IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

A Periodic Validation in Blockchain based Mobile Edge Computing (MEC) through Key Management

Dr. S. Sandosh[1], Aditya Kumar Singh[2], Aditya Gupta[3]
Assistant Professor (Sr.), School of Computer Science and Engineering[1]
Students, School of Computer Science and Engineering[2,3]
Vellore Institute of Technology, Chennai, India
sandosh.s@vit.ac.in, adityakumar.singh2020a@vitstudent.ac.in, aditya.gupta2020b@vitstudent.ac.in

Abstract: *In order to offer mobile consumers shared services and resources with high bandwidth and low latency, key management through blockchain technology is used. However, when shared resources are involved, the MEC infrastructure creates serious security risks. User sensitive and private information. This study presents a key management scheme which is generally used blockchain oriented technology for ensuring common conversation among the devices for they can able to flexibly switch between subnetworks. In the suggested method, when a mobile device joins a subnetwork, it generates compact shared key for electronic signatures and authentication when it joins a subnetwork. All of the public keys for mobile devices are combined by a block that is sent to additional users in the subnetwork by the network miner in the subnetwork. Experimental results demonstrate that the proposed strategy outperforms two baselines in respect of processing, communication, and storage.*

Keywords: MEC, Blockchain, Key Management, Periodic Authentication

I. INTRODUCTION

Mobile edge computing is currently perceived as a critical edge technology for enabling high throughput capacity wireless service with shared resources. Several of these applications will require transferring sensitive client data across a variety of communication devices, raising serious security issues [2]. The proposed system has demonstrated the MEC's current risks and vulnerabilities. It is important to note that in the MEC network, everyone is seen as being unreliable. Key management is a crucial part of every network's security architecture. With the help of the newly developed blockchain technology, wireless mobile edge networks might create a trustworthy, impartial, and decentralised environment for key management. It is one of the standard decentralised key management schemes. In the wireless context, there are numerous obstacles to implementing effective and secure key management. First of all, the blockchain network cannot effectively store a vast amount of data. Second, integrating the centralised third-party functions into the decentralised blockchain network is difficult. Thirdly, integrating a key management system with blockchain in a wireless mobile context is difficult. A safe and effective key management method is also suggested, one that avoids the usage of centralised third parties and common key materials. Because of this, the proposed key management system obviously differs from existing identity- or attribute-based systems. For the MEC network, a unique blockchain-based key management system is put forth that saves encryption keys on the blockchain without the use of a centralised trusted third party or shared key material.

II. RELATED WORKS

The membership and departure of members over time heavily influences of terminals in the effective management tree, which forms the basis of the bulk of standard key management schemes. Furthermore, certain key management strategies are built on organizational forms, and the key manager for each hierarchy can help with more practical key management. However, because more intermediate entities (such as intermediate key managers) are introduced into the key management procedures as a result of the hierarchical structure, there may be additional overheads. Recently, the new blockchain technology has given us access to a more

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

secure and decentralised environment, which has many researchers interested. This section introduces relevant works on blockchain-based key management schemes as well as centralised, distributed, decentralised (as defined in [12]), and distributed key management systems. And Table 1 provides a general comparison of the well-known current efforts.

2.1 Centralized key management:

A single central group is in responsible of developing, distributing, and upgrading the data encryption key in centrally group key management methods. It is one of the most well-known centralised key management schemes. The majority of the suggested centralised protocols make use of a single traffic encryption key for the entire organisation.

Comparision criteria	Without Third Party	Without Common TEK	Moving Member Authentication	Decentralized Approach
[5]	√	x	√	x
[6]	√	x	√	x
[7]	√	x	√	x
[8]	√	x	√	√
[10]	√	x	x	x
[11]	√	x	x	x
[12]	√	x	x	x
[13]	√	x	√	x
[14]	√	x	√	x
[15]	√	x	√	√
[16]	x	x	√	√
[17]	x	x	√	√
[18]	√	x	√	√
[19]	√	x	√	√
Our Work	√	√	√	√

Table 1: Difference between Key Management approaches

2.2 Shared Key management:

Key distribution centre (KDC) uses distributed key management schemes; thus, all participants can focus on managing traffic encryption key. The workload associated with key management can be consolidated thanks to distributed schemes, which can also lessen the need for centralised entities. Inside this scope of clustered and scattered key management architecture, it presented a lot of techniques and methods for maintaining secrecy alongside edge assurances using group-based keys.

2.3 Key management using a blockchain:

The openness and transparency of the blockchain's data, which was emphasised, can result in data leakage. Additionally, user privacy is involved with medical data, and user privacy on the blockchain needs to be guaranteed. Although it is possible to encrypt medical data before it is put on the blockchain, the process is impractical considering it would need a significant amount of computing and storage resources. Although they are separated and the services they offer could be halted if they are attacked, the centralised managers were kept in [28]. This paper lacks centralised entities, unlike [24]. A legal blockchain is created by all site nodes in to store public key hashes and confirm their legitimacy.

III. REVIEW ON EXISTING WORK

3.1 Blockchain:

It is a distributed append-only database. As seen in Fig., the blockchain is made up several block and a hash chain. 1. By examining the checksum of the block head before it, one can determine the order of the blocks. Some characteristics of blockchain include traceability, openness and transparency, decentralized, demonstrability, difficulty of manipulation, etc.

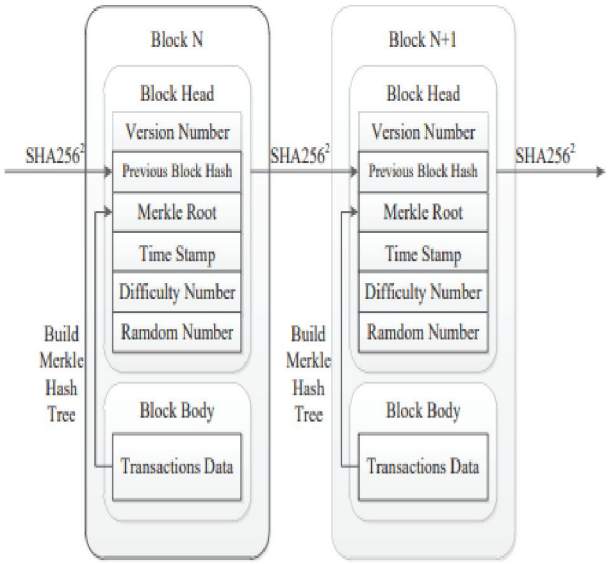

Fig.1. The Blockchain Architecture

3.2 E-Signatures:

E- signature is a computational method that verifies the authenticity of digital messages or documents during communication activities [22]. If the digital signature is legitimate, the recipient has reason to believe that the communication was made by a reliable, verified sender. The communication cannot be changed while in route, therefore the sender cannot claim they never sent it. In other words, the recipient would be able to tell right away if the message had been tampered with or otherwise compromised during transmission. The suggested approach makes use of a secure communication

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

mechanism based on ECDSA to guarantee data security during communication. And ECDSA, a variant of DSA developed by R.C. Merkle in [21] and Victor Miller in [23], combines DSA with Elliptic Curves Cryptography.

3.3 Problem Statement:

The frequency of updates and distribution of transmission key pairs for mobile devices may increase due to the portability of the mobile device. Every time a device enters, leaves, or switches to a new subnetwork, the key manager updates the key for the group members to ensure the privacy of group communication. In the meanwhile, the key manager must communicate the newly formed key to the group mates across the network. A communication base station that connects the wireless subnetworks enables the service providers in the network segment to offer one or more services for subnetworks. One circumstance in which all subnetworks are used as nodes in order to construct a tree is known as partition.

IV. THE SYSTEM MODEL

The system concept and security characteristics of the suggested approach are provided after a brief introduction to blockchain in this section.

4.1 Key Management Protocol for Blockchain:

A member in the proposed technique can join, move within, and exit any T subnetwork as shown in Fig. 2. The suggested method generates cryptographic keys for the ECDSA- based communications protocol's encryption without the need for a centralised authority, much like other blockchain-based applications already in use. According to our hypothesis, a network's resources will be more abundant the nearer it gets to the cloud, and vice versa. This is due to the presence of more mobile devices around the cloud, which should result in more robust services. The operational requirements of these devices can only be met by the abundant compute, communication, and storage resources.

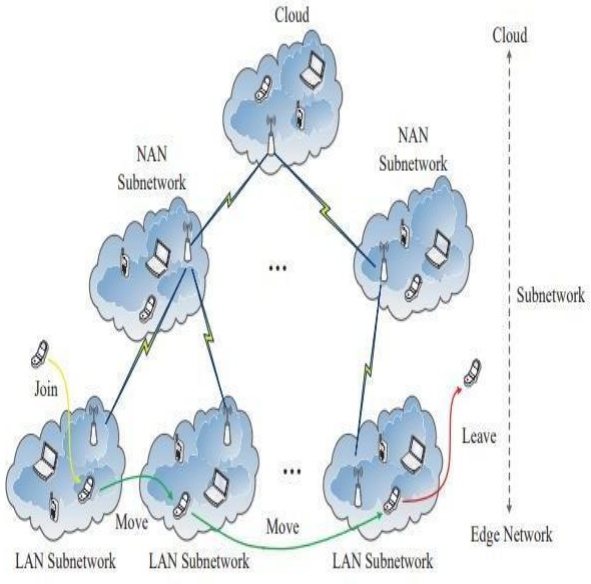

Figure 2. Model for the Proposed System

4.2 Mobility Model:

The scientific simulation of the proposed design is mainly concerned with the membership, migrate, and departure operations for participants among the sub networks. The mobility model of the proposed strategy is a random movement model, where all group members concurrently enter, travel through, and exit various subnetworks in a random and serial manner. The suggested method calls for each person in the group to progressively and deliberately join one sub networking of the tree network, move to any other network layer protocol at randomness, and then leave the sub network, taking into account the worst-case scenario.

Assume that the tree network has m members and n sub networks. Since each member has an equal and random chance of selecting any sub network, the likelihood that they will do so is (1/n). The Poisson distribution is obeyed by the movement process of the members, indicating that the process is random.

4.3 Security Properties:

Through the use of the same cryptographies used in Bitcoin, the suggested key management strategy can ward off numerous conventional security assaults [26]. In the meanwhile, the security of the suggested method can be ensured thanks to the use of digital signatures, which prevent attackers from simulating entities or forging their messages. These blockchain-related security characteristics can be present in the proposed blockchain-based key management scheme.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

(i) Centralized without a Third Party:
It is common knowledge that a service provider will almost certainly become the target of an attack, even if that third party is trusted. The private party's centralization of capabilities for products or user data is the cause of this. When a third party is compromised, services may be halted and user information may be made public. By utilising the decentralised blockchain approach, the suggested method can provide a secure and efficient service for authentication and key without help from a hierarchical reputable third party.

(ii) Protection of privacy:
The public key accuracy during transmission is ensured by the signature key pair. In addition, only the locally stored private key can be used to decrypt data encrypted using public key. In other words, only the receiver himself or herself can decrypt messages encrypted using the recipient's public key using the recipient's local private key.

(iii) Data Storage:
The digitally signed public key for communication and the decentralised nature of blockchain make it impossible for hackers to intercept any conversation or tamper with thenetwork. Because the bitcoin is a simply add distributed database, the network's nodes will have a replica of the information stored there. As a result, consensus has been achieved as perceived by all nodes. Additionally, changing data once it has been placed into a database block is extremely impossible.

V. ANALYSIS OF SECURITY

This section presents the 1-affects-n phenomena of the proposed design as well as the bitcoin network security investigation.

5.1 Threat model:

Even though all nodes in the bitcoin system consider the sequence as the genuine chain, the attacker in the community can undertake another well 51% attack [11] by aggregating more than halves of the network's processing power to construct a longer chain. Threat model is the likelihood that an attack will succeed and it represents the rate at which the attacker will use the blockchain network's processing capacity.

5.2 Forward and Backward Secrecy:

In contrast to conventional key management techniques, the suggested scheme enables users to interact between themselves using the digital certificates that are kept on the blockchain. Additionally, a user is not necessitated to create a new shared key (i.e., rekeying) whenever it changes into a small generation unless the quick verification is failed. The recommended blockchain-based scheme's rekeying process, as a result, is unique from earlier research. Participants always keep their login details on-site and create new ones if a subsequent group's quick verification is unable to guarantee secrecy with regard to backward secrecy. Therefore, it is nearly impossible for anyone to effectively conduct a 51% assault or gain the private key of a specific user in order to learn the security details of others.

5.3 Secure communication in BlockChain:

Despite the fact that blockchains' security is built on decentralization and consensus, has shown demonstrated by Bit coin, a justification for the security of the. This section contains a proposed blockchain-based strategy. Bitcoin security risks consist mostly of constructed using consensus methods[16][17]. First of all, we examine in a wireless mobile environment. After that, we provide a probability analysis of, which is a result of the 51% attack mechanism. An attacker in the suggested approach could be any subnetwork user. The longest chain is the only one that is recognised by all users of the blockchain, and the likelihood that a new block will be created depends on how much computing power is distributed among the subnetworks. The attacker can use the subnetwork's CPU resources to build a longer chain

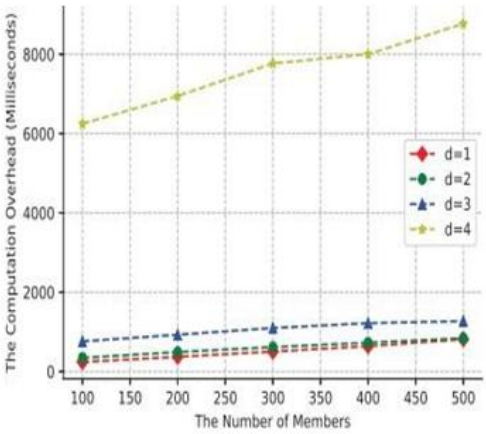

Figure 3. The computation Overhead

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

VI. PERFORMANCE ANALYSIS

In this paragraph, the performance of the proposed blockchain-based credential processing system is evaluated. However, the vast majority of works now in existence do not have overhead data that can be rekeyed. To deliver more complete and precise results, we separate maximal intensity overhead into three stages. In this area, there is computing, communication, and overhead storage. We also take into account the case in which each Member joins, moves, and leaves in turn. The rising membership in this section and the overheads' propensity to rise are both significantly influenced by the measuring method that the target defines function. The whole overhead is made up of storage, communication, and processing overheads when combined linearly, therefore a challenging complex composition is not necessary.

As an illustration, a miner who desires to compete for the Using the new block generator, a random number will be produced for hash the blockhead, boost the randomness, and blockhead number up till the first three digits of the hash value are 0 if the level of difficulty is 3.

6.2 The cost of communication:

The amount of data communicated it during retransmission procedures influences the transmission overhead. Each participant in the proposed scheme will broadcast their networking credentials, and miners will also publish the blocks they create to all participants.

The broadcasting of members' public keys causes a communication overhead. The network coding and key distribution mechanisms used by the Distributed key management scheme produce communication expenses. Key distribution is discussed in relation to the forward and backward security.

6.3 Repository running cost:

No centralized key management are used in the BKM proposal, and each participant maintains a copy of the blockchain. This maintains the members' public keys. The suggested method has an average Repository running cost that is 31.36% more than decentralized cryptographic keys and 36.68% higher than forward cybersecurity management. This is because building trust in a bitcoin blockchain without trustworthy private entities will always be expensive.

6.4 Periodic Validation (Authentication):

The premeditated parameters are the correction factors that uniformize the measuring unit of aggregate overheads. Simulations for parameter analysis are carried out to show the connection between the total overhead and the aforementioned parameters with an authority of pre-defined parameters and a changeable component of the parameters. The overall expense and the variable fraction of the parameters have a linear connection in which the overhead increases linearly as the parameters are raised. Additionally, the blockchain system's mining operations are the primary cause of the compute overhead. Key generation, network encryption, node clustering, and access control procedures are the main components of the analysis in the Integrated Key Management scheme operation.

VII. CONCLUSION

This paper has introduced and proposed a cryptography key distribution system that enables Mobile Edge Computing devices to freely migrate between subnetworks while maintaining secure communication. In addition to eliminating single point of attacks, the proposed method can reduce the processing, connectivity, and memory running costs involved in key generation, session key, and key storage, respectively. The proposed results carried up a thorough security research based on the 51% attack to demonstrate the suggested scheme's security prowess in a mobile environment. Experimental results show that the proposed system performs significantly better than the prior works Distributed Key Management (in terms of computation overhead) and TKM (in terms of

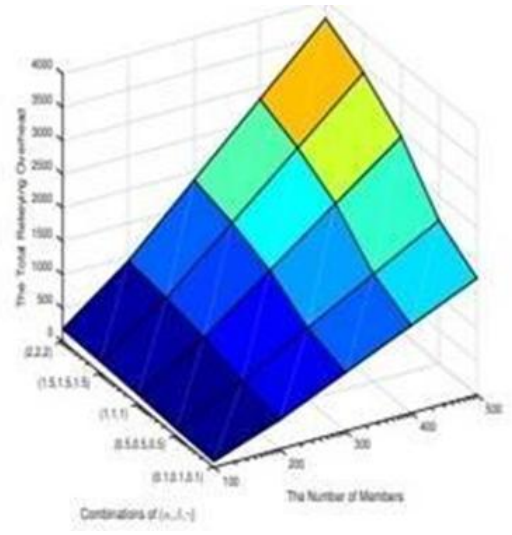

Figure 4. The total overhead with fixed proportion of pre-defined parameters

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

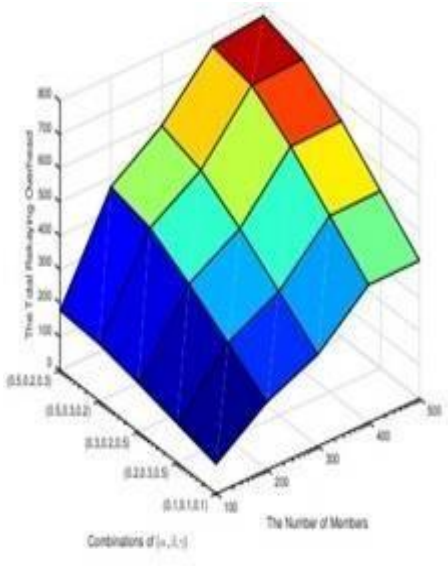

Figure 5. The total overhead with variable proportion of pre-defined parameters

REFERENCES

[1]. C. K. Wong, M. Gouda, and S. S. Lam, "Secure group communications using key graphs," IEEE/ACM Transactions on Networking (TON), vol. 8, no. 1, pp. 16– 30, 2000.

[2]. M.-L. Messai and H. Seba, "A survey of key management schemes in multi-phase wireless sensor networks," Computer Networks, vol. 105, pp. 60–74, 2016.

[3]. D. Wallner, E. Harder, and R. Agee, "Key management for multicast: Issues and architectures," Tech. Rep., 1999

[4]. S. Yi, Z. Qin, and Q. Li, "Security and privacy issues of fog computing: A survey," in international conference on wireless algorithms, systems, and applications. Springer, 2015, pp. 685– 695.

[5]. R. Roman, J. Lopez, and M. Mambo, "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges," Future Generation Computer Systems, vol. 78, pp. 680–698, 2018.

[6]. M. S. Yousefpoor and H. Barati, "Dynamic key management algorithms in wireless sensor networks: A survey," Computer Communications, 2018.

[7]. W. H. D. Ng, M. Howarth, Z. Sun, and H. Cruickshank, "Dynamic balanced key tree management for secure multicast communications," IEEE Transactions on Computers, vol. 56, no. 5, 2007.

[8]. D.-H. Je, J.-S. Lee, Y. Park, and S.-W. Seo, "Computation-andstorage-efficient key tree management protocol for secure multicast communications," Computer Communications, vol. 33, no. 2, pp. 136– 148, 2010.

[9]. Y. Sun and K. R. Liu, "Hierarchical group access control for secure multicast communications," IEEE/ACM Transactions on Networking, vol. 15, no. 6, pp. 1514–1526, 2007.

[10]. C. Esposito, M. Ficco, A. Castiglione, F. Palmieri, and A. De Santis, "Distributed group key management for event notification confidentiality among sensors," IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 3, pp. 566–580, 2020.

[11]. X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," Future Generation Computer Systems, 2017. [Online].

[12]. B. Daghighi, M. L. M. Kiah, S. Iqbal, M.

[13]. H. U. Rehman, and K. Martin, "Host mobility key management in dynamic secure group communication," Wireless Networks, pp. 1–19, 2017.

[14]. S. Hong, H.-I. Kim, and J.-W. Chang, "An efficient key management scheme for user access control in outsourced databases," World Wide Web, vol. 20, no. 3, pp. 467– 490, 2017.

[15]. Y. Challal, F. Z. Benhamida, and O. Nouali, "Scalable key management for elastic security domains in fog networks," in 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). IEEE, 2018, pp. 187–192.

[16]. Z. Q. Lou J and Q. Z, "A blockchain- based key management scheme for named data networking," in 1st IEEE International Conference on Hot Information-Centric Networking (HotICN). IEEE, 2018, pp. 141–146.

[17]. P. Vijayakumar, V. Chang, L. J. Deborah, and B. S. R. Kshatriya, "Key management and key distribution for secure group communication in mobile and cloud network," 2018.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 1, August 2023

[18]. J. Lou, Q. Zhang, Z. Qi, and K. Lei, "A blockchain-based key management scheme for named data networking," in Proceedings of 1st IEEE International Conference on Hot Information-Centric Networking, 2018, pp. 141–146.

[19]. M. Baugher, R. Canetti, L. Dondeti, and F. Lindholm, "Multicast security (msec) group key management architecture," Tech. Rep., 2005.

[20]. A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1832– 1843, 2017.

[21]. N. T. Courtois, M. Grajek, and R. Naik, "Optimizing sha256 in bitcoin mining," in International Conference on Cryptography and Security Systems. Springer, 2014, pp. 131–144.

[22]. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, 2008.

[23]. N. T. Courtois, M. Grajek, and R. Naik, "Optimizing sha256 in bitcoin mining," in International Conference on Cryptography and Security Systems. Springer, 2014, pp. 131–144.

[24]. B. Liu, X. L. Yu, S. Chen, X. Xu, and L. Zhu, "Blockchain based data integrity service framework for iot data," in Web Services (ICWS), 2017 IEEE International Conference on. IEEE, 2017, pp. 468–475.

[25]. Y. Hu, Y. Xiong, W. Huang, and X. Bao, "Keychain: Blockchainbased key distribution," in 2018 4th International Conference on Big Data Computing and Communications (BIGCOM). IEEE, 2018, pp. 126–131.

[26]. N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation, vol. 48, no. 177, pp. 203–209, 1987.