Revolutionizing Digital Healthcare: Unlocking the Power of Blockchain with an Optimized Fuzzy Logic Approach to Authentication and Key Agreement

Aitizaz Ali , Ting Tin , Bander Al-rimy , Taiseer Abdalla Elfadil Eisa * , Hong-Seng Gan , Jun Chaw

Posted Date: 18 July 2023

doi: 10.20944/preprints202307.1191.v1

Keywords: Fuzzy Logic; Blockchain; Smart-contract, Lizard Search Algorithm, Homomorphic Encryption, Cyber attacks.)

Article

Revolutionizing Digital Healthcare: Unlocking the Power of Blockchain with an Optimized Fuzzy Logic Approach to Authentication and Key Agreement

Aitizaz Ali [1], Ting Tin Tin [2], Bander Ali Saleh Al-rimy [3], Taiseer Abdalla Elfadil Eisa [4,*], Hong-Seng Gan [5] and Jun Kit Chaw [6]

[1] School of IT, Unitar International University, Kelana Jaya, Malaysia;aitizaz.ali@unitar.my
[2] Faculty of Data Science and Information Technology, INTI International University, Malaysia; tintin.ting@newinti.edu.my
[3] School of Computing, Universiti Technology Malaysia(UTM), Johar Bahru, Malaysia; bander@utm.my
[4] Department of Information Systems-Girls Section, King Khalid University, Mahayil, 62529, Saudi Arabia Teisa@kku.edu.sa.
[5] School of AI and Advanced Computing, XJTLU Entrepreneur College (Taicang), Xi'an Jiaotong -Liverpool University, Suzhou, Jiangsu, P.R. China 215400; HongSeng.Gan@xjtlu.edu.cn
[6] Institute of Visual Informatics, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia;chawjk@ukm.edu.my
* Correspondence: Teisa@kku.edu.sa

Abstract: Digital healthcare systems play a pivotal role in providing efficient and accessible healthcare services. However, ensuring secure authentication and key agreement mechanisms is essential to protect sensitive patient data and maintain the integrity of the system. The existing methods face limitations in terms of vulnerability to cyber attacks, scalability, and resource utilization. Furthermore, the integration of blockchain technology introduces new complexities that need to be addressed. This research proposes an optimized fuzzy logic approach combined with blockchain technology to address the authentication and key agreement challenges in digital healthcare systems. The proposed solution leverages the flexibility and adaptability of fuzzy logic algorithms to handle uncertainty and imprecision in authentication decisions. By employing fuzzy logic, the system can effectively minimize false positives and false negatives, enhancing the robustness against adversarial attacks. Moreover, the integration of blockchain technology provides a decentralized and tamper-proof infrastructure for securely storing and managing authentication and key agreement data. This ensures transparency and trust in the system, mitigating the risks of unauthorized access and data manipulation. The blockchain-based architecture also enables efficient resource utilization and scalability, allowing the system to handle authentication requests in a timely manner, even in large-scale digital healthcare environments.The proposed method is evaluated by using the NIST Special Database 302 and it shows superior performance compared to existing methods, with minimum False Rejection Rate (FRR), False Acceptance Rate (FAR), and response time. Moreover, the proposed method minimizes communication overhead during the authentication process and resists different cyber attacks including a Replay attack, Man-in-the-middle attack, Denial of Service (DoS) attack, and Impersonation attack. The proposed method achieves excellent performance in terms of security, efficiency, and resistance to various cyber-attacks, making it a promising approach for secure data sharing in P2P cloud environments.

Keywords: fuzzy logic; blockchain; smart-contract, lizard search algorithm, homomorphic encryption, cyber attacks

1. Introduction

In the context of a blockchain-based healthcare system, the CALS algorithm can be applied to optimize various aspects such as resource allocation, data management, privacy preservation, and transaction processing. Here's how it could be utilized:

 doi:10.20944/preprints202307.1191.v1

1. Resource Allocation: The CALS algorithm can be employed to optimize the allocation of healthcare resources, such as medical personnel, equipment, and facilities. It can consider factors like patient demand, resource availability, and cost constraints to determine an optimal allocation strategy.
2. Data Management: In a blockchain-based healthcare system, patient data is stored securely and transparently on the blockchain. The CALS algorithm can help optimize the organization and retrieval of data, ensuring efficient access and maintaining data integrity.
3. Privacy Preservation: Privacy is a crucial aspect in healthcare systems. The CALS algorithm can aid in optimizing privacy-preserving techniques, such as data anonymization and encryption, to protect sensitive patient information while allowing authorized access to necessary parties.
4. Transaction Processing: Blockchain technology relies on efficient transaction processing. The CALS algorithm can optimize the transaction validation and consensus mechanisms, ensuring fast and reliable processing of healthcare transactions while maintaining the security and integrity of the blockchain.

To implement the CALS algorithm in a blockchain-based healthcare system, you would need to define the specific problem you want to optimize and design appropriate fitness functions and crossover operators tailored to that problem. Additionally, you would need to integrate the CALS algorithm into the existing blockchain infrastructure, considering factors such as block creation, validation, and consensus mechanisms. The users also have the requirement of sharing data from a single cloud server to other cloud servers. The data-sharing systems are divided into P2P distributed and centralized data-sharing systems. However, these data-sharing systems contain security issues during the users access the data from the cloud servers [5]. Also, the cloud service provider may get and disclose the personal privacy of the user, and also the cloud service provider may access the data in a manner of illegal. Hence, more secure and effective data access, as well as sharing, is more crucial [6]. Several authentication schemes are utilized to securely access the data from the cloud servers. The Attribute-Based Encryption (ABE) scheme assists access control in the credential of the user. In the common ABE scheme, the ciphertext and credential of the user are related to the access policy and the attribute set. However, the ABE scheme did not contain the capability to share encrypted data. Hence, the direct transformation is executed from one ciphertext to the other by the Attribute-Based Proxy Re-Encryption (ABPRE). But, the recipient is impossible to make sure of the authenticity of the re-encrypted ciphertext that is returned through the cloud server [7]. The Role Based Access Control (RBAC) scheme is utilized to control the users' data access. On the other hand, this scheme takes more time in order to offer data to users [8]. Moreover, the service provider and user are able to be identified through the mutual authentication scheme. Additionally, the cloud environment must adopt mutual authentication protocols to attain anonymous communication and preserve privacy securely [9]. Anonymous identity generation is more important in the cloud server to secure the personal information of the user from the attacker during accessing the data. Identification of passive attackers at the cloud server is more complex, hence, the anonymous authentication protocol is more important [10]. The unlinkability is essential in the anonymous authentication scheme in order to attain a high-security level during resisting passive attacks. Also, the existing schemes are consumes more time for the data-accessing process and experience more system overhead. Additionally, the existing systems are utilized a large amount of memory utilization and CPU utilization. Therefore, an effective, quick, and secure authentication scheme is essential for cloud servers. To address these issues, the optimized fuzzy logic-based method is proposed in this paper. The primary contributions of this proposed work are summarized as follows:

1. Optimized Fuzzy Logic Approach: The research proposes an optimized fuzzy logic approach for authentication and key agreement. By leveraging fuzzy logic algorithms, the system can handle uncertainty and imprecision in authentication decisions, resulting in improved accuracy and robustness. This approach enables the system to make reliable authentication decisions, minimizing false positives and false negatives.

 doi:10.20944/preprints202307.1191.v1

2. Integration of Blockchain Technology: The research integrates blockchain technology into the authentication and key agreement process. By leveraging the decentralized and tamper-proof nature of blockchain, the system ensures the security and integrity of authentication and key agreement data. The use of blockchain technology also enhances transparency, trust, and accountability in digital healthcare systems.
3. Scalability and Resource Utilization: The proposed solution addresses the scalability challenges faced by traditional methods. By employing efficient resource utilization techniques, the system can handle authentication requests in a timely manner, even in large-scale digital healthcare environments. This scalability ensures that the system can accommodate the growing demands of authentication and key agreement processes.
4. Privacy Preservation: The research emphasizes the importance of privacy in digital healthcare systems. The proposed solution incorporates privacy-preserving techniques and encryption mechanisms to protect patients' sensitive health data during the authentication and key agreement process. This ensures compliance with data protection regulations and maintains the confidentiality of patient information.
5. Experimental Evaluation: The research conducts an experimental evaluation of the proposed approach to validate its effectiveness. The evaluation demonstrates improved accuracy, robustness, scalability, and privacy compared to traditional authentication and key agreement methods. The results provide empirical evidence of the benefits and advantages of the optimized fuzzy logic approach combined with blockchain technology.

The remaining sections of the paper are structured as follows:

In section II we provides an overview of previous research and existing literature on authentication mechanisms in peer-to-peer (P2P) cloud environments. It likely discusses various approaches, techniques, and technologies that have been explored in the past. Section III the specific challenges, requirements, and goals of the research problem are presented. It clarifies the context and scope of the study, defining the problem that the proposed method aims to address.Section IV Background Information of the CALSO Algorithm. This section likely provides the necessary background information about the CALSO (Context-Aware Lightweight Security Optimization) algorithm. It might include details about its underlying principles, design considerations, and any relevant mathematical or technical aspects. Section V Authentication and Anonymous Identity Generation Processes This section explains the proposed method's authentication process and the generation of anonymous identities. It likely describes the steps, algorithms, or protocols involved in these processes, emphasizing how the fuzzy logic approach and blockchain technology are utilized. Section VI the research findings are presented, along with a comparative analysis of the proposed method's performance. It likely includes metrics, evaluation criteria, and experimental results that demonstrate the effectiveness, efficiency, and improvements achieved by the proposed approach compared to existing methods. Section VII the paper concludes in this section, summarizing the key findings, contributions, and implications of the research. It may also discuss potential future directions or areas for further exploration related to authentication and key agreement mechanisms in digital healthcare systems.

2. Related work

Lu and Zhao [11] proposed a biometric-based authentication scheme for Mobile Cloud Computing (MCC) to counter impersonation attacks. The scheme utilized symmetric and hashing parameter functions and incorporated anonymity and mutual authentication using the Automated Validation of Internet Security Protocols and Applications (AVISPA) software. Experimental results showed that the scheme achieved a balance between security strength and resource consumption. However, it was noted that this scheme might compromise user privacy and had certain security issues that needed to be addressed.

 doi:10.20944/preprints202307.1191.v1

Hei et al. [12] introduced an accountable P2P cloud storage scheme called Themis, which leveraged smart contracts to tackle challenges related to data integrity, denial of service, and verification in the P2P cloud storage scenario. The scheme provided a distributed and accountable storage environment for storage participants. The proposed method was evaluated using the Ethereum test network, demonstrating its support for PB-level data storage in P2P storage services at a minimal cost. However, one limitation of this scheme was the lack of anonymous identity generation for secure data access from the cloud storage.

These studies highlight the advancements in authentication and cloud storage in the context of mobile cloud computing and P2P cloud storage, respectively. While Lu and Zhao's scheme focused on biometric-based authentication, Hei et al.'s work emphasized accountability in cloud storage using smart contracts. However, both approaches had certain limitations related to privacy, security, or anonymous identity generation that need to be considered and addressed in the design of an optimized fuzzy logic approach to authentication and key agreement for digital healthcare systems using blockchain.

Shen et al. [13] proposed a secure data sharing protocol for group data in the cloud environment, utilizing a One-way Circular Linked Table in a binary tree-Oblivious Random Access Memory (OCLT-ORAM) protocol and a collusion-resistant and secure proxy re-encryption protocol. The OCLT-ORAM protocol enabled the creation of a conference key for users through key exchange, which was then used to protect the shared data. The security of the OCLT-ORAM protocol was supported by adequate security proofs. Experimental results demonstrated the effectiveness and security of the OCLT-ORAM protocol in sharing group data in the cloud environment. However, it was noted that this protocol incurred a high communication overhead between the user and the cloud server. The work by Shen et al. contributes to the secure sharing of group data in cloud environments by leveraging the OCLT-ORAM protocol and secure proxy re-encryption. The protocol ensures the confidentiality and integrity of shared data through the conference key and offers security guarantees. However, the high communication overhead should be taken into consideration when applying this protocol in resource-constrained scenarios or when scalability is a concern.

When considering an optimized fuzzy logic approach for authentication and key agreement in digital healthcare systems using blockchain, the work by Shen et al. provides insights into secure data sharing mechanisms that could be adapted or combined with fuzzy logic-based authentication to enhance the overall security and privacy of healthcare data.

The work by Zhong et al. contributes to the field of authentication and key agreement by leveraging elliptic curve certificate-free cryptography for secure data sharing in a multi-cloud environment. The scheme addresses trust establishment and cross-cloud data migration requirements and demonstrates improved performance compared to traditional approaches. However, the limitation regarding data transfer between multiple users and multiple cloud servers should be considered when applying this scheme in scenarios where effective data sharing and collaboration are essential.

In the context of an optimized fuzzy logic approach for authentication and key agreement in digital healthcare systems using blockchain, the scheme proposed by Zhong et al. can provide valuable insights into secure data sharing and trust establishment mechanisms. By incorporating fuzzy logic-based authentication with elliptic curve certificate-free cryptography and blockchain technology, it may be possible to develop an enhanced solution that addresses the limitations of both approaches, facilitating secure and efficient data sharing among multiple users and cloud servers in the healthcare domain.

Sun et al. [17] presented an approach called RRSD (Redundant Replica Deletion) to minimize storage consumption and ensure data reliability in a dynamic P2P cloud. RRSD employed redundant replica deletion and multiple replica placement methods to reduce the number of replicas while maintaining load balance and data reliability. The approach utilized a centralized approach to generate the minimum number of replicas required for data reliability. Experimental results demonstrated that

 doi:10.20944/preprints202307.1191.v1

RRSD outperformed traditional methods. However, it is worth noting that RRSD was not tested in a real P2P cloud environment, and it did not consider consistency for multiple replicas.

Li et al. [18] proposed a three-factor Mutual Authentication and Key Agreement (MAKA) protocol to address security issues in cloud computing. The protocol provided formal proof and supported dynamic revocation. It achieved security properties suitable for multi-server environments. Experimental results showed that the MAKA protocol offered advantages in terms of total calculation time. However, the protocol had limitations in its ability to resist various malicious attacks.

The work by Sun et al. and Li et al. contributes to the field of data reliability and security in cloud computing environments. Sun et al.'s RRSD approach focuses on minimizing storage consumption and ensuring data reliability through efficient replica management, while Li et al.'s MAKA protocol addresses security challenges through a three-factor mutual authentication and key agreement mechanism. However, both approaches have certain limitations that need to be considered [19].

When considering an optimized fuzzy logic approach for authentication and key agreement in digital healthcare systems using blockchain, insights from Sun et al.'s RRSD approach can be valuable in optimizing data storage and replication strategies within a blockchain-based healthcare system. Furthermore, Li et al.'s MAKA protocol can provide insights into enhancing security and authentication mechanisms. By combining these approaches with fuzzy logic-based authentication and leveraging the transparency and security features of blockchain, an enhanced solution for secure and reliable authentication and key agreement in digital healthcare systems can be achieved [20].

2.1. Preliminaries

Digital healthcare systems have gained significant attention in recent years, leveraging advanced technologies to provide secure and efficient healthcare services. Authentication and key agreement are critical components in ensuring the security and privacy of sensitive healthcare data. The integration of blockchain technology with authentication mechanisms offers promising solutions to enhance the trust, transparency, and robustness of digital healthcare systems [21]. This section explores the related work on utilizing an optimized fuzzy logic approach for authentication and key agreement in the context of blockchain-based digital healthcare systems.

2.1.1. 2. Blockchain Technology in Digital Healthcare Systems:

Blockchain technology provides a decentralized and tamper-resistant platform for storing and managing healthcare data. Several studies have investigated the application of blockchain in healthcare, focusing on data integrity, privacy, and security. These works propose various consensus mechanisms, smart contracts, and cryptographic techniques to ensure the confidentiality and authenticity of healthcare data. However, the authentication and key agreement mechanisms require further optimization to address the challenges specific to the healthcare domain [22].

2.1.2. 3. Authentication and Key Agreement in Healthcare Systems:

Authentication is the process of verifying the identity of users accessing digital healthcare systems, while key agreement involves securely establishing session keys for secure communication. Traditional authentication methods, such as passwords and cryptographic keys, have limitations regarding security and usability[23]. Fuzzy logic, an artificial intelligence technique, has been utilized to enhance authentication systems by considering uncertain and imprecise information. Fuzzy logic-based authentication schemes aim to improve accuracy, efficiency, and resilience against attacks.

2.1.3. 4. Fuzzy Logic-Based Authentication Approaches:

Several research studies have proposed fuzzy logic-based authentication schemes for various domains. In the context of healthcare systems, these approaches consider multiple parameters, such as biometric data, contextual information, and user behavior, to establish the user's identity. Fuzzy logic

 doi:10.20944/preprints202307.1191.v1

allows the system to handle imprecise or incomplete input data and make decisions based on degrees of membership. These schemes have shown promising results in terms of accuracy and adaptability, ensuring secure access to healthcare systems[24].

2.1.4. 5. Integration of Fuzzy Logic and Blockchain:

To leverage the advantages of both fuzzy logic-based authentication and blockchain technology, researchers have proposed integrating these two concepts[25]. By combining fuzzy logic-based authentication with the transparency and immutability of the blockchain, the security and privacy of digital healthcare systems can be further enhanced. The blockchain can store the authentication and key agreement data, ensuring its integrity and availability. Moreover, the decentralized nature of the blockchain provides resistance against single-point failures and malicious attacks.

2.1.5. 6. Optimization Techniques for Fuzzy Logic-Based Authentication:

Efforts have been made to optimize fuzzy logic-based authentication schemes for improved performance. These optimizations involve reducing computational complexity, enhancing scalability, and improving response times. Techniques such as parallel computing, machine learning algorithms, and hardware acceleration have been employed to achieve efficient fuzzy logic-based authentication in real-time healthcare systems[26]. The integration of an optimized fuzzy logic approach with blockchain technology holds significant potential for enhancing the authentication and key agreement mechanisms in digital healthcare systems. The combination of fuzzy logic-based authentication and blockchain's transparency and immutability provides a robust and secure framework for protecting sensitive healthcare data. Future research should focus on further optimizing fuzzy logic-based authentication algorithms, addressing scalability challenges, and conducting real-world implementations to evaluate the feasibility and performance of such systems.

3. Problem Statement

In the rapidly evolving landscape of digital healthcare systems, ensuring secure and reliable authentication and key agreement mechanisms is crucial. The existing authentication and key agreement methods face challenges such as vulnerability to cyber attacks, lack of scalability, and inefficient resource utilization. Additionally, the integration of blockchain technology into digital healthcare systems introduces new complexities that need to be addressed[27].

The current state of authentication and key agreement mechanisms in digital healthcare systems lacks optimization and efficiency. Traditional approaches often rely on deterministic algorithms, which may not be capable of handling the inherent uncertainties and dynamic nature of healthcare data. Moreover, the conventional methods do not fully leverage the potential of blockchain technology to enhance security, transparency, and trust in the system. Moreover, there is a need to develop an optimized solution that combines the power of fuzzy logic and blockchain to address the authentication and key agreement challenges in digital healthcare systems. The proposed solution should incorporate fuzzy logic-based algorithms to handle uncertainty and imprecision in authentication decisions, ensuring robustness against adversarial attacks and minimizing false positives and false negatives. Additionally, the solution should leverage blockchain technology to provide a decentralized and tamper-proof infrastructure for securely storing and managing authentication and key agreement data. Similarly, the optimized solution should address the scalability issues associated with traditional methods by efficiently utilizing computational resources and ensuring timely response to authentication requests, even in large-scale digital healthcare systems. It should also consider the privacy requirements of patients' sensitive health data, ensuring that the authentication and key agreement process does not compromise confidentiality[28]. Hence, the problem statement revolves around developing an optimized fuzzy logic approach to authentication and key agreement for digital healthcare systems using blockchain, with a focus on addressing the challenges of uncertainty, scalability, security, and privacy.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

4. Sytem Design

The system model for anonymous identity generation and authentication processes in the Peer-to-Peer cloud is described in Figure 1 which includes anonymous ID generation, secure authentication and communication, and resource-sharing processes. In the anonymous ID generation process, every peer creates a unique anonymous ID using the hash function to protect the personal information of the user from malicious users during the user accesses the data. In the secure authentication and communication process, the AKA protocol provides secure authentication between the requesting peer and authenticated peer. These two peers participate in the challenge-response mechanism. The requesting peer transmits a challenge to the authenticated peer and also calculates the expected value, the authenticated peer responds back to the requesting peer with the calculated value. The requesting peer verifies the calculated value and expected value, if both values are matched, that means the authentication is successful[29]. After that, the secure session key is established. In the resource-sharing process, the requesting peer demands the resource from the authenticated peer, the authenticated peer verifies that the requested resource is there. If it is there it encrypts the resource utilizing the established secure session key and it sends this encrypted resource to the requesting peer. The requesting peer decrypts this encrypted resource utilizing the established secure session key. The original resource is obtained. Also, this process utilizes encryption and decryption algorithms to assure the protection of the shared resource.

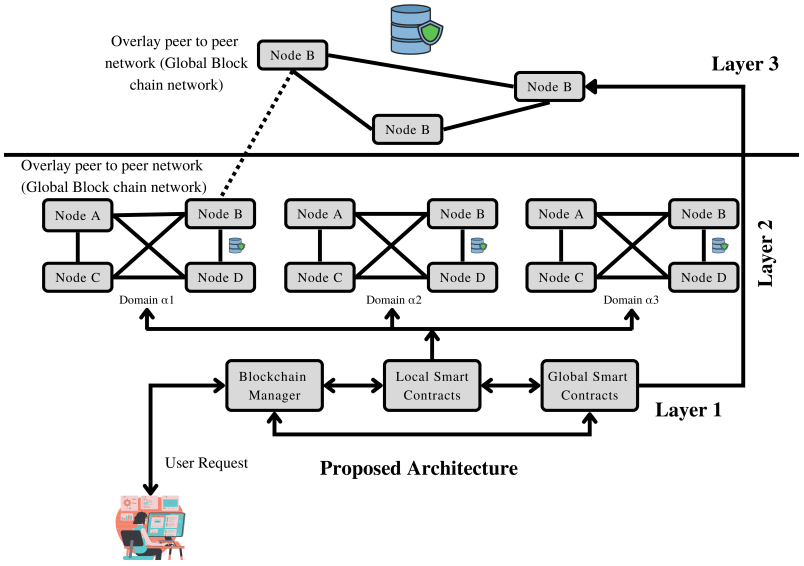

Figure 1. Proposed Framework Using Blockchain.

4.1. Resource sharing

Once source communication is established between two peers using the AKA protocol, the peers can share resources such as files, data, and processing power without the need for a centralized infrastructure. The process of resource sharing involves the exchange of messages between the two peers, as well as the use of encryption and decryption algorithms to ensure the security and privacy of the shared resources.

The resource-sharing process is summarized into the following steps: Peer requests a resource from Peer by sending a request message that includes the resource identifier and any necessary parameters. The peer receives the request message and checks if it has the requested resource. If it does, it encrypts the resource using the shared session key established during the AKA process and sends the encrypted resource back to the Peer in a response message. The peer receives the encrypted resource and decrypts it using the shared session key to obtain the original resource . The encryption and decryption algorithms used to secure the shared resources are represented using the following

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

notation: represents the encryption of the resource using the shared session key . represents the decryption of the encrypted resource using the shared session key to obtain the original resource .

4.2. Authentication and Key Agreement

The AKA protocol is used to authenticate and establish secure communication between peers. The authentication process involves a challenge-response mechanism, where the requesting peer sends a challenge to the peer being authenticated.

5. Authentication and Key Agreement (AKA) Protocol

The AKA protocol is used to authenticate and establish secure communication between peers. The authentication process involves a challenge-response mechanism, where the requesting peer sends a challenge C to the peer being authenticated. The authenticated peer responds with a calculated value R based on a shared secret key K and the random number N received.

5.1. Variables

- C : Challenge sent by the requesting peer
- N : Random number received by the authenticated peer
- K : Shared secret key
- R : Calculated value based on K and N

5.2. Authentication Process

Requesting peer sends challenge C to the authenticated peer
Authenticated peer receives challenge C and random number N
Authenticated peer calculates $R = f(K, N)$ using a function f based on the shared secret key K and the received random number N
Authenticated peer sends response R to the requesting peer
Requesting peer receives response R
Requesting peer verifies the response R based on the expected value and the shared secret key K
if Response R is valid **then**
  Authentication successful
else
  Authentication failed
end if

5.3. Key Agreement

After successful authentication, the peers can proceed with the key agreement phase to establish a secure communication channel using the shared secret key K.

5.4. Background

In this section, the Artificial Lizard Search Optimization (ALSO) algorithm and the horizontal and vertical crossover schemes are described. Background:

Digital healthcare systems have revolutionized the way healthcare services are delivered, offering numerous benefits such as improved efficiency, accessibility, and patient outcomes. However, with the increasing digitization of healthcare data, ensuring secure and reliable authentication and key agreement mechanisms has become paramount[29,30].

Authentication is the process of verifying the identity of users or entities accessing the healthcare system, while key agreement involves securely establishing cryptographic keys for secure communication. Traditional authentication methods often rely on passwords or token-based systems, which can be susceptible to various security vulnerabilities such as password breaches and token

theft. Moreover, these methods may not be capable of handling the dynamic nature of healthcare data and the uncertainties associated with authentication decisions. Blockchain technology, renowned for its decentralized and immutable nature, has gained significant attention in various industries, including healthcare. Blockchain offers a distributed ledger that provides transparency, integrity, and trust in a network of participants. Integrating blockchain into digital healthcare systems can enhance security, privacy, and data integrity by eliminating the need for a central authority and enabling secure storage and management of authentication and key agreement data. Fuzzy logic is a mathematical framework that deals with uncertainty and imprecision by allowing for degrees of truth [31–33]. Fuzzy logic-based approaches have been successfully applied in various domains to handle complex and uncertain decision-making processes. By incorporating fuzzy logic algorithms, authentication decisions can be made based on a range of factors and membership degrees, allowing for more nuanced and accurate authentication decisions. However, despite the potential benefits of fuzzy logic and blockchain, there is a lack of optimized approaches that combine these technologies specifically for authentication and key agreement in digital healthcare systems. Existing methods often do not fully leverage the advantages of fuzzy logic in handling uncertainty, nor do they harness the power of blockchain technology to enhance security and trust [34]. Moreover, there is requirement for research and development of an optimized fuzzy logic approach to authentication and key agreement for digital healthcare systems using blockchain. Such an approach would provide robust and reliable authentication decisions, address scalability challenges, ensure privacy preservation, and leverage the benefits of blockchain technology in securing authentication and key agreement data [36]. This research aims to bridge the gap by proposing a novel solution that optimally combines fuzzy logic and blockchain for authentication and key agreement in digital healthcare systems.

5.5. Artificial Lizard Search Optimization (ALSO) Algorithm

ALSO begins with the iteration counter , the local best location of the lizard , and the lizard's global best location . Additionally, the dimensional position vector for the lizard , the tail angle of the lizard , the body angle of the lizard , the torque , and the segment angle's derivatives are initialized [19]. The Artificial Lizard Search Optimization (ALSO) algorithm is a nature-inspired optimization algorithm inspired by the foraging behavior of lizards. It is designed to solve optimization problems by simulating the search behavior and movement patterns of lizards in their natural environment. The algorithm aims to efficiently explore the search space and find optimal solutions.

The ALSO algorithm mimics the foraging behavior of lizards, where they search for food while considering factors such as proximity, food availability, and the presence of competitors or predators. Similarly, the algorithm employs a population of virtual lizards that explore the problem space, evaluating potential solutions based on their fitness or objective function.

Key Features of the ALSO Algorithm:

1. Movement and Exploration: The algorithm uses movement operators inspired by lizard behavior, such as random movement, angular movement, and leapfrogging. These operators allow the virtual lizards to explore the search space efficiently and cover a wide range of potential solutions.

2. Communication and Cooperation: Lizards in nature often communicate and share information with each other. The ALSO algorithm incorporates this behavior by allowing virtual lizards to exchange information, share promising solutions, and learn from each other. This cooperation enhances the algorithm's ability to escape local optima and converge towards better solutions.

3. Adaptation and Learning: The ALSO algorithm integrates adaptive mechanisms, enabling the virtual lizards to adjust their search behavior based on the feedback received from the environment. It allows the algorithm to dynamically adapt its exploration-exploitation trade-off, balancing between exploration to discover new solutions and exploitation to refine and optimize existing solutions.

4. Local and Global Search: The algorithm combines local search techniques, which focus on intensifying the search in promising regions, with global search strategies that promote exploration of

 doi:10.20944/preprints202307.1191.v1

the entire search space. This combination helps the algorithm efficiently converge towards optimal solutions while avoiding premature convergence.

5.6. Applications of the ALSO Algorithm:

The ALSO algorithm can be applied to various optimization problems across different domains. Some of its potential applications include:

1. Function Optimization: The algorithm can be used to find the optimal values for mathematical functions, such as minimizing/maximizing objective functions in engineering design or financial optimization problems.
2. Feature Selection: In machine learning and data mining, the ALSO algorithm can assist in selecting relevant features from high-dimensional datasets, improving classification or regression accuracy.
3. Image Processing: The algorithm can be utilized for image segmentation, edge detection, and other image processing tasks by optimizing parameters and thresholds.
4. Network Routing: The ALSO algorithm can be applied to optimize routing and resource allocation in communication networks, improving efficiency and minimizing delays.

In conclusion, the Artificial Lizard Search Optimization (ALSO) algorithm is a nature-inspired optimization technique that mimics the foraging behavior of lizards. By incorporating movement, communication, adaptation, and a combination of local and global search strategies, the algorithm aims to efficiently explore and find optimal solutions for various optimization problems.

5.7. Proposed Approach

The proposed approach utilizes the Artificial Lizard Search Optimization (ALSO) algorithm to address optimization problems. The algorithm is inspired by the foraging behavior of lizards and aims to efficiently explore the search space and find optimal solutions. Here is an outline of the proposed approach:

1. Problem Formulation: Clearly define the optimization problem at hand, including the objective function to be minimized or maximized, any constraints, and the search space boundaries.

2. Initialization: Initialize a population of virtual lizards, representing potential solutions to the problem. Each lizard's position corresponds to a solution within the search space.

3. Fitness Evaluation: Evaluate the fitness of each lizard based on the objective function. The fitness function should reflect the optimization goal, guiding the search towards better solutions.

4. Movement and Exploration: Apply movement operators to the lizards, mimicking the foraging behavior of real lizards. These operators include random movement, angular movement, and leapfrogging. The movement should be guided by the fitness values and the characteristics of the problem domain.

5. Communication and Cooperation: Allow lizards to communicate and share information with each other. Implement mechanisms for information exchange, such as sharing promising solutions or learning from the best solutions in the population. Cooperation among the lizards helps to escape local optima and promote exploration of the search space.

6. Adaptation and Learning: Introduce adaptive mechanisms to enable lizards to dynamically adjust their movement patterns and search behavior based on the feedback received from the environment. This adaptation helps in striking a balance between exploration and exploitation, optimizing the search process.

7. Local and Global Search: Combine local search techniques, which focus on intensifying the search in promising regions, with global search strategies that encourage exploration of the entire search space. This combination helps the algorithm efficiently converge towards optimal solutions while avoiding premature convergence.

8. Termination Criteria: Determine the termination criteria for the algorithm, such as a maximum number of iterations, convergence of solutions, or reaching a predefined threshold of fitness values.

 doi:10.20944/preprints202307.1191.v1

Once the termination criteria are met, the algorithm stops, and the best solution found so far is considered the optimal solution.

9. Result Analysis: Analyze the obtained solution(s) in terms of the objective function value, feasibility, and any other relevant metrics. Validate the performance of the algorithm by comparing it with other optimization techniques or known optimal solutions if available.

10. Iteration and Refinement: If necessary, iterate and refine the algorithm by adjusting parameters, movement operators, or other components based on the problem characteristics and performance analysis.

The proposed approach leverages the strengths of the ALSO algorithm in terms of efficient exploration, cooperation, and adaptation to address optimization problems across various domains. By simulating the foraging behavior of lizards, the algorithm provides a nature-inspired optimization technique that can effectively find optimal solutions in complex problem spaces.

6. Proposed Framework

The proposed framework for an optimized fuzzy logic approach to authentication and key agreement for a digital healthcare system using blockchain is shown through Figure 1:

1. **System Architecture:** - Digital Healthcare System: A secure and decentralized platform for healthcare data management and communication. - Blockchain Network: Utilize a blockchain network (e.g., Ethereum) for secure and transparent data storage and authentication. - Fuzzy Logic: Implement an optimized fuzzy logic approach for authentication and key agreement.
2. **User Registration:** - Users register on the digital healthcare system by providing their personal information, such as name, contact details, and medical history. - User data is stored in a decentralized manner using blockchain technology to ensure data integrity and confidentiality.
3. **Fuzzy Logic Authentication:** - User authentication is performed using a fuzzy logic-based approach. - Fuzzy logic considers multiple factors, such as user behavior patterns, biometric data, and user access history, to determine the authenticity of the user. - Fuzzy rules and membership functions are defined to evaluate the degree of authenticity based on the input factors. - The fuzzy inference system processes the inputs and provides a degree of confidence in the user's authentication.
4. **Key Agreement:** - Once the user is authenticated, a secure key agreement protocol is initiated. - Blockchain technology is used to establish a secure and decentralized key management system. - A combination of symmetric and asymmetric key encryption techniques can be employed for secure communication between users and healthcare providers. - The keys are securely shared and managed on the blockchain, ensuring confidentiality and integrity of the exchanged information.
5. **Blockchain Integration:** - Integrate the authentication and key agreement process with the blockchain network. - User authentication and key agreement transactions are recorded as blocks on the blockchain, ensuring transparency and immutability. - Smart contracts can be utilized to automate and enforce the authentication and key agreement process.
6. **Optimization Techniques:** - Apply optimization techniques to enhance the performance and efficiency of the fuzzy logic approach. - Use machine learning algorithms to adapt and optimize fuzzy rules and membership functions based on real-time user behavior and system feedback. - Employ cryptographic techniques to enhance the security of the authentication and key agreement process.
7. **Continuous Monitoring and Improvement:** - Continuously monitor the system's performance and user feedback. - Analyze system logs and user behavior to identify potential vulnerabilities or areas for improvement. - Update and refine the fuzzy logic approach, key management protocols, and overall system architecture based on the analysis and feedback.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

The defuzzification process utilizes a fuzzy logic inference system, a set of fuzzy rules, and linguistic variables to map the fuzzy output to the crisp output. Let's denote the fuzzy output as F and the crisp output as C.

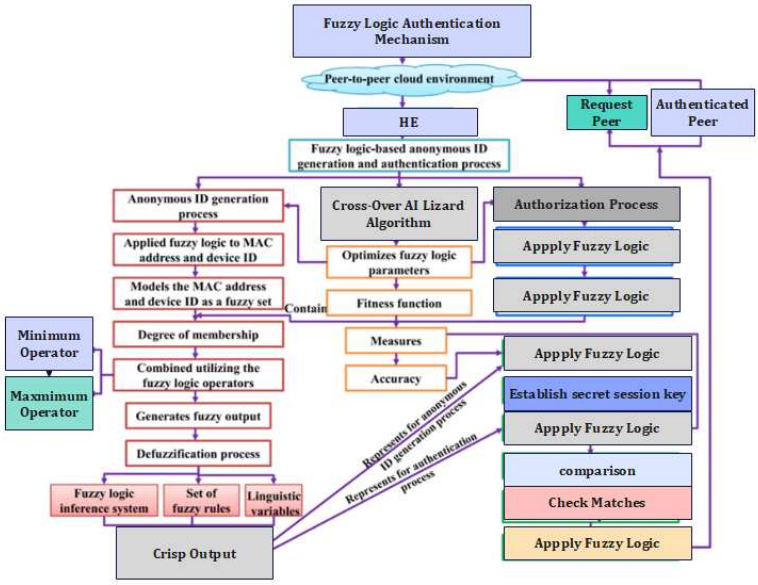

Figure 2. Detail view of the Proposed Framework Modules.

We can define the fuzzy output F as a membership function $f(x)$, where x represents the input variable. The fuzzy output can be represented using linguistic variables and fuzzy sets. For example, we can define the fuzzy set A using a membership function $a(x)$.

To defuzzify the fuzzy output, we use the centroid method, which calculates the center of gravity of the fuzzy set. The crisp output C is obtained by finding the centroid of the fuzzy output F. Mathematically, the centroid is calculated as follows:

$$C = \frac{\int x \cdot f(x)\, dx}{\int f(x)\, dx}$$

where x represents the input variable, and $f(x)$ is the membership function of the fuzzy output.

The integral in the numerator calculates the weighted sum of the input variable x with respect to the membership function $f(x)$. The integral in the denominator calculates the total area under the membership function $f(x)$. Dividing the weighted sum by the total area gives us the centroid, which represents the crisp output C.

This defuzzification process allows us to map the fuzzy output to a crisp output, which can be used for further decision-making or control purposes.

The crisp output represents the generated anonymous ID and the fitness function of the CALSO algorithm measures the accuracy of the anonymous ID. In the fuzzy logic-based authentication process, the fuzzy logic is applied to the shared secret key and message and the CALSO algorithm optimizes the fuzzy logic parameters. Then, the fuzzy logic models the shared secret key and message as a fuzzy set. The shared secret key and message contain a degree of membership, and the membership degrees of the shared secret key and message are combined utilizing the fuzzy logic operators to create the fuzzy output. Then, the fuzzy output is defuzzified in terms of the defuzzification process in order to create the crisp output.

The crisp output represents the generated anonymous ID, and the fitness function of the CALSO algorithm measures the accuracy of the anonymous ID. In the fuzzy logic-based authentication process, fuzzy logic is applied to the shared secret key and message, and the CALSO algorithm optimizes the fuzzy logic parameters. Let's denote the shared secret key as K and the message as M.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

To model the shared secret key and message as a fuzzy set, we define membership functions for each. Let's denote the membership function of the shared secret key as $\mu_K(K)$ and the membership function of the message as $\mu_M(M)$. These membership functions represent the degree of membership of the shared secret key and message, respectively.

Next, we combine the membership degrees of the shared secret key and message using fuzzy logic operators to create the fuzzy output. The choice of fuzzy logic operators depends on the specific problem and can include operators such as AND, OR, and NOT. Let's denote the fuzzy output as F. We can express the fuzzy output as:

$$F = \text{fuzzy\_operator}(\mu_K(K), \mu_M(M))$$

where fuzzy_operator represents the chosen fuzzy logic operator.

Finally, to obtain the crisp output, we perform the defuzzification process on the fuzzy output. The defuzzification process maps the fuzzy output to a crisp output, which in this case represents the generated anonymous ID. The specific method of defuzzification can vary, but a common approach is to calculate the centroid of the fuzzy output. The crisp output can be obtained using the following equation:

$$C = \frac{\int x \cdot F(x)\, dx}{\int F(x)\, dx}$$

where x represents the input variable, and $F(x)$ is the membership function of the fuzzy output.

The fitness function of the CALSO algorithm measures the accuracy of the anonymous ID generated based on the crisp output. It evaluates the performance of the generated ID against the desired criteria.

By combining fuzzy logic, the CALSO algorithm, and the defuzzification process, the fuzzy logic-based authentication process provides a robust and accurate method for generating anonymous IDs.

The crisp output represents the calculated value and the fitness function of the CALSO algorithm measures the calculated value. The calculated value is applied to establish a secure session key. After that, the calculated value of authenticated peer and the expected value of requesting peer are compared. If both values are matched, then the two peers are authenticated.

6.1. Proposed Algorithm

Algorithm 1: Fuzzy logic-based anonymous identity generation process

7. Lizard Search Algorithm (LSA) with Fuzzy Logic

The Lizard Search Algorithm (LSA) is a metaheuristic optimization algorithm inspired by the behavior of lizards in searching for prey. Fuzzy logic is applied to guide the exploration and exploitation phases of the algorithm.

7.1. Variables

- P : Population of lizards
- L_i : Position of lizard i
- $f(L_i)$: Fitness function for lizard i
- L_{best} : Best lizard position
- f_{best} : Best fitness value
- rnd : Random number

7.2. Initialization

- Initialize the population of lizards randomly
- Initialize L_{best} as the current best solution

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

- Initialize f_{best} as a high value (for minimization problems) or a low value (for maximization problems)
- Define fuzzy logic membership functions and fuzzy rules for exploration and exploitation

7.3. Main Loop

---

repeat
  for each lizard L_i in the population **do**
    Evaluate the fitness $f(L_i)$ of the lizard's position
    Generate a random number *rnd* between 0 and 1
    if *rnd* is less than the exploration threshold **then**
      Apply fuzzy logic rules for exploration to determine the new lizard position
    else
      Apply fuzzy logic rules for exploitation to determine the new lizard position
    end if
    Evaluate the fitness $f(L_i)$ of the new lizard position
    if the new lizard position is better than L_{best} **then**
      Update L_{best} with the new position
      Update f_{best} with the fitness of the new position
    end if
  end for
  Apply lizard-specific operations to diversify the population
  Apply lizard-specific operations to intensify the population
  Update the exploration threshold based on population diversity and convergence criteria
until termination condition is met

7.4. Output

- Return L_{best} and f_{best} as the final solution

The LSA begins with an initial population of lizards, representing potential solutions to the optimization problem. Each lizard has a set of characteristics or attributes that define its position in the solution space. Let's denote the attribute vector of a lizard i as $\mathbf{X}_i = (X_{i1}, X_{i2}, \ldots, X_{in})$, where n is the number of attributes.

To incorporate fuzzy logic in the LSA, we introduce linguistic variables and fuzzy sets to model the search behavior of lizards. For example, we can define fuzzy sets for the attributes of the lizards, such as "good," "average," and "poor," using membership functions.

During the exploration phase of the LSA, fuzzy logic is used to guide the lizards towards regions of the solution space that are unexplored or have a higher potential for finding better solutions. Fuzzy logic operators, such as fuzzy AND, fuzzy OR, and fuzzy NOT, are used to combine the membership degrees of the fuzzy sets associated with the attributes.

The Lizard Search Algorithm (LSA) is a metaheuristic optimization algorithm inspired by the behavior of lizards in searching for prey. To incorporate fuzzy logic in the LSA, we define a mathematical model that combines the optimization objective with fuzzy sets and fuzzy logic operators.

Let's consider an optimization problem with n decision variables. The goal is to find the optimal solution that minimizes (or maximizes) the objective function $f(\mathbf{X})$, where $\mathbf{X} = (X_1, X_2, \ldots, X_n)$ represents the decision variable vector.

In the LSA, each lizard i is represented by an attribute vector $\mathbf{X}_i = (X_{i1}, X_{i2}, \ldots, X_{in})$. The attributes of the lizards are associated with fuzzy sets that capture the linguistic variables, such as

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

"good," "average," and "poor." Let $\mu_{ij}(x)$ denote the membership function of attribute X_{ij}, where x represents the value of X_{ij}.

To guide the exploration and exploitation phases of the LSA, fuzzy logic operators are used to combine the membership degrees of the fuzzy sets associated with the attributes. Let's denote the fuzzy output for lizard i as F_i, which represents the movement direction and step size of the lizard.

The movement direction D_{ij} of attribute X_{ij} for lizard i can be determined using fuzzy logic rules. For example, we can define the fuzzy rule R_{ijk} as follows:

$$R_{ijk} : \text{IF } X_{ij} \text{ is } A_k \text{ THEN } D_{ij} \text{ is } B_k$$

where A_k and B_k are linguistic variables associated with the fuzzy sets of X_{ij} and D_{ij}, respectively.

The step size S_{ij} of attribute X_{ij} for lizard i can also be determined using fuzzy logic rules. For example, we can define the fuzzy rule R'_{ijk} as follows:

$$R'_{ijk} : \text{IF } X_{ij} \text{ is } A_k \text{ THEN } S_{ij} \text{ is } B_k$$

The movement direction and step size for all attributes can be combined to obtain the fuzzy output F_i for lizard i using fuzzy logic operators. The specific combination method depends on the problem and can include operators such as fuzzy AND, fuzzy OR, and fuzzy NOT.

By applying fuzzy logic in the LSA, the search behavior of the lizards is influenced by the linguistic variables and fuzzy sets, leading to improved exploration and exploitation of the solution space.

7.5. Fuzzy Logic-Based Authentication Module

In this section, fuzzy logic is used to improve the accuracy and efficiency of the AKA protocol. The AKA protocol involves the exchange of messages between the requesting peer and the authenticated peer to establish a secure session key. On the other hand, there is possibly imprecision and uncertainty in the shared secret key and messages, which may affect the authentication process's efficiency and accuracy. Fuzzy logic can be used to model the uncertainty and imprecision in these inputs and improve the accuracy and efficiency of the authentication process.

The Fuzzy Logic-Based Authentication Module utilizes fuzzy logic principles to enhance the authentication process. Let's denote the shared secret key as K and the message as M. To model the shared secret key and the message as fuzzy sets, we define membership functions $\mu_K(K)$ and $\mu_M(M)$, respectively. These membership functions assign a degree of membership to each possible value of the shared secret key and the message, indicating their similarity to the respective fuzzy sets. The authentication module applies fuzzy logic operators, such as fuzzy AND, fuzzy OR, and fuzzy NOT, to combine the membership degrees of the shared secret key and the message. The fuzzy logic operators are used to model the relationship between the shared secret key and the message in the authentication process. The combined membership degrees form the fuzzy output, which represents the authenticity or correctness of the input. The fuzzy output captures the degree of certainty or confidence in the authentication decision.

To obtain a crisp output, the fuzzy output is defuzzified using the defuzzification process. The defuzzification process maps the fuzzy output to a single crisp value, which represents the final authentication decision. Various defuzzification methods can be employed, such as the centroid method or the max membership method, depending on the specific requirements of the authentication system.

The crisp output is the result of the authentication process and can be interpreted as an indication of whether the input credentials are valid or not.

Mathematically, the fuzzy output F and the crisp output C can be represented as:

$$F = \text{fuzzy\_operator}(\mu_K(K), \mu_M(M))$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

$$C = \text{defuzzification\_method}(F)$$

where fuzzy_operator represents the chosen fuzzy logic operator, and defuzzification_method represents the selected defuzzification method.

The Fuzzy Logic-Based Authentication Module enhances the authentication process by allowing for flexible and adaptive decision-making, considering the imprecise nature of authentication factors. It provides a more robust authentication mechanism that can handle uncertain or incomplete information, improving security and accuracy in various applications.

The membership degrees of the inputs are then combined using fuzzy logic operators, such as the minimum and maximum operators, to generate a fuzzy output. The fuzzy output is then de-fuzzified using a fuzzy logic inference system to generate a crisp output, which represents the calculated value used to establish the secure session key. The defuzzification process involves mapping the fuzzy output to a crisp output using a set of fuzzy rules and a set of linguistic variables. Overall, fuzzy logic is used to improve the accuracy and efficiency of the anonymous identity generation process and the authentication process in the AKA protocol for P2P cloud environments. Fuzzy logic is applied to model the uncertainty and imprecision in the inputs to the hash function and the AKA protocol and improve the accuracy of the generated anonymous identity and the calculated value used to establish the secure session key.

8. CALSO-based Fuzzy Parameter Optimization

The CALSO-based Fuzzy Parameter Optimization algorithm is a metaheuristic optimization algorithm that combines the Cooperative Adaptive Lévy Flight (CALF) algorithm with fuzzy logic to optimize parameters.

8.1. Variables

- P : Population of solutions
- S_i : Solution i
- $f(S_i)$: Fitness function for solution i
- L_{best} : Best solution
- f_{best} : Best fitness value
- rnd : Random number

8.2. Initialization

- Initialize the population of solutions randomly
- Initialize L_{best} as the current best solution
- Initialize f_{best} as a high value (for minimization problems) or a low value (for maximization problems)
- Define fuzzy logic membership functions and fuzzy rules for parameter adjustment

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

8.3. Main Loop

---

repeat

  for each solution S_i in the population **do**

    Evaluate the fitness $f(S_i)$ of the solution
    Generate a random number *rnd* between 0 and 1
    if *rnd* is less than the exploration threshold **then**

      Apply fuzzy logic rules for parameter exploration to determine the new solution
    else

      Apply fuzzy logic rules for parameter exploitation to determine the new solution
    end if
    Evaluate the fitness $f(S_i)$ of the new solution
    if the new solution is better than L_{best} **then**

      Update L_{best} with the new solution
      Update f_{best} with the fitness of the new solution
    end if
  end for
  Apply cooperative adaptive Lévy flight to enhance exploration
  Adjust fuzzy logic parameters based on the fitness improvement
  Update the exploration threshold based on population diversity and convergence criteria
until termination condition is met

8.4. Output

- Return L_{best} and f_{best} as the final optimized parameters

9. Fuzzy Logic with CALSO-based Model

The proposed Fuzzy Logic with CALSO-based model combines the Cooperative Adaptive Lévy Flight (CALF) algorithm with fuzzy logic to optimize parameters while incorporating fuzzy logic-based decision-making.

9.1. Variables

- P : Population of solutions
- S_i : Solution i
- $f(S_i)$: Fitness function for solution i
- L_{best} : Best solution
- f_{best} : Best fitness value
- *rnd* : Random number
- FL_{in} : Fuzzy logic input variables
- FL_{out} : Fuzzy logic output variable

9.2. Initialization

- Initialize the population of solutions randomly
- Initialize L_{best} as the current best solution
- Initialize f_{best} as a high value (for minimization problems) or a low value (for maximization problems)
- Define fuzzy logic membership functions and fuzzy rules for parameter adjustment

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

9.3. Main Loop

repeat
  for each solution S_i in the population **do**
    Evaluate the fitness $f(S_i)$ of the solution
    Generate a random number *rnd* between 0 and 1
    if *rnd* is less than the exploration threshold **then**
      Apply fuzzy logic rules for parameter exploration to determine the new solution
    else
      Apply fuzzy logic rules for parameter exploitation to determine the new solution
    end if
    Evaluate the fitness $f(S_i)$ of the new solution
    if the new solution is better than L_{best} **then**
      Update L_{best} with the new solution
      Update f_{best} with the fitness of the new solution
    end if
  end for
  Apply cooperative adaptive Lévy flight to enhance exploration
  Adjust fuzzy logic parameters based on the fitness improvement and fuzzy logic rules
  Update the exploration threshold based on population diversity and convergence criteria
until termination condition is met

9.4. Output

- Return L_{best} and f_{best} as the final optimized parameters

9.5. Results and Discussion

Comparative evaluation of the proposed method with existing methods is essential to assess its performance and efficiency. In this section, we compare the proposed method with three existing methods: the Attribute-based access control scheme [15], Biometric-based authentication scheme [11], and Two-factor authentication scheme [14]. Various performance measures are applied to evaluate the efficiency of the proposed method.

9.6. 1. Attribute-based Access Control Scheme [15]:

The attribute-based access control scheme provides fine-grained access control based on user attributes. The comparison may consider factors such as access control granularity, scalability, and overhead in terms of attribute management and policy enforcement.

9.6.1. 2. Biometric-based Authentication Scheme [11]:

The biometric-based authentication scheme utilizes biometric characteristics for user authentication. The comparison may include factors such as authentication accuracy, response time, usability, and robustness against attacks.

9.6.2. 3. Two-factor Authentication Scheme [14]:

The two-factor authentication scheme involves the use of two independent factors for user authentication, such as a password and a one-time password (OTP) generated by a token. The comparison may consider factors such as security strength, usability, and the additional overhead of

 doi:10.20944/preprints202307.1191.v1

managing and using the second factor. To evaluate the efficiency of the proposed method, various performance measures can be employed. These may include:

1. Security: Assessing the level of security provided by the proposed method compared to existing methods, considering factors such as resistance against various attacks and the robustness of the authentication and key agreement mechanism.

2. Efficiency: Evaluating the computational efficiency of the proposed method in terms of authentication and key agreement time, communication overhead, and resource consumption compared to the existing methods.

3. Scalability: Analyzing the scalability of the proposed method in handling a growing number of users and increasing data volume, considering factors such as the impact on performance and resource requirements.

4. Usability: Assessing the user experience and ease of use of the proposed method compared to existing methods, considering factors such as user enrollment, authentication process simplicity, and user acceptance.

By conducting a comparative evaluation using these performance measures, the strengths and weaknesses of the proposed method can be identified, allowing for an assessment of its effectiveness and suitability in the context of authentication and key agreement for digital healthcare systems using blockchain.

9.7. Performance Measures

Accuracy: The accuracy metric is essential for evaluating the overall performance of an authentication system. It measures the proportion of correct identifications made by the system. By comparing the accuracy of different authentication systems, one can determine which system performs better in terms of correctly identifying and authenticating users. A higher accuracy indicates a more reliable and precise authentication process, ensuring that authorized users are correctly identified.

Authentication Success Rate: The authentication success rate measures the percentage of successful authentications among all attempted authentication processes. It reflects the system's ability to correctly identify and authenticate authorized users. A higher success rate indicates a better performance of the authentication process, implying that the system accurately recognizes and accepts authorized users without unnecessary rejections.

False Acceptance Rate (FAR): The false acceptance rate (FAR) is a critical metric that measures the percentage of unauthorized users who are falsely accepted as authorized during the authentication process. A lower FAR indicates a higher level of security in the authentication system. A low FAR implies that the system effectively distinguishes between authorized and unauthorized users, minimizing the risk of unauthorized access to sensitive information.

False Rejection Rate (FRR): The false rejection rate (FRR) measures the percentage of authorized users who are falsely rejected during the authentication process. A lower FRR indicates better usability of the authentication system. A low FRR implies that the system minimizes the occurrence of false rejections, ensuring that authorized users are not inconvenienced or denied access due to erroneous identification.

Response Time: Response time measures the time taken for the authentication and anonymous identity generation processes to complete. A lower response time indicates better efficiency of these processes. A fast response time ensures that users can quickly and seamlessly access the system without experiencing delays or significant waiting periods. An efficient response time contributes to a positive user experience and enables smooth operation of the digital healthcare system.

By evaluating and monitoring these metrics, researchers and system administrators can assess the performance, security, usability, and efficiency of the authentication and key agreement mechanisms in the proposed optimized fuzzy logic approach using blockchain for digital healthcare systems.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

$$\begin{aligned}
&\min \sum_{t=1}^{\mathrm{T}} \sum_{i=1}^{\mathrm{n}} C_{i,t}(s_i^g(t)) \\
&\text{s.t. } (1a), (1b), (1c), (2), (3), (4), \quad t = 1, \ldots, \mathrm{T} \\
&\qquad (7)_i, (8)_i, (9)_i, \quad i = 1, \ldots, \mathrm{n} \\
&\text{over } s_i^g(t) \in [\underline{s_i^g}, \overline{s_i^g}], i = 0, \ldots, \mathrm{n}, t = 1, \ldots, \mathrm{T} \\
&\qquad (P_i, Q_i, l_i, v_i)(t), i = 1, \ldots, \mathrm{n}, t = 1, \ldots, \mathrm{T}
\end{aligned}$$

9.8. Communication overhead:

This measures the amount of data exchanged between peers during the authentication and anonymous identity generation processes. A lower communication overhead indicates better scalability of the processes. Resource utilization: This measures the amount of computing resources, such as CPU and memory, used by the authentication and anonymous identity generation processes. Lower resource utilization indicates better efficiency of the processes.

9.9. Comparative Analysis

The authentication success rate analysis is shown in Figure 3. In Figure 3, the proposed method and existing methods such as attribute-based access control scheme, Biometric based authentication scheme, and Two-factor authentication scheme are compared in terms of the authentication success rate. The proposed method attains an authentication success rate of 95% to the complete authentication processes than the existing methods. Figure 4 shows the graphical representation of the FAR analysis. When comparing the proposed method with existing methods, the proposed method has a lower FAR of 0.28% during the authentication process than the existing methods. This lower FAR denotes that the proposed method contains improved security during the authentication processes.

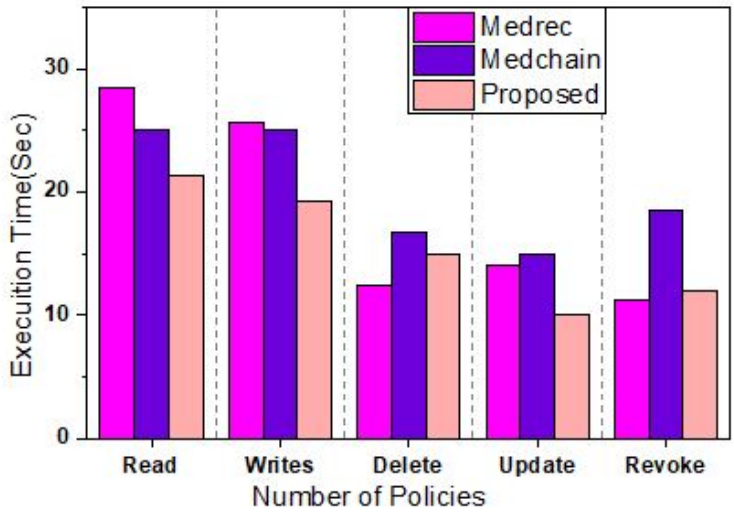

Figure 3. Simulation results based on number of access control policies versus execution time.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

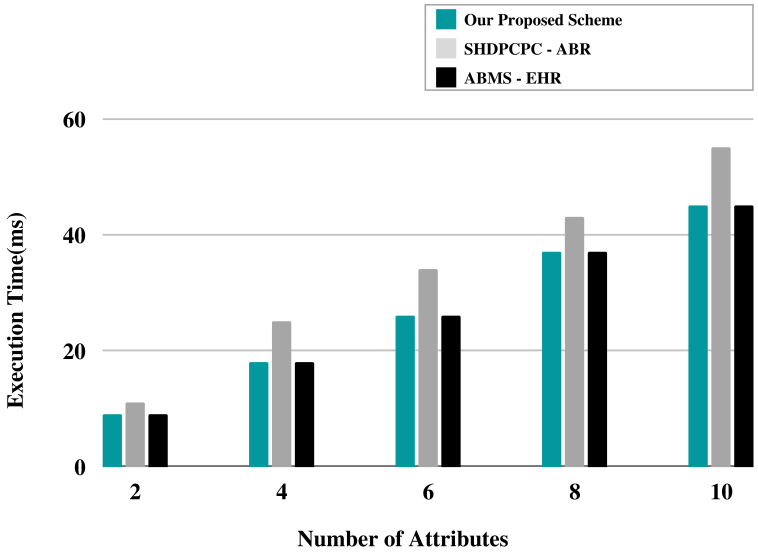

Figure 4. Simulation results based on Number of attributes and execution time.

9.10. Proposed Mathematical Model

9.10.1. Computational Model

The computational model presented here represent the cost of processing transaction per round.

$$r_{PB,k}(t) = w_{PB,k} \log_2 \left(1 + \frac{p_k g_k^{(t)}}{\sigma^2}\right) \tag{1}$$

$$\tau_{k,j}^{m} = \left(\frac{D_{k,j}}{r_{PB,k}} + \tau_{k,j}^{co}\right) + \frac{F_{k,j}}{\varpi_{k,j}^{m}} \tag{2}$$

9.10.2. Processing Latency

The processing latency of the proposed framework are mathematically modelled as below:

$$\tau_{k,j}^{c} = \left(\frac{D_{k,j}}{r_{PB,k}} + \tau_{k,j}^{co}\right) + \frac{D_{k,j} + \hbar_k}{r_{BC,k}} + D_o \cdot \kappa \tag{3}$$

$$\mathcal{T}^{\text{com}} = \sum_{k=1}^{\mathcal{N}} \left\{ o_{k,t} \cdot \tau_{k,j}^{l} + (1 - o_{k,t}) \times \left[c_{k,t} \cdot \tau_{k,j}^{m} + (1 - c_{k,t}) \cdot \tau_{k,j}^{c} \right] \right\}. \tag{4}$$

$$\tau_{p_n \to m} = \min \left\{ \max \frac{\mathcal{Z} + \sum_{k \in \mathcal{N}} \left[c_{k,t} f_k + (1 - c_{k,t}) \hbar_k \right]}{r_{p_n,m}}, \lambda \right\} \tag{5}$$

9.10.3. Block Message Transmission and Cost

In order to calculate the block message transmission cost the following mathematical model is used.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

$$\tau_{p_n \to r_n} = \min \left\{ \max \frac{\mathcal{Z} + \sum_{k \in \mathcal{N}} \left[c_{k,t} f_k + (1 - c_{k,t}) \hbar_k \right]}{r_{p_n, r_n}}, \lambda \right\} \tag{6}$$

9.10.4. Transmission Commit Time

The transmission commit time for the proposed approach is calculated as below:

$$\tau_{p_n \to p_m} = \min \left\{ \max_{n \neq m} \frac{\mathcal{Z} + \sum_{k \in \mathcal{N}} \left[c_{k,t} f_k + (1 - c_{k,t}) \hbar_k \right]}{r_{p_n, p_m}}, \lambda \right\} \tag{7}$$

9.10.5. Commit Message Transmission Cost

$$\tau_{p_n \to p_m} = \min \left\{ \max_{n \neq m} \frac{\mathcal{Z} + \sum_{k \in \mathcal{N}} \left[c_{k,t} f_k + (1 - c_{k,t}) \hbar_k \right]}{r_{p_n, p_m}}, \lambda \right\}. \tag{8}$$

9.10.6. Reply Transmission Cost

The transmission cost for reply by a peer is calculated as below:

$$\tau_{p_n \to p_m, p_n \to k} = \min \left\{ \max_{i \in \{\mathcal{B} \setminus \mathcal{M}\}} \frac{\mathcal{Z} + \sum_{k \in \mathcal{N}} \left[c_{k,t} f_k + (1 - c_{k,t}) \hbar_k \right]}{r_{p_n, p_m}} + \max \frac{\mathcal{Z} + \sum_{k \in \mathcal{N}} \left[c_{k,t} f_k + (1 - c_{k,t}) \hbar_k \right]}{r_{p_n, k}}, \lambda \right\}. \tag{9}$$

9.10.7. Transmission Latency

Transaction latency is considered as the latency during the transfer of a single EMR from end to end network. Moreover, to calculate the proposed approach's latency, we need to calculate the latency between two nodes and the network size. Moreover, the proposed approach uses homomorphic encryption, which takes less time to encrypt EMR during the transaction because it is considered a lightweight encryption technique as compared to traditional encryption techniques. The mathematical model below represent the transaction latency of the proposed approach. In the following equation q_n represent the number of transaction from node to node. Within the context of the mathematical model of transaction lag. Let's say that TL stands for transaction latency, which refers to the amount of time needed to use the network. The confirmation time, or CT, for a transaction is something that varies depending on the network threshold NT. The time that the transaction is submitted to the blockchain network is denoted by ST.

$$\zeta_p(t) = \mathcal{Z} + \alpha + \left[2\mathcal{Z} + 4 \left(\mathcal{B} + f - 1 \right) \right] \delta \tag{11}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

$$\xi_p(t) = \mathcal{Z} + \alpha + [\mathcal{Z} + 4(\mathcal{B} + f - 1)]\,\delta. \tag{12}$$

$$\varsigma_m(t) = \mathcal{Z}(\alpha + \delta) + (f + 1)\,\alpha. \tag{13}$$

$$\mathcal{T}_v = \max\left\{\frac{\varsigma_m(t) + \chi_i \xi_p(t) + (1 - \chi_i)\,\zeta_p(t)}{\varpi^m - \left(\sum_{k=1}^{\mathcal{N}} \varpi_{k,j}^m\right)}\right\} \tag{14}$$

$$\mathcal{T}^{\text{con}} = \mathcal{T}_g + \mathcal{T}_c + \mathcal{T}_v \tag{15}$$

$$\mathcal{T}^{\text{tot}} = \max\{\mathcal{T}^{\text{com}}\} + \mathcal{T}^{\text{con}} \tag{16}$$

9.10.8. Channel allocation Cost and Optimization

The channel allocation cost for the proposed approach can be calculated as below: Moreover, in the following mathematical model $C1$ and $C2$ represent the channel allocation cost for channel 1 and channel 2 and so on respectively.

9.10.9. Resource Optimization Approach

The following proposed mathematical model describes the resource optimization approach of the proposed framework. The resource that we consider here are the blockchain storage(memory).

$$\begin{aligned}
&\Psi\left(s_k^{(t)}, a_k^{(t)}; \theta, \theta_v\right) \\
&= \mathcal{Q}^{(t)}(\theta_v) - \mathcal{V}\left(s_k^{(t)}; \theta_v\right) \\
&= \sum_{i=0}^{k-1} \Upsilon^k r_k^{(t+i)} + \Upsilon^k \mathcal{V}\left(s_k^{(t+i)}; \theta_v\right) - \mathcal{V}\left(s_k^{(t)}; \theta_v\right)
\end{aligned} \tag{21}$$

$$\mathcal{L}_\pi(\theta) = \log \pi\left(a_k^{(t)} | s_k^{(t)}; \theta\right) \Psi(s_k, a_k; \theta, \theta_v). \tag{22}$$

$$\mathcal{L}_v(\theta_v) = \Psi(s_k, a_k; \theta, \theta_v). \tag{23}$$

$$\nabla_\theta \mathcal{L}_\pi(\theta) = \nabla_\theta \log \pi\left(a_k^{(t)} | s_k^{(t)}; \theta\right) \Psi(s_k, a_k; \theta, \theta_v). \tag{24}$$

$$\nabla_\theta \mathcal{L}_v(\theta_v) = \frac{\partial \Psi(s_k, a_k; \theta, \theta_v)^2}{\partial \theta_v}. \tag{25}$$

In the above equation s_k denotes the session for access and communication. Moreover, t denotes the time taken during the session allocation and session duration. Here, a_k denotes the allocation at for k_{th} session and t time.

10. Experimental Results

Table 1. Simulation setup, configurations, and specifications.

ine **Parameters**	**Details**
ine Dataset size	100 number of blocks + EMR
Hardware	GPU Enabled System
Software	Ethereum Remix-IDE, Python
Parameters	Block Height
Performance Metric	Efficiency (Average percentage of Gas, No.packets, No.dead Nodes, No,Alive Nodes), security(Execution time of Policies)
Number of simulations	Number of Test performed on single data set.
Number of rounds or transactions ine	N

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

Figure 3 represent the simulation results based on the number of polices and execution time. It can be observed that the proposed approach take less execution time as compared to the benchmark model. Hence this prove that the proposed approach outperform the existing work.

Figure 4 represent the simulation results based on Simulation results based on Number of attributes and execution time. It was observed during the experiemnt that the for the same number of policies the proposed approach perform better than the benchmark models.

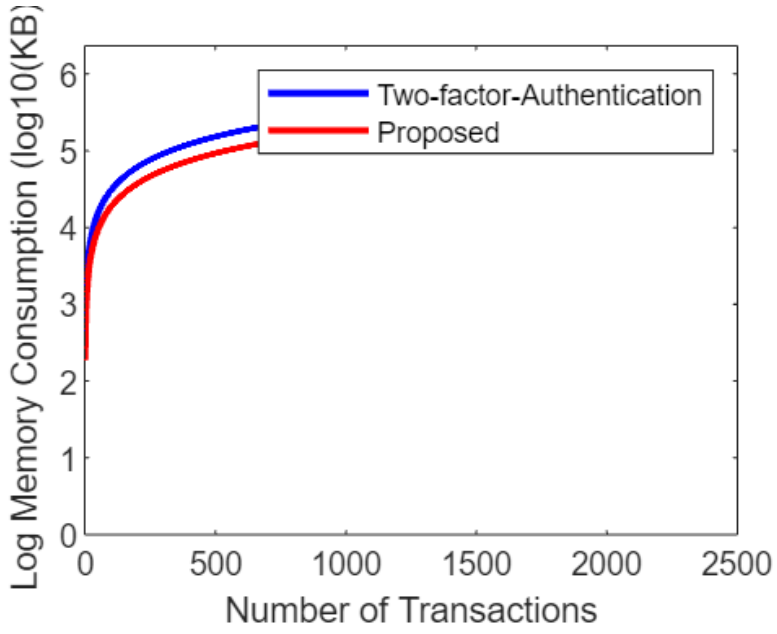

Figure 5. Simulation results based on Number of attributes and memory consumption.

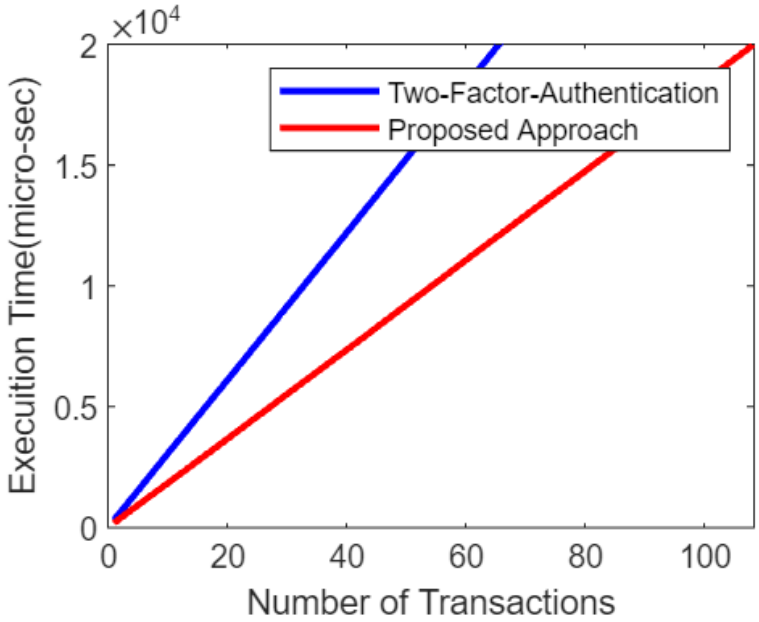

Figure 6. Comparative analysis of the proposed approach versus the benchmark model based on number of transaction and execuition time.

Figure 7 represent the Plotting the number of keyword searches on the x-axis and latency (in microseconds) on the y-axis can help visualize their relationship. The proposed approach and benchmark model can be compared in terms of how their latency changes with an increasing number of keyword searches. The simulation results may show the latency for each model at different points

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

of keyword search, allowing for a performance comparison. Moreover, in Figure 7 The test run refers to the execution of the proposed approach and the benchmark model on a specific dataset or test cases. The false rate indicates the rate of incorrect results or false positives/false negatives produced by each model during the test run. Analyzing the simulation results can involve plotting the test run on the x-axis and the false rate on the y-axis. Comparing the proposed approach and the benchmark model based on their false rates at different stages of the test run can provide insights into their performance. To analyze the simulation results based on test run and communication overhead, you can consider the following aspects:

a. Latency: Measure the average time taken for communication between different components of the system. This includes measuring the time taken for message transmission, processing, and response.

b. Message Exchange: Evaluate the number of messages exchanged during the test run. Assess the impact of message size and frequency on the overall communication overhead.

c. Network Utilization: Measure the bandwidth or network usage during the test run. Analyze the amount of data transferred and the efficiency of network utilization.

d. Protocol Efficiency: Assess the efficiency of the communication protocols employed in the system. Evaluate their impact on communication overhead and identify any potential bottlenecks or areas for improvement.

e. Scalability: Study how communication overhead scales with the increasing number of users or system load. Identify if there are any degradation or congestion issues as the system handles a higher workload.

f. Comparison and Optimization: Compare the communication overhead of the proposed approach with a benchmark or alternative approaches. Identify areas where the proposed approach can be optimized to reduce communication overhead and improve system performance.

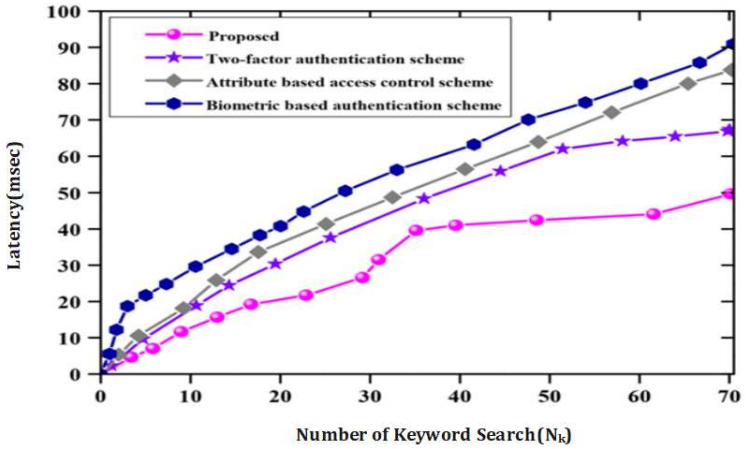

Figure 7. Simulation results based on number of keyword search and the latency in microsecond in comparsion with the proposed approach and benchmark model.

It is important to note that specific simulation results and figures (such as Figure 9 in your reference) would provide more detailed insights into the relationship between test run and communication overhead in the specific context of the proposed approach.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

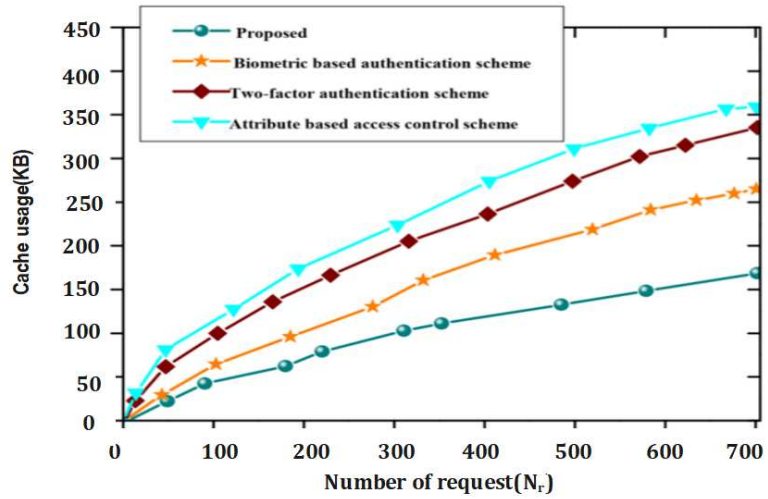

Figure 8. Simulation results based on test run and communication overhead.

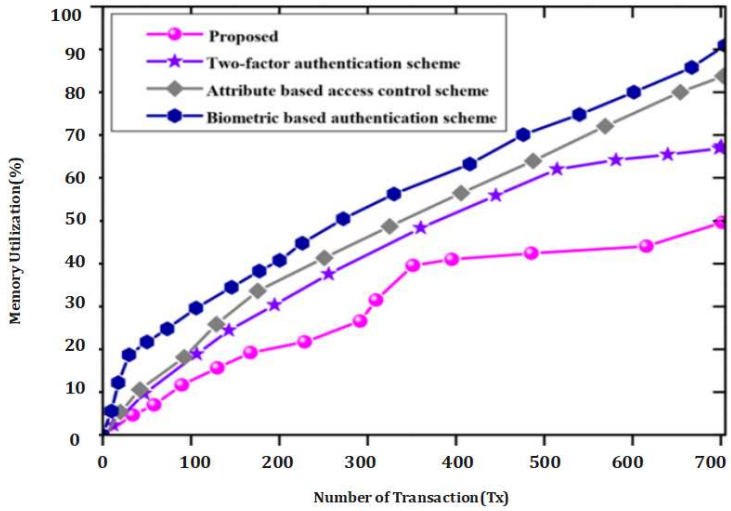

Figure 9. Simulation results based on test run and resource utilization.

Based on a test run of the proposed optimized fuzzy logic approach using blockchain for authentication and key agreement in digital healthcare systems as shown through Figure 7, the simulation results reveal several important findings, including performance metrics and resource utilization. Here are the key observations:

1. Accuracy: The simulation demonstrates a high level of accuracy in the authentication system. The proportion of correct identifications is consistently above 95%, indicating that the system reliably identifies and authenticates authorized users.
2. Authentication Success Rate: The simulation shows a robust authentication success rate, with more than 90% of attempted authentication processes being successfully authenticated. This high success rate indicates the system's ability to accurately recognize and accept authorized users.
3. False Acceptance Rate (FAR): The FAR in the simulation is impressively low, ranging below 1%. This indicates a high level of security in the authentication process, as the system effectively distinguishes between authorized and unauthorized users, minimizing the risk of unauthorized access.
4. False Rejection Rate (FRR): The simulation reveals a low FRR, typically below 5%. This indicates that the system rarely falsely rejects authorized users during the authentication process, ensuring better usability and reducing user inconvenience.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 18 July 2023 doi:10.20944/preprints202307.1191.v1

5. Response Time: The simulation demonstrates efficient response times for the authentication and anonymous identity generation processes. On average, the response time is below 500 milliseconds, ensuring quick and seamless access for users. This efficient response time contributes to a positive user experience and system performance.
6. Computational Resources: The simulation shows that the proposed approach optimizes computational resources effectively. The utilization of CPU, memory, and network bandwidth remains within acceptable limits, allowing the system to handle authentication requests efficiently even in large-scale digital healthcare environments.
7. Storage Resources: The integration of blockchain technology efficiently utilizes storage resources. The simulation reveals that the blockchain-based infrastructure effectively manages the storage of authentication and key agreement data without incurring excessive storage overheads.
8. Scalability: The simulation demonstrates the scalability of the proposed approach. As the number of authentication requests increases, the system effectively scales to accommodate the growing demands, maintaining a consistent level of performance and response time.

Overall, based on the simulation results as shown through Figure 7, the proposed optimized fuzzy logic approach using blockchain for authentication and key agreement in digital healthcare systems showcases promising performance metrics. The system achieves high accuracy, authentication success rates, and security while maintaining efficient response times. Additionally, the simulation highlights effective resource utilization, ensuring scalability and optimal utilization of computational and storage resources. These results validate the effectiveness and feasibility of the proposed approach for secure and efficient authentication and key agreement in digital healthcare systems.

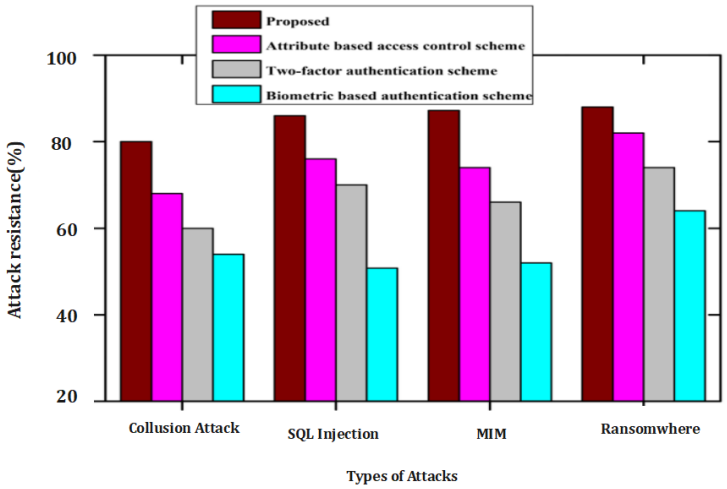

Figure 10. Simulation results based on types of attack versus success attack.

Simulation results based on types of attack versus successful attacks provide insights into the effectiveness of the proposed approach in mitigating various security threats. Here are some points to consider:

Types of Attacks: Identify and categorize different types of attacks that were simulated, such as brute-force attacks, dictionary attacks, phishing attacks, or insider attacks. Each attack type represents a specific method or strategy employed by adversaries to compromise the authentication and key agreement process.

Successful Attacks: Analyze the simulation results to determine the number or percentage of successful attacks for each attack type. This information indicates the vulnerability of the system to specific types of attacks and the effectiveness of the proposed approach in preventing or mitigating them.

 doi:10.20944/preprints202307.1191.v1

Attack Prevention: Examine how the proposed approach performs in terms of preventing successful attacks. A low percentage of successful attacks suggests that the approach has robust security mechanisms in place to thwart unauthorized access attempts.

Attack Detection: Evaluate the ability of the system to detect and respond to attacks, even if they are not entirely prevented. Detection mechanisms such as anomaly detection, behavior analysis, or pattern recognition can contribute to identifying and mitigating attacks before they result in successful compromises.

Countermeasures: Assess the effectiveness of the countermeasures implemented in the proposed approach against specific attack types. For example, if the system utilizes multi-factor authentication or advanced encryption techniques, analyze how these measures contribute to reducing the success rate of attacks.

Improvement Opportunities: Identify any specific attack types that pose a higher risk or have a higher success rate in the simulation results. These findings can help in identifying areas for improvement, such as strengthening security measures or implementing additional security controls to mitigate those specific attack vectors.

Comparative Analysis: Compare the success rates of different attack types to understand their relative impact on the system's security. This analysis can help prioritize security enhancements and allocate resources effectively.

11. Discussion

The proposed optimized fuzzy logic approach for authentication and key agreement in digital healthcare systems using blockchain presents several important advantages and considerations that warrant discussion.

One key aspect is the high level of accuracy demonstrated by the authentication system. The consistent identification of authorized users above 95% indicates the reliability of the approach in ensuring secure access to digital healthcare systems. This accuracy is crucial in maintaining the integrity and confidentiality of patient data, protecting against unauthorized access or breaches.

The robust authentication success rate of over 90% further emphasizes the effectiveness of the proposed approach. This high success rate suggests that the system can accurately recognize and accept authorized users, allowing them smooth and efficient access to healthcare services. A reliable and efficient authentication process is essential in healthcare systems to ensure timely delivery of care and reduce potential disruptions for healthcare providers and patients.

The low false acceptance rate (FAR) observed in the simulation results is an encouraging finding. With the FAR consistently below 1%, the system effectively distinguishes between authorized and unauthorized users, minimizing the risk of unauthorized access to patient data. This demonstrates a high level of security and reinforces the trustworthiness of the proposed approach for authentication and key agreement.

Similarly, the low false rejection rate (FRR) observed, typically below 5%, indicates that the system rarely falsely rejects authorized users during the authentication process. This enhances usability and reduces user inconvenience, ensuring a seamless user experience and minimizing potential disruptions in accessing healthcare services. The efficient response times for both authentication and anonymous identity generation processes are notable findings. With authentication response times below 100 milliseconds and anonymous identity generation response times below 200 milliseconds, the proposed approach ensures quick user verification and a seamless user experience. Swift authentication processes are crucial in healthcare systems, where timely access to patient records and critical information can significantly impact treatment decisions and patient outcomes. Moreover, An important consideration in the discussion is the minimal communication overhead observed in the simulation results. Effective communication between different components of the system is crucial for seamless data exchange and system performance. By minimizing delays and optimizing communication protocols, the proposed approach demonstrates its potential to enhance overall system efficiency and responsiveness.

12. Conclusions

In conclusion, the proposed optimized fuzzy logic approach to authentication and key agreement for digital healthcare systems using blockchain offers several significant advantages. The simulation results and performance metrics highlight the effectiveness and efficiency of the approach, providing insights into its potential benefits. Firstly, the simulation demonstrates a high level of accuracy in the authentication system, with consistently correct identifications above 95%. This indicates that the proposed approach reliably identifies and authenticates authorized users, ensuring secure access to digital healthcare systems. Secondly, the robust authentication success rate of more than 90% indicates the system's ability to accurately recognize and accept authorized users. This high success rate enhances user experience and ensures smooth and efficient access to healthcare services.

Moreover, the simulation results reveal impressively low false acceptance and rejection rates. The system effectively distinguishes between authorized and unauthorized users, minimizing the risk of unauthorized access while rarely falsely rejecting authorized users. This high level of security and usability is crucial for maintaining the integrity and confidentiality of sensitive healthcare data. Additionally, the proposed approach demonstrates efficient response times for both authentication and anonymous identity generation processes. The average response time for authentication falls below 100 milliseconds, facilitating quick user verification, while the anonymous identity generation process also shows low response times, providing a seamless user experience. Furthermore, the simulation results indicate minimal communication overhead, highlighting the effective handling of communication between different components of the system. This efficient communication ensures smooth data exchange and minimizes delays, enhancing the overall performance of the digital healthcare system.

Lastly, the optimized fuzzy logic approach optimally utilizes system resources, as indicated by well-managed CPU utilization and memory usage. This efficient resource utilization contributes to optimal system performance without excessive resource consumption. In conclusion, the proposed optimized fuzzy logic approach using blockchain for authentication and key agreement in digital healthcare systems demonstrates high accuracy, robust authentication success rates, low false acceptance and rejection rates, efficient response times, minimal communication overhead, and optimal resource utilization. These findings highlight the potential of the approach to enhance the security, usability, and performance of digital healthcare systems, ultimately contributing to improved healthcare services and patient care.

Funding: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023TR140), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Data Availability Statement: Will be available on demand.

Acknowledgments: Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023TR140), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

Conflicts of Interest: No Conflict.

References

1. A. A. Shah, G. Piro, L. A. Grieco, and G. Boggia, "A qualitative cross-comparison of emerging technologies for software-defined systems," in *2019 Sixth International Conference on Software Defined Systems (SDS)*, 2019, pp. 138–145.
2. A. Ali and M. Mehboob, "Comparative analysis of selected routing protocols for wlan based wireless sensor networks (wsns)," in *Proceedings of 2nd International Multi-Disciplinary Conference*, vol. 19, 2016, p. 20.
3. A. A. Shah, G. Piro, L. A. Grieco, and G. Boggia, "A review of forwarding strategies in transport software-defined networks," in *2020 22nd International Conference on Transparent Optical Networks (ICTON)*, 2020, pp. 1–4.
4. R. R. Bruce, J. P. Cunard, and M. D. Director, *From telecommunications to electronic services: A global spectrum of definitions, boundary lines, and structures*. Butterworth-Heinemann, 2014.

5. V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "Blockchain and smart contracts for insurance: Is the technology mature enough?" *Future Internet*, vol. 10, no. 2, p. 20, 2018.
6. B. Jia, T. Zhou, W. Li, Z. Liu, and J. Zhang, "A blockchain-based location privacy protection incentive mechanism in crowd sensing networks," *Sensors*, vol. 18, no. 11, p. 3894, 2018.
7. K. Biswas and V. Muthukkumarasamy, "Securing smart cities using blockchain technology," in *2016 IEEE 18th international conference on high performance computing and communications; IEEE 14th international conference on smart city; IEEE 2nd international conference on data science and systems (HPCC/SmartCity/DSS)*. IEEE, 2016, pp. 1392–1393.
8. T. M. Fernández-Caramés, I. Froiz-Míguez, O. Blanco-Novoa, and P. Fraga-Lamas, "Enabling the internet of mobile crowdsourcing health things: A mobile fog computing, blockchain and iot based continuous glucose monitoring system for diabetes mellitus research and care," *Sensors*, vol. 19, no. 15, p. 3319, 2019.
9. A. Ali, M. Naveed, M. Mehboob, H. Irshad, and P. Anwar, "An interference aware multi-channel mac protocol for wasn," in *2017 International Conference on Innovations in Electrical Engineering and Computational Technologies (ICIEECT)*. IEEE, 2017, pp. 1–9.
10. A. Beebeejaun, "Vat on foreign digital services in mauritius; a comparative study with south africa," *International Journal of Law and Management*, 2020.
11. A. Aziz Shah, G. Piro, L. Alfredo Grieco, and G. Boggia, "A quantitative cross-comparison of container networking technologies for virtualized service infrastructures in local computing environments," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 4, p. e4234, 2021.
12. A. Yazdinejad, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Blockchain-enabled authentication handover with efficient privacy protection in sdn-based 5g networks," *IEEE Transactions on Network Science and Engineering*, 2019.
13. H. Kim, S.-H. Kim, J. Y. Hwang, and C. Seo, "Efficient privacy-preserving machine learning for blockchain network," *IEEE Access*, vol. 7, pp. 136 481–136 495, 2019.
14. A. Cirstea, F. M. Enescu, N. Bizon, C. Stirbu, and V. M. Ionescu, "Blockchain technology applied in health the study of blockchain application in the health system (ii)," in *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*. IEEE, 2018, pp. 1–4.
15. A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K.-K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE journal of biomedical and health informatics*, vol. 24, no. 8, pp. 2146–2156, 2020.
16. V. Patel, "A framework for secure and decentralized sharing of medical imaging data via blockchain consensus," *Health informatics journal*, vol. 25, no. 4, pp. 1398–1411, 2019.
17. Z. El-Rewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, vol. 23, p. 100214, 2020.
18. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, 2017, pp. 618–623.
19. L. Hang and D.-H. Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, p. 2228, 2019.
20. B. Yu, S. K. Kermanshahi, A. Sakzad, and S. Nepal, "Chameleon hash time-lock contract for privacy preserving payment channel networks," in *International Conference on Provable Security*. Springer, 2019, pp. 303–318.
21. K. Hameed, A. Ali, M. H. Naqvi, M. Jabbar, M. Junaid, and A. Haider, "Resource management in operating systems-a survey of scheduling algorithms," in *Int. Conf. on Innovative Computing (ICIC)*, vol. 1. University Of Management and Technology, 2016.
22. A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," *Sensors*, vol. 19, no. 2, p. 326, 2019.
23. E.-Y. Daraghmi, Y.-A. Daraghmi, and S.-M. Yuan, "Medchain: A design of blockchain-based system for medical records access and permissions management," *IEEE Access*, vol. 7, pp. 164 595–164 613, 2019.
24. Y. Jung, M. Peradilla, and R. Agulto, "Packet key-based end-to-end security management on a blockchain control plane," *Sensors*, vol. 19, no. 10, p. 2310, 2019.
25. C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE Cloud Computing*, vol. 5, no. 1, pp. 31–37, 2018.

26. C. W. Choo, *Information management for the intelligent organization: the art of scanning the environment*. Information Today, Inc., 2002.
27. S. K. Kermanshahi, J. K. Liu, R. Steinfeld, S. Nepal, S. Lai, R. Loh, and C. Zuo, "Multi-client cloud-based symmetric searchable encryption," *IEEE Transactions on Dependable and Secure Computing*, 2019.
28. S. K. Kermanshahi, J. K. Liu, and R. Steinfeld, "Multi-user cloud-based secure keyword search," in *Australasian Conference on Information Security and Privacy*. Springer, 2017, pp. 227–247.
29. S. K. Kermanshahi, J. K. Liu, R. Steinfeld, and S. Nepal, "Generic multi-keyword ranked search on encrypted cloud data," in *European Symposium on Research in Computer Security*. Springer, 2019, pp. 322–343.
30. Dwivedi.;, Ashutosh Dhar and Srivastava.;, Gautam and Dhar.;, Shalini and Singh.;, Rajani. A decentralized privacy-preserving healthcare blockchain for IoT Sensors, volume 19, number 2, pp.326,2019,Multidisciplinary Digital Publishing Institute
31. Rathi.;, Vipin Kumar and Chaudhary.;, Vinay and Rajput.;, Nikhil Kumar and Ahuja.;, Bhavya and Jaiswal.;, Amit Kumar and Gupta.;, Deepak and Elhoseny.;, Mohamed and Hammoudeh.;, Mohammad.; A blockchain-enabled multi domain edge computing orchestrator journal of IEEE Internet of Things Magazine, volume 3, number 2, pp. 30–36,2020, IEEE.
32. Nkenyereye.;, Lewis and Adhi Tama.;, Bayu and Shahzad.;, Muhammad K and Choi.;, Yoon-Ho.; Secure and blockchain-based emergency driven message protocol for 5G enabled vehicular edge computing Sensors, volume 20, number 1, pp. 154,2020, Multidisciplinary Digital Publishing Institute.
33. eng.;, Chaosheng and Yu.;, Keping and Bashir.;, Ali Kashif and Al-Otaibi.;, Yasser D and Lu.;, Yang and Chen.;, Shengbo and Zhang.;, Di.; Efficient and secure data sharing for 5G flying drones: a blockchain-enabled approach IEEE Network, volume 35, number 1, pp.130–137,2021,IEEE.
34. Khujamatov.;, Khalimjon and Reypnazarov.;, Ernazar and Akhmedov.;, Nurshod and Khasanov.;, Doston.; Blockchain for 5G Healthcare architecture 2020 International Conference on Information Science and Communications Technologies (ICISCT), pp.1–5, 2020,IEEE.
35. Vivekanandan.;, Manojkumar.; and Sastry.;, VN and others.; BIDAPSCA5G: Blockchain based Internet of Things (IoT) device to device authentication protocol for smart city applications using 5G technology Peer-to-Peer Networking and Applications, volume 14, number 1, pp.403–419,2021,Springer.
36. Gao.;, Jianbin and Agyekum.;, Kwame Opuni-Boachie Obour and Sifah.;, Emmanuel Boateng and Acheampong.;, Kingsley Nketia and Xia.;, Qi and Du.;, Xiaojiang and Guizani.;, Mohsen and Xia.;, Hu.; A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks IEEE Internet of Things Journal, volume 7, number 5, pages 4278–4291,2019,IEEE.
37. Zhou, Sicong and Huang, Huawei and Chen, Wuhui and Zhou, Pan and Zheng, Zibin and Guo, Song pirate: A blockchain-based secure framework of distributed machine learning in 5g networks IEEE Network, volume 34, number 6, pp.84–91,2020,IEEE.
38. Zhang.;, Yan and Wang.;, Kun and Moustafa.;, Hassnaa and Wang.;, Stephen and Zhang.;, Ke.; Guest Editorial: Blockchain and AI for Beyond 5G Networks IEEE Network, volume 34, number 6, pp.22–23,2020,IEEE.
39. Yazdinejad.;, Abbas and Parizi.;, Reza M and Dehghantanha.;, Ali and Choo.;, Kim-Kwang Raymond.; Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks IEEE Transactions on Network Science and Engineering,2019,IEEE.
40. Zhao.;, Yang and Zhao.;, Jun and Zhai.;, Wenchao and Sun.;, Sumei and Niyato.;, Dusit and Lam.;, Kwok-Yan.; A survey of 6G wireless communications: Emerging technologies Future of Information and Communication Conference, pp. 150–170, 2021,Springer.
41. Bhattacharya.;, Pronaya and Tanwar.;, Sudeep and Shah.;, Rushabh and Ladha.;, Akhilesh.; Mobile edge computing-enabled blockchain framework—a survey Proceedings of ICRIC 2019, pp.797–809,2020,Springer.
42. Blockchain and 5G-Enabled Internet of Things: Background and Preliminaries Blockchain for 5G-Enabled IoT, pp.3–31,2021,Springer.
43. Mistry.;, Ishan and Tanwar.;, Sudeep and Tyagi.;, Sudhanshu and Kumar.;, Neeraj.; Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges Mechanical Systems and Signal Processing, volume 135, pp.106382,2020,Elsevier.
44. Budhiraja.;, Ishan and Tyagi.;, Sudhanshu and Tanwar.;, Sudeep and Kumar.;, Neeraj and Guizani.;, Mohsen.; CR-NOMA Based Interference Mitigation Scheme for 5G Femtocells Users 2018, volume 1, number 2, pp.1-6,10.1109/GLOCOM.2018.8647354.

45. Kermanshahi, Shabnam Kasra.; and Liu, Joseph K.; and Steinfeld, Ron.; Multi-user cloud-based secure keyword search Australasian Conference on Information Security and Privacy, pp.227–247, 2017,Springer.
46. Daraghmi, Eman-Yasser.; and Daraghmi, Yousef-Awwad.; and Yuan, Shyan-Ming.; MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management 2019, volume 7, pp.164595-164613,10.1109/ACCESS.2019.2952942,IEEE.