Journal of Theoretical and Applied Information Technology
29th February 2024. Vol.102. No 4

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REVOLUTIONIZING HEALTHCARE: UNLEASHING BLOCKCHAIN BRILLIANCE THROUGH FUZZY LOGIC AUTHENTICATION

TAYSEER ALKHDOUR[1], MOHAMMED AMIN ALMAIAH[2, 3], AITIZAZ ALI[4], ABDALWALI LUTFI[5, 6], MAHMAOD ALRAWAD[5] , TING TIN TIN[7]

[1] Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa 31982, Saudi Arabia
[2]King Abdullah the II IT School, The University of Jordan, Amman 11942, Jordan
[3]Applied Science Research Center, Applied Science Private University, Amman 11931, Jordan
[4] school of technology, Asia Pacific University, Malaysia
[5] College of Business, King Faisal University, Al-Ahsa, 31982, Saudi Arabia
[6] MEU Research Unit, Middle East University, Amman, Jordan
[7] Faculty of Data Science and Information Technology, INTI International University, Malaysia

E-mail: Corresponding authors: talkhdour@kfu.edu.sa and m.almaiah@ju.edu.jo

ABSTRACT

In the ever-evolving landscape of digital healthcare, security and authentication emerge as paramount concerns. This paper introduces an innovative strategy aimed at tackling these challenges by melding the robustness of blockchain technology with the precision of advanced fuzzy logic authentication. We embark on an exploration of this fusion of cutting-edge technologies, diving deep into how they collaboratively enhance the security, privacy, and efficiency of healthcare systems. This pioneering approach has the potential to revolutionize the management, accessibility, and protection of healthcare data, ushering in a new era characterized by secure and patient-centric digital healthcare. Digital healthcare systems play a crucial role in delivering efficient and accessible healthcare services. Nevertheless, ensuring the existence of secure authentication and key agreement mechanisms is imperative to safeguard sensitive patient data and uphold the system's integrity. Current methodologies grapple with constraints related to vulnerability to cyberattacks, scalability challenges, and optimizing resource allocation. Furthermore, the integration of blockchain technology introduces additional layers of complexity that necessitate careful consideration. This research advocates for an optimized approach that combines fuzzy logic with blockchain technology to address authentication and key agreement challenges within digital healthcare systems. The proposed solution harnesses the adaptability and versatility of fuzzy logic algorithms to navigate the realm of uncertainty and imprecision inherent in authentication decisions. By leveraging fuzzy logic, the system can effectively reduce false positives and false negatives, thereby reinforcing its resilience against adversarial attacks. Moreover, the integration of blockchain technology provides a decentralized and tamper-resistant infrastructure tailored for securely storing and managing authentication and key agreement data. This promotes transparency and trust within the system, mitigating the risks associated with unauthorized access and data tampering. Additionally, the blockchain-based architecture lends itself to efficient resource allocation and scalability, enabling the system to promptly process authentication requests, even in expansive digital healthcare environments. The effectiveness of the proposed method is evaluated using the NIST Special Database 302, with results demonstrating superior performance compared to existing approaches. It achieves minimal False Rejection Rate (FRR), False Acceptance Rate (FAR), and response time. Furthermore, the proposed method minimizes communication overhead during authentication processes and exhibits resilience against a spectrum of cyberattacks, including Replay attacks, Man-in-the-middle attacks, Denial of Service (DoS) attacks, and Impersonation attacks. The combination of exceptional security, efficiency, and resilience against diverse cyber threats positions this solution as a promising choice for secure data sharing within peer-to-peer (P2P) cloud environments.

Keywords: *Fuzzy Logic; Blockchain; Smart-contract, Lizard Search Algorithm, Homomorphic Encryption, Cyber-attacks and Sustainable Development Goals (SDG).*

1. INTRODUCTION

In the context of a blockchain-based healthcare system, the CALS algorithm holds the potential for optimizing various facets, including resource allocation, data management, privacy protection, and transaction processing. Now, how it could be harnessed:

• Resource Optimization: The CALS algorithm's application can extend to enhancing the allocation of healthcare resources, encompassing medical staff, equipment, and facilities. It can take into account factors such as patient demand, resource availability, and cost constraints to devise an optimal allocation strategy.

• Effective Data Management: Within a blockchain-based healthcare system, patient data is securely and transparently stored on the blockchain. The CALS algorithm can play a role in streamlining the organization and retrieval of data, ensuring efficient access while upholding data integrity.

• Preserving Privacy: Privacy preservation is of paramount importance in healthcare systems. The CALS algorithm can contribute to optimizing privacy-preserving techniques, such as data anonymization and encryption. This enables the safeguarding of sensitive patient information while permitting authorized access to pertinent parties.

• Streamlined Transaction Processing: The efficiency of transaction processing is central to blockchain technology. The CALS algorithm can optimize transaction validation and consensus mechanisms, guaranteeing swift and reliable processing of healthcare transactions while maintaining the security and trustworthiness of the blockchain.

In order to integrate the CALS algorithm into a blockchain-based healthcare system, it is essential to precisely define the specific optimization problem at hand. Custom fitness functions and crossover operators should be developed accordingly. Moreover, it is crucial to consider the seamless integration of the CALS algorithm into the existing blockchain infrastructure, including aspects such as block creation, validation, and consensus mechanisms. Furthermore, when it comes to sharing data among cloud servers in healthcare systems, two categories of existing data-sharing systems are commonly observed: P2P distributed and centralized. Nevertheless, these systems display security vulnerabilities when users access data from cloud servers, potentially leading to privacy breaches and unauthorized data access. Hence, the paramount objective is to ensure secure and efficient data access and sharing. To achieve this, various authentication schemes are employed for securely accessing data from cloud servers. Attribute-Based Encryption (ABE) schemes are used to control access based on user credentials. However, traditional ABE schemes lack the capability to directly share encrypted data. Attribute-Based Proxy Re-Encryption (ABPRE) is employed for this purpose, but it presents challenges in verifying the authenticity of re-encrypted ciphertext provided by the cloud server.

Role-Based Access Control (RBAC) schemes are utilized to regulate user data access, but they may introduce delays in delivering data to users. Mutual authentication schemes are implemented to identify both the service provider and the user. In the context of cloud environments, mutual authentication protocols are critical for achieving anonymous communication and robust preservation of privacy. The generation of anonymous identities within the cloud server is vital to safeguard user personal information from potential attackers during data access. Identifying passive attackers within the cloud server is a complex task, highlighting the significance of anonymous authentication protocols.

In summary, the CALS algorithm holds promise for optimizing various aspects of blockchain-based healthcare systems, and robust security measures must be implemented to ensure the confidentiality and integrity of patient data in cloud environments. The unlinkability is essential in the anonymous authentication scheme in order to attain a high-security level during resisting passive attacks. In addition, 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.

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, capability, 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.

2. RELATED WORKS

In this section, we provides an overview of previous research and existing literature. on authentication mechanisms in peer-to-peer (P2P) cloud environments. We discuss the various approaches, techniques, and technologies that have been explored in the previous works. For example, 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. 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.

The above 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. In [13] introduced a protocol designed for secure data sharing among user groups in cloud environments. Their approach employed an innovative combination of a One-way Circular Linked Table in a binary tree-Oblivious Random Access Memory (OCLT-ORAM) protocol and a secure proxy re-encryption protocol with built-in resistance against collusion.

The OCLT-ORAM protocol played a pivotal role in creating a conference key through key exchange, which was then utilized to safeguard the shared data. Importantly, this protocol came with robust security proofs to support its claims. Empirical assessments underscored the efficacy and security of the OCLT-ORAM protocol in facilitating group data sharing within cloud environments. However, it was noted that this protocol incurred substantial communication overhead in interactions between users and cloud servers. Shen et al.'s work advances the field of secure group data sharing in cloud settings by harnessing the OCLT-ORAM protocol and secure proxy re-encryption. This protocol ensures the confidentiality and integrity of data by utilizing conference keys, providing dependable security assurances. However, it is important to carefully consider the communication

overhead associated with this method, especially in situations with limited resources or scalability concerns. When contemplating the adoption of an enhanced fuzzy logic-based authentication and key agreement approach in blockchain-driven digital healthcare systems, Shen et al.'s research provides valuable insights for strengthening data sharing mechanisms. These insights can be seamlessly integrated or harmonized with fuzzy logic-based authentication, enhancing overall healthcare data security and privacy.

Similarly, the work in [12] represents a significant contribution to the field of authentication and key agreement. Their approach leverages elliptic curve certificate-free cryptography to ensure secure data sharing in multi-cloud environments, addressing the complexities of trust establishment and cross-cloud data migration. Importantly, this approach outperforms traditional methods. However, it is crucial to recognize the challenges associated with data transfers among multiple users and diverse cloud servers when considering its application in scenarios where seamless data sharing and collaboration are vital. In most of the research offers a promising avenue for improving the security and efficiency of data sharing in blockchain-based digital healthcare systems. In the context of enhancing a fuzzy logic-based authentication and key agreement approach, their proposal provides valuable insights into mechanisms for secure data sharing and trust establishment. The combination of fuzzy logic-based authentication, elliptic curve certificate-free cryptography, and blockchain technology has the potential to create an enhanced solution that addresses the inherent limitations of both approaches, ultimately facilitating secure and efficient data sharing among various stakeholders in the healthcare domain and across different cloud servers. Shifting our focus to the contribution made in [13] their RRSD (Redundant Replica Deletion) approach strives to reduce storage consumption and maintain data reliability within dynamic P2P cloud environments. This method employs strategies such as redundant replica deletion and optimal replica placement to minimize the number of redundant copies while ensuring load balancing and data integrity. It employs a centralized approach to determine the minimum required number of replicas for data reliability.

Empirical assessments demonstrate that RRSD outperforms conventional methodologies in terms of performance. However, it is worth noting that RRSD has not yet been validated in an authentic P2P cloud setting and lacks provisions for ensuring consistency when dealing with multiple replicas. In a related context, Li et al. propose a three-factor Mutual Authentication and Key Agreement (MAKA) protocol aimed at addressing security concerns in cloud computing. This protocol not only offers formal proof but also supports dynamic revocation, making it suitable for multi-server environments. Empirical findings indicate that the MAKA protocol excels in terms of overall computation time. However, it does exhibit vulnerabilities in terms of resilience against a variety of malicious attacks. The research conducted in [15] and [16] significantly enriches the domain of data reliability and security within cloud computing environments. Sun et al.'s RRSD methodology is centered on the minimization of storage consumption and the preservation of data reliability through efficient replica management. In contrast, MAKA protocol addresses security challenges by introducing a three-factor mutual authentication and key agreement mechanism.

However, it is essential to acknowledge the inherent limitations present in both of these approaches. When contemplating the improvement of a fuzzy logic-based approach for authentication and key agreement in blockchain-driven digital healthcare systems, the valuable insights from Sun et al.'s RRSD approach can greatly contribute to refining data storage and replication strategies in the healthcare ecosystem supported by blockchain technology. Furthermore, Li et al.'s MAKA protocol provides valuable insights for enhancing security and authentication mechanisms. By combining these methodologies with fuzzy logic-based authentication and harnessing the inherent transparency and security attributes of blockchain, the potential for achieving an advanced solution for secure and reliable authentication and key agreement in digital healthcare systems becomes feasible.

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.

2.2 Background

In recent years, the healthcare sector has been undergoing a profound transformation due to technological advancements and an increasing focus on patient-centered care. Among the most promising technological innovations in healthcare, blockchain technology stands out. Blockchain has the potential to completely transform healthcare by offering a secure, transparent, and immutable platform for the management and sharing of sensitive patient data, medical records, and clinical information. Nevertheless, the integration of blockchain technology in healthcare presents unique challenges, with a primary focus on security, privacy, and access control. It is crucial to ensure that only authorized individuals can access and modify patient data to uphold patient confidentiality and data integrity. Conventional authentication methods, such as username-password combinations, are susceptible to breaches, rendering them insufficient for securing patient data within a blockchain-based ecosystem. This is where the concept of "Fuzzy Logic Authentication" comes into play. Fuzzy logic, a mathematical framework that deals with uncertainty and imprecision, offers an innovative approach to authentication in healthcare blockchain systems. Unlike traditional binary authentication methods, fuzzy logic authentication allows for a more nuanced and context-aware approach to verifying the identity and access rights of users. By leveraging fuzzy logic, healthcare blockchain systems can:

• Enhance Security: Fuzzy logic authentication considers a user's identity as a continuum rather than a binary yes/no decision. This means that even if some authentication parameters deviate slightly, access can still be granted with certain restrictions, providing an additional layer of security.

• Improve Privacy: Patients and healthcare providers can benefit from fine-grained control over access permissions. Fuzzy logic allows for dynamic adjustments of access rights based on the specific context, ensuring that only the necessary information is shared while preserving privacy.

• Enable Granular Access Control: Fuzzy logic enables the creation of flexible access control policies. For instance, healthcare blockchain systems can use fuzzy logic to grant varying levels of access to medical records based on the urgency of the situation or the trustworthiness of the requesting party.

• Adapt to Real-World Scenarios: Healthcare is a dynamic field with constantly changing conditions. Fuzzy logic authentication can adapt to evolving circumstances, making it suitable for complex healthcare environments where decisions are rarely black and white. In this context, the paper titled "Revolutionizing Healthcare: Unleashing Blockchain Brilliance Through Fuzzy Logic Authentication" explores the potential of fuzzy logic authentication to address the unique challenges of securing and managing patient data within blockchain-based healthcare systems. By combining the strengths of blockchain technology and fuzzy logic authentication, this research aims to pave the way for a safer, more efficient, and patient-centered healthcare ecosystem.

2.2.1. 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].

2.2.2. Authentication and Key Agreement in Healthcare Systems:

Authentication is the process of verifying the identity of users accessing digital health-care 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.

2.2.3. 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 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].

2.2.4. 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.

2.2.5. 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 STATMENT

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.

4. SYSTEM DESIGN

This section depicts the system model of anonymous ID generation, secure authentication and communication, and resource sharing in the Peer-to-Peer cloud. In order to keep the user's private information safe while they access the data, each peer generates their own anonymous ID using a hash function. The AKA protocol ensures the privacy of the seeking peer and the authenticity of the authorized peer during the secure authentication and communication procedure. Both of these friends take part in the challenge-response process. A challenge and expected value are sent from the asking peer to the authenticated peer, and the latter then sends the calculated value back to the former. In order to determine whether or not authentication was successful, the requesting peer compares the

calculated value to the expected value [29]. After that, the encrypted session key is created. The asking peer makes the demand of the authenticated peer, and the latter confirms the availability of the requested resource. If it is, it uses the secure session key to encrypt the resource before sending it to the asking peer. This encrypted resource is then decrypted by the requesting peer using the previously established secure session key. Additionally, encryption and decryption algorithms are used in this procedure to safeguard the communal asset.

4.1. Resource sharing

Blockchain technology has evolved beyond its initial applications in cryptocurrencies and is now being explored in various domains, including supply chain management, healthcare, and IoT. One critical challenge in blockchain systems is efficient resource sharing and allocation, which is essential for optimizing system performance and ensuring fair access to resources among participants. This paper proposes a novel approach to resource sharing in blockchain systems using fuzzy logic, aiming to improve resource allocation efficiency, enhance decision-making processes, and promote fairness among network participants. Blockchain technology has gained prominence for its ability to provide transparent, secure, and tamperresistant distributed ledgers. However, as blockchain systems continue to scale and diversify, effective resource management and allocation become crucial. Fuzzy logic, known for its ability to handle uncertainty and imprecise data, can be a powerful tool to address these challenges.

4.1.1 Fuzzy Logic-Based Resource Sharing

• Resource Allocation

Introduce a fuzzy logic-based approach to allocate resources within the blockchain network. Fuzzy rules and membership functions to model resource requirements, availability, and priority.

• Resource Optimization

Utilize fuzzy logic for optimizing resource allocation decisions, considering factors like network load, transaction priority, and historical usage patterns. Fuzzy Logic in Decision-Making.

• Trust and Reputation Incorporate fuzzy logic to evaluate trust and reputation scores of network participants. Fuzzy inference for decision-making, ensuring that resources are allocated to trusted nodes. Compare performance metrics, such as resource utilization, fairness, and response time, with traditional allocation methods. Adopting fuzzy logic for resource sharing in blockchain systems offers several significant benefits:

• Handling Uncertainty: Fuzzy logic can effectively manage uncertainty and imprecise 397 data, allowing blockchain systems to make resource allocation decisions in situations where exact information may be lacking or ambiguous.

• Enhanced Efficiency: Fuzzy logic-based resource allocation can optimize decision-making processes, considering factors like network load, transaction priority, and historical usage patterns. This leads to improved resource utilization and overall system efficiency.

• Fairness and Equity: Fuzzy logic enables the modeling of fairness metrics, ensuring that resources are distributed more equitably among network participants. This promotes fairness and prevents resource hoarding by specific nodes.

• Trust and Reputation: Fuzzy logic can assess trust and reputation scores of network participants, enhancing the allocation of resources to trusted nodes. This helps maintain the security and reliability of blockchain systems.

• Adaptive Decision-Making: Fuzzy logic allows for adaptive decision-making, where resource allocation strategies can be adjusted dynamically based on changing conditions, ensuring that resources are allocated where they are most needed.

• Real-World Applicability: Fuzzy logic-based resource sharing has practical applications in various use cases, including supply chain tracking, smart contracts, and decentralized applications (dApps), making it versatile and applicable across different domains.

• Improved System Performance: Through fuzzy logic, resource sharing can lead to better overall system performance, as resources are allocated more intelligently, reducing bottlenecks and improving response times.

In summary, adopting fuzzy logic for resource sharing in blockchain systems empowers these networks to handle uncertainty, optimize resource allocation, ensure fairness, and adapt to changing conditions, ultimately leading to more efficient and reliable blockchain systems with broader real-world applicability. Emphasize the potential for improved efficiency, fairness, and decision-making in resource allocation processes.

4.2. Authentication and Key Agreement

The AKA protocol is employed for peer authentication and the establishment of secure communication. In the authentication procedure, a challenge-response mechanism is employed, wherein the requesting peer transmits a challenge to the peer-undergoing authentication.

5. AUTHENTICATION AND KEY AGREEMENT (AKA) PROTOCOL

The AKA protocol serves the purpose of authenticating and establishing secure peer-to-peer communication. The authentication process is structured around a challenge-response mechanism, wherein the requesting peer initiates the process by transmitting a challenge denoted as *C* to the peer undergoing authentication. In response, the authenticated peer generates a calculated value *R* derived from a shared secret key denoted as *K* and the random number *N* that was 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.

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. Artificial Lizard Search Optimization (ALSO) Algorithm

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

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 including:

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

5.5. 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- 538 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.

5.6. 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. 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: To 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.

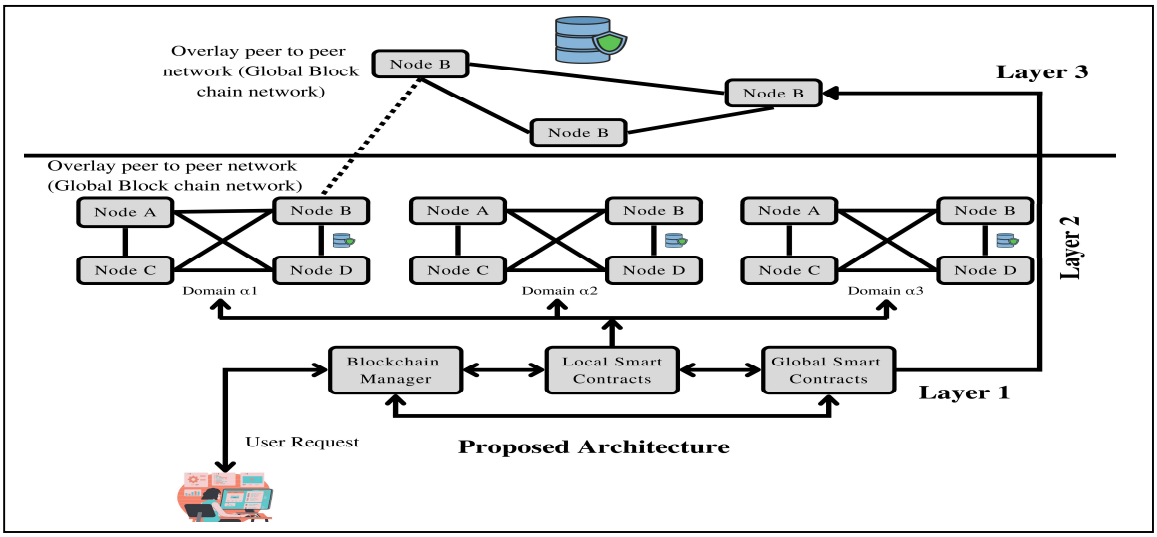

Figure 1. Proposed Framework.

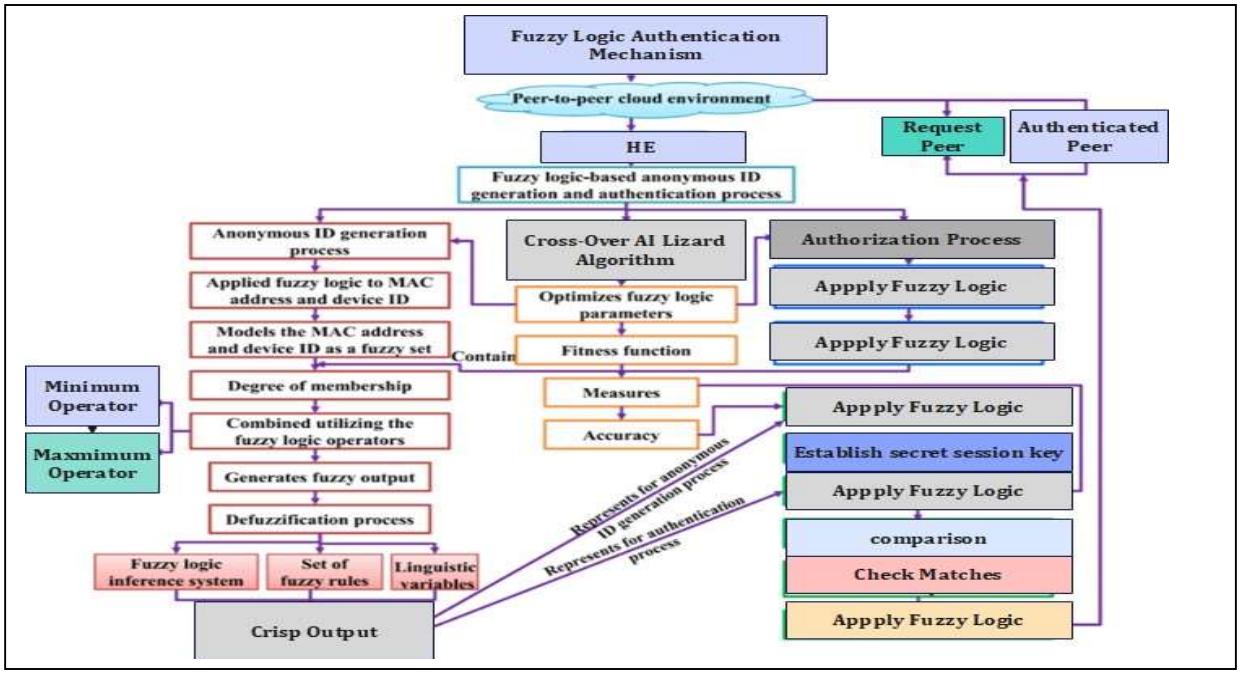

Figure 2. *Detail View Of The Proposed Framework Modules*

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*.

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 result corresponds to the anonymous id generated, and the calso algorithm's fitness function evaluates the accuracy of this anonymous *id*. Within the authentication process based on fuzzy logic, we apply fuzzy logic to both the shared secret key and the message, while the calso algorithm fine-tunes the parameters of the fuzzy logic. Let's designate the shared secret key as k and the message as m. In order to represent the shared secret key and message as fuzzy sets, we establish membership functions for each. Specifically, we denote the membership function for the shared secret key as *μk(k)* and for the message as *μm(m)*. These membership functions signify the level of association for the shared secret key and message, respectively. Subsequently, we amalgamate the membership degrees of the shared secret key and message through the application of fuzzy logic operators to yield the fuzzy output. The selection of fuzzy logic operators depends on the specific problem and may include operators such as and, or, or not. Let's symbolize the fuzzy output as f. we can represent the fuzzy output as follows:

$$f = fuzzy\_operator(\mu k(k), \mu m(m))$$

Where fuzzy_operator represents the chosen fuzzy logic operator.

7. LIZARD SEARCH ALGORITHM (LSA) WITH FUZZY LOGIC

The Lizard Search Algorithm (LSA) is a metaheuristic optimization technique inspired by the foraging behavior of lizards. Fuzzy logic is harnessed to direct both the exploration and exploitation phases of this algorithm.

7.1. Variables

- *P:* Population of lizards
- *Li:* Position of lizard i
- *f (Li):* Fitness function for lizard i
- *Lbest:* Best lizard position
- *fbest:* Best fitness value
- *rnd:* Random number

7.2. Initialization

- Initialize the population of lizards randomly
- Initialize Lbest as the current best solution
- Initialize fbest as a high value (for minimization problems) or a low value (for maximization problems).

7.3. Main Loop

Each lizard Li in the population Evaluate the fitness *f (Li)* of the lizard's position Generate a random number *rnd* between 0 and 1 *rnd* is less than the exploration threshold Apply fuzzy logic rules for exploration to determine the new lizard position Apply fuzzy logic rules for exploitation to determine the new lizard position Evaluate the fitness *f (Li)* of the new lizard position the new lizard position is better than *Lbest* Update *Lbest* with the new position Update *fbest* with the fitness of the new position 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 termination condition is met.

7.4. Output

- Return Lbest and fbest 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 Xi = (Xi1, Xi2, . . . , Xin), 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 $f(X)$, where $X = (X1, X2, \ldots, Xn)$ represents the decision variable vector. In the LSA, each lizard i is represented by an attribute vector $Xi = (Xi1, Xi2, \ldots, Xin)$. The attributes of the lizards are associated with fuzzy sets that capture the linguistic variables, such as "good," "average," and "poor." Let $\mu ij(x)$ denote the membership function of attribute Xij, where x represents the value of Xij. 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 Fi, which represents the movement direction and step size of the lizard. The movement direction Dij of attribute Xij for lizard i can be determined using fuzzy logic rules. For example, we can define the fuzzy rule $Rijk$ as follows:

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

Where A_k and B_k are linguistic variables associated with the fuzzy sets of Xij 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:

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

The movement direction and step size for all attributes can be combined to obtain the fuzzy output Fi 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 μK(K) and μM(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:

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

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

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.

Algorithm 1: Lizard Search Algorithm (LSA)

Data: Problem-specific objective function f (x)
Result: Optimal solution x∗
Initialization: Generate an initial population of lizard agents;
While Stopping criteria not met **do**
  for Each lizard agent **do**
    Explore: Use fuzzy logic to determine the exploration direction;
    Update lizard agent's position based on exploration;
    Evaluate the fitness of the new position using f (x);
    Exploit: Use fuzzy logic to determine the exploitation direction;
    Update lizard agent's position based on exploitation;
    Evaluate the fitness of the new position using f (x);
    Select the lizard agents with the best fitness values for the next generation;
return The best solution found, x∗;

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
- Si: Solution i
- f (Si) : Fitness function for solution i
- Lbest: Best solution
- fbest: Best fitness value
- rnd: Random number
- FLin: Fuzzy logic input variables
- FLout: Fuzzy logic output variable.

9.2. Initialization

- Initialize the population of solutions randomly
- Initialize Lbest as the current best solution
- Initialize fbest as a high value (for minimization problems) or a low value (for maxi-mization problems).
- Define fuzzy logic membership functions and fuzzy rules for parameter adjustment.

9.3. Main Loop

Each solution *Si* in the population Evaluate the fitness *f (Si)* of the solution Generate a random number rnd between 0 and 1 *rnd* is less than the exploration threshold Apply fuzzy logic rules for parameter exploration to determine the new solution Apply fuzzy logic rules for parameter exploitation to determine the new solution Evaluate the fitness *f (Si)* of the new solution the new solution is better than Lbest Update Lbest with the new solution Update *fbest* with the fitness of the new solution 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 termination condition is met.

9.4. Output

• Return *Lbest* and *fbest* as the final optimized parameters.

10. 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.

11. EXPERIMENTAL RESULTS

According to the findings, 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.

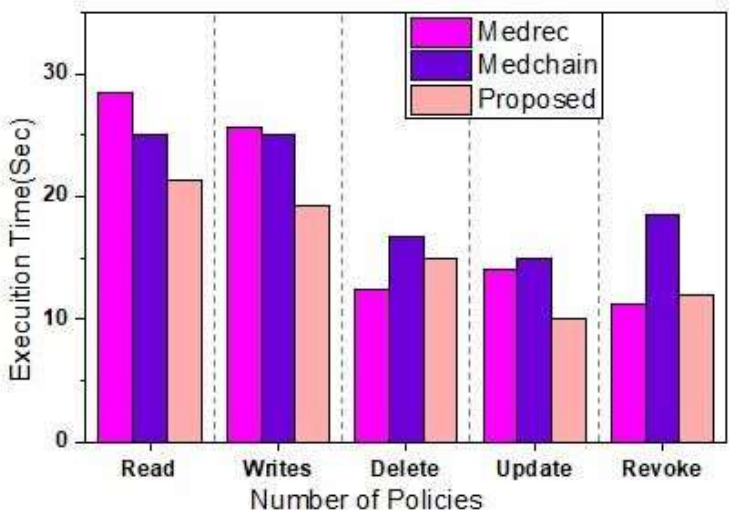

Figure 3. Simulation Results Based On Number Of Access Control Policies Versus Execution Time.

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

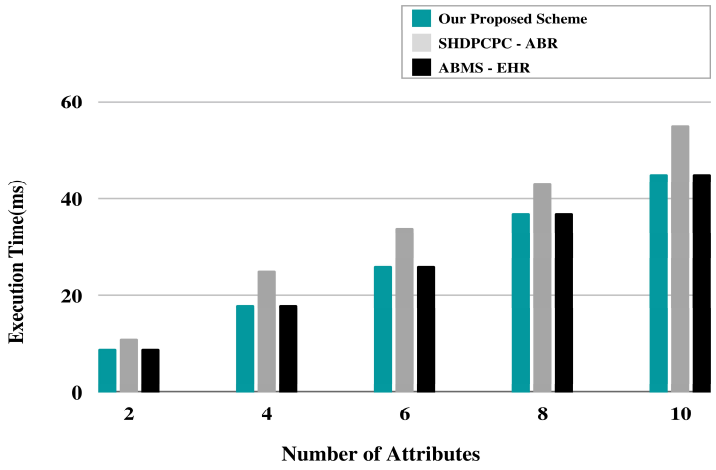

Figure 4. Simulation Results Based On Number Of Attributes And Execution Time.

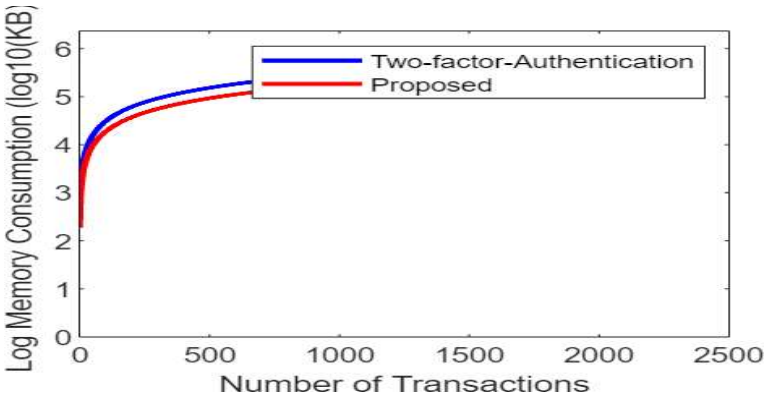

Figure 5. Simulation Results Based On Number Of Attributes And Memory Consumption.

Figure. 6 The comparative analysis between the proposed approach and the benchmark model, focusing on the number of transactions and execution time, is crucial in assessing the effectiveness and efficiency of the new approach. This discussion delves into the key aspects of this comparison and the insights it offers. The number of transactions processed per unit of time, also known as transaction throughput, is a fundamental performance metric in any blockchain system. In the comparative analysis, the proposed approach should be evaluated against the benchmark model in terms of how many transactions it can handle concurrently or within a specified time frame.It's essential to quantify the transaction throughput achieved by the proposed approach. Higher transaction throughput often indicates improved scalability, which can be a significant advantage, especially in applications requiring a high volume of transactions, such as financial systems or supply chain tracking. Compare the transaction throughput of the benchmark model under similar conditions. This provides a baseline for evaluating the proposed approach's performance. Execution time refers to the time taken to complete a specific task or operation. In blockchain systems, it's vital to measure how quickly transactions are processed, validated, and added to the blockchain. The comparative analysis should consider execution time as a critical factor affecting overall system efficiency. Assess how the proposed approach affects transaction execution time. A faster execution time may indicate improved processing efficiency and reduced confirmation delays for users. Measure the execution time of the benchmark model for the same set of transactions and conditions. This allows for a direct comparison with the proposed approach. Comparing scalability is essential, especially in scenarios where blockchain networks need to accommodate an increasing number of users and transactions. Assess how well

the proposed approach scales with growing demands and how efficiently it utilizes network resources. Evaluate the scalability of the proposed approach by analyzing its performance as transaction loads increase. Consider aspects such as network bandwidth, computing power, and memory utilization. Assess the scalability of the benchmark model under similar conditions. Look for signs of resource saturation or bottlenecks that may limit its ability to handle increased transaction volumes. In addition to raw performance metrics, consider the robustness and reliability of both the proposed approach and the benchmark model as shown through Figure.6. Robustness refers to the system's ability to handle unexpected scenarios and adversarial conditions, while reliability assesses the system's consistency in processing transactions correctly. Evaluate how well the proposed approach handles unexpected events, such as network disruptions or malicious attacks. Robustness and reliability are essential for ensuring the security and integrity of transactions. Assess the robustness and reliability of the benchmark model. Any vulnerabilities or limitations should be identified and compared to those of the proposed approach. In conclusion, a comprehensive comparative analysis between the proposed approach and the benchmark model based on the number of transactions and execution time provides valuable insights into the potential advantages and trade-offs of adopting the new approach. This analysis helps stakeholders make informed decisions about the suitability and feasibility of implementing the proposed solution in various blockchain applications.

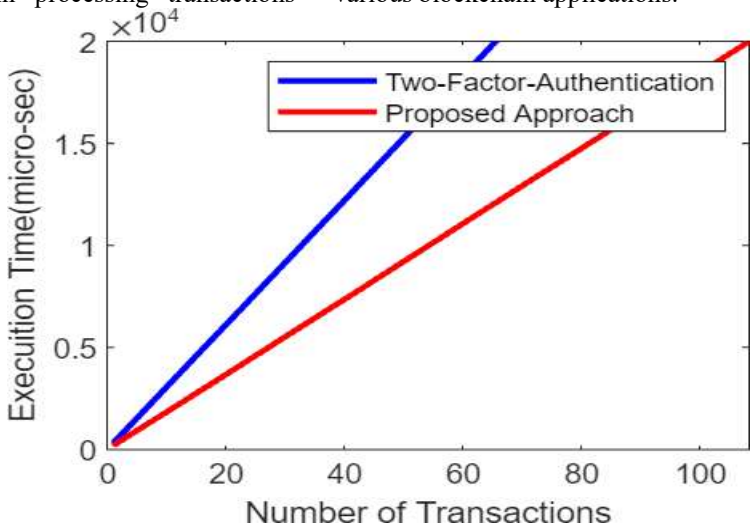

Figure 6. Comparative Analysis Of The Proposed Approach Versus The Benchmark Model Based On Number Of Transaction And Execution Time.

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 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.

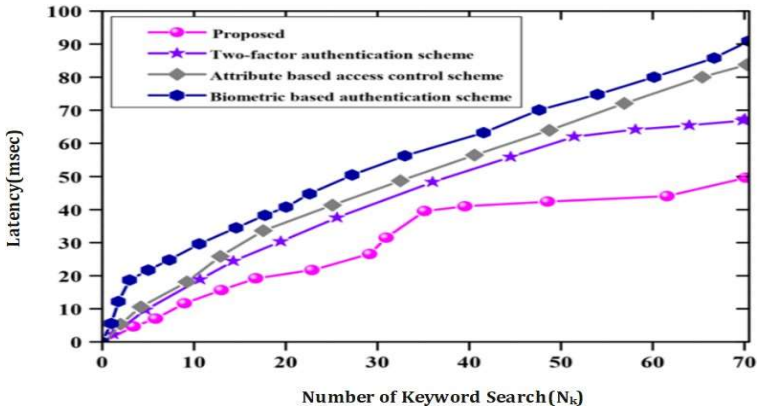

Figure 7. Simulation Results Based On Number Of Keyword Search And The Latency In Microsecond In Comparison With The Proposed Approach And Benchmark Model.

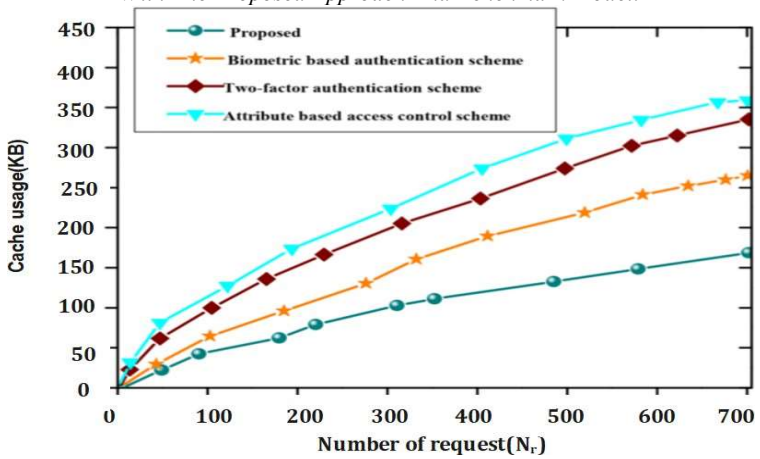

Figure 8. Simulation Results Based On Test Run And Communication Overhead.

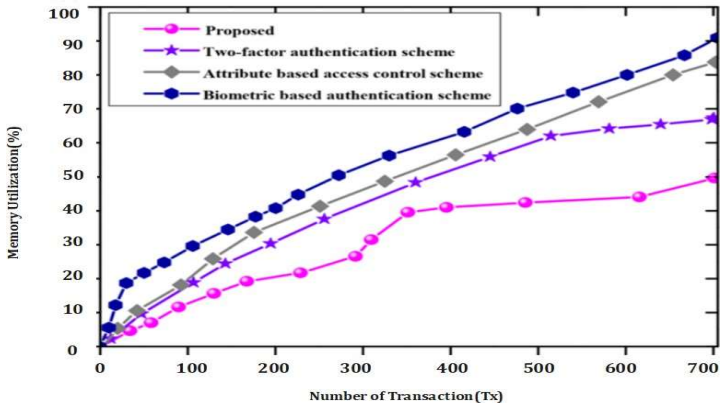

Figure 9. Simulation Results Based On Test Run And Resource Utilization.

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.
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.

Simulation results in Figure 10 based on types of attack versus successful attacks provide insights into the effectiveness of the proposed approach in mitigating various security threats.

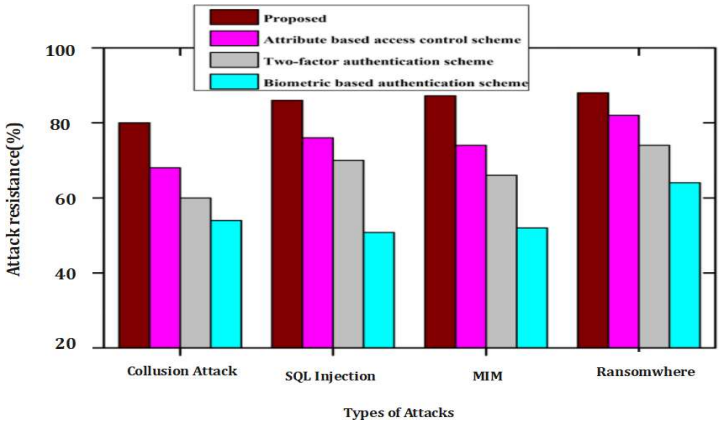

Figure 10. Simulation Results Based On Types Of Attack Versus Success Attack.

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 it's 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.

ACKNOWLEDGMENT

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia (Project No. Grant No. 5919).

RFERENCES

[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]. Surono, S., Goh, K. W., Onn, C. W., Nurraihan, A., Siregar, N. S., Saeid, A. B., & Wijaya, T. T. (2022). Optimization of Markov weighted fuzzy time series forecasting using genetic algorithm (GA) and particle swarm optimization (PSO). Emerging Science Journal, 6(6), 1375-1393. http://dx.doi.org/10.28991/ESJ-2022-06-06-010