Blockchain Based Mutual Authentication for VoIP Applications with Biometric Signatures

Mustafa Kara
Computer Engineering Departmant
National Defence University Huten
Istanbul, Turkey
mkara@hho.msu.edu.tr

Şevki Gani Şanlıöz
Computer Engineering Departmant
National Defence University Huten
Istanbul, Turkey
ganisanlioz@hho.msu.edu.tr

Hisham R. J. Merzeh
Computer Engineering Departmant
Yıldız Technical University
Istanbul, Turkey
f0115067@std.yildiz.edu.tr

Muhammed Ali Aydın
Computer Engineering Departmant
Istanbul University-Cerrahpaşa
Istanbul, Turkey
aydinali@istanbul.edu.tr

Hasan Hüseyin Balık
Computer Engineering Departmant
National Defence University Huten
Istanbul, Turkey
balık@hho.msu.edu.tr

2021 6th International Conference on Computer Science and Engineering (UBMK) | 978-1-6654-2908-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/UBMK52708.2021.9558972

***Abstract*— In this study, a novel decentralized authentication model is proposed for establishing a secure communications structure in VoIP applications. The proposed scheme considers a distributed architecture called the blockchain. With this scheme, we highlight the multimedia data is more resistant to some of the potential attacks according to the centralized architecture. Our scheme presents the overall system authentication architecture, and it is suitable for mutual authentication in terms of privacy and anonymity. We construct an ECC-based model in the encryption infrastructure because our structure is time-constrained during communications. This study differs from prior work in that blockchain platforms with ECC-Based Biometric Signature. We generate a biometric key for creating a unique ID value with ECC to verify the caller and device authentication together in blockchain. We validated the proposed model by comparing with the existing method in VoIP application used centralized architecture.**

Keywords*— *P2P network, blockchain, secure communication, authentication, VoIP

I. INTRODUCTION

The authentication mechanism basically has two important tasks. The first is to enable the secure and accurate installation of the communication infrastructure between the hardware units of the network, and the second is to provide system resources only to the service of real users. However, the shared data that requires security and privacy during the transmission of information in a public channel that is not secure, required the development of new approaches to authentication that are more secure. In particular, video communication platform or online IP based telephony systems is one of the most widely used network applications recently. Therefore authentication between users is vital issue in multimedia communication [1].

The identification process is usually based on the user name and password. Any user who requests access to the platform or service will be asked for credentials. These methods separate malicious and legitimate users from each other. Every user of the system applies to access the platform properly. Authentication is a verification process that detects valid users. To summarize, authentication is the method or performance of verifying the identity of a user or process [2]. Therefore, we propose an alternative authentication method to replace the centralized approaches which can violate privacy both for the caller and callee. Also, centralized authentication has some concerns with availability for the server.

The proposed schema uses biometric data which generates a 512-byte template for the authentication process. In our scheme, the paper proposes using the ECC algorithm throughout biometric private keys to create digital signatures and distribute the public key among peers via blockchain. At this point, we use biometrics template. Because biometric data is based on who the user is or some unique features, not what the user knows or what type of validation device is using. Biometric data of the caller contribute unique ID generation and this value provides security for both the device and the caller in our scheme.

There are many common protocols and methods used in Voice over IP (VoIP) applications to provide verification and security concepts. Protocols such as S/MIME or TLS in the signaling process depend on Certificate Authority (CA) or Trusted Third Party(TTP) for key distribution and verification. However, these approaches cannot provide privacy and have drawbacks as a single point of failure [3]. Also, TLS does not provide end-to-end verification [4]. Implementation of these protocols in VoIP applications does not solve Man in the Middle Attacks (MITM) problem and against this kind of attack, IP-based communication is still vulnerable.

If authentication does not occur, the session key is vulnerable to attacks and can easily be obtained by the attacker while transmitting over a public channel. However, if the session key is not understood by the attacker, it means meaningless. Encryption provides protection transmitted multimedia data over public channels. It converts clear data into a form that cannot be easily decrypted [5]. Encrypted data should only decrypt and validate when it reaches the correct destination. This is the most effective way to secure data. To extract an encrypted file, you must have a master key or session key to decrypt it. In VoIP applications some of the most popular protocols have been designed for key distribution and authentication are respectively Session Description Protocol Security Descriptions (SDES), Secure Real-time Transport Protocol (SRTP) and Composed of Z and Real-time Transport Protocol (ZRTP) protocols. ZRTP protocol is a key management protocol [6]. It performs authentication between peer to peer (P2P). However, this protocol uses the same session key as the previous session. This approach has an issue is unable to provide Perfect Forward Secrecy [7]. This is a problem that creates weakness within the multimedia transmission system. The vulnerabilities in the existing protocols inspire us for a new decentralized authentication scheme.

Blockchain is a distributed technology that overcomes threats and issues that exist in authentication platform. In our scheme main purpose of using blockchain platform is to provide high levels of security and to perform operations in a transparent structure. This method eliminates the need for

trusted party or certificate authority. Blockchain keeps all record for performed transactions over the network and provide non-repudiation [8]. Blockchain make our structure more secure with its cryptographic infrastructure [9]. This technology, which includes the Smart Contract and Consensus Algorithms is a database that ensures a suitable environment as an alternative to Public Key Infrastructure (PKI).

In this study, blockchain establishes the secure environment for shared secret in IP based communication before implementation of mutual authentication. Blockchain technology includes the proper infrastructure for a secure real-time multimedia communication system. In addition, the authentication process integrates with a biometric-based model in our scheme for a better solution.

The main contributions of this study are respectively:

- P2P mutual authentication scheme is proposed for VoIP applications by utilizing blockchain to eliminate the need for trusted third party or certificate authority.
- Every transaction of this communication is stored in the distributed network through the smart contracts. The structure has been stabilized by Consensus algorithms.
- We addressed the secure key distribution in VoIP applications before multimedia data transmission. We generated key pairs via the Elliptic-curve cryptography (ECC) algorithm and create a unique ID with these keys in terms of security. An ECC based biometric signature is formed by means of generating a private key from biometric data and employing that private key to perform a digital signature in our system.
- For the VoIP application is to provide non-repudiation and privacy properties by eliminating a single point of failure. Finally, we created a security requirement comparison table to compare with existing works.

II. BACKGROUND

A. Decentrialized Mechanism

PKI is an important component to resolve authentication challenges between peers. It is a kind of methodology to distribute secure certificates via CA or TTP. CA verifies the identity of the public keys and allows peers to perform cryptographic operations, such as encryption and digital signature. However, in terms of Authentication and Identity Validation use the central mechanism for PKI which can cause single point of failure [10].

The blockchain is one of the best option for authentication scenarios. No need for data storage or confirmation of data entries only by one unit is not suitable for blockchain technology. In these cases, the traditional database solve the shortcoming of system. However, the blockchain technology is very convenient to perform a distributed verification model. To summarize of authentication steps, the first operation is to costruct a transaction to send Smart Contract in blockchain. Smart contracts are a piece of a code on working such as Ethereum or Ripple blockchain platforms. The smart contract verifies the certificate and extract the values and store transactions. Next, it sends the values of certificates to the blockchain network to verify them. This transaction is approved or terminated on the blockchain network according to results. The verification requires that caller and callee must register to blockchain system. If any transaction validate once, it store and maintain in the distributed ledger as a block and the transaction between caller and callee is non-repudiation anymore. Validation process is completely transparent and public throughout the miners [11]. Fig. 1 depicts the authentication mechanism by considering blockchain network for VoIP applications. The blockchain provides an authenticated channel by eliminating mechanism such as TTP, and perform P2P key distribution.

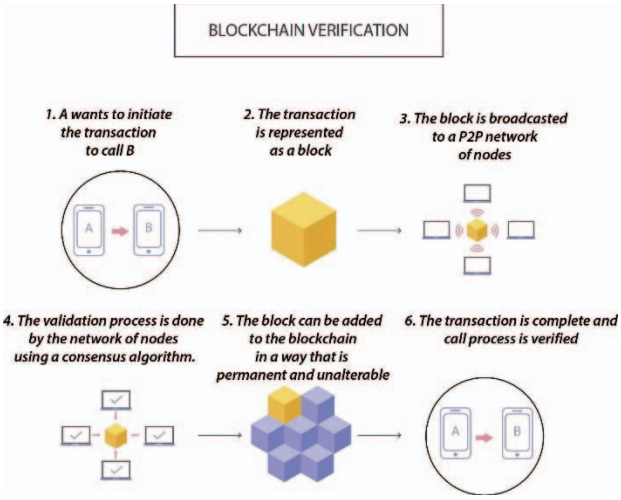

Fig. 1. Blockchain verification schemes

All participant information such as ID or public key is distributed across all the network on blockchain. Their transactions verify securely by considering via the consensus protocols amongs the miners [12]. If an attacker want to change any part of chain, he or she must alter each block on blockchain. Attackers must access more than %51 device on blockchain at the same time to change any block which is practically impossible. Transaction on blockchain is almost immutable. It is very hard to alter, modify or delete. As the number of blocks increases, the chain extends and the blockchain network becomes stronger. Finally, we call caller and callee as a peer on our scheme. The blockchain platform validates these participants without TTP or CA.

B. Public Key Cryptography

Communication is a sustainable process as long as information security is provided. The proposed scheme uses ECC asymmetric cryptography to prevent the malicious attacks while data transportation among the peers. ECC algorithm handle security concern with small key size an it is better towards traditional asymmetric encryption model. Also ECC provides an effective solution for time constraints [13]. This algorithm is an effective solution for encryption in time-constrained IP based communications. Traditional asymmetric encryption algorithms are generally based on the difficulty of multiplying two or more large prime numbers into their multiplication. ECC assumes that it is impossible to find discrete logarithm according to a known point of the elliptical curve. The robustness of the elliptic curve is based on the calculation speed of the point multiplication and the calculation of the point obtained by the start point and multiplication point. As a result, encryption and decryption speed is better than traditional encryption algorithm because the ECC algorithm requires small key size. From this perspective, ECC seems better option in our multimedia communication scheme rather than other algorithms.

C. VoIP Security System

There are lots of protocols to ensure security in VoIP applications on each layer according to OSI reference model [6]. We divide the VoIP architecture into two layers to show all security process step by step. Layers call as Host and Media respectively. Fig.2 depicts us the VoIP layered architecture which is consists of three components as protocol, security and sections. In addition to understanding the overall security structure of VoIP, it aims to understand the proposed model.

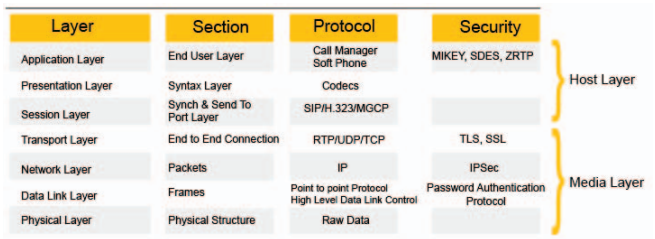

Fig. 2. Voip layered architecture

In this study is a recommended distributed model that aims P2P VoIP applications, unlike traditional client-server approaches. Blockchain technology has been used as a potential solution to ensure data integrity and to increase the resistance of cryptographic methods. Besides integrity and secure communication, blockchain network provide us secure mutual authentication.

III. Security Model

A. System Architecture

All P2P methods needs a more secure structure day by day. Key management, which is the most important issue in the secure multimedia communication in the current technology, is considered by P2P key exchange. Along with the need for secured data transmission that has emerged recently, meetings, lectures and phone calls that require confidentiality demonstrate the importance and timeliness of this issue. Fig. 3 shows system architecture that is divided into three layers to understand IP based communication. The VoIP devices is reviewed by each network layer. This system architecture describes the key elements of the VoIP component and we proposed a novel authentication method using Blockchain to this system architecture.

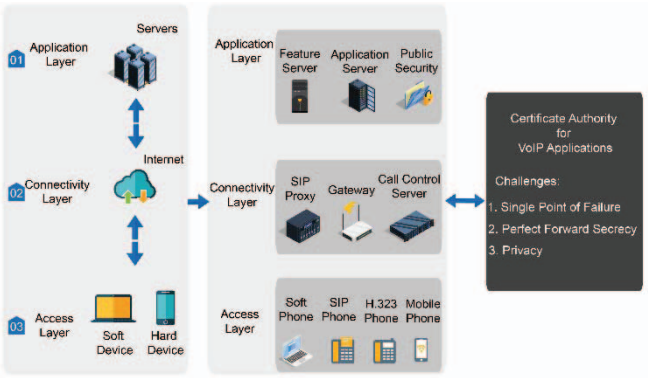

Fig. 3. System architecture

The Ripple platform is a protocol based on the compromise of trusted subnets on a large network. During the evaluation of a transaction for validation in this platform, the consensus of the participating nodes is to decide, if this ratio reaches a value of 80% and above, the transaction is validated and published for the entire network. Therefore, the Ripple algorithm is an accurate method for our system architecture [14].

In this VoIP architecture proposed using the ECC along with biometric private keys to perform digital signatures and distribute the public key between caller and callee via blockchain. Next section is explained biometric key generation in details.

B. Biometric Key Generation

There are three component of digital signature. This steps are respectively Initialize, Signature and Verification.

1) Initialize

E is an eliptic curve and the caller find a prime number q. p is a prime number to choose randomly [15]. q must be a multiple of (p-1). Note that Discrete Logarithm Problem (DLP) should be hard. g is the generator point on the curve E. It must be primitive root in Zp^*.

$$x \equiv g^{\frac{p-1}{q}} \bmod p \tag{1}$$

$$x^q \equiv 1 \bmod p \tag{2}$$

512 bytes caller biometric data convert a hash value by using SHA-256 hash algorithm. This hash value become a number less than p that is the order of the curve. We call this number as A which must be kept in secret.

$$1 \leq A \leq q-1 \tag{3}$$

Calculates b and publishes (p, q, x, b), such that;

$$b \equiv x^a \bmod p \tag{4}$$

2) Signature

The caller first generates a unique ID through hash function for blockchain that is made up of the public values such as p, q, x and b. The last 5 digit of the hash value is the ID value.

$$ID = SHA(p+q+x+b) \tag{5}$$

Choose a secret number k.

$$0 < k < q-1 \tag{6}$$

Computes r value.

$$r = (x^k \bmod p) \bmod q \tag{7}$$

Computes s value.

$$s = k^{-1}(ID + A.r) \bmod q \tag{8}$$

ID, r and s value is the signature. These three value is sent to the smart contract.

3) Verification

p, q, x and b are avaliable to the smart contract. The smart contract must verify the signature as follow:

Computes $v1$ and $v2$ respectively;

$$v1 = (s^{-1}.m) \bmod q \tag{9}$$

$$v2 = (s^{-1}.r) \bmod q \tag{10}$$

$$v = (x^{V1}.\ b^{V2} \bmod p) \bmod q \tag{11}$$

If v is equal to r, the signature is accepted. Otherwise verification process is invalid.

C. Registration Phase

The registration phase is completed in 5 steps. Fig. 4 depicts the registration algorithm. Moreover, these steps are as follows;

1) Caller produces the key pairs and ID value as mentioned in Biometric Key Generation Section. Caller sends its public key and ID value for registration to the smart contract. Creates a transaction for this process.

2) Smart Contract extracts this transaction and ID and public key are sent to blockchain network for validation. We create a timestamp for checking whether the caller is available to register or not. Also this timestamp blocks some attacks such as replay attack.

3) All devices in the network we call miner control to validate or terminate this transaction. (Within certain rules)

4) If caller ID and public key is unique and not registered on blockchain, transaction is validated. If the transaction is approved, information of caller is stored on the blockchain network as a block. ID, public key and a Map Address generated from these two values are recorded on blockchain.

5) To send an acknowledgement packet and certificate to the caller when registration process is done. The caller is provided by smart contract an authentication certificate that is created for authentication process. Caller use its certificate to authenticate itself if it wants to make a VoIP call.

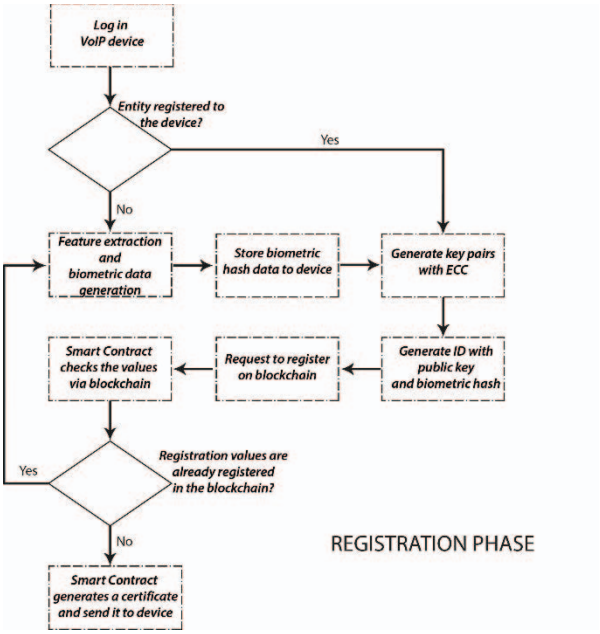

Fig 4. Registration Phase Algorithm

D. Authentication Phase

Each certificate is approved by smart contract in this section. But the certificate extracts and send to blockchain for verification. After SIP registration, and before multimedia transmission, authentication is performed via blockchain network. Fig. 5 illustrates the algorithm of the authentication system, in which the essential components are shown.

1) Caller send its certificate on blockchain with VoIP phone number of callee. First of all, Smart Contract confirms validation of the timestamp.

2) Smart Contract extracts the packet and sends the values to the blockchain for verifying the information of this certificate.

3) The existence of ID and public key is verified by checking if given values are registered in the blockchain or not. Map Address value is constructed using public key and ID and compared with certificate Map Address value on blockchain. If the results are different, the transaction is terminated.

4) Otherwise correct result is obtained on blockchain network smart contract allow the transaction. Once the transaction is verified and stored on blockchain, it is very hard to change it.

5) Finally, the registration of callee is checked on blockchain and the authentication is confirmed or rejected for the call.

6) Mutual authentication via blockchain is complete.

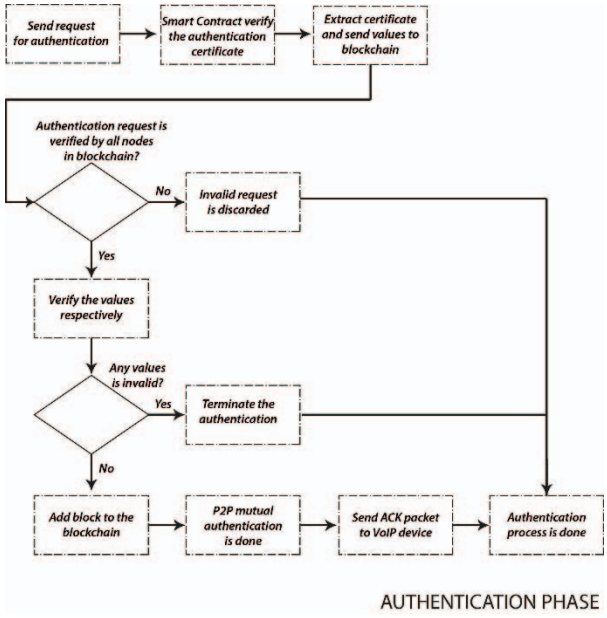

Fig 5. Authentication Algorithm in Blockchain Network

E. Message Authentication

After mutual authentication in the blockchain, the session key is generated using the symmetric encryption algorithm for faster multimedia transmission. Caller encrypts session key with callee's public key and send it to callee. Callee extracts the packet with its own private key and obtain the session key. Next, with a new timestamp, Callee creates an acknowledgment (ACK) packet and sends it to caller for approval. The SRTP protocol uses this session key for encryption during the communcation. The symmetric encryption is an effective solution to overcome the time limit during multimedia communication. P2P authentication also provides Perfect Forward Secrecy (PFS) in the proposed scheme. Moreover, after call process a new block is established to reduce the authentication process in the blockchain, whenever caller and callee decide to communicate with each other.

IV. Discussion

Decentralized mutual authentication in VoIP provides for its applications privacy and secure. Because the centralized authentication system approach includes some shortcomings.

It is essential to handle secure communication issues. In this paper, we show blockchain based mutual authentication for VoIP applications with ECC based Biometric Signatures. This is a robust approach in multimedia communication security.

An ECC-based biometric signature is used for generating a private key via using a biometric sample [16]. After the generation of this private key is to perform as a key component to make a robust digital signature. The major advantage of biometric signatures is not to need a storage center for the biometric template or the private key. In blockchain is one of the main issues to store the private key securely. This biometric template should be rapidly definable and always it must be accurate in order to provide the same private key creation.

Any transaction in the blockchain cannot be changed or deleted. If an attacker try to alter any transactions in the blockchain, it must modify the whole blocks in ledgers. Because all the blocks are connected via hashes. Through smart contracts, the system is autonomous for all activities. SIP and RTP protocols work together respectively on multimedia communications systems. SIP protocol includes security vulnerability because it is an open text-based protocol [17]. For this reason, it is not enough to just prefer SIP based model for authentication process. RTP is a protocol that provides real-time performance because it is essentially UDP protocol. Each message must be encrypted quickly during media section which use RTP protocol. In order to ensure secure communication in the proposed scheme, the key exchange is to perform peer to peer.

Besides, one of the best alternative platforms of applications for authentication, there are some difficulties in blockchain technology at the same time. The blockchain models that use some consensus protocols like Proof of Work are consuming enormous amounts of energy and also need expensive computer systems. Moreover, there are some limitations in terms of time. Therefore, no transaction is processed during real-time data transfer. All registration and authentication processes are to perform before communication. It is inadequate compared to traditional databases in terms of performance. Except for the ECC algorithm, the other protocols such as RSA may not be applied to our structure due to time constraints. Otherwise, in VOIP applications, message authentication and must be transmitted to the other side within a maximum in 150 milliseconds.

In multimedia communication in terms of security issues of previously transmitted data, the network should provide PFS. One of the traditional methods for P2P VoIP applications, the ZRTP protocol uses the previous session key again in the next session. The network can not provide PFS.

In literature, we detected that the proposed schemas were generally authenticated based on a central structure such as CA or TTP [17-19]. For example, PKI-based solutions require a Certificate Authority system, while identity-based solutions are based on key escrow. Without solving the key escrow problem, the scheme is vulnerable to trust issues to store the key anywhere.

According to the above comparison analysis, the proposed scheme is more efficient than a centralized architecture. Table 1 summarizes the attacks on the schemes and the proposed protocol, which shows us using trusted authority schemes might suffer Anonymity, Single Point of failure and Non-repudiation. All the Peers require to protect the data during the multimedia transmission that could be exploited by an attacker. Ref. [7] use SAS authentication that can not provide PFS. Moreover, lack of non-repudiation is the critical factor for VoIP applications.

TABLE 1. SECURITY REQUIREMENT COMPARISON OF SCHEMES

Security Requirements	Ref. [18]	Ref. [7]	Ref. [19]	Ref. [17]	The Proposed Scheme
Data Integrity	Yes	Yes	No	Yes	Yes
Person/Device ID Anonymity	No	No	Yes	No	Yes
Resistance to Spoofing Attacks	Yes	Yes	No	Yes	Yes
Resistance to Replay Attacks	Yes	Yes	Yes	Yes	Yes
Resistance to MITM	No	Yes	Yes	Yes	Yes
Single Point Failure	No	No	No	No	Yes
Non-Repudiation	No	No	No	No	Yes

V. CONCLUSION

In this study, we implemented the structure of our scheme which is realized upon existing technologies, namely, blockchain. We constructed a system that achieves hundreds of thousands of transactions per second. For this reason, a robust secure scheme meets a blockchain-based mutual authentication system for VoIP applications

We have designed blockchain-based mutual authentication for VoIP applications with biometric signatures. For mutual authentication, we have proposed distributed technology on IP-based communications systems and introduced a novel approach. With the blockchain, we solve non-repudiation and data integrity concerns. It prevents an unauthenticated call in the scheme. An ECC based biometric signature is formed by means of generating a private key from biometric data and employing that private key to perform a digital signature in our system. In addition, with the biometric signature used in this scheme for VoIP communication guarantee that all transmission data security concern is overcome. We have eliminated the need for centralized structure in the VoIP application. We have proposed a more reliable scheme against MITM attacks using a timestamp and distributed architecture.

Future works will be constructed to improve distributed technology via blockchain in terms of P2P key exchange after authentication. Finally, the proposed scheme is configured as a secure IP-based multimedia communication system.

REFERENCES

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Commun. Surv. Tutorials, vol. 16, no. 3, pp. 1550–1573, 2014, doi: 10.1109/SURV.2014.012314.00178.

[2] M. Bayat, M. Pournaghi, M. Rahimi, and M. Barmshoory, "NERA: A new and efficient RSU based authentication scheme for VANETs," Wirel. Networks, vol. 26, no. 5, pp. 3083–3098, 2020, doi: 10.1007/s11276-019-02039-x.

[3] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," Comput. Secur., vol. 78, no. 2018, pp. 126–142, 2018, doi: 10.1016/j.cose.2018.06.004.

[4] J. Choi, S. Jung, K. Bae, and H. Moon, “A lightweight authentication and hop-by-hop security mechanism for sip network,” Proc. - 2008 Int. Conf. Adv. Technol. Commun. ATC 2008, Held Conjunction with REV Meet., pp. 235–238, 2008, doi: 10.1109/ATC.2008.4760563.

[5] A. Mukherjee, “Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints,” Proc. IEEE, vol. 103, no. 10, pp. 1747–1761, 2015, doi: 10.1109/JPROC.2015.2466548.

[6] P. Gupta and V. Shmatikov, “Security analysis of voice-over-ip protocols,” in 20th IEEE Computer Security Foundations Symposium (CSF’07), 2007, pp. 49–63.

[7] R. Pecori and L. Veltri, “3AKEP: Triple-authenticated key exchange protocol for peer-to-peer VoIP applications,” Comput. Commun., vol. 85, pp. 28–40, 2016.

[8] A. A. N. Patwary, A. Fu, S. K. Battula, R. K. Naha, S. Garg, and A. Mahanti, “FogAuthChain: A secure location-based authentication scheme in fog computing environments using Blockchain,” Comput. Commun., vol. 162, pp. 212–224, Oct. 2020, doi: 10.1016/j.comcom.2020.08.021.

[9] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, “Blockchain Meets Edge Computing: A Distributed and Trusted Authentication System,” IEEE Trans. Ind. Informatics, vol. 16, no. 3, pp. 1972–1983, 2020, doi: 10.1109/TII.2019.2938001.

[10] C. Lin, D. He, N. Kumar, X. Huang, P. Vijayakumar, and K. K. R. Choo, “HomeChain: A Blockchain-Based Secure Mutual Authentication System for Smart Homes,” IEEE Internet Things J., vol. 7, no. 2, pp. 818–829, 2020, doi: 10.1109/JIOT.2019.2944400.

[11] F. Lin et al., “Survey on blockchain for internet of things,” J. Internet Serv. Inf. Secur., vol. 9, no. 2, pp. 1–30, 2019, doi: 10.22667/JISIS.2019.05.31.001.

[12] D. Han, H. Kim, J. J.-2017 I. conference On, and U. 2017, “Blockchain based smart door lock system,” 2017, doi: 10.1109/ICTC.2017.8190886.

[13] X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, “A robust ECC-Based provable secure authentication protocol with privacy preserving for industrial internet of things,” IEEE Trans. Ind. Informatics, vol. 14, no. 8, pp. 3599–3609, 2018, doi: 10.1109/TII.2017.2773666.

[14] U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty, “A decentralized lightweight blockchain-based authentication mechanism for IoT systems,” Cluster Comput., pp. 1–21, 2020.

[15] D. Johnson, A. Menezes, and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA),” Int. J. Inf. Secur., vol. 1, no. 1, pp. 36–63, 2001, doi: 10.1007/s102070100002.

[16] V. Kumar, M. Ahmad, A. Kumari, S. Kumari, and M. K. Khan, “SEBAP: A secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing,” Int. J. Commun. Syst., vol. 34, no. 2, pp. 1–21, 2021, doi: 10.1002/dac.4103.

[17] A. Irshad, M. Sher, Eid Rehman, S. A. Ch, M. U. Hassan, and A. Ghani, “A single round-trip SIP authentication scheme for Voice over Internet Protocol using smart card,” Multimed. Tools Appl., vol. 74, no. 11, pp. 3967–3984, 2015, doi: 10.1007/s11042-013-1807-z.

[18] D. Xu, S. Zhang, J. Chen, and M. Ma, “A provably secure anonymous mutual authentication scheme with key agreement for SIP using ECC,” Peer-to-Peer Netw. Appl., vol. 11, no. 5, pp. 837–847, 2018.

[19] S. Kumari, M. Karuppiah, A. Kumar Das, X. Li, F. Wu, and V. Gupta, “Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography,” J. Ambient Intell. Humaniz. Comput., vol. 9, pp. 643–653, 2018, doi: 10.1007/s12652-017-0460-1.

Bilgisayar Mühendisliği
Bölüm Başkanları

10.08.2021

Sayın MUSTAFA KARA

mkara@hho.edu.tr

Bilgisayar Mühendisliği Bölüm Başkanları Kurulu'nun IEEE ile birlikte düzenlediği VI. Uluslararası Bilgisayar Bilimleri ve Mühendisliği Konferansı'na göndermiş olduğunuz aşağıda başlık bilgileri verilen bildirileriniz üç aşamalı değerlendirme sonucunda konferansa sözlü sunum olarak kabul edilmiştir.

Bildiriniz konferans elektronik kitabında ve sunulduktan sonra IEEE Explore'de yayımlanacaktır.

Prof. Dr. Eşref ADALI

UBMK Başkanı

Bildiri No ve Başlığı : **[1304] Blockchain Based Mutual Authentication for VoIP Applications with Biometric Signatures**

IEEE
Advancing Technology for Humanity

BMBB Computer Engineering Department Heads Board
www.ubmk.org

UBMK'21

ULUSLARARASI BİLGİSAYAR BİLİMLERİ VE MÜHENDİSLİĞİ KONFERANSI

INTERNATIONAL CONFERENCE ON COMPUTER SCIENCE AND ENGINEERING

IEEE Advancing Technology for Humanity

Certificate of Participation

Mustafa KARA

"Blockchain Based Mutual Authentication for VoIP Applications with Biometric Signatures"

has participated and presented the article given above at the UBMK'21
organized by Gazi University, İstanbul Technical University, Atılım University
on 15-17 September 2021, held in Gazi University, Ankara / TURKEY.

Prof. Dr. Eşref ADALI
UBMK Genereal Chair, BMBB Board Chair

Prof. Dr. Şeref SAĞIROĞLU
UBMK Local Chair, Gazi University

Prof. Dr. Ali YAZICI
UBMK Co-Chair, Atılım University