Journal of Information Hiding and Multimedia Signal Processing ©2025 ISSN 2073-4212
Ubiquitous International Volume **16**, Number **2**, June **2025**

A Decentralized System Utilizing Blockchain Technology to Safeguard Sensitive Data from Unauthorized Access

Ahmed A. El-Douh

Cybersecurity Technology Engineering Department
College of Engineering Technology, Ashur University, Baghdad, Iraq
Applied Science Research Center
Applied Science Private University, Amman, Jordan
ahmed.abdelrahim@au.edu.iq

Tareef S. Alkellezli

Department of Cybersecurity Engineering
Ashur University, Baghdad, Iraq
tareef.alkellezli@au.edu.iq

Humam M. Al-Doori

Department of Computer Engineering Techniques
Al-Yarmok University College, Diyala, Iraq
humam.aldoori@al-yarmok.edu.iq

Received January 14, 2025, revised April 22, 2025, accepted April 23, 2025.

Abstract. *Abstract: The rapid growth of the internet and online services has provided customers with a vast array of PC services, particularly in the COVID-19 age. Data sharing is an important application that has several benefits. Certain nations have enacted regulatory measures to rectify data privacy violations and reinstate user control over data. Numerous academics have developed security strategies to solve access control, security, and privacy concerns. Existing solutions contain shortcomings and must be overseen carefully. This study proposes the Confidence Clans Model (CCM) to solve these gaps. The proposed model presents a blockchain-based data-sharing system optimized for closed groups of non-anonymous users. The proposed model overcomes the verification problem, making the system more robust. A detailed investigation into the amount of necessary effort and time was carried out. Moreover, the results were compared to those of comparable works. The proposed model is efficient and reliable.*
Keywords: Cybersecurity, Blockchain, Authentication, Privacy-preserving, COVID-19.

1. **Introduction.** Today's communications are driven primarily by the desire to share data. Data sharing across organizations has become a requirement for modern systems [1]. These systems rely heavily on trustworthy third parties for data transit, storage, and protection. However, consumers face a number of privacy and security issues as a result of their greater reliance on trustworthy third parties and the sophistication of cyberattacks [2]. Certain governments have taken the lead in enacting regulatory measures to address such data privacy infractions and to reintroduce users' control over their data. General Data Protection Regulation (GDPR) became law in May 2018 in the European Union. A wide range of situations where personal data is processed is covered by GDPR. It implies some significant legal duties that data controllers and data processors must adhere to

protect data subjects. For example, GDPR defines the conditions for lawful processing of personal data, including the data subject's explicit consent, data processing that is fair, lawful, and transparent, and data correction and deletion [3]. In the financial sector, blockchain has proved that transparent, secure, and auditable transactions are achievable when a decentralized network of peers is paired with a public ledger [4].

The peer-to-peer network's role is to support, maintain, and facilitate the blockchain. These participants may be anonymous individuals cooperating to provide computational capacity for a public network or diverse organizations providing computing infrastructure for an enterprise blockchain application via a permissioned consortium network. Each participant maintains the same version of this ledger locally and agrees on any changes to its status [5]. In a wide range of fields, blockchain-based solutions are increasing in number. Due to blockchain's capacity to provide a safe and transparent application infrastructure, it has been used to create a secure data management environment that enables sharing of personal data via encryption and access control [6]. Several studies have examined blockchain's legal and technical feasibility to create GDPR-compliant personal data management systems [7]. Others have leveraged blockchain technology to develop solutions that enable secure data sharing while auditing and tracing data operations for increased transparency, accountability, and provenance tracking [8][9][10]. However, only users who have been authenticated and allowed permission to access the system can do so. In such circumstances, it will be vulnerable to a variety of security concerns, including the unauthorized acquisition of data, the modification of data, and the theft of an individual's identity. Indeed, security concerns continue to be the primary impediment to widespread adoption and deployment.

2. **Background.** The emergence of public-key cryptography is the most significant and the major revolution in cryptography's history [11]. The notion of public key cryptography was developed in order to overcome the most baffling issue inherent in conventional symmetric cryptosystems: the proliferation of private keys and their lack of confidentiality. Public-key cryptography represents a significant departure from prior generations of cryptography [12]. For one thing, public-key algorithms are based on mathematical functions rather than substitution and permutation. Additionally, public-key cryptography is asymmetric, requiring the use of two distinct keys, as opposed to symmetric encryption, which uses a single key. Two keys have significant implications for key distribution, confidentiality, and authentication. The public-key cryptography consists of two keys, the first of which is used for data encryption and the second of which is used for data decryption. Public-key encryption gained prominence as a result of the development of two pioneering concepts: first, a solution to the key distribution problem inherent in symmetric key cryptography, and second, a digital signature system [13]. Elliptic curve cryptography (ECC), a recent type of public-key encryption, offers more security per bit than is currently used in other forms of cryptography [14]. Furthermore, it is feasible to think of a hash function as a building block of an algorithm, as it is a fundamental component of numerous cryptographic techniques. Hash functions utilized in cryptography are mathematical constructs that cannot be conceptualized in any other context. Hash functions are a form of cryptographic primitive that does not require the use of a key and are commonly used in protocols. Secure Hash Algorithms, popularly known as SHA, are a collection of cryptographic methods meant to maintain the confidentiality of data [15]. The Keccak algorithm was chosen as the winner of the SHA-3 competition for a variety of reasons, including its large security margin, novel design approach, and excellent performance in hardware implementations. However, the speed of algorithms (together with security) is a critical factor in algorithm selection [15].

3. **Literature Review.** This section reviews the most recent work relevant to the proposed scheme. It examines the literature regarding the vision and identifies the strengths and flaws of pertinent models. Numerous researchers have made significant contributions to the literature by developing security schemes aimed at addressing the efficiency, security, and privacy concerns associated with access control and data exchange [16].

In the scheme in [17], the authors presented a blockchain-based data-sharing system to address the access control issues associated with sensitive data hosted in the cloud. They deployed secure cryptographic techniques to control access to sensitive data pools via a permissioned blockchain. After verifying their identities and cryptographic keys, users/owners of data can access electronic medical records from a shared repository. There may not be enough security for sensitive data because of this solution's user-level access control mechanism. The article [18] proposed an IoT architecture based on blockchain technology. In their system, there are three distinct blockchains that all work together: a private blockchain that is specific to each use case, a public blockchain that all users can access, and an underlying blockchain that serves as a layer of security (public). Despite resolving the identification issue, the proposed solution has several drawbacks, such as the fact that each operation causes at least eight network connectivity, which can quickly flood the entire medium of communication in the event of high node activity, and the fact that local blockchains are not distributed but centralized, which goes against the principle of blockchains since it limits their advantage and availability. The scheme in [19] utilizes cryptography schemes and blockchain contracts to allow cloud data access control without involving the provider in the realm of data sharing. To do this, encrypted data is stored in the storage, and access to this data is facilitated via numerous contracts. This article [20] uses blockchain and several cryptographic algorithms to propose a novel mutual authentication scheme for IoT devices that achieves anonymity and privacy. Detailed authentication procedures for both stationary and mobile IoT devices are described. However, this scheme lacks resource efficiency and is complicated. These distinctions make our work more realistic.

To address security concerns, we examine a selection of blockchain-based methods that seek to achieve such integration and demonstrate their effectiveness. Due to their computational and communication complexity, however, several of these solutions do not meet the efficiency requirements for security issues.

4. **Proposed Model.** The primary goal of our proposed model is to establish safe virtual zones in a variety of settings. The focus of our approach is on tracking down the contacts of an infected person and ensuring that information can be safely shared between various parties involved in the system as a whole. Our scheme will incorporate a variety of different gadgets. Every single physical or virtual device needs to be reachable, and there ought to be content that users are able to access regardless of where they are located. However, it is very necessary for there to be no users of the system who are not authenticated and permitted. In that case, it will be susceptible to a wide range of security concerns, such as the theft of data, the modification of data, and the takeover of an individual's identity.

The proposed solution is an innovative decentralized architecture dubbed the Confidence Clans Model (CCM) that enables robust device identification and authentication. Additionally, it safeguards the integrity and availability of data. To accomplish this, we will leverage the security features of blockchains to establish safe virtual zones where the members can identify and trust each other.

4.1. **Architecture Model.** The establishment of safe virtual regions across a variety of environments is our primary objective with this strategy; we introduce a solution based

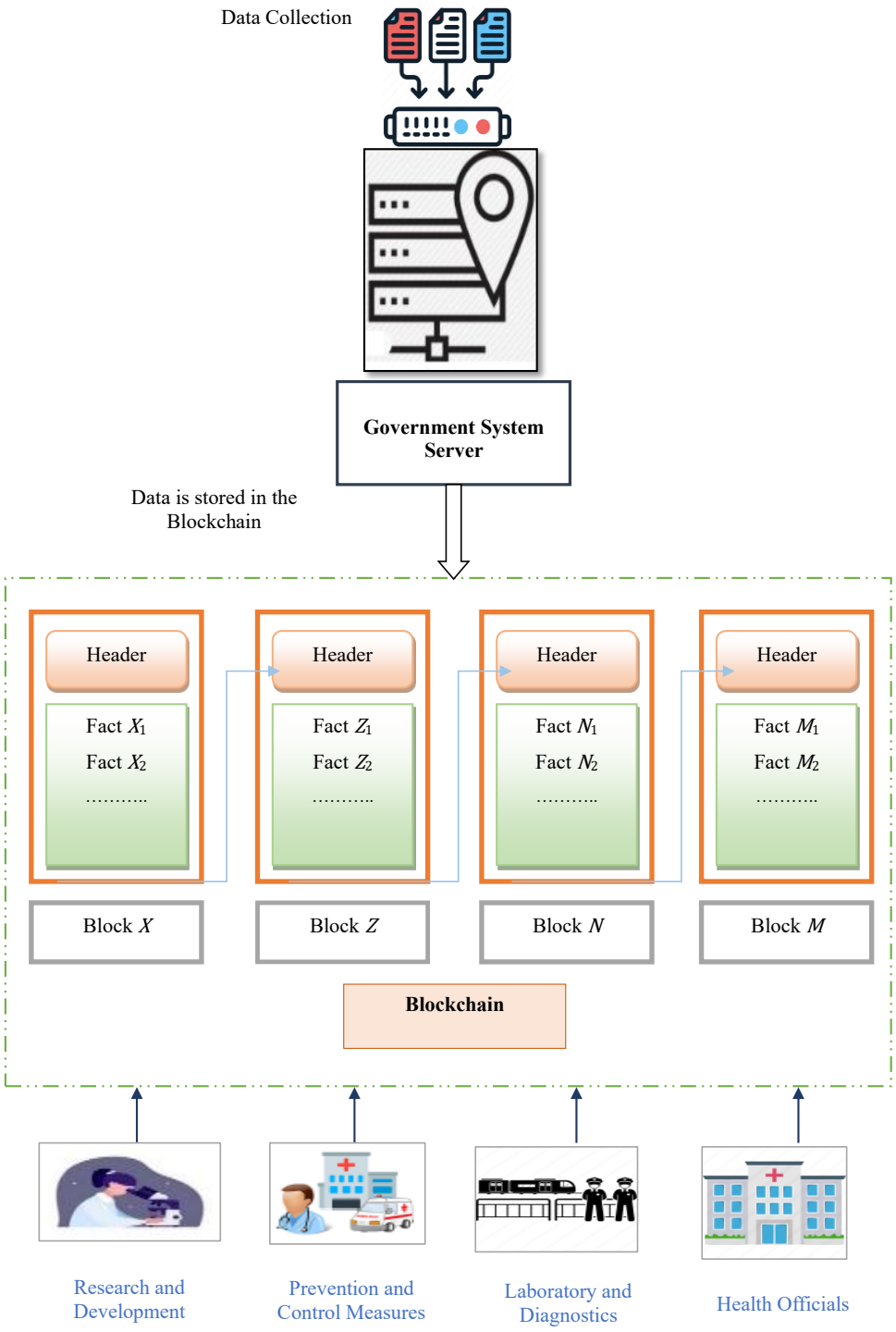

FIGURE 1. The General Model of the CCM Scheme

on the blockchain as an innovative decentralized architecture that enables robust device identification and authentication. The proposed CCM scheme architecture and all the ecosystem's components are illustrated in Fig.1. To begin with, the Government System Server stores shared data. Second, the members who are connected belong to distinct zones (Health Officials, Laboratory and diagnostics, Prevention and control measures, Research and development). Only these zones will be granted access to data. We refer to these zones as trust clans. Thus, a trustworthy clan is a community in which every single person has complete confidence in the other people in the clan. It is guarded and inaccessible to devices that are not members of the clan. Communication in the system is thought of as a transaction, and the blockchain must check it to make sure it is real before it can be regarded. For illustration, suppose device A wants to communicate with device B; (1) A will transmit the message to the blockchain, and (2) the blockchain will verify the transaction if device A is trustworthy. Finally, (3) B can read the message.

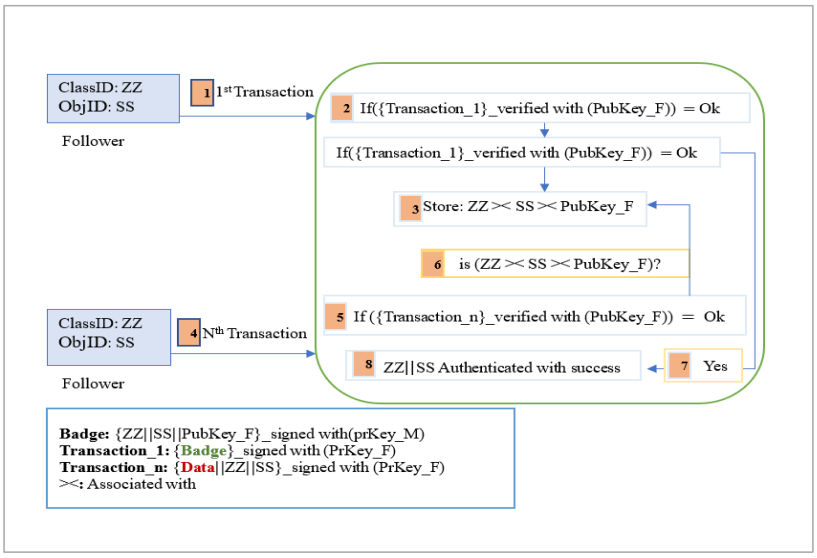

FIGURE 2. The Communication Process within the CCM Scheme

4.2. **System Operation Model.** The operation of our model and the ecosystem's lifecycle is illustrated in the following stages. The connected nodes belong to a variety of categories (Health Officials, Laboratory and diagnostics, Prevention and control measures, Research, and development). Preparing Phase: Our approach can be applied to a vast array of use situations and requires no specific hardware. However, a startup phase is necessary. In the latter, just one device is identified as the Master of the clan, akin to a certification authority. Additionally, each object that is a part of the system is referred to as a Follower. Using an Elliptic Curve, each Follower creates a pair of keys that can be either private or public (EC). Then, a structure known as a badge is given to each Follower. This badge is a 64-byte lightweight certificate and contains the following information about the Follower's status:

1. Use a ClassID, which identifies the group that the object will be part of once it has been created.
2. Avoid An objectID (objID), also known as an identifier, represents the Follower within the clan.

3. A PkAdd, also known as a public key address, is the address that the Follower makes public. It includes the first twenty bytes of the Keccak (SHA-3) hash that is associated with the Follower's public key.
4. A Signature structure that is generated by the Elliptic Curve Digital Signature Algorithm (ECDSA) signature using the private key of the Master.

ECDSA has some benefits, including smaller key sizes and faster signature times. The Signature encompasses the Keccak hash of the ClassID, the objectID, and the PkAdd concatenation. The initialization phase, during which the Master selects a Class identifier (ClassID). Additionally, each object comes with a badge signed by the Master. Afterward, the next stage is to create the clan on the blockchain. The transaction that the Master starts off with must include both his personal identity and the identifier of the new group that he wants to create. The group's formation involves the clan's development at the blockchain level. The blockchain verifies that both the classID and the Master's objectID are unique. The clan is produced if the transaction is valid. Due to the public nature of the blockchain, any user can build a clan. Following that the followers send transactions to relate to their particular clans. At the blockchain level, a smart contract makes sure that the Follower's object ID is unique and then checks the validity of the Follower's badge using the Master public key. Once a Follower's initial transaction (association request) is successful, the latter is no longer required to identify oneself using its badge (sends it within the exchanged messages). The object cannot be associated with the clan if one of the prerequisites is not met. The processes are illustrated in Fig.2 as the following:

1. An association request is reflected in the transaction that was completed for the first customer. The message that was delivered includes the badge of the Follower, as well as a cryptographic signature that was generated using the Follower's private key.
2. When the blockchain receives the transaction, it verifies the validity of the transaction by com-paring the signature to the public key of the Follower. Verifying the Follower's badge with the Master's public key is the next stage in the process because the Master's public key represents the entity that signed the badge.
3. If the badge is authentic, the blockchain will store an association between the badge's classID, objectID, and public key. This association will be used to verify the badge in the future. As a consequence of this, it stores the values (ZZ, SS, and PubKey F).
4. The fourth step provides an explanation of the situation in which the Follower sends a transaction that is distinct from the association request (transaction n). This transaction consists of four parts: the data that was sent, ZZ, SS, and an ECDSA signature that was generated by utilizing the Follower's private key.
5. Once the transaction has been received by the blockchain, the blockchain will verify its authenticity by comparing the signature to the Follower's public key.
6. If the signature is legitimate, the blockchain will check to make sure that the public key that was used to validate the transaction is stored and connected to the class ID and object IDs that were given as part of the transaction; if this is the case, then the transaction will be allowed to proceed.
7. If the association has been stored and is still valid.
8. The authorization of the node was completed without any problems.

The scalability of the suggested Confidence Clans Mechanism (CCM) is a vital criterion for evaluating its efficacy across various network sizes. With the escalation of participating devices and users, the system must uphold its efficiency, security, and minimal communication expenses. The utilization of a public blockchain guarantees that CCM reaps the advantages of decentralized security features; yet, the transaction overhead and processing duration may fluctuate based on the network size. In small-scale networks, transaction

validation and data transfers transpire with low latency, however in larger-scale implementations, heightened blockchain traffic may adversely affect performance. Our methodology mitigates these issues by optimizing communication through the reduction of unnecessary contacts and the utilization of a hierarchical hierarchy within the clans. The consolidation of followers beneath a master node facilitates transaction execution, minimizing computational burden. Furthermore, the implementation of lightweight cryptographic operations guarantees that scalability is intact. Future improvements will concentrate on adaptive scaling strategies to boost CCM's performance in dynamic and expansive situations.

5. **Security Analysis and Discussion.** Any scheme must adhere to security criteria in order to maintain the ecosystem's longevity and resilience. In this subsection, we examine how our proposed model satisfies various security requirements and how is protected against various attacks.

- Mutual Authentication and Message Integrity: Each object in the ecosystem utilizes a badge (for the initial transaction), which is a certificate equivalent, as explained previously. During the initialization phase, the badges are only delivered to genuine objects. All communications exchanged are signed using the ECDSA technique using the private keys associated with those badges. Thus, signatures secure both the device's authentication and the message's integrity.
- Identification: Each object has a unique identifier (objID), which is linked to a classID, and a public address (generated from its public key) that it can use to communicate. The Master's signature on the badge serves as a seal of approval for this identity. This object's private key is used to sign each message it sends. This key is tied to the object's unique identity. Because of this, the system is able to recognize it with ease.
- Non-repudiation: Since the messages are signed with a private key that is only known by the object's owner, only the owner can use them. This is because only the owner of the private key knows it. Consequently, it is unable to contest the fact that a message was signed.
- Scalability: The proposed scheme is designed over a public blockchain, which is built above a peer-to-peer network. Peer-to-peer networks are one of the most effective methods for attaining scalability on a big scale.
- Sybil Attack Protection: In the proposed scheme, we can only assign a single identity to each object, and we can only assign a single key pair to each identity at a given time. Every communication message needs to be signed with the private key associated with the identity. An additional benefit is that an attacker is unable to use counterfeit identities because the system requires verifying each and every identity.
- Spoofing Attack Protection: Similar to authentication defenses outlined above, an attacker is unable to spoof the identity of another object because he lacks the object's private key.
- Protection Against Message Replay: Every message is considered a transaction. A timestamp is needed to identify each transaction uniquely, and an acceptable level is required for a transaction to be valid. Therefore, an intruder will be unable to respond to messages, as the consensus mechanism will ignore them. Examines the resistance of blockchains against attacks utilizing the replay protocol.
- Protection against DoS Attacks: Because blockchains are completely decentralized, they are resistant to DoS attacks. In fact, services are replicated and spread over multiple network nodes. That is, even if an attacker successfully blocks one node, cannot block all the other nodes. Additionally, because transactions are costly, an

Table 1. Nodes Capability

Node	CPU	CPU Speed	RAM	OS
HP	X64	1.99 GHZ	12 GB	Ubuntu
Asus	X64	2.00 GHZ	8 GB	Ubuntu

attacker is discouraged from spending money by sending a large number of transactions.

6. **Evaluation Framework.** The proposed model was implemented based on the characteristics detailed in Table 1. The applications for the end nodes are written in the C++ programming language. We used Ethereum as the blockchain. We used TestRPC, an Ethereum utility for testing and development purposes that simulates blockchain interactions without the cost associated with running an actual Ethereum node. On the public Ethereum blockchain, an approach deployed using TestRPC behaves identically. A C++ interface was developed to facilitate the encoding and decoding of data to and from Ethereum9, specifically to facilitate interactions between end nodes and the blockchain. These exchanges are accomplished through the use of JSON11.We utilized TestRPC, an Ethereum tool designed for testing and development, which simulates blockchain interactions without incurring the expenses of operating a real Ethereum node. On the public Ethereum blockchain, an approach deployed using TestRPC behaves identically. As a result, our solution is fully compatible with Ethereum. Indeed, our proposed scheme is dependent on a public blockchain, we collect all our analytics at the device level to determine the efficacy of our strategy. The following results pertain to the experiments in which we determined:

1. The time required to prepare the association request.
2. The amount of time required to prepare a data message.
3. The amount of Central Processing Unit (CPU) power consumption required to prepare an association request.
4. The amount of power that must be consumed by the central processing unit in the preparation of a data message.
5. Power consumption of the Network Interface Card (NIC) when sending an association.
6. The amount of power consumed by NIC when sending a data message.

In the framework of this scheme, our principal focus pertains to the aggregate number of Followers that are assimilated. In actuality, the Master is merely required to execute a solitary transaction to facilitate the establishment of the clan. The follower aligns themselves with a particular entity, but the badge is not displayed, the underlying transaction remains unchanged. Consequently, the diminished capabilities of this have resulted in a positive outcome of reduced communication costs. Once the establishment of the clan has taken place, the Master will possess the capacity to assume the role of a Follower.

This role encompasses the responsibility of engaging in communication with the clan through the exchange of messages. Additionally, the Master will be entrusted with the task of signing badges.

7. **Performance Analysis.** In this section, we conduct the performance evaluation of our model. The comparative performance comparison is based on the three parameters: transaction time (T.P.), CPU power consumption (CPU P.C.), and NIC power consumption (NIC P.C.). The computational cost of the proposed CCM Scheme is listed in Table 2. The time is measured in milliseconds, while the CPU power consumption and NIC power

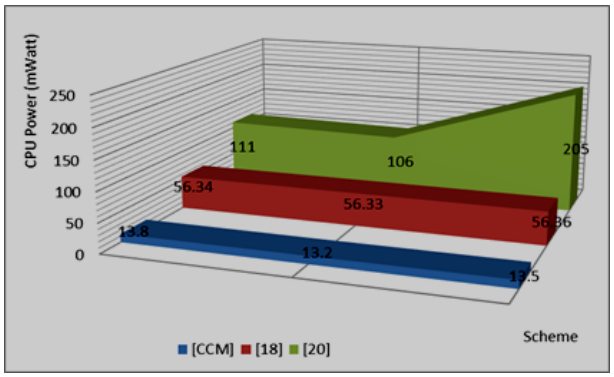

FIGURE 3. Evaluation of Energy Consumption

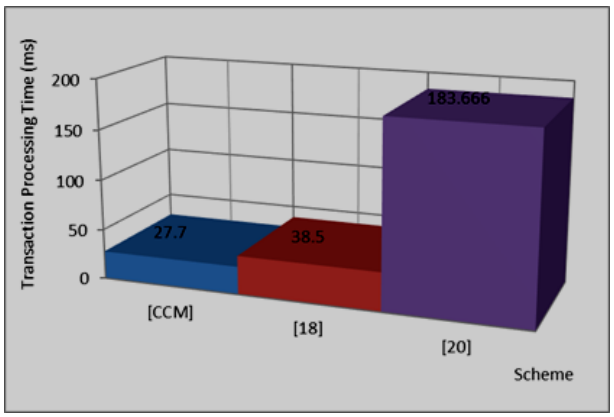

FIGURE 4. The Average Transaction Processing Time

TABLE 2. Experimental Results of the Proposed CCM Model

Samples	T.P. Time	CPU P.C.	NIC P.C.
Round 1	27.2	13.8	28.2
Round 2	25.4	13.2	31.1
Round 3	30.5	13.5	30.2
Round 4	32	13.2	32.3

consumption are in mWatt. The existing methods that are used by more researchers build authentication models that can adequately secure data. But we try to achieve in the proposed CCM Model more security and robustness better than the normal methods or the enhanced method.

Next, we will take into account the analysis of the computational cost in the CCM model and other related schemes A. Dorri et al. [18], H. Guo et al. [20]. The comparative performance comparison is based on some parameters mentioned above. The execution times are measured in milliseconds, and different rounds of plain text were used. The CCM model was developed in contrast to the work of [18] and [20]. Fig.3 demonstrates the superiority of the CCM over the [18] and [20]. schemes in terms of energy consumption. Furthermore, for comparative value approximation, we also present the average performance of the algorithms given in Fig.4 In comparison with [18] and [20]. The CCM model consumes less time according to the average time in all phases.

8. **Conclusions.** In this paper, we proposed a novel approach called Confidence Clans Mechanism, or CCM for short. In this approach, protected virtual zones are created so that electronic devices can connect with one another in the most foolproof way conceivable. It is possible to apply the CCM strategy to a wide variety of different sorts of industries, services, and settings. As a result of the fact that it is built on top of a public blockchain, it is able to make use of all of the safety features that are offered by other blockchains. In addition, we set the security criteria for the access control of sensitive data, and we verified that the security standards were adhered to throughout the process. A detailed investigation into the amount of effort and time that was necessary was carried out, and the findings were compared to those obtained from comparable work. We intend to enhance the concept further in future work so that it can permit controlled communication between certain clan groupings. This will require more work on our part. In addition, the construction of a system for the elimination of certificates that have been compromised on various devices. The scheme that has been proposed is one that is not only successful but also adaptable to changing circumstances. Additionally, our proposed scheme is both efficient and scalable.

REFERENCES

[1] Dao, T.K., Trong-The Nguyen, Thi-Xuan-Huong Nguyen and Nguyen, T.D., 2024. Recent Information Hiding Techniques in Digital Systems: A Review. J. Inf. Hiding Multim. Signal Process., 15(1), pp.10-20.

[2] Fraga-Lamas, P. and Fernández-Caramés, T.M., 2019. A review on blockchain technologies for an advanced and cyber-resilient automotive industry. IEEE access, 7, pp.17578-17598.

[3] Labadie, C. and Legner, C., 2023. Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. Journal of Information Technology, 38(1), pp.16-44.

[4] Hegde, Sandeep Kumar, and Rajalaxmi Hegde. "An Efficient and Transparent Financial Transaction System using Decentralized Finance (DeFi) based on Blockchain Technology." In 2024 2nd International Conference on Recent Advances in Information Technology for Sustainable Development (ICRAIS), pp. 18-23. IEEE, 2024.

[5] L. Ismail, "Lightweight Blockchain for Healthcare," IEEE Access, vol. 7, pp. 149935–149951, 2019, doi: 10.1109/ACCESS.2019.2947613.

[6] Agrawal, K., Aggarwal, M., Tanwar, S., Sharma, G., Bokoro, P.N. and Sharma, R., 2022. An extensive blockchain based applications survey: tools, frameworks, opportunities, challenges and solutions. IEEE Access, 10, pp.116858-116906.

[7] L. Campanile, M. Iacono, F. Marulli, and M. Mastroianni, "Designing a GDPR compliant blockchain-based IoV distributed information tracking system," Inf. Process. Manag., vol. 58, no. 3, p. 102511, 2021, doi: 10.1016/j.ipm.2021.102511

[8] Hader, M., Tchoffa, D., El Mhamedi, A., Ghodous, P., Dolgui, A. and Abouabdellah, A., 2022. Applying integrated Blockchain and Big Data technologies to improve supply chain traceability and information sharing in the textile sector. Journal of Industrial Information Integration, 28, p.100345.

[9] Hasan, H.R., Salah, K., Jayaraman, R., Omar, M., Yaqoob, I., Pesic, S., Taylor, T. and Boscovic, D., 2020. A blockchain-based approach for the creation of digital twins. IEEE Access, 8, pp.34113-34126.

[10] Fraga-Lamas, P. and Fernandez-Carames, T.M., 2020. Fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality. IT professional, 22(2), pp.53-59.

[11] Ryan, M. and Ryan, M., 2021. Evolution of Applied Cryptography. Ransomware Revolution: The Rise of a Prodigious Cyber Threat, pp.33-41.

[12] Rana, S., Parast, F.K., Kelly, B., Wang, Y. and Kent, K.B., 2023. A comprehensive survey of cryptography key management systems. Journal of Information Security and Applications, 78, p.103607.

[13] El-Dalahmeh, A., El-Dalahmeh, M., Razzaque, M.A. and Li, J., 2024. Cryptographic methods for secured communication in SDN-based VANETs: A performance analysis. Security and Privacy, 7(6), p.e446.

[14] O. Kebir, I. Nouaouri, L. Rejeb, and L. Ben Said, "Atipreta: An Analytical Model for Time-Dependent Prediction of Terrorist Attacks," Int. J. Appl. Math. Comput. Sci., vol. 32, no. 3, pp. 495–510, 2022, doi: 10.34768/amcs-2022-0036.

[15] Alkakjea, H.A.M., Obaid, A.L., Rasool, Z.I. and Fakhruldeen, H.F., 2025. Security Encryption Processes Based on Deep Learning Systems. J. Inf. Hiding Multim. Signal Process., 16(1), pp.389-400.

[16] Zubaydi, H.D., Varga, P. and Molnár, S., 2023. Leveraging blockchain technology for ensuring security and privacy aspects in internet of things: A systematic literature review. Sensors, 23(2), p.788.

[17] Xia, Q.I., Sifah, E.B., Asamoah, K.O., Gao, J., Du, X. and Guizani, M., 2017. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain. IEEE access, 5, pp.14757-14767.

[18] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," 2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.

[19] I. Sukhodolskiy and S. Zapechnikov, "A blockchain-based access control system for cloud storage," Proc. 2018 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. ElConRus 2018, vol. 2018-January, pp. 1575–1578, 2018, doi: 10.1109/EIConRus.2018.8317400.

[20] H. Guo, W. Li, M. Nejad, and C. C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," Proc. - 2019 2nd IEEE Int. Conf. Blockchain, Blockchain 2019, pp. 44–51, 2019, doi: 10.1109/Blockchain.2019.00015.