 2: Public Private Key Pairs Generation

Both the IP phone and the blockchain device generate the public/private key pairs using the ECC public-key cryptography method. With asymmetric encryption, the signature is irreversible. Also, it cannot be copied by any method.

PKuser = Public Key of IP Telephone

SKuser = Private Key of IP Telephone

PKbc = Public Key of Blockchain Device

SKbc = Private Key of Blockchain Device

Step 3: Distribution of Public Key for Authentication

In the proposed architecture, public key distribution will occur once and reciprocally between the endpoint IP telephony device and the blockchain device. Secure communication between two communication devices with a digital signature is achieved after the public key exchange takes place. Because the identities of both parties can be verified through digital signature.

Step 3.1. The IP phone sends a registration request to the blockchain. For this request, it sends the GSM number to the blockchain device over the unsecured channel (public channel).

Step 3.2. The blockchain device creates a Nonce value. This Nonce value is called the registration code (Registration Code, RCode). This RCode is valid for a maximum of 2 min. For this reason, a timestamp is created (z1). RCode value and timestamp (z1) are sent to IP phone over GSM channel.

Step 3.3. The IP phone uses the RCode value it receives and creates a transaction for this transmission (T1). A timestamp check is performed before processing.

$\Delta z = z2 - z1 \geq 2$. minutes transaction is invalid.

If $\Delta z \leq 2$ minutes;

If the timestamp is valid, the SHA-256 hashing algorithm and the endpoint IP phone device's public key PKuser and the RCode value from the blockchain device are concatenated and hash the resulting value. It adds the IP phone's public key (PKuser) to this digest and sends it to the blockchain device over the public channel.

T1 = (PKuser + SHA (PKuser ‖ RCode))

Step 3.4. When the T1 transaction arrives on the blockchain device, the RCode value in the blockchain and the IP phone public key (PKuser) is digested with the SHA-256 hash algorithm. If the hash values with T1 and the newly created hash values are equal, the public key of the IP phone is verified by the blockchain device. Using the IP phone's public key (PKuser), the blockchain device public key (PKbc), the blockchain device ID value (BID), and the BID and RCode are combined (concentination) after hashing over the SHA-256 hash algorithm and encrypted. The T2 transaction is sent to the IP phone over the public channel.

T2 = PKuser (PKbc + BID + SHA (BID ‖ RCode))

Step 3.5. The T2 transaction is extracted with the IP phone's private key (SKuser). The public key of the blockchain device (PKbc), the blockchain ID value (BID), and the RCode and hash of the BID are obtained. The content of the incoming packet is verified by creating the hash value of the BID value with the RCode value that was previously received by the IP phone. In this way, secure key exchange takes place.

Step 4: Registration Process

Step 4.1. In this step, transaction T3 is created to be sent to the blockchain network for registration of endpoint IP phone values. Also, a timestamp is created (z3). The IP phone's ID value (UID) and SIPURI address are combined and signed with the IP phone's private key (SKuser). This signature is encrypted with the public key (PKbc) of the blockchain device.

$\Delta z = z4 - z3 \geq 2$ minutes transaction is invalid.

$\Delta z \leq 2$ minutes;

T3= PKbc (SKuser(UID ‖ SIPURI Address ‖ z3))

Step 4.2. On the blockchain device, the timestamp is first checked over the smart contract. If the timeout occurs, the transaction is cancelled. If the timestamp is confirmed, the IP phone's SIPURI address and ID value (UID) is checked if it was previously registered in the blockchain network. If any of the values has already registered to the blockchain network, the transaction is invalid and the registration is terminated.

Step 4.3. If the values are checked in the blockchain network and it is confirmed that they have not been registered before, the smart contract allows the registration process. The UID Value, SIPURI address and public key of the IP phone are stored in the blockchain. It also creates a new block with the name of a validation map (MapAddress) with the UID Value, the SIPURI address and the public key of the IP phone. This block endpoint is used as the authentication map of the IP phone. The MapAddress block is broadcasted to other blockchain devices in the blockchain network.

Step 5: Token Certificate

Step 5.1. If the IP phone is successfully registered with the blockchain, the blockchain device issues an authentication certificate for the IP phone. This certificate is referred to as Token. The T4 transaction is created by combining the UID value of the IP phone device and the private key of the blockchain device, which has been digested with the SHA-256 hashing algorithm, the SIP URI address, the ID value (UID) and the private key of the blockchain (SKbc). This transaction is sent to the endpoint IP telephony device. The T4 transaction is encrypted with the private key of the blockchain device (PKbc). For this reason, the Token certificate can only authenticate and unlock the blockchain device. For token certificate transmission, T4 transaction is sent to IP phone via public channel.

SKuser(PKuser(PKbc(SHA(UID ‖ SKbc) + SIPURI Address + UID+ PKuser)))

Step 5.2. The endpoint IP phone unpacks its private key and obtains the Token certificate.

SKuser(PKuser(PKbc(SHA(UID ‖ SKbc) + SIPURI Address + UID+ PKuser)))

= PKbc(SHA(UID ‖ SKbc) + SIPURI Address + UID+ PKuser) => TOKEN

The IP phone device that will make the call will send the Token, which is the authentication certificate, to the blockchain device for verification before the call. The blockchain registration process in the proposed architecture is shown in Fig. 5 generally.

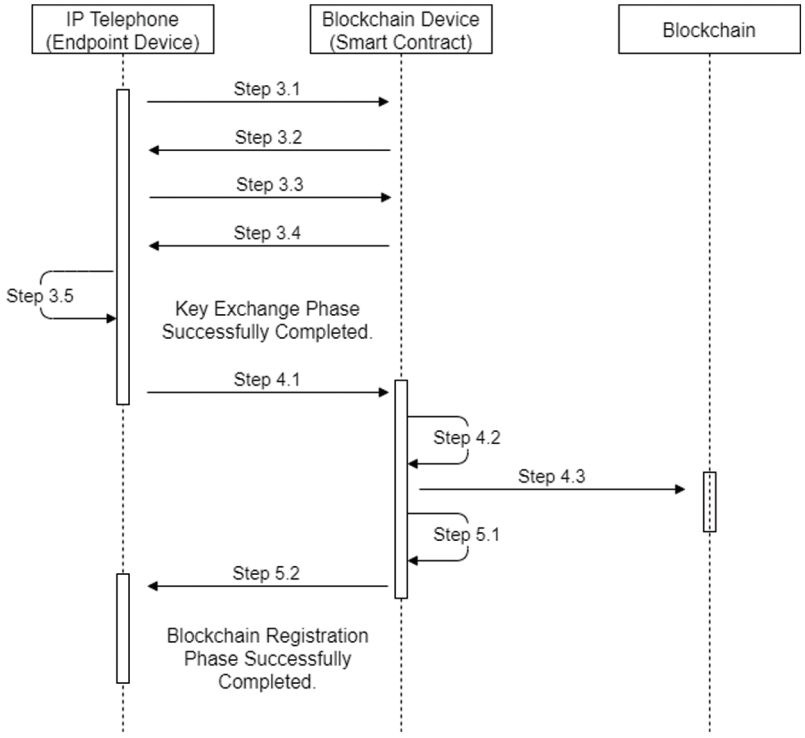

Figure 5: Blockchain registration phase of the proposed model

4.2.3 Blockchain Authentication Phase

At this stage, authorized VoIP application devices with Token certificate can join the network. If the endpoint IP phone is registered to the blockchain, it applies to the relevant blockchain device in the network with the token certificate it has obtained. The blockchain device simply checks whether this certificate was sent with its own signature. The verification process takes place entirely on the blockchain. Authentication is completed if the token certificate is approved after being broadcast on the blockchain and checked by devices on the network. With no central authority in between, the authenticated IP phone device communicates confidently that the phone it's calling is the right person. The following steps describes this authentication process for the system authentication phase in order.

Step 1: The calling IP phone device requests authentication to the blockchain device by signing its own Token certificate and the SIPURI address of the calling IP Phone device with its private key (SKuser). The caller IP phone creates the T5 transaction and sends it to the corresponding blockchain device.

T5= SKuser(Token ‖ Callee SIPURI Address)

Step 2: The blockchain device decrypts the incoming T5 transaction with the IP phone's public key (PKuser). The package contains the Token certificate and the searched SIPURI address.

PKuser(SKuser(Token ‖ Callee SIPURI Address))

The blockchain device checks the validity of the self-signed Token certificate and extracts the certificate content with its private key.

Skbc(PKbc(SHA(UID ‖ SKbc)+SIPURI Address+UID+ PKuser))

= Hash Value, SIPURI Address, UID, PKuser

Step 3: It takes the hash of its private key and the incoming UID value with the SHA-256 hash algorithm and compares the hash values obtained from the certificate. If the hash value is verified, Token integrity is verified and moves on to the next step.

Step 4: Here, the smart contract validates its UID on the blockchain network. For the verification process, the answer comes in the blockchain network. If the UID value does not exist in the blockchain network, the authentication is not validated. If the UID is confirmed in the blockchain, the next step is taken.

Step 5: Searched and Seeking SIPURI addresses are verified on the blockchain network. If both SIPURI addresses are verified, the next step is taken. Otherwise, the verification is canceled.

Step 6: The Smart Contract creates a map address (MapAddress) with SIPURI address, UID and PKuser values and validates this MapAddress value on the blockchain. Otherwise, the session will not continue and authentication will not occur.

Step 7: After all the steps are verified on the blockchain, the smart contract allows the transaction and creates and sends a MapAddress to the blockchain network that there is a conversation between SIPURI addresses.

Create_MapAddress(Caller SIPURI Address, Callee SIPURI Address)

The blockchain-based decentralized end-to-end authentication step is completed as shown in Fig. 6.

5 Secure Performance Analysis and Formal Verification

In this section, the study first analyzes the security of the proposed method by examining its robustness against different attacks and features. Next, the AVISPA tool formally proves the security of the proposed model. In addition, performance analysis is evaluated over communication and calculation costs, and its superior aspects are revealed compared to studies in the literature.

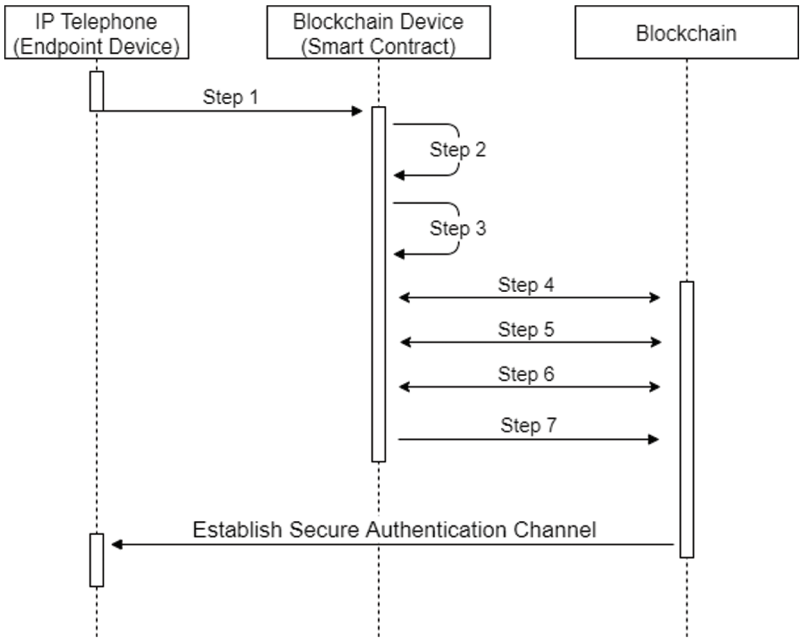

Figure 6: Authentication of IP telephone device on blockchain network

5.1 Informal Security Analysis

Security principles must be provided for a secure conversation over the IP network. In VoIP applications, the security infrastructure is brought together to provide full protection against attacks on the public network during multimedia data transmission over the IP network. In this section, security concerns will be analyzed within the proposed scheme for decentralized end-to-end secure communication. Then, the secure communication structure provided by the proposed scheme on the authentication side will be examined according to each attack model. Thus, the effective aspects of our study are revealed. In general, the security infrastructure for secure voice communication includes integrity, confidentiality, availability and authentication mechanisms, respectively.

1. **Confidentiality:** Confidentiality is ensured by preventing unauthorized access to devices and transmitted voice data content in VoIP applications. A common approach to ensuring confidentiality is to encrypt and decrypt media data transmission between authenticated users. During the registration to the blockchain network, the ID value of the endpoint IP phone is never transmitted over the insecure channel before the key exchange takes place. During the first registration, secure communication is realized by encrypting the ID value. The proposed blockchain-based model does not require the use of Public Key Infrastructure (PKI), which is an expensive solution for key distribution. Key distribution is faster and less costly. Public keys distributed over the blockchain, once published and verified, cannot be changed again. Confidentiality for communication between then authenticated users is provided via key pairs generated by asymmetric encryption methods.
2. **Integrity:** The Integrity security principle consists of two parts. Data Integrity and Message Integrity. Access and modification of stored data by an unauthorized user is called an attack for data integrity. Changing the transferred data by the attacker threatens the message integrity status. The hashing algorithms used are over SHA-256. In this way, the integrity of the information sent via the public channel is ensured. An example of this is that during the initial key distribution, the device that shares its public key with the blockchain device sends the RCode value by

hashing it with its public key. In addition, thanks to the Blockchain network, the integrity of each transaction once submitted, cannot be changed again. It is guaranteed by blockchain technology within the Message Integrity authentication scheme. On the other hand, in terms of Data Integrity, the data is sent by signing with a private key in the proposed structure. Since the blockchain (Ethereum) uses ECDSA technology, Data Integrity is easily provided. With the 256-bit Hash Algorithm, integrity control can be provided on the receiver side, as the data is hashed in the recording phase and transferred over the insecure channel.

3. **Availability:** Availability means that legitimate users or communication device can easily access the VoIP system in the proposed system. The sustainability of the structure has been ensured by using an end-to-end, that is, decentralized structure with the public blockchain against DDoS-like attacks. In addition, the "Single Point of Failure" error is eliminated thanks to the distributed architecture of the blockchain network.
4. **Non-Repudiation:** In the proposed model, users cannot deny the transaction thanks to the digital signature method used over the secure key exchange between the endpoint IP phone and the blockchain device. In addition, each checked transaction is confirmed by validating values within the blockchain. The transaction is recorded in the system to not be deleted in the blockchain network. Once the block is created and the transaction is confirmed and written to the Distributed Ledger, it will not be worthwhile if the 51 percent number is not reached even if changes are made on the ledgers. The message sent or the conversation made is published by creating MapAddrees transparently in the network and can never be denied.
5. **Mutual Authentication:** Each user registered to the system with a unique ID receives a "Token" certificate. This certificate is signed with the private key of the corresponding blockchain device in the blockchain. If the user does not have this certificate, authentication cannot occur. The token value is distributed to be stored on the endpoint device as a certificate signed with the private key of the relevant blockchain device to be used in each authentication process. The caller and the callee who will make the communication must have a valid token registered in the blockchain infrastructure. In this respect, mutual authentication, which is the first and important step of secure communication, is provided within the proposed scheme by creating map addresses in the blockchain network during registration and saving the values to the network in an unchangeable way. In addition, even during the first registration using a digital signature during the public key exchange, the IP phone and blockchain device, mutual authentication process takes place.
6. **Identification:** Each device is registered to the system with a unique ID (Hash Value of Device MAC Address). In the proposed model, transmission is not performed over the insecure channel unless the ID value is encrypted. After the secure key distribution, it is sent to the relevant blockchain for registration. Smart contracts control the ID of the endpoint IP phone device in the blockchain network. If it has not been registered before, it is registered with this ID value. The ID value, which is very difficult to obtain in this way, is associated with a Token certificate specific to the ID value of the blockchain system. In the authentication phase, device identification is easily performed over the ID value.
7. **Scalability:** is the situation in which users of a system want to perform an action at the same time, but fulfill these requests. In a blockchain-based system, the number of users has quite a lot of capacity. Public Blockchain means anyone can join the network. Blockchain is a distributed and direct peer-to-peer system. In this respect, anyone who wants to register with the system will not have any problems in terms of scalability.
8. **Sybil Attack:** In the proposed model, each endpoint IP telephony device is unique in the blockchain network with its SIPURI address, ID value, and device-specific map address. If the unique ID value

is verified together with the SIPURI address and public key during registration, the transaction is created and recorded in the block in the blockchain. It cannot be changed again within the blockchain network. Also, when the Token certificate is sent by the device to the blockchain for authentication, the system validates the UID, SIPURI address, timestamp and Map Address on the blockchain network respectively. If no error occurs during verification, device authentication is confirmed. In the proposed architecture, a fake user cannot act like someone else thanks to the Token certificate. In addition, the timestamp is a real-time countermeasure against fake messages.

9. **Spoofing Attack:** The attack model that introduces itself to the target system by changing the legitimate user's identity and enters the network to gain benefits is called spoofing [12]. In the proposed method, the ID value of the endpoint IP telephony device is transmitted in an encrypted form over the insecure channel only after the key distribution is done securely. A spoofing attack can only occur in the proposed model when the private key is compromised. In this respect, it is very difficult for the attacker to capture the device, ID, and private key that the persons keep securely in themselves, which is signed and encrypted in the proposed method. In short, the proposed structure is resistant to spoofing attacks as long as it cannot obtain the signer's private key.
10. **Substitution Attack:** During the blockchain registration, before the key exchange, a nonce value is generated and sent over a secure channel, namely GSM, via SMS. (Trusted Means is SMS.) The Nonce value, namely the RCode, is generated and transmitted via SMS. Thus, the parties verify each other before the key exchange. For this reason, it is very difficult to change the message since it is not sent over the internet (public channel). In addition, mutual data transmission is supported with a timestamp, preventing it from being changed later and using the same message.
11. **Man in the Middle Attack**: Public key distribution by methods similar to Diffie-Hellman Key Exchange is vulnerable to Man in the Middle Attack. However, in the proposed structure, Key Exchange prevents this attack at the registration stage. In order to check the integrity of the token certificate, the blockchain device, its private key and the ID value of the IP phone device are hashed with the SHA-256 hashing algorithm. The token certificate is transmitted encrypted with the public key of the blockchain device. Thus, the certificate sent for authentication can only be decrypted and verified with the private key of the blockchain device. In VoIP architecture, data transmission can be monitored or viewed by the attacker by passive attack during mutual conversation. Data content can be changed with active attack when necessary. In this respect, the SRTP protocol is used for data encryption in the media part. The SRTP protocol uses the symmetric encryption method, and therefore the initial key distribution for the session key to be used in encryption must be performed securely. SDES, MIKEY and ZRTP are used in this key exchange, but as mentioned in the previous sections, these protocols contain some vulnerabilities. In the proposed architecture, the interviewees obtain the public key over the blockchain. Thus, they can transmit the session key to each other by encrypting them with public keys. This method is very effective against eavesdropping and impersonation attacks.
12. **Replay Attack**: The unique ID is signed with the sender's private key at the initial registration stage. It is then encrypted with the receiver's public key. In this respect, the ID value can be registered once in the blockchain. Once recorded on the blockchain, the transaction cannot be changed. In addition, the use of timestamps used in the registration phase is a powerful method to prevent replay attack scenarios. The RCode value is a randomly generated numeric value used for authorization purposes. A secure and synchronized communication channel is created by sending it in SMS format. A security measure is provided against repetition attacks by providing an average of 2 min validity.
13. **DDoS:** Authentication with distributed architecture eliminates the need for a central server. In this respect, the single-point failure vulnerability is eliminated. In addition, key distribution is carried out

in a distributed architecture completely different from central authority-like methods, providing an effective method against denial-of-service attacks. DDoS to be done to the device is not covered by presented method. In this method, only possible DDoS attacks to the authentication mechanism will be prevented.

5.1.1 Formal Security Verification

AVISPA is an application package for analyzing patterns of security protocols. These protocols to be analyzed are written with High Level Protocol Specification Language (HLPSL) [24]. For the security testing of the proposed algorithm, the application under OFMC backend of AVISPA is chosen. This is because OFMC is effective at detecting attacks as well as validating protocols.

OFMC checks if the proposed scheme prevents attacks like replay attack and MITM. In general, the results obtained using the AVISPA tool show that the proposed scheme is safe against active and passive attacks. Fig. 7 shows the AVISPA output of the security analysis of the proposed scheme. The first figure shows that the OFMC backend visited and analyzed 2 nodes with the search time of 0.01 sec.

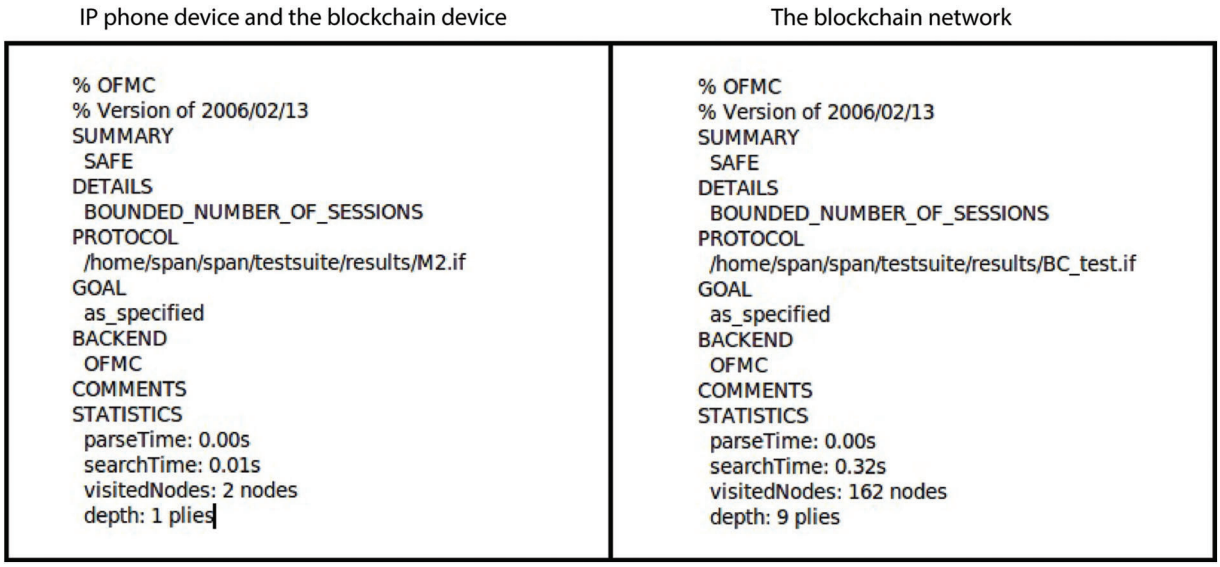

Figure 7: The result of the analysis using OFMC backend of our scheme in AVISPA tool

This indicates that the process of validating the corresponding certificate by the IP phone device and the blockchain device sending the Token for authentication is secure. The second figure shows that there is no security vulnerability in the distributed blockchain network if the blockchain devices are directly attacked in the blockchain network. In addition, reference [5] test results show that the SAS authentication method used in authentication just before the peer-to-peer key distribution with the ZRTP protocol over AVISPA contains vulnerability against cyberattacks. The second simulation result of the analysis using OFMC of our proposed scheme in the blockchain.

5.2 Performance Analysis Against Server Based Schemes

In this section, the performance analysis of the proposed scheme is carried out over message size and by comparing security features. The prominent features in the authentication of the proposed model are presented by comparing the papers using the central architecture in the literature. The comparison is done with Nikooghadam et al. [4], Qui et al. [18], Jiang et al. [14] and Zhang et al. [17], respectively.

As shown in Tab. 1, the proposed model is secure against all specified attacks and can meet security requirements including single-point failure and non-repudiation. In other words, the proposed scheme provides a high level of security compared to studies using the centralized structure. Single-point failure and non-repudiation features are the most important features that blockchain technology provides to our structure.

Table 1: Security comparison of centralized authentication method's different schemes

Evaluation Criteria	Ref. [4]	Ref. [18]	Ref. [14]	Ref. [17]	Presented study [BcVoP2P]
Single Point Failure	No	No	No	No	**Yes**
Mutual Authentication	Yes	Yes	Yes	Yes	**Yes**
Non-Repudiation	No	No	No	No	**Yes**
DDoS	Yes	No	Yes	Yes	**Yes**
User Anonymity	Yes	Yes	Yes	Yes	**Yes**
Replay Attack	Yes	Yes	Yes	Yes	**Yes**

Tab. 2 shows the comparison of the communication costs (according to the number of exchanged message bits) of the proposed method through the schemes of Nikooghadam et al. [4], Qui et al. [18], Jiang et al. [14] and Zhang et al. [17], at the authentication stage. Considering the message cost over the standard values, assuming that the digest (output) of the Hash function is 160 bits, the user ID (ID Value) is 160 bits, the pseudo-ID (PId) is 160 bits, and the random number generation is 160 bits, the realm value is 32 bits, and the timestamp is 32 bits. In addition, encryption and decryption operations are 128 bits, Elliptic Curve Point Multiplication is 320 bits [4,25].

Table 2: Communication cost comparison

Schemes	Message size (bits)	Number of messages
BcVoP2P	1376	2
Ref. [4]	1280	3
Ref. [18]	1440	3
Ref. [14]	1536	3
Ref. [17]	1376	3

According to server-based schemes, the proposed model, which takes place with 2 message steps, performs authentication with 1376 bits, with less cost than other methods. Here, it seen that this scheme has higher communication cost compared to the scheme of Nikooghadam et al. [4]. However, this cost is negligible as the proposed scheme provides stronger security than the related scheme.

The blockchain device acts as a central authority for once, verifying the Token certificate before authentication and sending value to the blockchain network for authentication purposes. The comparison between these schemes in this respect is purely the transaction between the endpoint IP telephony device and the blockchain device. The cost on the blockchain network for transactions in this section is completely ignored.

6 Conclusion

The presented paper, which aims traditional authentication methods in VoIP applications based on centralized models and target errors and vulnerabilities that occur during authentication, proposes a decentralized authentication scheme based on blockchain. A unique end-to-end authentication model was created directly between peers just before multimedia communication by combining blockchain technology having a distributed architecture with the distributed structure of endpoint IP phone devices.

This study, which explains all the stages of a multimedia communication in order, presents the authentication model as a whole within the schema. The IP telephony device is authenticated on the blockchain network, avoiding single-point failure. In addition, IP phone systems operate with significantly minimum latency requirements. It is not enough to provide security in terms of confidentiality and privacy alone. For this reason, the proposed model performs all validations just before the transmission of multimedia data without real-time communication. In addition to providing security by generating certificates over a distributed network created by blockchain devices, delays in accessing the system through the distributed model are considerably reduced. Moreover, performance analysis shows that the model has real safety and efficiency. Formal security analysis and validation were performed using the AVISPA tool, and this proves that the proposed schema provides a more secure model compared to other relevant schemes such as ZRTP protocol. Finally, the communication cost was calculated and compared with the central structure and communication cost comparison is showed in detail. In future works, performance evaluation will be made with traditional methods for key exchange mechanism.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] H. P. Singh, S. Singh, J. Singh and S. A. Khan, "VoIP: State of art for global connectivity—A critical review," *Journal of Network and Computer Applications,* vol. 37, pp. 365–379, 2014.

[2] P. K. Dhillon and S. Kalra, "Secure and efficient ECC based SIP authentication scheme for VoIP communications in internet of things," *Multimedia Tools and Applications*, vol. 78, no. 16, pp. 22199–22222, 2019.

[3] M. A. Ferrag, L. Maglaras, A. Derhab and H. Janicke, "Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues," *Telecommunication Systems*, vol. 73, no. 2, pp. 317–348, 2020.

[4] M. Nikooghadam and H. Amintoosi, "A secure and robust elliptic curve cryptography-based mutual authentication scheme for session initiation protocol," *Security and Privacy*, vol. 3, no. 1, e92, 2020.

[5] P. Gupta and V. Shmatikov, "Security analysis of voice-over-ip protocols," in, *20th IEEE Computer Security Foundations Symposium (CSF'07)*, Venice, Italy, pp. 49–63, 2007.

[6] L. Salgarelli, M. Buddhikot, J. Garay, S. Patel and S. Miller, "Efficient authentication and key distribution in wireless IP networks," *IEEE Wireless Communications*, vol. 10, no. 6, pp. 52–61, 2003.

[7] R. Pecori and L. Veltri, "3AKEP: Triple-authenticated key exchange protocol for peer-to-peer VoIP applications," *Computer Communications*, vol. 85, pp. 28–40, 2016.

[8] M. A. Jan, J. Cai, X. C. Gao, F. Khan, S. Mastorakis *et al.*, "Security and blockchain convergence with internet of multimedia things: Current trends, research challenges and future directions," *Journal of Network and Computer Applications*, vol. 175, pp. 2067–2087, 2020.

[9] M. T. Hammi, B. Hammi, P. Bellot and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Computers & Security*, vol. 78, pp. 126–142, 2018.

[10] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq *et al.*, "A decentralized lightweight blockchain-based authentication mechanism for IoT systems," *Cluster Computing*, vol. 23, no. 3, pp. 2067–2087, 2020.

[11] S. Guo, X. Hu, S. Guo, X. Qiu and F. Qi, "Blockchain meets edge computing: A distributed and trusted authentication system," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2020.

[12] Y. Xu, J. Ren, G. Wang, C. Zhang, J. Yang *et al.*, "A blockchain-based nonrepudiation network computing service scheme for industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3632–3641, 2019.

[13] T. Liu, G. Huang and P. Zhang, "A user authentication protocol combined with the trust model, biometrics and ECC for wireless sensor networks," *Intelligent Automation and Soft Computing*, vol. 24, no. 3, pp. 519–529, 2018.

[14] Q. Jiang, J. Ma and Y. Tian, "Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol of zhang et al.," *International Journal of Communication Systems*, vol. 28, no. 7, pp. 1340–1351, 2015.

[15] P. Segeč, M. Moravčík, J. Hrabovský, J. Papán and J. Uramová, "Securing SIP infrastructures with PKI—The analysis," in *15th Int. Conf. on Emerging ELearning Technologies and Applications (ICETA)*, Slovakia, pp. 1–8, 2017.

[16] E. J. Yoon, K. Y. Yoo, C. Kim, Y. S. Hong, M. Jo *et al.*, "A secure and efficient SIP authentication scheme for converged VoIP networks," *Computer Communications*, vol. 33, no. 14, pp. 1674–1681, 2010.

[17] L. Zhang, S. Tang and S. Zhu, "An energy efficient authenticated key agreement protocol for SIP-based green VoIP networks," *Journal of Network and Computer Applications*, vol. 59, pp. 126–133, 2016.

[18] S. Qiu, G. Xu, H. Ahmad and Y. Guo, "An enhanced password authentication scheme for session initiation protocol with perfect forward secrecy," *PLOS One*, vol. 13, no. 3, pp. e0194072, 2018.

[19] A. Levi and C. B. Güder, "Understanding the limitations of S/MIME digital signatures for e-mails: A GUI based approach," *Computers & Security*, vol. 28, no. 3–4, pp. 105–120, 2009.

[20] G. Glissa and A. Meddeb, "6LowPSec: An end-to-end security protocol for 6LoWPAN," *Ad Hoc Networks*, vol. 82, pp. 100–112, 2019.

[21] R. Zhang, X. Wang, X. Yang and X. Jiang, "On the billing vulnerabilities of SIP-based VoIP systems," *Computer Networks*, vol. 54, no. 11, pp. 1837–1847, 2010.

[22] J. Wang, W. Chen, L. Wang, Y. Ren and R. S. Sherratt, "Blockchain-based data storage mechanism for industrial internet of things," *Intelligent Automation and Soft Computing*, vol. 26, no. 5, pp. 1157–1172, 2020.

[23] P. Leach, M. Mealling and R. Salz, "A universally unique IDentifier (UUID) URN namespace," 2005, Accessed: May 31, 2021. [Online]. Available: https://www.hjp.at/doc/rfc/rfc4122.html.

[24] D. Von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," 2005, Accessed: June 01, 2021. [Online]. Available: http://www.davoh.de/cs/talks/AVISPA-HLPSL.pdf.

[25] S. Kumari, M. Karuppiah, A. K. Das, X. Li, F. Wu *et al.*, "Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, pp. 643–653, 2018.