JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Blockchain-Based Secure Key Management for Mobile Edge Computing

Mrs. K. RASHMI - Assistant Professor, Department of Computer Science and Engineering, Anurag University

K. SAI LOKESH - Student, Department of Computer Science and Engineering, Anurag University

P. RITHVIK - Student, Department of Computer Science and Engineering, Anurag University

G. MANI AKSHAYA - Student, Department of Computer Science and Engineering, Anurag University

Abstract

Mobile edge computing (MEC) is a promising edge technology to provide high bandwidth and low latency shared services and resources to mobile users. However, the MEC infrastructure raises major security concerns when the shared resources involve sensitive and private data of users. This paper proposes a novel blockchain-based key management scheme for MEC that is essential for ensuring secure group communication among the mobile devices as they dynamically move from one subnetwork to another. In the proposed scheme, when a mobile device joins a subnetwork, it first generates lightweight key pairs for digital signature and communication, and broadcasts its public key to neighboring peer users in the subnetwork blockchain. The blockchain miner in the subnetwork packs all the public key of mobile devices into a block that will be sent to other users in the subnetwork. This enables the system device to communicate with its peers in the subnetwork by encrypting the data with the public key stored in the blockchain. When the mobile device moves to another subnetwork in the tree network, all the devices of the new subnetwork can quickly verify its identity by checking its record in the local or higher hierarchy subnetwork blockchain. Furthermore, when the device leaves the subnetwork, it does not need to do anything and its records will remain in the blockchain which is an append-only database. Theoretical security analysis shows that the proposed scheme can defend against the 51 percent attack and malicious entities in the blockchain network utilizing Proof-of-Work consensus mechanism. Moreover, the backward and forward secrecy is also preserved. Experimental results demonstrate that the proposed scheme outperforms two baselines in terms of computation, communication, and storage.

1. INTRODUCTION

Mobile edge computing (MEC) is now recognized as a key edge technology for supporting low latency and high bandwidth mobile services with shared resources [1]. Many of these services will involve transferring private and sensitive information of the users among a group of communicating devices, which give rise to major security concerns [2]. Roman et al. in [1] and Yi et al. in [2] have shown the existing vulnerability and threats in MEC. It is worthwhile pointing out that all participants are assumed to be untrusted in the MEC network. Key management is an essential component for providing security in any network [3], [4]. In a MEC infrastructure, the security of key management should allow nodes to establish pairwise keys in order to facilitate secure communication between the nodes in the network [4]. The mobility of devices brings a new challenge for ensuring group communication in a MEC network, i.e., how to transfer keys to members moving from one subnetwork (group) to another while still remaining in communication. Since the members of the new subnetwork do not recognize the newly joined member, an additional overhead will be incurred for key

generation, key distribution and key storage, i.e., computation overhead, communication overhead and storage overhead, respectively. Meanwhile, the group key management schemes must not only handle dynamic group membership (joining or leaving), but they must also handle dynamic member location (moving). Therefore, there is an urgent requirement for a group key management scheme to protect the security of keys, both for the members joining or leaving the group and for moving across network areas. Key management in MEC has attracted the interest of many researchers in recent years. A typical method in centralized key management schemes is the logical key hierarchy-based scheme that was proposed by several research groups almost at the same time [5], [6]. The key tree adopted in such schemes is able to reduce the number of messages required for key updating. For distributed key management schemes, a typical scheme is the distributed group management scheme that is proposed in [7]. One of the typical schemes in the decentralized key management schemes is the mobile key management scheme for dynamic secure group communication which is proposed in [8].

There exist many challenges in achieving efficient and secure key management in the wireless environment. The first challenge is dealing with large-scale mobile devices in a wireless network. Secondly, with the increasing mobility of users, the real-time services are demanding higher performance on rekeying process such as recalculating, redistributing and restoring new keys for backward and forward secrecy. Thirdly, the security issues are a major concern especially when a centralized entity is relied upon for ensuring security of the key management system. The emerging blockchain technique offers the potential to build a trusted, fair-minded and decentralized environment for key management scheme in wireless mobile edge networks. Besides, keeping private keys locally and storing public keys in the blockchain can reduce the overhead of rekeying process. Because when users move into a new group, their records (i.e., public keys) can be traced in the previous blocks in local or higher hierarchical blockchain, so that their identities can be verified quickly. Meanwhile, only if the quick verification is failed, the users need to generate a new key pair (i.e., rekeying) which will be appended to the blockchain. Moreover, the key pair of users will be invalid once they generate a new one, which can reduce the overhead of backward and forward secrecy in the rekeying process. However, blockchain cannot be directly applied to the existing key management schemes, especially in wireless mobile environments, due to the following challenges. Firstly, it is inefficient for the blockchain to store a large volume of data in the blockchain network. Secondly, it is a challenge to adapt the centralized functions of the third party to the decentralized blockchain network. Thirdly, it is a challenge to combine blockchain with a key management scheme in the wireless mobile environment. This paper aims to reduce the rekeying overhead and improve the security of key management in MEC network.

In order to deal with all the challenges mentioned above, we analyze the characteristics of key management schemes and blockchain technique, and then we construct a blockchain based key management scheme. In the proposed scheme, we first partition the wireless base stations into groups (i.e., subnetworks), then build a tree network by treating these groups as nodes, according to the number of members (i.e., users) and the resources of the groups. Then in each group, all members maintain a blockchain network. And the data will be collected into the blockchain of the higher hierarchical nodes, and to be gathered into the root node. Therefore, the members of a group can quickly verify the new group member by tracing the records in the local or higher hierarchical blockchain.

1.2 Scope of the Project:

The scope of the project encompasses the development and implementation of a novel blockchain-based key management scheme tailored for Mobile Edge Computing (MEC) networks. This scheme aims to address security concerns associated with group communication among mobile devices by efficiently managing key generation, distribution, and storage within the blockchain network. The project will integrate the key management scheme into the existing MEC infrastructure, ensuring compatibility and seamless operation. Additionally, the scheme will support dynamic group communication, allowing devices to join or leave subnetworks while maintaining secure communication. Security analysis, performance evaluation, and experimental validation will be conducted to assess the effectiveness and efficiency of the proposed solution, with documentation and reporting of findings included as part of the project scope.

2. LITERATURE SURVEY

The literature surrounding edge computing and wireless sensor networks is rich with research focusing on enhancing security mechanisms, optimizing key management systems, and exploring the potential of

emerging technologies like quantum computing. "Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges" [1] explores the emergence of fog computing, mobile edge computing, and mobile cloud computing as alternative paradigms to address limitations in cloud computing, particularly concerning latency, context awareness, and mobility support. The paper aims to holistically analyze security threats, challenges, and mechanisms inherent in all edge paradigms, while also highlighting potential synergies and collaboration opportunities.

Key management remains a crucial aspect in wireless sensor networks, especially in multi-phase deployments, where specific solutions are required to ensure network connectivity, replace dead sensor nodes, or extend coverage areas [2][3]. In "Dynamic key management algorithms in wireless sensor networks: A survey" [2], researchers review key management schemes, emphasizing the need for solutions adapted to multiple deployments of sensor nodes. Similarly, "A survey of key management schemes in multi-phase wireless sensor networks" [3] provides insights into the advantages and disadvantages of existing key management schemes.

Security mechanisms, including dynamic key management systems, play a vital role in safeguarding wireless sensor networks from vulnerabilities inherent in their wireless nature [4]. In "Dynamic outsourced auditing services for cloud storage based on batch-leaves-authenticated Merkle hash tree" [4], the focus is on security mechanisms for wireless sensor networks, particularly through dynamic key management systems.

Furthermore, advancements in quantum computing have sparked interest in exploring the efficiency of quantum algorithms for cryptographic applications, such as computing elliptic curve discrete logarithms [5]. "Quantum resource estimates for computing elliptic curve discrete logarithms" [5] provides insights into the efficiency of quantum algorithms in cryptography.

3. OVERVIEW OF THE SYSTEM

3.1 Existing System

One of the most popular centralized key management schemes is the logical key hierarchy (LKH) which was proposed by Wong et. al in [5] and Wallner et. al in [6]. Most of the proposed centralized protocols utilize a common TEK for all group members. The key tree in the LKH-based schemes reduces the number of messages to log(n), where n is the number of group members. These messages are required for updating the TEK whenever there are member changes. Baugher et al. defined a common architecture for multicast security key management protocols. Sun et al. proposed a multigroup key management scheme which achieves hierarchical group access control.

3.1.1 Disadvantages of Existing System

i. Existing centralized key management schemes, such as the logical key hierarchy (LKH), often rely on a common temporary encryption key (TEK) for all group members, leading to potential security vulnerabilities.
ii. Key tree-based schemes used in traditional systems can result in inefficiencies, particularly in managing node join and leave operations over time.
iii. Hierarchical structures in key management introduce additional overhead due to the involvement of intermediate entities, such as intermediate key managers, which can complicate the management process.

3.2 Proposed System

The emerging blockchain technique offers the potential to build a trusted, fair-minded and decentralized environment for key management scheme in wireless mobile edge networks. Besides, keeping private keys locally and storing public keys in the blockchain can reduce the overhead of rekeying process. Because when users move into a new group, their records (i.e., public keys) can be traced in the previous blocks in local or higher hierarchical blockchain, so that their identities can be verified quickly. Meanwhile, only if the quick verification is failed, the users need to generate a new key pair (i.e., rekeying) which will be appended to the blockchain. Moreover, the key pair of users will be invalid once they generate a new one, which can reduce the overhead of backward and forward secrecy in the rekeying process.

3.2.1 Advantages of Proposed System

i. The proposed blockchain-based key management scheme offers a decentralized and trustworthy environment for key management in wireless mobile edge networks.
ii. By storing public keys in the blockchain and keeping private keys locally, the system reduces the overhead of rekeying processes.
iii. Quick verification of public key records from previous blockchain blocks minimizes the need for rekeying, enhancing efficiency in group communication.
iv. Generating a new key pair renders the previous pair

invalid, reducing overhead related to backward and forward secrecy in rekeying processes.

3.3 Proposed System Design

In this project work, there are five modules and each module has specific functions, they are:

1. Owner Module

2. Block Chain Manager Module

3. Node server Module

4. Receiver User Module

5. LAN Networks Module

3.3.1 Owner Module:

This module is responsible for managing user registration, login, and authentication processes within the application. It ensures secure access to the platform by verifying user identities and credentials. Additionally, the module handles user roles and permissions, allowing administrators to control access to specific features and functionalities based on user roles. By implementing robust authentication mechanisms, such as password hashing and multi-factor authentication, the module enhances security and protects user accounts from unauthorized access.

3.3.2 Block Chain Manager Module:

Block chain manager will login generate block chain for each group view block chain details of each group view users requests for changing subnetwork assign new block chain key.

3.3.3 Node server Module:

Node server will login to application and show data based on group wise block chain, encrypted data , show user details based on group selection show users who left group and who join in other group.

3.3.4 Receiver User Module:

Receiver Using will login to appication same as mobile user who will request for data and user same group public key to download no need to request if user is in same group just use public key to decrypt data and download.

3.3.5 LAN Networks Module

Using this module LAN Networks will register with application and Login to Add Groups View Changed Users Groups View List of Groups and View Users In Each Group With Block Chain.

3.4 Architecture

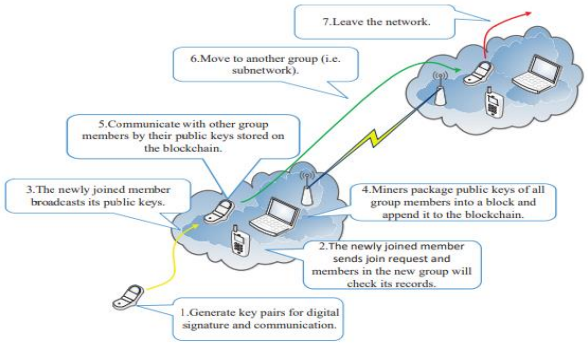
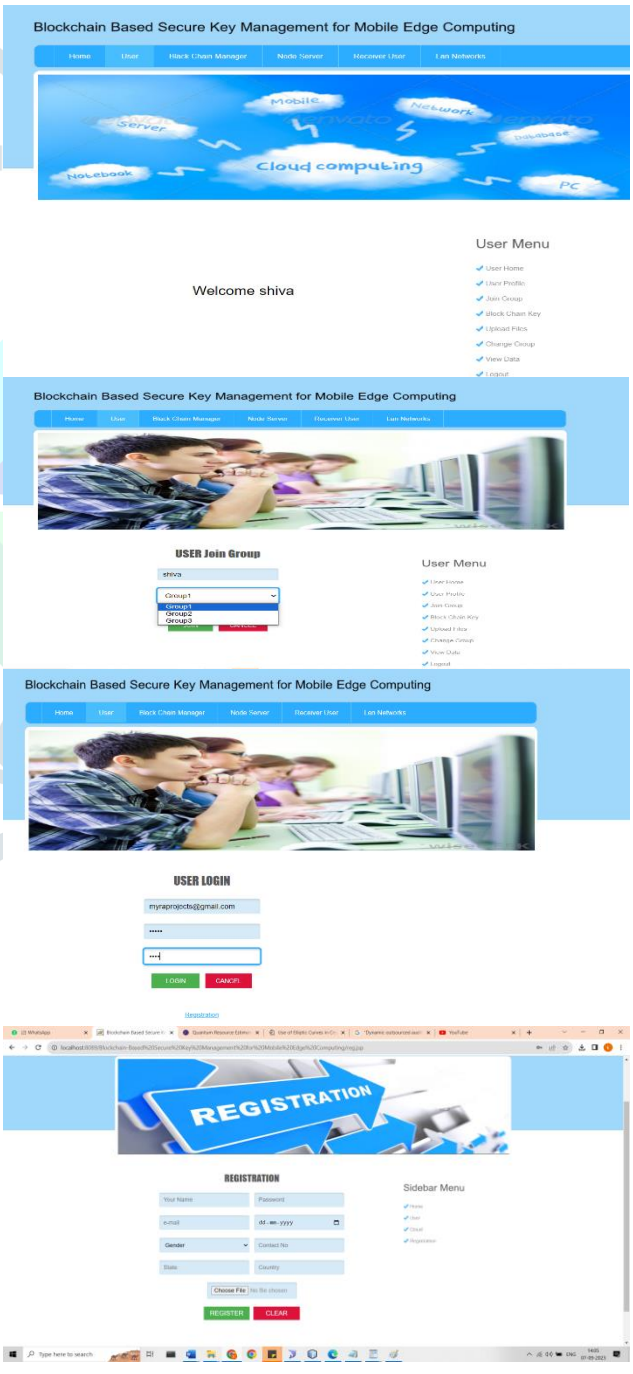
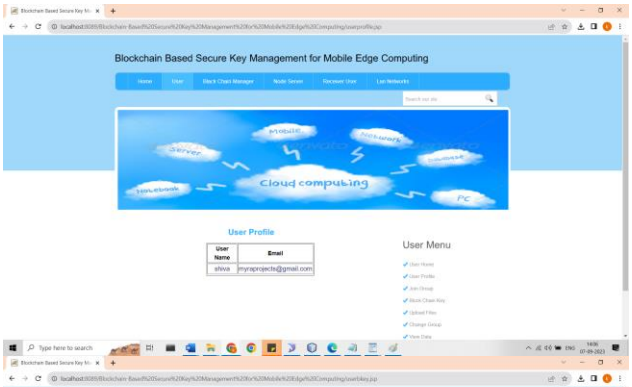


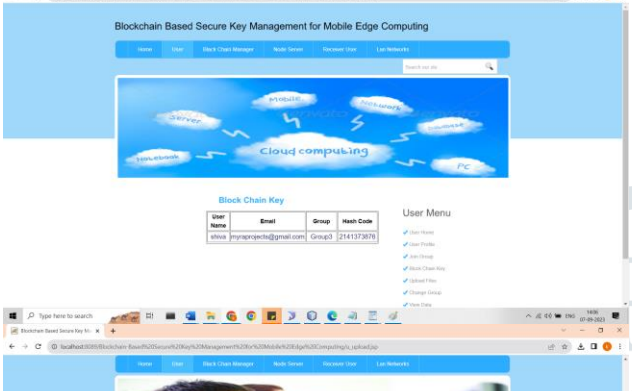
Fig 1: System Architecture

4. RESULT SCREEN SHOTS

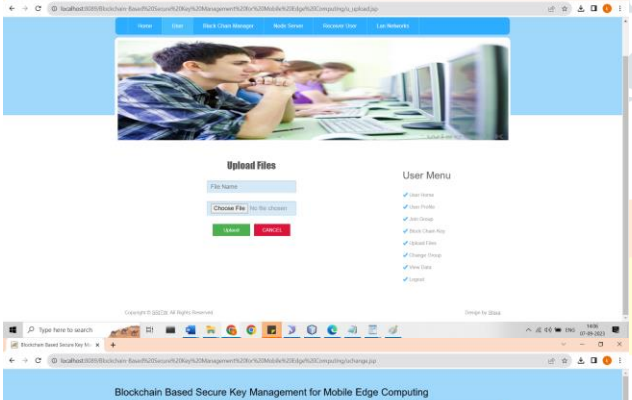


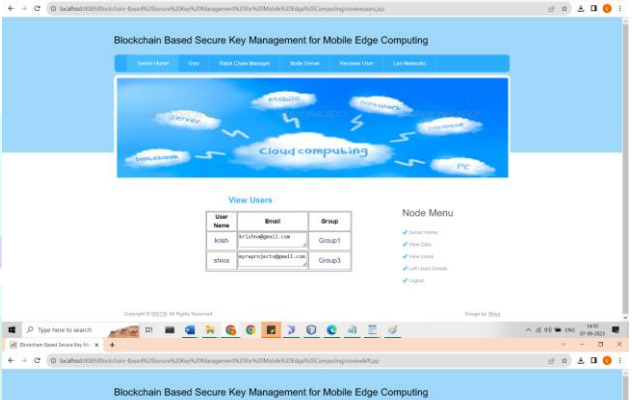

Blockchain Based Secure Key Management for Mobile Edge Computing
User Profile
User Menu


Blockchain Based Secure Key Management for Mobile Edge Computing
Block Chain Key
User Menu

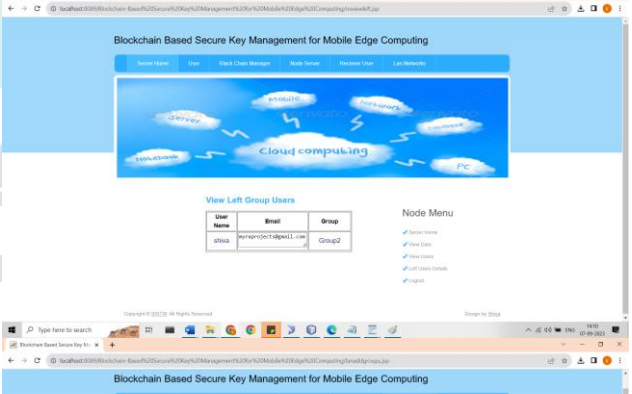

Blockchain Based Secure Key Management for Mobile Edge Computing
Block Chain Key
User Menu

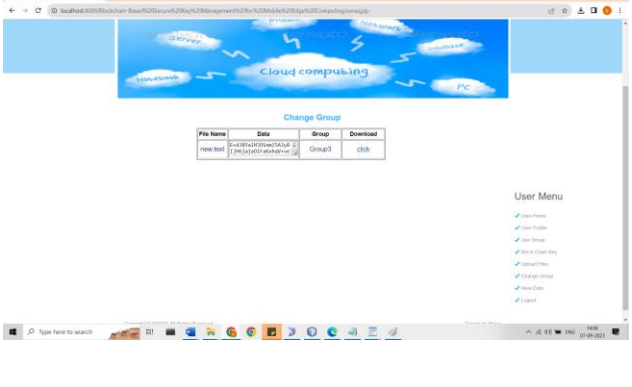

Blockchain Based Secure Key Management for Mobile Edge Computing
View Data
Node Menu

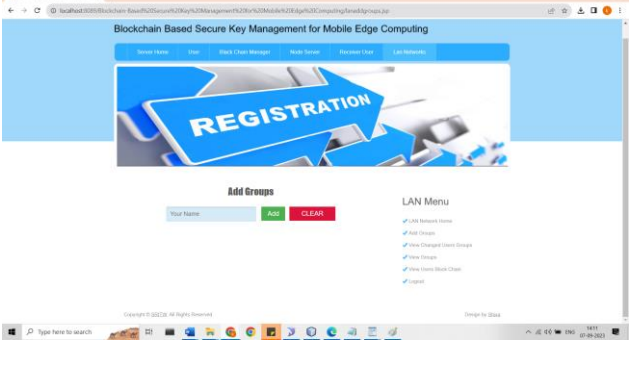

Upload Files
User Menu

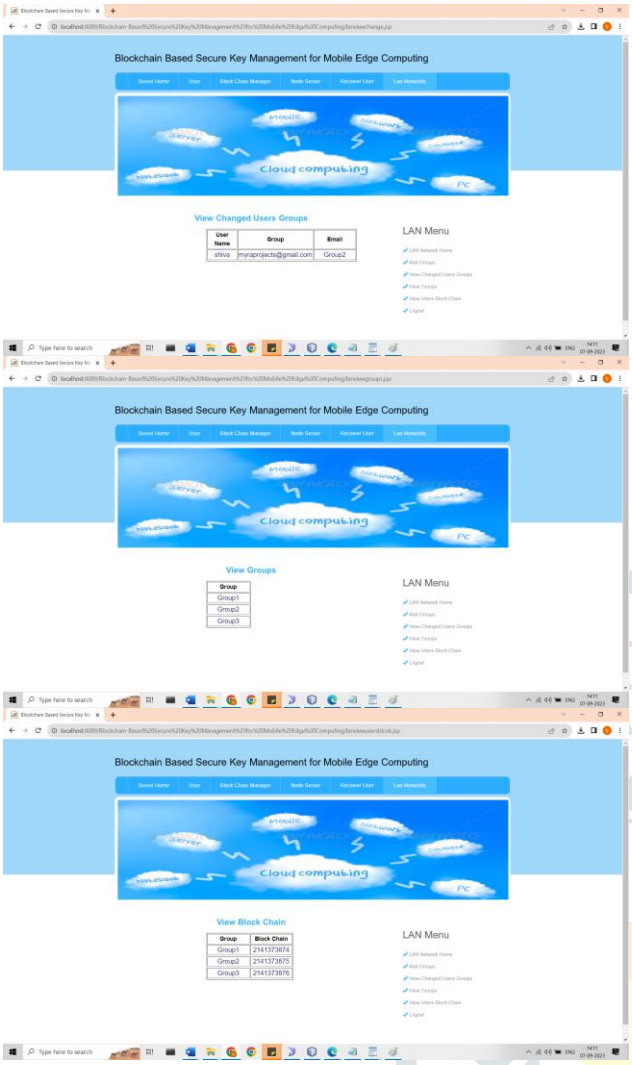

Blockchain Based Secure Key Management for Mobile Edge Computing
View Users
Node Menu


Blockchain Based Secure Key Management for Mobile Edge Computing
Change Group
User Menu


Blockchain Based Secure Key Management for Mobile Edge Computing
View Left Group Users
Node Menu


Change Group
User Menu


Blockchain Based Secure Key Management for Mobile Edge Computing
REGISTRATION
Add Groups
LAN Menu



5. CONCLUSION

We proposed a blockchain-based key management scheme that enables mobile devices in MEC to communicate securely while enjoying the flexibility of moving between subnetworks. In addition to avoiding single point of attacks, the proposed scheme can minimize the computation, communication, and storage overheads, that are associated with key generation, key distribution and key storage respectively. We performed a detailed security analysis of the proposed scheme based on the attack to demonstrate its security strength in a mobile environment. Experimental results are undertaken to show that the proposed scheme significantly outperforms the existing works DKM (in terms of computation overhead) and TKM (in terms of computation and communication overhead). Finally, utilizing the deep reinforcement learning to train the optimal parameters will be the future work.

6. REFERENCES

[1] (2019). Wikipedia: E-coupon. [Online]. Available: https://en.wikipedia.org

[2] C. Blundo, S. Cimato, and A. De Bonis, "Secure E-coupons," Electron. Commerce Res., vol. 5, no. 1, pp. 117_139, Jan. 2005.

[3] (2016). World Mobile Coupons Market to Grow at 73.1% CAGR to 2020. [Online]. Available: https://www.prnewswire.com/news-releases/world-mobile-coupons-market-to% -grow-at-7314-cagr-to-2020-603320306.html

[4] (2017). Coupon Fraud is Crime, Even if it Feels Harmless: Coupon Counselor. [Online]. Available: https://goo.gl/2emab1.

[5] S.-C. Hsueh and J.-H. Zeng, "Mobile coupons using blockchain technology," in Proc. Int. Conf. Intell. Inf. Hiding Multimedia Signal Process. Springer, 2018, pp. 249_255.

[6] A. Knight and N. Dai, "Objects and the web," IEEE Softw., vol. 19, no. 2, pp. 51_59, Mar. 2002.

[7] (2018). Quorum. [Online]. Available: https://github.com/jpmorganchase/quorum

[8] (2017). Coupon Statistics: The Ultimate Collection. [Online]. Available: https://blog.accessdevelopment.com/ultimate-collection-coupon-statistic%s

[9] (2017). emphDigital Coupon Marketing_Statistics and Trends. [Online]. Available: https://www.invespcro.com/blog/digital-coupon-marketing

[10] (2019). Digital Coupons Continue to be the Fastest Growing Method of Redemption due to Shoppers' Increased Demand for Convenience. [Online]. Available: https://www.globenewswire.com/news-release/2019/02/13/1724510/0/en/Digi%tal-Coupons-Continue-to-be-the-Fastest-Growing-Method-of-Redemption-Due-to-Sho%ppers-Increased-Demand-for-Convenience.html

[11] (2017). The Coupon Insider: Digital vs. Paper Coupons. [Online]. Available: https://livingonthecheap.com/coupon-insider-digital-paper-coupons//

[12] R. G.-P. M.-V. Agarwal and N. Modani, "An architecture for secure generation and verification of electronic coupons," in Proc. USENIX Annu. Tech. Conf., Boston, MA, USA, Jun. 2001, p. 51.

[13] S.-C. Hsueh and J.-M. Chen, "Sharing secure m-coupons for peer-generated targeting via eWOM communications," Electron. Commerce Res. Appl., vol. 9, no. 4, pp. 283_293, Jul. 2010.

[14] R. Rivest, "The MD5 message-digest algorithm," Tech. Rep., 1992.

[15] C.-C. Chang, C.-C. Wu, and I.-C. Lin, "A secure e-coupon system for mobile users," Int. J. Comput. Sci. Netw. Secur., vol. 6, no. 1, p. 273, 2006.

[16] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," Appl. Innov., vol. 2, nos. 6_10, p. 71, 2016.

[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008.

[18] M. Szydlo, "Merkle tree traversal in log space and time," in Proc. Int. Conf. Theory Appl. Cryptograph. Techn. Springer, 2004, pp. 541_554.
[19] M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc. OSDI, vol. 99, 1999, pp. 173_186.
[20] N. Szabo, "Smart contracts: Building blocks for digital markets," Tech. Rep., 2018.
[21] V. Buterin, "A next-generation smart contract and decentralized application platform," Tech. Rep., 2014.