cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

# IoT-Enabled Secure and Scalable Cloud Architecture for Multi-User Systems: A Hybrid Post-Quantum Cryptographic and Block Chain-Based Approach towards a Trustworthy Cloud Computing

**Seun Adeoye**
Masters in Information Technology, University of the People, Colorado, USA
Email: adeoyelambert@gmail.com

**Russel Adams**
Masters in Health Information Management, Kenyatta University, Nairobi, Kenya
Email: russeladams8@gmail.com

**DOI: 10.47760/cognizance.2024.v04i10.013**

**Abstract:**
Cloud computing remains one of the most significant advancements in resource provision to organizations in the latest decades since they initiate conveniences on demand access. The adoption of the IoT has brought about a new era of collaborative computing by employing a pool of linked smart sensors and devices that will produce and analyze great amounts of data, thus creating new related problems in terms of size and security, hence increasing even more the importance of traditional security measures. Therefore, in this paper, we synthesize a new SSCA that combines IoT and cryptographic mechanisms, to build highly available and secure cloud systems, which makes these systems multi-users and fully usable by many users at the same time. The design resolves to a distributed structure where sever al cloud nodes will address user s requests proficiently and it uses Multicast and Broadcast Rekeying Algorithm (MBRA) to maintain the privacy and the confidentiality of the users' detail, employing a cryptosystem that integrates MBRA, Post Quantum Cryptography (PQC) and block chain. The architecture using IoT devices collects data from the distributed sensing resources through the data storage layer; it enforces the security integrity of the information collected by employing the MBRA-PQC encryption algorithms; the blockchain provides the security for the confidential data by storing it in unalterable and dispersed registers. The proposed approach is then demonstrated with different data sets and its performance is measured based on the response time, the throughput and scalability, security and reliability. The outcome of the expressions reveals the efficiency of the proposed SSCA compared to MHE-IS-CPMT as it reduced by 1. 67 seconds and 0. 97 seconds at 250 and 1000 devices respectively. Similarly, the result as AUC value for SSCA showed a better improvement than the MHE-IS-CPMT, EAM, SCSS, and SHCEF models with improvements in percent at 25-user level: 6. 30%, 6. 90%, 7. 60%, and 7. 30%, respectively as well as; at 50-user level: 5. 20%, 9. 30%, 11. 50%,

**Keywords**: Advanced cloud-based models, Internet of Things (IoT), Next-Generation Cryptography, Big Data & Analytics or AI, Distributed systems, Modular systems

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

## Introduction

The implementation of cloud computing has continuously improved the control of information, processing, and data storage by leaving out the traditional capital intensiveness in equipment and network hardware [1]. It provides a means by which a firm and even an individual can harness computing resources located on the internet and distance themselves from the limitations of centralized computing [2]. The metamorph nature of the expanding data is a fundamental element that is well met by cloud computing where there is the flexibility of offering the necessary expansion to meeting demands [3]. The existing conventional infrastructures within organizations exhibit a weakness in coping up with the amount of information that is continuously growing. It makes it easy for organizations to deal with these challenges since cloud computing provides a pliant infrastructure that organizations can use to augment or lessen as per the requirement [4]. In the diagram shown in figure 1_CRYPTO, it can be clearly seen that cloud computing plays an important role in addressing new and emergent forms of information. It can be performed by the networked computers as shown in figure 1 through cloud technology as shown below [5]. Therefore, there is no necessity of having or operating any physical hard ware or structure; this also favors the managing of voluminous data more easily and at a lower cost. In addition, cloud service is typically a package that providers may supply in form of computing, analytics or storage thus creating options to fit the needs of the organizations. The subsequent subsections introduce on some of the imperative characteristics of the cloud, and emphasize on the necessity of cloud security, which is the driving force behind this work [6].

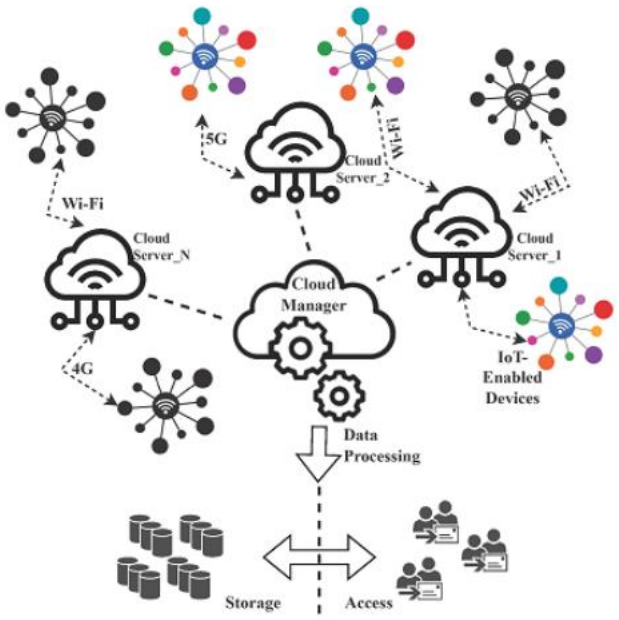


**Figure 1. An illustration of the significance of cloud computing in managing the diverse IoT information**

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

### 1.1. COMPONENTS OF CLOUD INFRA

There are various types of cloud computing models and services, out of which the most commonly used models are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) [7]. Selecting the right cloud solution that suits the organization's specific needs is central as organizations deal with dynamic and ever evolving needs for data. The different services present can also be helpful if one is knowledgeable about them. In the clouds deployment there is categorization of clouds as; public/open cloud, private/personal cloud, hybrid/converged cloud and multiple cloud. It is important to make this distinction in order to determine which of the approaches to deployment is applicable for a particular enterprise [8]. It is worth mentioning that there are a number of possibilities provided by the concept of cloud computing when it comes to data management in terms of storage and data processing possibilities as well as data scalability. In summary, organisations requite robust knowledge of these options and how they can be utilised to govern and retain records within the cloud environment. Services to organizations enable access of data with little cost and flexibility offered by cloud-based storage [9]. However, it also calls for new issues on how one can ensure that data is preserved and who is in charge of supervising it. Employers should therefore endeavour to ensure that they have appropriate policies and mechanisms through which they can collect, manage, protect and retain organisational data and in this process meet the relevant legal regulations [10]. Information governance is very relevant in scenarios where an organization hosts its data and applications in the cloud because it helps the organization manage its data through its data lifecycle. This includes the creation of guidelines as to how long data will be kept, who will have access to it, and how it will be deleted A [11]). Today, data is moving online in great part to be stored and analyzed in cloud systems, which is why security should be put in the foreground and compliance with the standards and norms established by law should be maintained. Literature suggests that security in the virtual world depends on the extent that providers' compliance and security options are known to the user and the extent to which the user engages in correct action[12]. Cloud service solutions providers today have a number of measures for compliance and security to provide to customers, which may range from encryption and access solutions to data backup and recovery. These are the basic frameworks, and it is important for an organization to understand these options and to select the ones, which would be most suitable for the organization [13]. Also, regulations governing the protection of data, including the GDPR or HIPAA, must be considered for data storage and processing in the cloud, especially in situations when it affects the personal data of specific individuals. Legal and compliance guidelines state that all organizations have to have policies and measures in place to meet these rules and any other rules that apply to the specific industry the organization belongs to [14]. In conclusion, cloud has to be protected by implementing adequate security measures and promoting user consciousness. It means that organisations have to align security and compliance guidelines with cloud providers where necessary. Furthermore, in order to

 

ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

avoid security breaches, it is important to train workers about properly using cloud-based platforms and recognising laws and regulations that should be followed [15].

That is why the main strategy for the effective work in the field of cloud services should include strict control of expenses and optimization not to waste resources in this sphere, while cloud services may become a cost-efficient solution as far as the growing volumes of huge data are concerned. Based on this understanding, the cost structure can be identified and optimization strategies need to be put in place in order to reach cost optimums and, on the other hand, to achieve organizational targets concerning required capacity expansions [16]. Unfortunately, cloud service providers if they charge their customers, do so in a way that enables customers to have some level of flexibility in terms of the price that they are to be charged. There are different charges that exist, which include pricing models like pay-as-you go and reserved instances among others and its implications. Likewise, such abilities as the automated allocation of resources and their direct usage in optimized processes can contribute to the minimization of costs and improvement of the general performance. Other advantages of cloud service providers also include the possibility to use tools for tracking the demand for resources and finding ways for their effective utilization [17].

**NECESSITY OF CLOUD SECURITY**

Risks involved with hacking, cyber-attacks and other type of threats have further increased the need for implementing high end security for cloud computing [18]. Therefore, contributing to the design, implementation and advancement of advanced, secure frameworks, architectures and general mechanisms that would help in early identification and prevention of instances of cyber-crimes being executed within versatile cloud computing technology is an important topic of discussion in current prominent research. This makes it important to have security systems that are capable of elastic and automatic growth or shrinkage depending on currents workload to ensure that business can maintain secure state without relaxing or tightening security measures to match the current throughput. More research is also done in order to provide data storage that is secure and also efficient for cloud computing. The incorporation of sound structures in the storage of data reduces on safety concerns for example; hacking of data, access of data by unauthorized persons and, respectively handling of records [19]. From the current studies, there is a growing focus on integration and deployment of encryption solutions for data security during transit and storage in cloud technologies. This calls for the concept of new sorts of encryption methods that are capable of processing big data and at the same time mitigate against the dangers of compromise of privacy [20].

## 1.2. MOTIVATION AND SCOPE OF THE WORK

IoT in conjunction with cloud technology has facilitated development of multiuser platforms with necessary computing power enabling near-real time data and efficient and easy access to services [21].

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

The integration of cloud computing capacities into IoT has provided an opportunity to construct collective platforms through sharing capabilities with multiple users having resourceful and feasible access to their data at any given place. Some of the new challenges that arise when extending the IoT to the multiuser systems include security concerns when embedding a security infrastructure for the architecture of the system. This is especially key in the current context where users are multiple and use similar information and capabilities [22].

It is therefore vital that IoT is well aligned in a secure cloud based platform for multitudes of users. It is thus important to design a secure cloud architecture that will be suitable for hosting and managing the IoT devices and the IoT data involved. From this point of architecture, different methods in security, for instance, authority, identity confirmation, access regulation, and risk identification of data security and data privacy, among others, are implemented to manage possible threats [23]. Ensuring that the system which is being developed has several participants demands that the secure cloud architecture developed includes understanding that different users will have different abilities and permissions. Therefore, appropriate and global security for access control necessity must be developed to control user authorities and restrict access to the necessary data [24]. For managing such a big number of devices and types of data, it is necessary to have a safe cloud for storing the data received from IoT customers. One of the most significant aspects is to use robust storage facilities where there could be extensive data storage and the data needs to be protected and easily retrievable [25].

As the research subject, the general goal of creating a secure cloud architecture based on the IoT for a multi-user system may include a large number of directions for investigation related to various study fields [26]. The research objectives of this study are to design a security mechanism that would allow the embracing of multi-user cloud and data handling capability in a large number of users without compromising the network performance. The objective of this first phase of the specific research is therefore to come up with a suitable cloud architecture that could handle many users and data from the IoT devices. Some of the challenges include scalability, high performance with several petabytes of data, reliability, and maintenance. Moreover, as proposed the architecture should be dynamic in order to accommodate IoT devices that collect information from multiple sensing domains [27]. The information gathered has to be safe and be highly protected during the whole integration course. It also integrates privacy and security to safeguard user details through a use of cryptographic technology which utilizes PQC and block chain technology [28][29]. For data protection from secure challenges, the Hybrid PQC-Block chain system incorporates the PQC encryption [30]. As mentioned above, this method of data encryption reduces the vulnerability of sensitive information to contamination. since adopting the block chain part of the system, a means of storing sensitive information such as records into distributed and unalterable blocks is developed. The adopted PQCBlockchain is a hybrid where data submitted goes through a secure and reliable process of examination through consensus and mining before integration into the block chain. The use of IoT and the PQC-block chain hybrid system in the creation of this secure

 

ISSN: 0976-7797
Impact Factor: 4.843
Index Copernicus Value (ICV) = 77.57

cloud environment allows for the effective handling of numerous users while offering them very strict network privileges. Furthermore, by supporting the effective approach of access control method, the system can effectively limit the users' access and privilege only to the authorized ones in order to avoid various security risks [32]. Using PQC-Block chain hybrid system, distributed systems can afford protection against threats that range from simple hacker attacks to more complex and dangerous threats, besides which, users will be able to gain direct access to data and services immediately. This makes a society and a world more connected and effective since more people are using IoT devices in infrastructure [33].

### 1.3. MAIN CONTRIBUTION

In this research our principal aim can be singled out in three clear points that can reflect on the relations and issues which are described in the Introduction.

Therefore, based on the findings, we have proposed an IoT and Cryptography enabled novel cloud architecture – Scalable and Secure Cloud Architecture (SSCA), which encompasses IoT and cryptographic techniques to counter the issues involved in integrating IoT and cryptographic techniques to design and establish efficient, safe, effective, and scalable cloud systems in the long run. To add, by using cryptographic techniques in the design, the architecture has secured the privacy and integrity of the data as well as features measures to address possible threats that might pose a threat to the informations privacy. At the same time, the architecture implemented directs special attention to the scalability and views for accommodation of multiple IoT devices as well as catering for increased cloud demand, which ensures efficient handling of greater data from each device.

To scale the cloud computing services to the multi-user support and allow many users to access cloud resources at the same time, the proposed architecture would come in handy. It follows a distributed model, with a number of clouds in order to serve user's requests satisfactorily and to protect the user information, the control algorithms uses cryptographic method which includes a combination of MBRA, PQC and block chain. In addition, we also provide a detailed description to the MBRA, PQC and Block chain hybridization and carry out a detailed analysis on how these components can be hybridized. In these steps, it is possible to achieve the rational use of the available resources, thus increasing the effectiveness of the system as a whole.

## RELATED WORK

To this end, the present section of the study will provide an extensive literature review regarding the state of the art in designing secure cloud architectures for IoT platforms, significant consideration of the issue of scalability for these architectures. Sharma et al. [34] used a similar methodology of assessing the roles played by technologies at the macro-level, with their study focusing on IoT as a revolutionary means by which interactions between two physically undeveloped objects can be created. The study

 

also looked at the significance of achieving IoT integration with cloud services as a way of ensuring that data from different devices are buffered and analyzed to create the impact that could be from home automation, automated farming, and smart medical care among others. But the use of these technologies has various issues especially in the area of security of the common technology platform. In light of these challenges, the researchers used a Secure, hybridized, Cloud-Enabled Framework (SHCEF) protocol for IoT that supports both private and public clouds for handling privacy, scalability, and connectivity issues. The study also point to some academic challenges that still require to be cleared before full implementation of the hybrid cloud architecture. In general, the study provides a nice summary and apposites the method and ideas for possibility of synergies and issues of IoT with cloud processing cooperation

Wu et al. , in their study [35], have investigated the weaknesses of the authentication method presented by Zhou et al. [36] Here, the authors claimed that the mutual verification process and anonymity were not adequately managed. In order to solve these problems and improve the capability of detecting in accurate input at the early stage, the authors saw a new certification system with an extra detection parameter. They also proposed an enhanced IoT based verification method for cloud computing where they compared the desired metrics like computational efficiency with the IoT based verification and it depicted the thought security performance of the said field. This advancement can be seen as setting the basis for a new form of lightweight authentication IoTA that is capable of withstanding multiple attacks while efficiently handling key security roles including user auditing, a collaborative authentication function as well as session encryption. The authors confidently investigate the applicability of such verification mechanism for open IoT devices. Security is considered by Sarkar et al. [37] as the important factor to be taken into consideration and so they suggest a new machine-learning technique known as IntruDTRee. The resulting model is tailored for use in building up a tree-based architecture for security breaches identification. The authors amplify this notion indicating that IntruDTRee substantially minimizes the computational complexity while maintaining improved accuracy when estimating unknown test instances. The model emerges as efficient when tested on cybersecurity datasets, and it has been compared with several standard machine learning methods. In their paper on SCSS, Unal et al. [38]', the SCSS combines IBC and decentralized key administration and encryption technique. This architecture mitigates the drawbacks associated with the PKI solutions of the large scale and longer time required in the protection and retrieval of the data in cloud. Adding to it, stringent security is provided and ensured by the use of multiple Public Key Generators (PKGs) as well as through decentralized key governance. Furthermore, there is elongation of scalability in the decryption process, which has made forensic examination easier in cases with encrypted cloud data. Altogether, this study provides a beneficial way of executing cryptographic algorithms to control cloud storage that can be used by many individuals at the same time; In IoT mechanism that is hosted by cloud, the concern of authentication is discussed by Irshad et al. [39] They proposed a new ElGamal of Authentication Method

 

**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

(EAM) method, which is known as SAS-Cloud. The method encompasses the use of passcodes and the unique physiological aspects of the user as security features to ensure that the identity of the user is authenticated. The authors of the paper describe how SAS-Cloud operates and establish its security alongside with the augment of demonstrating its efficiency from potential security threats and show that SAS-Cloud is more effective than other existing solutions. Thus, the proposed communication system for authentication has both complexity by implementing a passcode and biometric traits to make the system more secure. The paper discusses an important issue of security in the context of cloud based IoT applications and presents a proposed method by name SAS-Cloud which seeks to fill this gap. Recently, Ahmad et al. , for instance, have put forward the new two-tiered cryptographic model [40] to improve the Key Administration System (KAS) function in cloud computing. It utilizes both authenticated digital encryption by using ECC together with AES; both are shorten as Elliptic Curve Cryptography and Advanced Encryption Standard respectively. It uses the attributes of both ECC and AES in proliferation for information security and decryption. Data encryption employs a key derived from a random large prime number, an authoritative master key, and an associated value. It does, however, have a slight advantage over traditional methods in the best case scenario using time complexity analysis and the tests done in the encryption and decryption time. The method provides much more improvements in these areas; hence, it is more rigorous and ideal for cloud computing environments. According to the research there are several benefits possible in its adoption that can ensure reliable encryption mechanisms for the secure management of medical data in the cloud. Uppuluri et al. [41] proposed a new approach known as Modified Honey Encryption which incorporates Inverse Sampling Conditional Probability Model Transform (MHE-IS-CPMT) integrated with ECC for identification and secret key interchange within a home environment. It has four folds, which are initialization, enrollment, login, and credential renewal that would make an effective and secure linkage between the uses and their operands. The MHE-IS-CPMT with ECC is used to encode user and device data, which serve as a strong start to the security arrangement for communication and access control. It is with the proposed system determines reliable properties, providing safe communication and protection against unauthorized access. Another significant factor revolves around demand by authorized users to change their keys as appropriate. In this regard, Bomu et al. [42] have presented a conceptual example on how an IoT system for smart cities can be developed using an IaaS grade cloud computing platform. Specifically, the IaaS level design realistically implements the enhanced smart city topology to provide the desired performance. The envisioned smart city IoT system may capture metrics like transport, water quality, solar intensity, noise level, air quality, and CCTV record with thermal camera to identify people sick with Covid19. To deal with the routing and QoS, a network topology analysis is performed at the simulative level. The selected decentralized concept of block chain technology is aimed at increasing the safety performance of IoT systems.

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

MULTI-USER SYSTEMS The proposed SSCA architecture Currently, multi-user systems are in wide sighted use all over the world being an inevitable part of the development of new farming techniques and improvement on the old techniques of farming.

IoT and cloud computing have interacted to facilitate the development of a great many reliable multi-user communication systems suitable for many uses. However, this integration also brings up new issues of security concern that require efficient methods of identification and prevention [46, 47]. Thus, in reducing the security risks of these systems, we introduce a combined model of AI on PQC and a Block chain-based security model. Intrusion detection mechanisms on the other hand, are always running in the background, constantly scanning for any violations that may compromise security and will alert the system administrators for necessary actions. That is why, the second method: Multicast Broadcast Rekeying Algorithm (MBRA) as a kind of threat detection in the Cloud-IoT model is proposed. Moreover, this hybrid approach entails a comprehensive safety paradigm that includes texting, authentication, explanation, access regulation, and detection of intrusions. With the help of improved PQC introduced through the MBRA-based optimal selection of keys, the system is protected from quantum computer attacks, which are a threat to classical cryptography [49]. The Block chain component is an ideal platform because it is distributed and the original information cannot be altered which guarantees the credibility of the information. In addition, the hybrid system enables the secure user authentication to the IoT devices and cloud services to minimize risks of unauthorized access through valid hash validation and block Identification No (ID) of each block [50]. Security measures protect the security of the transfer of privacy sensitive information within the system. . This arrangement enables efficient regulation of users and their features such as permissions, and authorities. These approaches have been integrated into the framework of smart IoT and cloud settings, and by doing so, help to strengthen the security of the MBRA hybrid in response to its unique difficulties in addressing the intricacies of these complex structures [51].

## 1.4. THE ARCHITECTURE OF THE PROPOSED SSCA WITH THREAD DETECTION MECAHANISM

To understand how the architecture of the proposed SSCA works and how the thread detection mechanism has been designed, a detailed discussion is presented in the following sub-sections The architecture and the thread detection mechanism of the SSCA has been illustrated in the figure below as shown in figure 2:. The figure shows that SSCA model which has been proposed is aimed to provide support and control over the IoT devices which basically include detectors, actuators, regulators, and sensors among others. The cloud servers receive all data that these devices generate at their own convenience. The system consists of several imperative parts that interoperate to create a stable infrastructure for a significant number of individuals. The functional behavior of the various components within the threat model (Figure 2) is described as follows: The functional behavior of the various components within the threat model (Figure 2) is described as follows:

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

1) Virtual servers: These are the fundamental virtualized resources that can be implemented as the basis for hosting and ensuring the management of IoT devices and the data they generate. They offer the required computational resource and the hard disk space.

2) Server farms: The server farms include several physical hosting servers to provide linking solutions for processing and storing frameworks of the IoT connected instruments. These help to guarantee high availability and configurability of the cloud platform.

3) Block chain nodes: These nodes are involved in the block chain network, in order to keeping and managing the distributed ledger, where IoT device data are stored and controlled [52]. Block chain data has accuracy and immutability as aspects of its security since it is transparent in its operations.

4) PQC encryption: In multi-user communication, PQC encryption techniques are used to ensure the content of the communication before it is delivered to the intended target cloud servers. PQC algorithms have better PXP security against attacks from quantum computers and therefore provide confidentiality and data integrity of the data being transmitted [53].

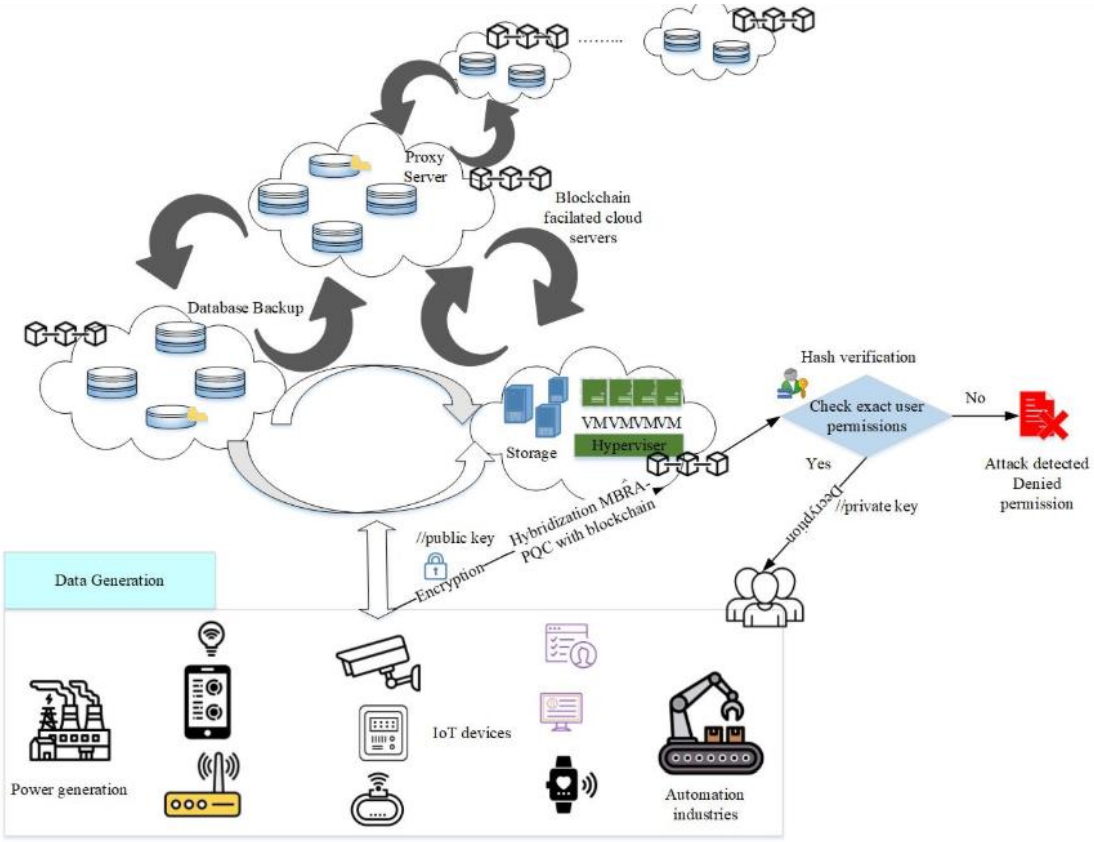


**Figure 2. A Visual representation illustrating the Proposed Scalable and Secure Architecture for Multi-User Systems, outlining the attacks and the corresponding preventive mechanisms of the proposed SSCA**

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

## 1.5. THE MECHANISM OF MULTICAST AND BROADCAST REKEYING ALGORITHM FOR THREAD DETECTION

The strategy recommended in this context draws inspiration from the battle royal algorithm (BRA) video game subgenre. The core idea of BRA is to select a sample of citizens that are random and broadly dispersed throughout the issue areas. In this scenario whereas a soldier/player studies the neighborly soldier/player as the target, the process resembles that of aiming a gun. Command-position soldiers thus influence their immediate neighbors, and as a result, outcomes are swiftly shifted round their network of affiliation. During every turn, a soldier suffers damage levels which are acquired each time the soldier engages in an attack. Furthermore, the wounded ones do not want to stay in their positions and try to quickly move to different directions, trying to attack from another position. The movement trace of the wounded soldier is constructed being directed to the area with coordinates situated in the middle between the current position of the soldier and the optimal one, which is the position of the elite player, which highlights the strategic aspect. From the above-discussed function, it is applicable within PQCrypto for attack detection and prevention. The mathematical representation of this interaction can be represented with the accuracy of the following equation. (1).

$$x_{s.i} = x_{s.i} + rand(x_{best.i} - x_{s.i})$$

Where cand represents a random value drawn fromthe unit interval independently, and, xs. i is defined as the least favorable position of the ath dimension. If relative to the parameters of its adversary the parameter with the poorest location can affect the subsequent iteration, then xi. s will be set to zero as well. Here, xi. s defines the lowest level of the ith parameter and its interaction is represented by xi. s + 1. If a given parameter has a leveraged level of damage above a fixed condition limit which is defined as 3, then the parameter is taken to be in a critical status. At this point, the parameter in question is randomly redefined in the potential problem space, and its harm level is set at xi. s=0 at this point. This mechanism provides the same message as the previous one: Explore more, you have been here only for 5 minutes. After being gruesomely killed, a soldier gets redeployed into the problematic area as affirmed by Eq. (2).

$$x_{s.i} = rand(Ub_i - Lb_i) + Lb_i \qquad (2)$$

For convenience the constraints for the ith dimension of the problem space is restricted within the lower limit L bi and upper limit U bi . Also, with each iteration Δ, the domain of the problem reduces within the feasible solutions, which are ideally optimal. First, an initial calculation assigns Δ equal to Δ = log10( Hk), then revises the value of Δ as Δ = Δ + round( Δ 2 ). Here, Hk stands for the largest number of iterations allowed. Exploration is achieved by expanding the set of opportunities that are investigated for offering or purchasing, while exploitation is attained by moving through this set as efficiently as possible.

Hence, based on the above derivative analysis, changing the lower bound and the upper bound follows the above equation. (3)

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

$$Ub_i = x_{best.i} + \sigma(\bar{x}_i) \quad (3)$$

$$Lb_i = x_{best.i} - \sigma(\bar{x}_i) \quad (4)$$

**Algorithm 1** MBRA-PQC based Encryption Algorithm

1: **Input:** IoT devices, Cloud servers, datasets
2: **Output:** Encrypted data
3: **for all** IoT device $D_n$ **do**
4: Generate $\kappa_{OPQC_i}, \kappa_{OPQC_i^{-1}}$ ▷ *by MBRA method*
5: $x_i \leftarrow \Upsilon_E(\kappa_i, \kappa_{OPQC_i})$ ▷ *Encryption*
6: Send $(x_i, \zeta_i) \rightarrow C$
7: **end for**

In the pseudocode, κi indicates the symmetric key, κOP QCi stands for the optimal PQC public derived using MBRA as well as κOP QC−1 i is the corresponding optimal PQC private key; xi indicates the cipher text, while ζi refers to additional data transmitted by the IoT device from cloud server.

**RESULT DISCUSSION**

In this section, an elaborate comparison analysis of the proposed SSCA is explained as follows. Originally, this approach intends to combine MBRA with PQC and block chain in an integrated manner to enhance data communication in cloud-IOT networks. To support the comparative analysis, the subsequent sections provide an overview of the experimental setup of the environment, the specification of data received and analysis of the features used. Therefore, we provide the following comparative analysis comprising both qualitative and quantitative assessment comparing the proposed SSCA with other existing state-of-the-art methodologies for security. Within this integrated presentation, it is of prime importance to offer, firstly, a general evaluation of the novel SSCA in comparison with existing models

**EXPERIMENTAL SETUP**

Table 1 lists the details of the testbed elements that were used in the experimental setup as part of the experiment and are critical in enabling the development of a realistic emulation of the proposed system. Available on Amazon Web Services as the Cloud Platform, the solution comes with highly flexible storage, networking, and computing abilities. Edge Devices serve as middlemen, receiving and analyzing data collected by IoT Devices and relaying messages from the Cloud to these devices. Smart Sensors, RFID readers, cameras, and actuators are used for data acquisition and the ability to command devices remotely through the Internet. Quantum cryptography is used in the safe and sure transmission of data since it provides key distribution and encryption. Similarly, through decentralised and public record-

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

keeping models such as Ethereum, the Block chain System is capable of recording and authenticating transactions. A typical Network Traffic Generator application generates traffic that is similar to that of real users in a given network. Last, an Attack Simulator examines security against an emulatory assault with the use of Metasploit, Nmap and Wireshark. As such, they collectively form a realistic and comprehensive testbed in evaluating the prowess and efficacy of the proposed system in a real-world setup.

## DATASETS DESCRIPTION

As illustrated in table 2 in [67] and table 3, the experimental setup involves the use of a variety of datasets that include Numenta Anomaly Benchmark (NAB) [68] datasets used for use cases in cloud computing, cloud security, industrial control systems, and healthcare. The NAB dataset is very useful for the SCA as it allows testing the properties of the multi-user system in regards to scalability and security. It allows for realistic evaluation of system performance and can be used to compare different classifiers' efficiency in processing immense data variations, recognizing anomalies, or maintaining users' privacy. Table 2 gives the Essential Attributes of NAB Datasets for Cryptosystem Assessment that include providing viable qualitative measures to evaluate the efficiency of a cryptosystem. Specifically, the real-world NAB [68] dataset is used to assess the performance efficacy of the proposed security system with multiple important threat criteria in the context of Cloud with IoT platforms. The NAB dataset is otherwise called the real-world datasets that are used to assess and test numerous streaming works especially for anomaly detection using the NAB as

**Algorithm 2** Determination of the Hashing Values

**Require:** Private key $SK$ and public key $PK$
**Ensure:** Hashing value $H$

**Initialization:**
Generate a random number $R$ as a nonce
Compute $\mathcal{H}(\beta_{i-1}) \leftarrow \beta_{i-1}$ ▷ *Hash value of* $\beta_{i-1}$
Compute $\mathcal{H}[\Upsilon_E(_i, \kappa_{OPQC_i})] \leftarrow x_i(\beta_i)$ ▷ *Hash of* $\beta_i$
Choose randomized $\eta_i$
Estimate $\mathcal{H}[\eta_i||(\mathcal{H}(\beta_{i-1})||\mathcal{H}(_{OPQC_i}, P_i))] \leftarrow S_c(\beta_i)$
**SHA Hashing:**
Calculate the hash of the private key
$H_{SK} \leftarrow \text{Hash}(SK)$ ▷ *Compute the hash value of the private key*
Calculate the hash of the public key
$H_{PK} \leftarrow \text{Hash}(PK)$ ▷ *Compute the hash value of the public key*
Concatenate $H_{SK}$, $H_{PK}$, and $R$
$H \leftarrow \text{Hash}(H_{SK}||H_{PK}||R)$ ▷ *Concatenate the hash values and the nonce*
Apply additional cryptographic operations (e.g., encryption, signing)
Perform any required additional cryptographic operations on $H$ ▷ *Perform additional cryptographic operations for enhanced security*
Store the hashing value $H$ securely
Store the resulting hashing value $H$ in a secure location
Verify the integrity of $H$ during retrieval
When retrieving $H$, verify its integrity using error-checking techniques
Handle collisions, if any
If a collision occurs, employ collision resolution techniques
Monitor and update cryptographic standards
Regularly monitor and update cryptographic standards for improved security
**Output:** Hashed verification is done $H$

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

**Algorithm 3** MBRA-PQC based Decryption

**Input:** Encrypted IoT data, Hashed verification value, private key
**Output:** Decrypted data
**for all** Cloud server $C$ **do**
    Obtain $\kappa_{OPQC_i^{-1}} \rightarrow \zeta_i$
**end for**
$\kappa_i \leftarrow d(x_i, \kappa_{OPQC_i^{-1}})$ ▷ *Decryption*

Benchmarking cryptosystems. Consequently, the NAB dataset can be cited as an indispensable performance benchmark in designing anomaly detection algorithms that operate in multi-user environments involving multiple IoT devices. This in turn gives us the ability to coach the algorithm under varying conditions and therefore be able to validate the effectiveness of the developed algorithm in different real world scenarios. The other dataset includes specifications of the cloud, computing, security, industrial control system, and healthcare consist of certain attributes as shown in Table 3 such as; no. of users, platform/environment, data type, threat type and compliance standards. These datasets enable the consideration of various contexts and enable the measure the effectiveness of solutions of the proposed solutions through application of real-life use cases.

## PERFORMANCE EVALUATION CRITERIA

Accessibility analysis is an important part of performance analysis since the goal of the given research is to define the efficiency and productivity of each strategy utilized. That is why pursuing outcomes contributes to the research and development of more possibilities that help people with mental disorders. To evaluate the efficacy of the proposed SSCA model, a comparative study is performed in this paper in terms of the following contributions: MHE-ISCPMT [41], EAM [39], SCSS [38], SHCEF [34]. Furthermore, the effectiveness of the suggested architecture is also assessed in terms of response time, capability for scaling, throughput, security and dependability (reliability). These are 6 of the indicators which can be used to evaluate the level of success in implementing the architecture and the appropriateness of the proposed architecture in achieving the outlined goals and objectives. According to the above criterions the proposed architecture shall be validated in the following.

### Response time and Scalability

To compare the scalability of the architecture one has to determine the number of users; as for the performance aspect, one has to look at the response time. By measuring the response time over the users counts, it possible to determine the ability of the system to performance well when faced with higher loads and with a rapid response time will. This is important to guarantee the application and efficiency of the software that is going to be developed.

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

In the above-said equation, the term 'α' is the processing time which denotes a time taken for computational arithmetic and cryptographic operations involved in completing transaction or any request such as purchase order. The transmission time (β) therefore includes all the time which may be lost as a result of some of the aspects of the network including: Latency, availability of resources, congestion, etc. The queuing time (q) refers to the amount of time a customer spends waiting within a queue before carrying out a particular transaction or making a certain request. Additionally, the arrival rate (λ) represents the rate of incoming requests the system can handle within a given amount of time, while the waiting time (γ) is the time taken by the system to respond or acknowledge a request. Altogether, these elements help at influencing the total response time of the system. As it shows in the Figure 3(a), the performance of the proposed MHE-IS-CPMT model is compared with other related models such as EAM, SCSS, SHCEF, and SSCA with regards to the numbers of users and their average response time. Therefore, the number of users constitutes a part of the architecture's capacity, which defines the flexibility of the architecture's ability to expand by adding more users without compromising the architectural performance standards significantly. On the other side, the response time determines the time required by the system to undertake activities requested by the user.

| Platform/Devices | Platform/Devices | Description |
|---|---|---|
| Cloud Platform | AWS | Expandable and flexible storage, networking, and processing power; physical/virtual computable resources |
| Edge Device | Raspberry Pi | Network-edge tools that interact with IoT devices collect data, do analytics, and exchange messages with the support of the cloud |
| IoT Devices | Values of Smart sensors, RFID readers, cameras, actuators | Sensors integrated with actuators in a network acquire data concerning their surroundings and can be controlled remotely. |
| Multi-objective Royal Battle algorithm | Attack detection, optimal key generation | Provide excellent outcomes for real-world applications. |
| Quantum Cryptography | Quantum Key Generators | Technologies based on quantum encryption and the distribution of quantum keys enables safe data transfer among cloud and IoT nodes |
| Blockchain System | Ethereum | Transactions between the cloud and IoT nodes are tracked and verified using a distributed, trustworthy, and tamper-proof ledger system. |
| Network Traffic Generator | Tcpreplay / iPerf | Provides a means of simulating network applications and usage behavior via generating realistic traffic |
| Attack Simulator | Metasploit, Nmap, Wireshark | The capabilities associated with the cloud, cutting-edge gadget defence, and responsiveness is tested through attacks generated in a simulated environment |

**TABLE 1. The components of the testbed and descriptions**

Moving directly to the interface and impacting the system's possibilities in working conditions. These observations concluded from the evaluation of the models depict a correlation in all the models whereby the AAR increases as the number of users increases. This infers that augmenting the load of the users lowers the capability of all models to respond optimally thus degrading the response time.

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

However, one must observe that the degree of this impact varies from the analyzed models, which in turn suggests that they possess different levels of tolerance to increased user load and efficiency with handling of such conditions. However, it is possible to note certain disparities and identify that further analysis needs to be conducted in terms of the scalability and response time of each of the models that was presented above. As shown in the evaluation and analysis of the results, SSCA has the lowest average of response time as compared with the other models. Based on this observation, SSCA has less reaction to the growing number of users with fast response time than LSA. Therefore, SSCA is viewed to possess superior scalability and efficiency to the other models. This only proves that in terms of response time, SSCA outperforms the other methods, which is a testament to its efficiency in handling user requests and returning quick responses, making it a candidate for use in large-scale systems that can accommodate an enormous number of users. Alternatively, from the results presented in Figure 3(b), it can be noticed that also the response time of each model escalates as the number of devices grows. However, the behavior of the different models is not uniform, especially when more devices from the current model are connected. For example, for the MHEIS-CPMT model it is possible to obtain such parameters as response time of 7,69 sec.

| Attribute | Required value/range | Description |
|---|---|---|
| Dataset | 'realAWSCloudwatch' or 'realKnownCause' | Multiple datasets are included in the NAB dataset, but the realAWSCloudwatch or realKnownCause dataset is the most appropriate for assessing a cryptosystem. For example, host parameters from Amazon Web Services (AWS) are included in the realAWSCloudwatch dataset. In contrast, synthesized and actual data sets with confirmed causes of abnormalities are included in the realKnownCause dataset. |
| Time resolution | 5 minuntes or 1 hour | The precision of anomaly detection depends on the temporal resolution of the data. The temporal resolution of the realAWSCloudwatch dataset is 5 minutes, whereas that of the realKnownCause dataset is 1 hour. |
| Assault type | Varies depending on the dataset | The NAB dataset incorporates several datasets, including singular, contextual, and group abnormalities. In addition, the properties of the data being analyzed and the intended application inform the decision as to which kind of anomaly to utilize. |
| Evaluation metric | ROC AUC or precision@k | ROC-AUC, or precision at k (precision@k), is often used as an assessment statistic for anomaly detection systems. Selecting an appropriate metric for evaluation requires considering the scenario at the moment and the limitations between inaccurate and incorrect results (false positives and false negatives). |
| Training data | First 80% of the data | Around 80% of the dataset is employed to train the cryptosystem, while the remaining 20% is used to examine and assess the cryptosystem's efficacy. |
| Test data | Last 20% of the data | The remaining 20% of the data is utilized to assess the efficiency of the cryptosystem. |

**TABLE 2. Essential Attributes of Numenta Anomaly Benchmark (NAB) [68] Datasets for Cryptosystem Assessment**

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

To clarify, the response time typically takes 4. 39 seconds when dealing with 250 devices, which subsequently rises to 9. 19 when dealing with 1000 devices. Further, the proposed SSCA model also deploys a response time of 6. 02 seconds for 250 devices and reaches up to the maximum of 8. 22 seconds for 1000 devices. With regards to the depth dimension, it can therefore be stated that the number of devices provides valuable information with respect to the scalability of the architecture part while response time and scalability factors point towards actual performance characteristics of an architecture part. In general, sCCA performs well high cognitive performance regarding response time compared with other models at any number of devices. The trend of lower average response time all point out that the SSCA model is scalable and is performing better than the MACA model under high load devices. These two time series raise great implication about the capability of the SSCA model to handle more loads of device and still respond faster in terms of time These results place the SSCA model as a highly scalable and performant solution.

The tendencies displayed in Figure 3(c) include the efficiency of different models including MHE-IS-CPMT, EAM, SCSS, SHCEF, and SSCA considering the number of transactions and the response times of the transactions. The transactions are used to measure the amount of work, or in the case of online systems, the number of transactions per day/ hour/minute that the system has to handle; the response time reflects the time that a system takes to respond to each of the above transactions. As expected given the specific architecture of each model, the results corroborate that with higher volumes of transactions, the corresponding response time increases as well, signaling the effects of workload. Just as was noted earlier, response time is another area where the SSCA model outperforms the other models, recording lower response times even with increasing transaction values. This prove the fact that the SSCA model is more adaptable for handling the increase in workload when compared to the response time of the other model. These findings have clearly shown that, the SSCA model outperforms its competitor in its ability to execute increased number of, transactions at an increased efficiency.

**2) Security**

To conduct a system security evaluation, it is necessary to analyze the inherent threats in a system and find out whether the applied security articulations are competent and efficient in preventing possible threats. Cryptography's important components including the handling of a cryptographic key; the incorporation of cryptographic methods; and the adoption of secure communication protocols are significantly important is maintaining the security of the system. Therefore, equation (10) offers a computational formula to quantify the extent of protection afforded by each model against possibly vulnerable areas. By invoking this equation, one can make a quantitative identification of the effectiveness of a given model and compare it with other models.

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

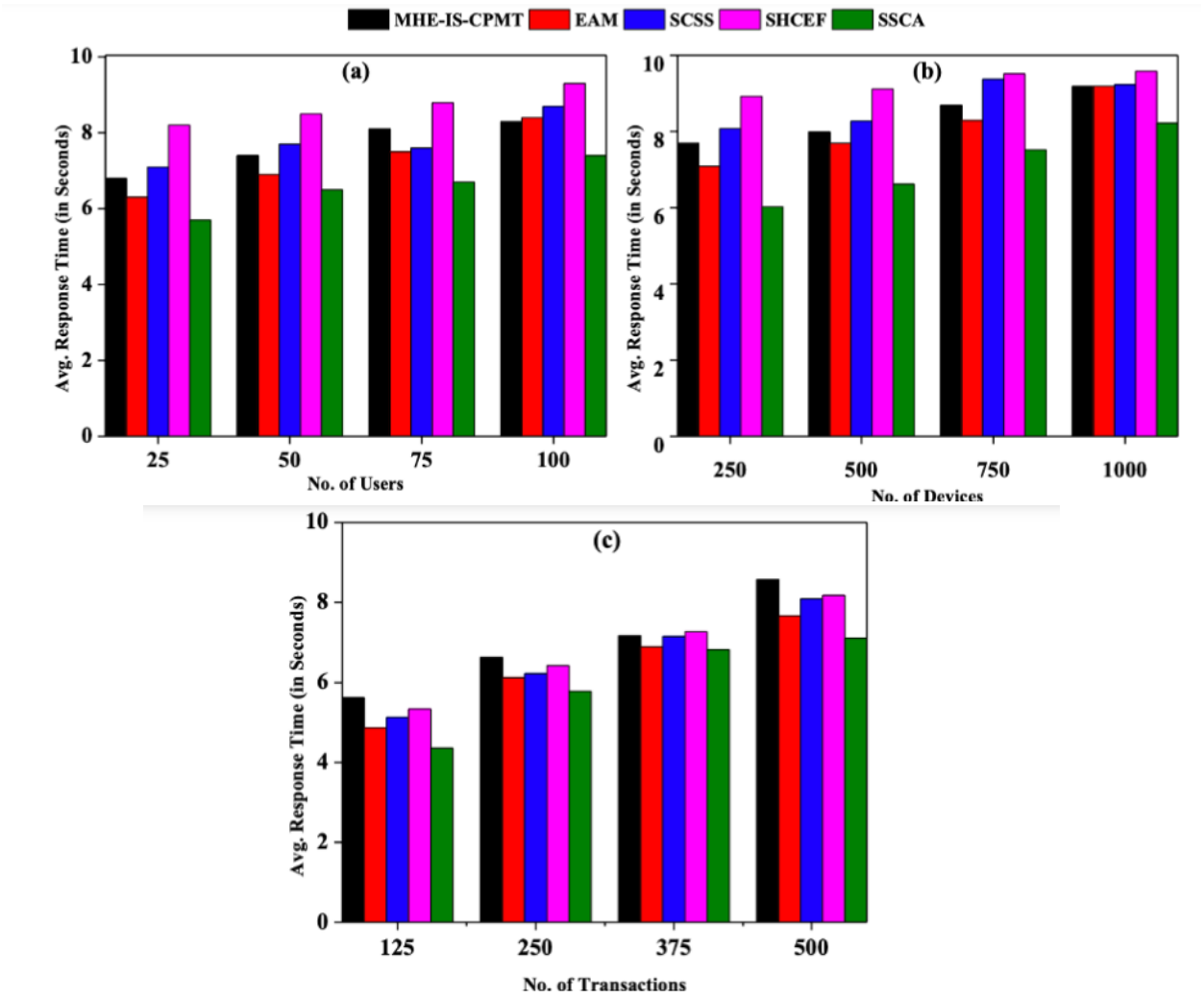


**FIGURE 3. Fig shows the result of simulation runs of average value of (τ) with the number of users, devices, and number of transactions as follows:**

The various parameters that can be used are the Rt which represents reliability at the time t whereas F represents the failure rate and finally the U represents uptime duration of the system. The failure rate is a statistical value calculated by taking the average number of system breakdowns to occur within a certain period of time – usually expressed as failures per unit of time such as failures per hour. Due to attack, frequencies of failure can be estimated by the total number of failure scored the overall system operation time by using the formula, Total number of system failure ÷ Total operational time of the system

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

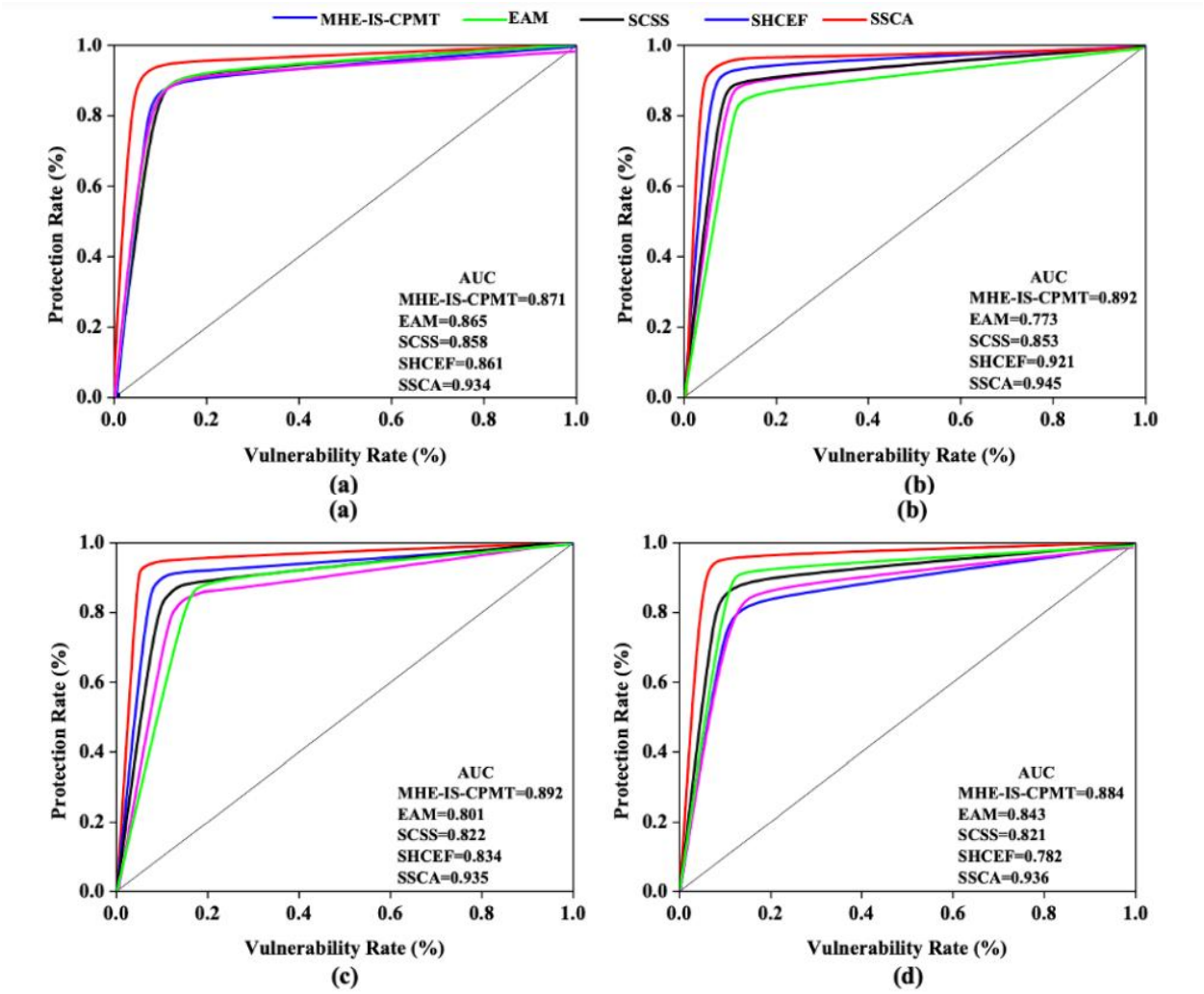


**FIGURE 4. A comparison of the security utilizing the Area under the curve(AUC). (a) AUC at 25 User Level, (b) AUC at 50 User Level, (c) AUC at 75 User Level, and (d) AUC at 100 User Level**

 

cognizancejournal.com
Seun Adeoye *et al*, Cognizance Journal of Multidisciplinary Studies, Vol.4, Issue.10, October 2024, pg. 183-209
**(An Open Accessible, Multidisciplinary, Fully Refereed and Peer Reviewed Journal)**
**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

| References | methodology | Reliability | Response time (s) | Prediction rate (%) | Overall execution time | Complexity |
|---|---|---|---|---|---|---|
| Sharma et al. [34] | SHCEF | moderate | 7.9 | 0.86 | 90 | High |
| Wu et al. [35] | certification system | Low | 10.5 | 0.782 | 65 | High |
| Sarker et al. [37] | IntruDTRee | Moderate | 8.05 | 0.812 | 82 | Low |
| Unal et al. [38] | SCSS | High | 7.8 | 0.821 | 75 | Moderate |
| Irshad et al. [39] | EAM | Low | 7.65 | 0.785 | 82 | Moderate |
| Ahmad et al. [40] | KAS-ECC | High | 8.2 | 0.86 | 76 | High |
| Uppuluri et al. [41] | MHE-IS-CPMT | Low | 7.5 | 0.75 | 72 | High |
| Bommu et al [42] | IaaS | Very low | 7.4 | 0.84 | 86 | Moderate |
| Sharma et al [43] | PA | low | 9.5 | 0.79 | 89 | High |
| Selvarajan et al [44] | COSNN-AILBSM | High | 8.94 | 0.895 | 91 | Moderate |
| Jalasri et al [45] | Clustering-noise protocol framework | Low | 7.91 | 0.75 | 85 | High |
| Proposed | SSCA | Very low | 3.85 | 0.975 | 94.5 | Very low |

**TABLE 3. A comparative study of the proposed SSCA with the cutting-edge security approaches**

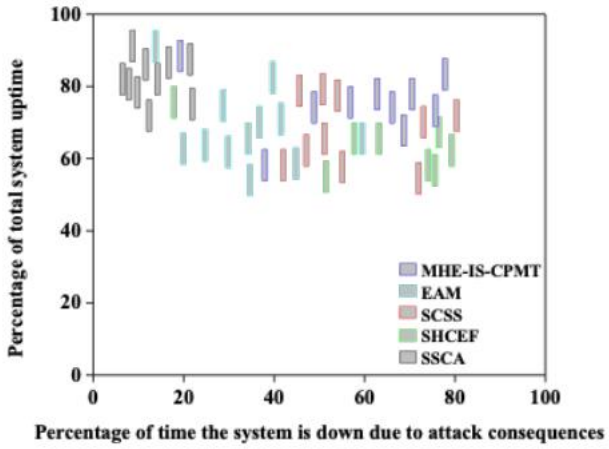


**FIGURE 5. A comparison of the reliability of the proposed SSCA against the MHE-IS-CPMT, EAM, and SCSS, approaches**

And optimal security functions. The developed model utilized the best keys obtained from MBRA for PQC encryption and decryption function and the hash function based on the block chain is implemented in this function. , so the authorized person can only receive and decode the data to utilize it further voluntarily. This does not necessarily mean that this method is not valid, it is just as valid as using other real-world data that are usually incorporated into various projects. But still, more elaborate study is required to reveal the application of the proposed approach in various situations.

 

**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

## CONCLUSION AND FUTURE DIRECTION

In this paper, we presented the use of a newer model of cloud architecture called the Scalable and Secure Cloud Architecture, which is Internet of Things-based and successfully met the complex issues of scalability and security integrated within cloud computing domain. Decentralized Cloud Nodes: Due to the decentralized nature of cloud nodes, the multiple layers of the proposed architecture filter all the user requests and provide an efficient path to the desired information to be provided to the user. It was noted that the architecture of the engine used for the model was tailored for this purpose and was thoroughly tested on big troves of data and placed under undue stress. The outcome revealed that the proposed SSCA was generally accurate and significantly better than the prior methodologies such as MHE-IS-CPMT, EAM, SCSS, and SHCEF in terms of response time, scalability and security aspects. It was found that when using the MHEIS-CPMT model, the actual response time for 250 and 1000 devices was 7. 69 and 9. 79 seconds, respectively, whereas, following the implementation of the proposed SSCA model, optimum response times of 6. 02 and 8. 22 seconds were noted, respectively. Expressed in numbers this results in an improved response time by a factor of 1. 67 and 0. 97 seconds in favor of the SSCA against MHE-IS-CPMT. In addition, at 25-users scale of the experiments, normalized AUC value for SSCA was 0. 934, but MHE-IS-CPMT, EAM , SCSS and SHCEF achieved 0. 871, 0. 865, 0. 858 and 0. 861 respectively. Similarly at the 50-users level, SSCA reach normalized AUC value of . 936 followed by the MHE-IS-CPMT with the normalized AUC value of . 884 with other algorithms EAM, SCSS, SHCEF were recorded to possess normalized AUC value of 0. 843, 0. 821 and 0. 782 respectively. These outcomes validate the proposition that among all the models, SSCA holds a superior predictive proficiency and has achieved significant increases of AUC values, which is at 6. 30% and 5. 20% for the 25- user level and 50-user level respectively against MHE-IS-CPMT and EAM, SCSS, whereas, SHCEF has been improved for the 25- user level at 7. 60% and

However, as a reminder it can be pointed that though the proposed SSCA has been assessed using a sufficient number of datasets further assess VOLUME 4, 2016 17 However, as a reminder it is important to note that although the proposed SSCA has been characterized on the basis of the datasets presented above the further assessments over a larger datasets and introduction of auto scaling features would aid in ascertaining the scalability of the entire architecture. This future direction needs to be as follows: This future direction intends to offer additional insights as to how SSCA can handle more enormous datasets and back even more complex programs in the future. Therefore, future improvements of SSCA will employ incorporation of auto-scaling features and security features concurrently Collectively, future improvements of SSCA will involve testing the architecture with varied datasets and users to make sure that it offers suitable, protected, and scalable cloud gains.

**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

# REFERENCES

1. Anabel Gutierrez, Elias Boukrami, and Ranald Lumsden. Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the uk. Journal of enterprise information management, 2015.
2. Alexander Benlian, William J Kettinger, Ali Sunyaev, Till J Winkler, and Guest Editors. The transformative value of cloud computing: a decoupling, platformization, and recombination theoretical framework. Journal of management information systems, 35(3):719–739, 2018.
3. Xiaochuan Luo, Song Zhang, and Eugene Litvinov. Practical design and implementation of cloud computing for power system planning studies. IEEE Transactions on Smart Grid, 10(2):2301–2311, 2018.
4. Samir A El-Seoud, Hosam F El-Sofany, Mohamed Abdelfattah, and Reham Mohamed. Big data and cloud computing: Trends and challenges. International Journal of Interactive Mobile Technologies, 11(2), 2017.
5. Keyur K Patel, Sunil M Patel, and P Scholar. Internet of things-iot: definition, characteristics, architecture, enabling technologies, application & future challenges. International journal of engineering science and computing, 6(5), 2016.
6. Syed Noorulhassan Shirazi, Antonios Gouglidis, Arsham Farshad, and David Hutchison. The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective. IEEE Journal on Selected Areas in Communications, 35(11):2586–2595, 2017.
7. B Hari Krishna, S Kiran, G Murali, and R Pradeep Kumar Reddy. Security issues in service model of cloud computing environment. Procedia Computer Science, 87:246–251, 2016
8. Dimitris Zeginis, Francesco D'andria, Stefano Bocconi, Jesus Gorronogoitia Cruz, Oriol Collell Martin, Panagiotis Gouvas, Giannis Ledakis, and Konstantinos A Tarabanis. A user-centric multi-paas application management solution for hybrid multi-cloud scenarios. Scalable Computing: Practice and Experience, 14(1):17–32, 2013
9. Rabi Prasad Padhy, Manas Ranjan Patra, and Suresh Chandra Satapathy. Cloud computing: security issues and research challenges. International Journal of Computer Science and Information Technology & Security (IJCSITS), 1(2):136–146, 2011.
10. Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, pages 523–548, 2010
11. Robert F Smallwood. Information governance: Concepts, strategies and best practices. John Wiley & Sons, 2019.
12. Shahla Asadi, Mehrbakhsh Nilashi, Abd Razak Che Husin, and Elaheh Yadegaridehkordi. Customers perspectives on adoption of cloud computing in banking sector. Information Technology and Management, 18:305–330, 2017.

 

13. Sandesh Achar. Cloud computing security for multicloud service providers: Controls and techniques in our modern threat landscape. International Journal of Computer and Systems Engineering, 16(9):379–384, 2022.
14. Shahid Munir Shah and Rizwan Ahmed Khan. Secondary use of electronic health record: Opportunities and challenges. IEEE access, 8:136947–136965, 2020.
15. Jonathan JM Seddon and Wendy L Currie. Cloud computing and trans-border health data: Unpacking us and eu healthcare regulation and compliance. Health policy and technology, 2(4):229–241, 2013
16. Yali Zhao, Rodrigo N Calheiros, Athanasios V Vasilakos, James Bailey, and Richard O Sinnott. Profit maximization and time minimization admission control and resource scheduling for cloud-based big data analytics-as-a-service platforms. In Web Services– ICWS 2019: 26th International Conference, Held as Part of the Services Conference Federation, SCF 2019, San Diego, CA, USA, June 25–30, 2019, Proceedings 26, pages 26–47. Springer, 2019
17. Feng-Kwei Wang and Wu He. Service strategies of small cloud service providers: A case study of a small cloud service provider and its clients in taiwan. International Journal of Information Management, 34(3):406– 415, 2014.
18. K. M. K. Raghunath and N. Rengarajan. Response time optimization with enhanced fault-tolerant wireless sensor network design for on-board rapid transit applications. Cluster Computing, 22(S4):9737–9753, 2017.
19. AKM Bahalul Haque, Bharat Bhushan, and Gaurav Dhiman. Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. Expert Systems, 39(5):e12753, 2022.
20. Benjamin Fabian, Tatiana Ermakova, and Philipp Junghanns. Collaborative and secure sharing of healthcare data in multi-clouds. Information Systems, 48:132–150, 2015.
21. Iftak Hussain Sarker, Yassir Bin Abushark, Fahd Alsolami, and Atta ul Khan. Intrudtree: A machine learning based cyber security intrusion detection model. Symmetry, 12(5):754, 2020.
22. Omerah Yousuf and Roohie Naaz Mir. A survey on the internet of things security: State-of-art, architecture, issues and countermeasures. Information & Computer Security, 2019.
23. Ashish K. Pandey, Asif Iqbal Khan, Yasser Basem Abushark, Md. Mahmudul Alam, Akshat Agrawal, Rakesh Kumar, and Rizwan Ahmad Khan. Key issues in healthcare data integrity: Analysis and recommendations. IEEE Access, 8:40612–40628, 2020
24. Sergio Gusmeroli, Salvatore Piccione, and Domenico Rotondi. A capability-based security approach to manage access control in the internet of things. Mathematical and Computer Modelling, 58(5-6):1189–1205, 2013.
25. Kyle Chard, Steven Tuecke, and Ian Foster. Efficient and secure transfer, synchronization, and sharing of big data. IEEE Cloud Computing, 1(3):46–55, 2014.

 

26. A.Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari. Towards a blockchain-sdnbased secure architecture for cloud computing in smart industrial IoT. Digital Communications and Networks, 2022.
27. G. Kuldeep and Q. Zhang. Multi-class privacypreserving cloud computing based on compressive sensing for IoT. Journal of Information Security and Applications, 66:103139, 2022.
28. L. Malina, L. Popelova, P. Dzurenda, J. Hajny, and Z. Martinasek. On feasibility of post-quantum cryptography on small devices. IFAC-PapersOnLine, 51(6):462–467, 2018
29. F. Zhang, H. Wang, L. Zhou, D. Xu, and L. Liu. A blockchain-based security and trust mechanism for aienabled IIoT systems. Future Generation Computer Systems, 146:78–85, 2023.
30. T. Nouioua and A. H. Belbachir. The quantum computer for accelerating image processing and strengthening the security of information systems. Chinese Journal of Physics, 81:104–124, 2023.
31. A.EL Azzaoui, P. K. Sharma, and J. H. Park. Blockchain-based delegated quantum cloud architecture for medical big data security. Journal of Network and Computer Applications, 198:103304, 2022
32. Sabah Suhail, Rasheed Hussain, Abid Khan, and Choong Seon Hong. On the role of hash-based signatures in quantum-safe internet of things: Current solutions and future directions. IEEE Internet of Things Journal, 8(1):1–17, 2020.
33. Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, and Marimuthu Palaniswami. Internet of things (iot): A vision, architectural elements, and future directions. Future generation computer systems, 29(7):1645–1660, 2013.
34. Anupam Sharma, Tarun Goyal, Emmanuel S Pilli, Anirban Pal Mazumdar, Mayank C Govil, and Ramesh C Joshi. A secure hybrid cloud enabled architecture for internet of things. In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pages 357–362. IEEE, December 2015.
35. Hsin-Liang Wu, Chih-Chin Chang, Yu-Zhen Zheng, LiSong Chen, and Chao-Chin Chen. A secure iot-based authentication system in cloud computing environment. Sensors, 20(19):5604, 2020
36. Li Zhou, Xiaolong Li, Kuo-Hui Yeh, Chunhua Su, and Wei Chiu. Lightweight iot-based authentication scheme in cloud computing circumstance. Future Generation Computer Systems, 91:244–251, 2019.
37. Imtiaz Hossain Sarker, Yaser B Abushark, Fahad Alsolami, and A. I. Khan. Intrudtree: A machine learning based cyber security intrusion detection model. Symmetry, 12(5):754, 2020.
38. Derya Unal, Abdullah Al-Ali, Fatih Orhan Catak, and Mohammad Hammoudeh. A secure and efficient internet of things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption. Future Generation Computer Systems, 125:433–445, 2021.
39. Adnan Irshad and Shahzad A. Chaudhry. Comment on "elgamal cryptosystem-based secure authentication system for cloud-based iot applications". IET Networks, 2021.
40. Shafay Ahmad, Shadab Mehfuz, and Jamshed Beg. Hybrid cryptographic approach to enhance the mode of key management system in cloud environment. The Journal of Supercomputing, 2022.

 

41. Satya Uppuluri and G. Lakshmeeswari. Secure user authentication and key agreement scheme for iot device access control based smart home communications. Wireless Networks, 2022.
42. Babburu K. N S. Thalluri L.N. Gopalan A. Mallapati P.K. Guha K. Bommu, S. and H.R Mohammad. Smart city IoT system network level routing analysis and blockchain security based implementation. Journal of Electrical Engineering Technology, 18(2):1351–1368, 2023.
43. Namasudra S. Crespo R.G. Parra-Fuente J. Sharma, P. and M.C Trivedi. Ehdhe: Enhancing security of healthcare documents in iot-enabled digital healthcare ecosystems using blockchain. Information Sciences, 629:703–718, 2023
44. Srivastava G. Khadidos A.O. Khadidos-A.O. Baza M. Alshehri A. Selvarajan, S. and J.C.W Lin. An artificial intelligence lightweight blockchain security model for security and privacy in iiot systems. Journal of Cloud Computing, 12(1):38, 2023.
45. M. Jalasri and L. Lakshmanan. Managing data security in fog computing in iot devices using noise framework encryption with power probabilistic clustering algorithm. Cluster Computing, 26(1):823–836, 2023
46. Khizar Abbas, Lo'Ai A Tawalbeh, Ahsan Rafiq, Ammar Muthanna, Ibrahim A Elgendy, and Ahmed A Abd El-Latif. Convergence of blockchain and iot for secure transportation systems in smart cities. Security and Communication Networks, 2021:1–13, 2021.
47. Reyazur Rashid Irshad, Shahid Hussain, Shahab Saquib Sohail, Abu Sarwar Zamani, Dag Øivind Madsen, Ahmed Abdu Alattab, Abdallah Ahmed Alzupair Ahmed, Khalid Ahmed Abdallah Norain, and Omar Ali Saleh Alsaiari. A novel iot-enabled healthcare monitoring framework and improved grey wolf optimization algorithm-based deep convolution neural network model for early diagnosis of lung cancer. Sensors, 23(6):2932, 2023.
48. Reyazur Rashid Irshad, Shahid Hussain, Ihtisham Hussain, Ibrar Ahmad, Adil Yousif, Ibrahim M Alwayle, Ahmed Abdu Alattab, Khaled M Alalayah, John G Breslin, Mohammed Mehdi Badr, et al. An intelligent buffalo-based secure edge-enabled computing platform for heterogeneous iot network in smart cities. IEEE Access, 2023.
49. David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. Transitioning organizations to postquantum cryptography. Nature, 605(7909):237–243, 2022
50. Osama Alkadi, Nour Moustafa, Benjamin Turnbull, and Kim-Kwang Raymond Choo. A deep blockchain framework-enabled collaborative intrusion detection for protecting iot and cloud networks. IEEE Internet of Things Journal, 8(12):9463–9472, 2020.
51. Aitizaz Ali, Muhammad Fermi Pasha, Jehad Ali, Ong Huey Fang, Mehedi Masud, Anca Delia Jurcut, and Mohammed A Alzain. Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: a novel approach to cryptography. Sensors, 22(2):528, 2022.

 

52. Ibrar Yaqoob, Khaled Salah, Raja Jayaraman, and Yousof Al-Hammadi. Blockchain for healthcare data management: opportunities, challenges, and future recommendations. Neural Computing and Applications, pages 1–16, 2021.
53. Swati Kumari, Maninder Singh, Raman Singh, and Hitesh Tewari. Post-quantum cryptography techniques for secure communication in resource-constrained internet of things devices: A comprehensive survey. Software: Practice and Experience, 52(10):2047–2076, 2022.
54. Usman Khalil, Owais Ahmed Malik, Saddam Hussain, et al. A blockchain footprint for authentication of iot-enabled smart devices in smart cities: State-of-theart advancements, challenges and future research directions. IEEE Access, 10:76805–76823, 2022.
55. Carlos Andres Lara-Nino, Miguel Morales-Sandoval, and Arturo Diaz-Perez. Post-quantum cryptography on wireless sensor networks: Challenges and opportunities. Integration of WSNs into Internet of Things, pages 81–99, 2021.
56. Imran Memon, Mohammed Ramadan Mohammed, Rizwan Akhtar, Hina Memon, Muhammad Hammad Memon, and Riaz Ahmed Shaikh. Design and implementation to authentication over a gsm system using certificate-less public key cryptography (cl-pkc). Wireless personal communications, 79:661–686, 2014
57. Tiziano Bianchi, Alessandro Piva, and Mauro Barni. On the implementation of the discrete fourier transform in the encrypted domain. IEEE Transactions on Information Forensics and Security, 4(1):86–97, 2009.
58. Reyazur Rashid Irshad, Shahab Saquib Sohail, Shahid Hussain, Dag Øivind Madsen, Mohammed Altaf Ahmed, Ahmed Abdu Alattab, Omar Ali Saleh Alsaiari, Khalid Ahmed Abdallah Norain, and Abdallah Ahmed Alzupair Ahmed. A multi-objective bee foraging learning-based particle swarm optimization algorithm for enhancing the security of healthcare data in cloud system. IEEE Access, 2023.
59. Linghe Kong, Liang He, Xiao-Yang Liu, Yu Gu, MinYou Wu, and Xue Liu. Privacy-preserving compressive sensing for crowdsensing based trajectory recovery. In 2015 IEEE 35th International Conference on Distributed Computing Systems, pages 31–40. IEEE, 2015.
60. Marwa E Saleh, Abdelmgeid A Aly, and Fatma A Omara. Data security using cryptography and steganography techniques. International Journal of Advanced Computer Science and Applications, 7(6), 2016
61. Guard Kanda and Kwangki Ryoo. Vedic multiplierbased international data encryption algorithm cryptocore for efficient hardware multiphase encryption design. Webology, 19(1), 2022
62. Bela Gipp, Norman Meuschke, and André Gernandt. Decentralized trusted timestamping using the crypto currency bitcoin. arXiv preprint arXiv:1502.04015, 2015
63. Hyungmin Cho. Asic-resistance of multi-hash proof-ofwork mechanisms for blockchain consensus protocols. IEEE Access, 6:66210–66222, 2018.

 

**ISSN: 0976-7797**
**Impact Factor: 4.843**
**Index Copernicus Value (ICV) = 77.57**

64. Claudia Pop, Tudor Cioara, Marcel Antal, Ionut Anghel, Ioan Salomie, and Massimo Bertoncini. Blockchain based decentralized management of demand response programs in smart energy grids. Sensors, 18(1):162, 2018.
65. P Geetha, VS Jayanthi, and AN Jayanthi. Optimal visual cryptographic scheme with multiple share creation for multimedia applications. computers & security, 78:301–320, 2018.
66. Reyazur Rashid Irshad, Shahid Hussain, Ihtisham Hussain, Ahmed Abdu Alattab, Adil Yousif, Omar Ali Saleh Alsaiari, and Elshareef Ibrahim Idrees Ibrahim. A novel artificial spider monkey based random forest hybrid framework for monitoring and predictive diagnoses of patients healthcare. IEEE Access, 2023.
67. Nader Albishry, Rayed AlGhamdi, Ahmed Almalawi, Azeem Iqbal Khan, Pramod R. Kshirsagar, and Udai BaruDebtera. An attribute extraction for automated malware attack classification and detection using soft computing techniques. Computational Intelligence and Neuroscience, 2022:e5061059, 2022.
68. Numenta. Numenta anomaly benchmark. https://www.numenta.com/resources/htm/numentaanomoly-benchmark/, n.d. Accessed May 10, 2023.

 