IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 29 August 2023, accepted 15 September 2023, date of publication 25 September 2023, date of current version 2 October 2023.

*Digital Object Identifier 10.1109/ACCESS.2023.3318755*

RESEARCH ARTICLE

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

**REYAZUR RASHID IRSHAD[1], SHAHID HUSSAIN[2], IHTISHAM HUSSAIN[3], JAMAL ABDUL NASIR[4], ASIM ZEB[5], KHALED M. ALALAYAH[1], AHMED ABDU ALATTAB[1], ADIL YOUSIF[1], AND IBRAHIM M. ALWAYLE[1]**

[1]Department of Computer Science, College of Science and Arts, Najran University, Najran 68341, Saudi Arabia
[2]Innovative Value Institute (IVI), School of Business, National University of Ireland Maynooth (NUIM), Maynooth, W23 F2H6 Ireland
[3]Department of Computer Science, Abdul Wali Khan University of Mardan (AWKUM), Shaheed Rashid Hussain (SRH) Campus, Nowshera 24210, Pakistan
[4]School of Computer Science, University of Galway, Galway, H91 TK33 Ireland
[5]Department of Computer Science, Abbottabad University of Science and Technology, Abbottabad 22500, Pakistan

Corresponding authors: Shahid Hussain (shahid.hussain@mu.ie) and Jamal Abdul Nasir (jamal.nasir@universityofgalway.ie)

The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work, under the Distinguish Research Funding Program grant code (NU/DRP/SERC/12/11).

**ABSTRACT** Cloud computing has revolutionized organizational operations by providing convenient, on-demand access to resources. The emergence of the Internet of Things (IoT) has introduced a new paradigm for collaborative computing, leveraging sensors and devices that generate and process vast amounts of data, thereby resulting in challenges related to scalability and security, making the significance of conventional security methods even more pronounced. Consequently, in this paper, we propose a novel Scalable and Secure Cloud Architecture (SSCA) that integrates IoT and cryptographic techniques, aiming to develop scalable and trustworthy cloud systems, thus enabling multi-user systems and facilitating simultaneous access to cloud resources by multiple users. The design adopts a decentralized approach, utilizing multiple cloud nodes to handle user requests efficiently and incorporates Multicast and Broadcast Rekeying Algorithm (MBRA) to ensure the privacy and confidentiality of user information, utilizing a hybrid cryptosystem that combines MBRA, Post Quantum Cryptography (PQC) and blockchain technology. Leveraging IoT devices, the architecture gathers data from distributed sensing resources and ensures the security of collected information through robust MBRA-PQC encryption algorithms, while the blockchain ensures that the confidential data is stored in distributed and immutable records. The proposed approach is applied to several datasets and the effectiveness is validated through various performance metrics, including response time, throughput, scalability, security, and reliability. The results highlight the effectiveness of the proposed SSCA, showcasing a notable reduction in response time by 1.67 seconds and 0.97 seconds for 250 and 1000 devices, respectively, in comparison to the MHE-IS-CPMT. Likewise, SSCA demonstrated significant improvements in the AUC values, exhibiting enhancements of 6.30%, 6.90%, 7.60%, and 7.30% at the 25-user level, and impressive gains of 5.20%, 9.30%, 11.50%, and 15.40% at the 50-user level when compared to the MHE-IS-CPMT, EAM, SCSS, and SHCEF models, respectively.

**INDEX TERMS** Blockchain, IoT-enabled cloud architecture, post-quantum cryptography, artificial intelligence, scalability, multi-user systems, decentralized approach.

The associate editor coordinating the review of this manuscript and approving it for publication was Xianzhi Wang.

## I. INTRODUCTION

The widespread adoption of cloud computing has significantly enhanced the management of information, processing, and storage by eliminating the requirement for upfront capital expenditures on equipment and network infrastructure [1]. It enables individuals and businesses to access and utilize computing resources on-demand through the global web, allowing for greater flexibility and scalability [2]. The ability to quickly adapt to meet the growing demands of expanding data is a critical feature of cloud computing [3]. Traditional IT infrastructures are struggling to handle the continually increasing volume of information. Cloud computing offers a flexible and scalable solution to these challenges by allowing businesses to adjust their technology resources as needed, whether it be to scale up or down [4]. The graphical representation in Figure 1 illustrates the importance of cloud computing in managing new and evolving forms of information. Data storage, processing, and access can occur through a distributed network of computers, as illustrated in Figure 1, facilitated by cloud technology [5]. Consequently, there is no need for physical hardware or infrastructure, making the management of large amounts of data more convenient and cost-effective. Moreover, cloud service providers often offer a range of services, including computing, analytics, and storage, enabling businesses to customize their strategies based on their specific needs. The subsequent subsections present some of the key features of the cloud and highlight the importance of cloud security, which serves as the motivation for this work [6].

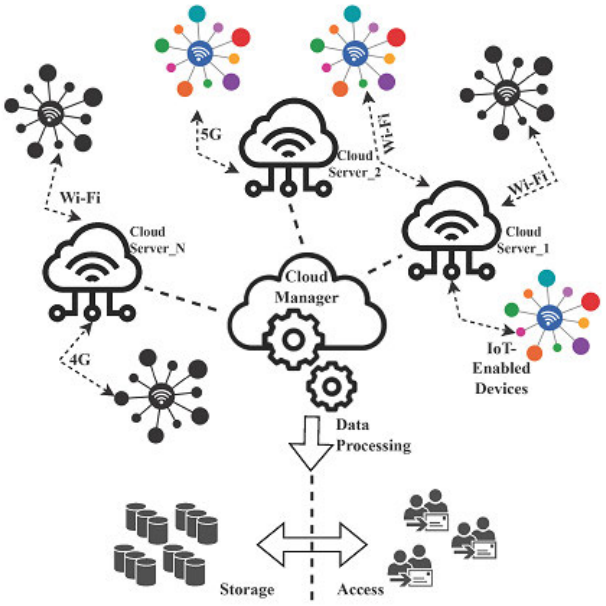


**FIGURE 1.** An illustration of the significance of cloud computing in managing the diverse IoT information.

### A. COMPONENTS OF CLOUD INFRA

There are several different types of cloud computing services, with the most prevalent being Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) [7]. Choosing the most suitable cloud service is critical to effectively managing an organization's dynamic and evolving data needs. Expertise in the various available services can assist in making an informed decision. There are several models for deploying clouds, including the public/open cloud, private/personal cloud, hybrid/converged cloud, and multiple cloud options. Understanding the differences between these approaches is crucial in selecting the most appropriate cloud deployment strategy for a given business [8].

Cloud computing offers various options for storing and managing data, including the ability to handle large and scalable datasets. To effectively govern and preserve records in the cloud, organizations need to have a solid understanding of these options and how they work. Cloud-based storage provides organizations with the ability to store data in a cost-effective and scalable manner [9]. However, it also introduces new challenges related to data preservation and oversight. Organizations must ensure that they have adequate policies and procedures in place to manage and secure their data, as well as comply with any relevant regulatory requirements [10]. Information governance is critical in cloud-based environments, as it enables organizations to effectively manage their data throughout its lifecycle. This includes establishing policies for data retention, access, and disposal, as well as ensuring that data is properly secured and protected from unauthorized access [11].

As data increasingly migrates to cloud infrastructure for storage and processing, it becomes crucial to prioritize the protection of information and ensure compliance with relevant regulations. Security in the virtual world relies on users' familiarity with the compliance and security options provided by cloud service providers, as well as their ability to take appropriate actions [12]. Cloud service providers typically offer a variety of compliance and security options, which may include encryption, access controls, and data backup and recovery. It is vital for organizations to understand these options and select the ones that best align with their needs [13].

Moreover, compliance with pertinent regulations, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), is of utmost importance when storing and processing sensitive data in the cloud. Organizations must ensure the implementation of suitable policies and procedures to adhere to these regulations, as well as any other applicable industry-specific regulations [14]. Ultimately, protecting data in the cloud necessitates a combination of technical solutions and user awareness. Organizations should collaborate closely with their cloud service providers to establish appropriate security and compliance measures. Additionally, it is crucial to provide training to employees on how to utilize the cloud securely and in compliance with relevant regulations [15].

Effective control of expenses and optimization are crucial in minimizing resource wastage when utilizing cloud services, which can otherwise offer a cost-effective solution for managing growing volumes of data. Organizations can achieve cost savings and meet their capacity expansion targets by developing a solid understanding of the cost elements involved and implementing optimization strategies [16]. Cloud service providers typically offer flexible pricing models that can be tailored to suit an organization's specific needs. It is important to comprehend the various pricing structures, such as pay-as-you-go or reserved instances, and their impact on costs. Additionally, employing optimization techniques like automated resource allocation and utilization can help reduce expenses and enhance overall efficiency. Cloud service providers also provide tools for monitoring resource utilization and identifying areas for optimization [17].

### B. NECESSITY OF CLOUD SECURITY

The hazards of hacking, cyber-attacks, and other security threats have elevated the importance of ensuring robust protection for cloud-based computing [18]. Consequently, the development of innovative secure frameworks, architectures, and mechanisms that can effectively detect and prevent cybercrimes on cloud platforms has become a key focus in contemporary research on versatile cloud computing technology. It is imperative to have security systems that can dynamically scale up or down in response to fluctuating workloads, enabling businesses to maintain a high level of security without compromising performance.

Ongoing research also focuses on developing secure and scalable data storage solutions for cloud computing. The integration of secure data-storing architectures helps mitigate safety concerns such as security breaches, unauthorized data access, and improper handling of stored records [19]. The current research landscape emphasizes the widespread implementation of encryption tools to safeguard information during data transfer and storage in cloud environments. This necessitates the development of novel encryption techniques that can efficiently handle massive datasets while ensuring robust security to withstand potential breaches of confidentiality [20].

### C. MOTIVATION AND SCOPE OF THE WORK

The convergence of Internet of Things (IoT) and cloud technology has paved the way for the development of multi-user platforms that provide near-real-time data and seamless access to services [21]. The incorporation of cloud computing capabilities into IoT has allowed the creation of multi-user platforms, empowering users with instant access to their information and resources from any location. New security concerns emerge when integrating IoT devices into multi-user systems, making it crucial to ensure the security of the system's architecture. This is particularly important since multiple users will be accessing and utilizing similar information and capabilities [22].

The implementation of IoT in a secure cloud infrastructure for multi-user applications is essential. A secure cloud architecture is necessary to effectively host and manage IoT devices and data while ensuring their safety. Within this architecture, various security techniques, such as authorization, authentication, access management, and threat detection, are incorporated to mitigate potential risks to data integrity and privacy [23]. The secure cloud architecture of a system involving multiple participants needs to be designed to accommodate users with varying capabilities and permissions. Consequently, an effective and scalable access control system must be implemented to manage user privileges and limit data access to authorized parties [24]. The vast amounts of data generated by IoT devices require a secure cloud infrastructure. The crucial aspect is to utilize scalable storage systems that can handle large volumes of data while ensuring security and accessibility are not compromised [25].

The objective of establishing a secure cloud architecture utilizing IoT for multi-user systems encompasses a broad scope, offering potential investigation opportunities in numerous study domains [26]. The proposed research aims to develop a secure, scalable, and efficient cloud architecture capable of supporting multi-user systems and managing large volumes of data while maintaining security and network performance. In the initial phase of the research, the focus is on designing an effective cloud architecture that can accommodate multiple users and process data from IoT devices. Key design goals include scalability, efficiency, and the ability to handle vast amounts of data. Furthermore, the suggested architecture must be flexible to support IoT devices gathering data from diverse sensing sources [27]. The collected data must be securely stored and protected throughout the integration process. The design also incorporates cryptographic techniques to ensure the privacy and confidentiality of user information, utilizing a hybrid cryptosystem that combines Post Quantum Cryptography (PQC) [28] and blockchain technology [29]. To safeguard data against robust threats, the hybrid PQC-Blockchain system utilizes PQC encryption [30]. This encryption method helps protect sensitive information from being compromised. By leveraging blockchain technology, the system ensures that confidential data is stored in distributed and immutable records. In the hybrid PQC-Blockchain system, data undergoes secure and reliable examination and integration into the blockchain through consensus mechanisms and mining procedures.

The integration of IoT and the hybrid PQC-blockchain system [31] in constructing this secure cloud architecture enables effective management of multiple users with fine-grained access rights. Moreover, the implementation of a robust and scalable access control method ensures that data is accessible only to authorized users, mitigating various security risks [32]. By leveraging a PQC-Blockchain hybrid system, distributed systems can ensure the security of their infrastructure against a broad spectrum of threats while

simultaneously providing users with immediate access to data and services. This enables a more interconnected and productive world as more individuals utilize IoT devices within shared infrastructures [33].

### D. MAIN CONTRIBUTION

In this research, our main contribution can be described in three distinct aspects, each addressing the interconnections and challenges discussed in the introduction.

- We have developed Scalable and Secure Cloud Architecture (SSCA), an IoT-enabled, cryptographically-secure cloud architecture that effectively addresses the challenges associated with integrating IoT and cryptographic techniques, ultimately leading to the development of scalable and trustworthy cloud systems. By leveraging advanced cryptographic techniques, the architecture effectively safeguards the confidentiality and integrity of the data, providing robust security measures to counter potential threats and ensuring the privacy of sensitive information. Simultaneously, the architecture is designed with a strong emphasis on scalability, enabling the seamless integration of numerous IoT devices and effectively meeting the escalating demands for cloud-based services, thus facilitating the efficient management and processing of large volumes of data generated by these devices.
- The proposed architecture supports multi-user systems and enables simultaneous access to cloud resources by multiple users. It adopts a decentralized approach, utilizing multiple cloud nodes to efficiently handle user requests and leverages cryptographic techniques to ensure the privacy and confidentiality of user information, utilizing a hybrid cryptosystem that combines MBRA, PQC and blockchain technology. Furthermore, we offer a comprehensive thread model and delve into the exploration of the underlying mechanisms behind the hybridization of MBRA, PQC, and Blockchain. This approach ensures efficient resource allocation and utilization, improving overall system performance.
- The proposed SSCA is applied to various use case scenarios, including Cloud Computing Use Case Attributes, Industrial Control Systems, and Healthcare Use Case Datasets. To validate its effectiveness, we have compared SSCA against cutting-edge Modified Honey Encryption utilizing Inverse Sampling-Conditional Probability Model Transform, ElGamal-based Authentication Method, Safe Cloud Storage System, and Secure, hybridized, Cloud-Enabled Framework, approaches and the performance is evaluated through throughput, scalability, security, and reliability.

### E. PAPER ORGANIZATION

The research investigation is structured as follows: Section II provides an overview of recent and relevant work in the proposed domain, highlighting key points essential to understanding the context and significance of the research. Section III presents the architecture of the scalable and secure cloud architecture, detailing its components and design principles. Section IV focuses on the proposed security architecture, outlining the core security features of the PQC-blockchain system and explaining how they contribute to safeguarding data and ensuring trustworthiness. Section V discusses the experimental outcomes observed in the research, comparing them with existing models to assess the effectiveness and performance of the proposed approach. Finally, in section 6, the research work concludes with endnotes summarizing the key findings and insights obtained from the study, along with suggestions for possible future directions and areas of further exploration.

## II. RELATED WORK

This section of the study offers a comprehensive overview of the existing research landscape concerning the design of secure cloud architectures for IoT platforms, emphasizing the importance of scalability.

Sharma et al. [34] conducted a study that focused on the emergence of the IoT as a transformative platform enabling interactions between previously inaccessible physical entities. The research highlighted the advantages of combining IoT with cloud services to effectively preserve and analyze data generated by diverse devices, with potential applications ranging from home automation and automated farming to smart medical care. However, the integration of these technologies faces significant challenges, particularly in terms of security. To address these challenges, the researchers proposed a Secure, hybridized, Cloud-Enabled Framework (SHCEF) for IoT, which combines both private and public platforms to address concerns related to privacy, scalability, and connectivity. The study also acknowledged the academic obstacles that need to be resolved before the full implementation of the hybrid cloud architecture. Overall, the study effectively summarizes the key findings and provides insights into the potential synergies and challenges associated with the collaboration between IoT and cloud processing.

In a study by Wu et al. [35], they analyzed the authentication technique proposed by Zhou et al. [36] and identified vulnerabilities in the handling of mutual verification and anonymity. To address these issues and enhance the detection of inaccurate input at an earlier stage, the authors proposed a new certification system that incorporates an additional detection parameter. They also introduced an improved IoT-based verification approach for cloud computing, demonstrating its favorable computational efficiency and robust security performance. This advancement lays the foundation for a lightweight authentication method based on the IoT that can effectively withstand multiple attacks and fulfill critical security functions such as user auditing, collaborative authentication, and session encryption. The authors express confidence in the applicability of their proposed verification mechanism to open IoT devices.

Sarker et al. [21] address the crucial aspect of security by proposing an innovative machine-learning model

called IntruDTRee. This model is specifically designed for constructing a tree-based framework for detecting security breaches. The authors highlight that IntruDTRee effectively reduces computational complexity without compromising accuracy when predicting unknown test instances. The model's performance is evaluated through experiments using cybersecurity datasets, and its efficacy is compared to that of several conventional machine-learning techniques.

Unal et al. [37] propose a Safe Cloud Storage System (SCSS) that utilizes Identity-based Cryptography (IBC) and a decentralized key administration and encryption approach. This architecture addresses the limitations of traditional Public Key Infrastructure (PKI) solutions in terms of scalability and speed in protecting and retrieving data in the cloud. By employing multiple Public Key Generators (PKGs) and decentralized key governance, the system enhances security. Moreover, the improved scalability simplifies forensic investigations on encrypted cloud data. Overall, this research offers a promising approach to implementing cryptographic algorithms for cloud storage, enabling multiple users to utilize the system simultaneously.

Irshad and Chaudhry [38] propose a novel ElGamal-based Authentication Method (EAM) called SAS-Cloud to address the authentication challenges in cloud-hosted IoT systems. The method combines the user's passcode and biometric data to verify their identity. The authors analyze the security and effectiveness of SAS-Cloud and demonstrate its resilience against potential attacks while achieving higher efficiency compared to existing alternatives. By incorporating both a passcode and biometric characteristics, the authentication method offers enhanced security. The study highlights the critical need for secure authentication in cloud-based IoT applications and introduces a novel technique, SAS-Cloud, to address this requirement.

Ahmad et al. [39] proposed a novel hybrid cryptographic methodology to enhance the Key Administration System (KAS) in cloud environments. The method combines authenticated digital encryption using ECC (Elliptic Curve Cryptography) with AES (Advanced Encryption Standard). It leverages the strength of both ECC and AES cryptographic systems for secure information encryption and decryption. The encryption process utilizes a secure key derived from an arbitrary prime scale, an authoritative secret key, and an associated value. The suggested approach outperforms traditional techniques in terms of time complexity, encryption time, and decryption time. The method offers significant improvements in these areas, making it more efficient and suitable for cloud-based scenarios. The research suggests that adopting this methodology in the cloud can provide robust security measures for handling sensitive medical data.

Uppuluri and Lakshmeeswari [40] proposd a novel approach called Modified Honey Encryption utilizing Inverse Sampling-Conditional Probability Model Transform (MHE-IS-CPMT) with ECC for identification and key exchange in a home framework. The protocol encompasses several components, including initialization, enrollment, login, and credential renewal, which collectively ensure secure data transmission between users and their devices. The MHE-IS-CPMT with ECC is employed to encrypt user and device information, providing a robust foundation for secure communication and access management. The suggested system exhibits dependable characteristics, facilitating secure interaction and access control between users and their devices. A reliable key exchange method ensures that legitimate users can modify their keys as needed.

The creation of an IoT system for smart cities using Infrastructure as a Service (IaaS) grade cloud computing platform is demonstrated in this study by Bommu et al. [41]. The IaaS level design realistically implements the performance-enhanced smart city topology. The envisaged smart city IoT system may track key factors like transportation, water quality, sun radiation, sound pollution, air quality, and surveillance footage with a thermal camera to detect Covid-19 afflicted individuals. To enhance routing as well as QoS, a network topology study at the simulation stage is carried out. Decentralization based on blockchain technology is used to improve the safety performance of IoT systems.

Healthcare certificates are established, maintained, and validated via a secure blockchain-based Proposed Application (PA) as demonstrated by Sharma et al. [42]. The PA serves as a communication channel between the backend of the blockchain system and various application domains, including medical facilities, patients, healthcare providers, and IoT devices, enabling the generation and verification of medical certificates. By employing the concept of smart contracts, it also ensures multiple security features, including confidentiality, authentication, and access control.

To ensure the confidentiality and security of Industrial IoT systems, Selvarajan et al. [43] aim to develop a Convivial Optimised Sprinter Neural Network (COSNN)-based Lightweight Blockchain Security Model (AILBSM). In this context, an Authentic Intrinsic Analysis (AIA) model is employed to transform characteristics into encoded data, mitigating the substantial impact of potential attacks. The system is subjected to extensive testing using diverse attack datasets to validate its effectiveness. Thanks to the incorporation of auto-encoder-based conversion and blockchain authentication, the suggested model's anomaly detection performance is notably improved compared to previous methods.

To tackle this concern, Jalasri and Lakshmanan [44] propose a clustering algorithm and cryptography method to manage data security in a distributed environment. Prior to conducting the clustering procedure for data transmission in fog systems, the cluster heads are identified using the power probabilistic criterion. Data security is ensured during data transfer through the utilization of the noise protocol framework encryption procedure. Additionally, the approach outlined aims to mitigate intermediate attacks and address the issue of excessive energy consumption by nodes during data transfer.

## III. THE PROPOSED SSCA ARCHITECTURE FOR MULTI-USER SYSTEMS

The convergence of IoT and cloud computing has enabled the development of robust multi-user communication systems for various applications. However, this integration also introduces new security challenges that necessitate effective detection and mitigation strategies [45], [46]. To ensure the security of these systems, we propose a novel hybrid model based on artificial intelligence (AI) [47] with PQC and a Blockchain-based security approach. Intrusion detection mechanisms continuously monitor system activities and identify potential security breaches, enabling prompt responses and mitigation. In this context, the Multicast & Broadcast Rekeying Algorithm (MBRA) is introduced as a method for detecting threats in the Cloud-IoT model. Furthermore, this hybrid approach incorporates robust security mechanisms including authentication, encryption, access control, and intrusion detection. Through the integration of enhanced PQC via MBRA-based optimal key generation, the system can withstand attacks from quantum computers, which pose a threat to traditional cryptographic algorithms [48]. The Blockchain component provides a decentralized and tamper-resistant infrastructure, ensuring data integrity and immutability. Moreover, the hybrid system facilitates secure user authentication, preventing unauthorized access to IoT devices and cloud resources through hash validation and block IDs for each block [49]. Encryption mechanisms safeguard the confidentiality and privacy of sensitive data transmitted within the system. Access control mechanisms allow for meticulous control over user permissions and privileges. The incorporation of the hybrid MBRA with PQC-Blockchain system in IoT and cloud environments enhances security by addressing the specific challenges associated with these intricate ecosystems [50].

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

To grasp the underlying mechanism of the proposed SSCA, we unveil an intricate exploration of the architecture and the thread detection mechanism, as depicted in Figure 2. The figure illustrates that the proposed SSCA model is designed to host and manage IoT devices, encompassing detectors, actuators, regulators, and sensors. All data generated by these devices is transmitted to the cloud servers. The system comprises several vital components that cooperate to establish a secure and stable environment for numerous users. The functional behavior of the various components within the threat model (Figure 2) is described as follows:

1) *Virtual servers:* These virtualized resources serve as the foundation for hosting and managing IoT devices and their associated data. They provide the necessary computing power and storage capabilities.
2) *Server farms:* The server farms consist of multiple physical servers interconnected to handle the processing and storage requirements of the IoT devices. They ensure high availability and scalability of the cloud platform.
3) *Blockchain nodes:* These nodes participate in the blockchain network, maintaining a distributed ledger that records and manages the IoT device data [51]. The blockchain ensures data accuracy and immutability due to its secure and transparent nature.
4) *PQC encryption:* PQC encryption techniques are employed to protect the communication content during transit between multi-users and the cloud servers. PQC algorithms are resistant to attacks from quantum computers, ensuring the confidentiality and integrity of the transmitted data [52].

The architecture integrates a range of security mechanisms to ensure the secure transmission, storage, and management of data within the cloud platform. These mechanisms operate at different stages of the data flow process, guaranteeing the confidentiality, integrity, and availability of the IoT device data.

- *Authorization:* This mechanism verifies and grants appropriate access permissions to users, ensuring that only authorized individuals can interact with the IoT devices and cloud services.
- *Access management:* Access management controls and monitors user access to different resources and functionalities within the cloud platform, preventing unauthorized actions and ensuring data confidentiality.
- *Attack detection via MBRA:*The proposed SSCA capitalizes on the intrusion detection and anomaly detection capabilities offered by the MBRA Technique. This strategic integration significantly bolsters its proficiency in effectively identifying and preemptively addressing potential security threats, thereby reinforcing its resilience against various forms of attacks.
- *Security:*Subsequently, the system engages in data encryption and decryption processes to preemptively prevent any unauthorized modifications or tampering attempts, thus ensuring the robust integrity and confidentiality of the transmitted information.
- *Access control:* Access control mechanisms regulate the permissions and privileges granted to users, enforcing granular control over their actions and ensuring the privacy and security of the data throughout its journey from cloud servers to multi-users via IoT devices.

The proposed SSCA system is built around a hybridized MBRA with PQC-Blockchain cryptosystem, which serves as the core security mechanism. This advanced cryptographic system combines varying significant components, namely, MBRA for attack detection and optimal key generation, PQC and Blockchain for encryption, to provide robust security measures throughout the system [52]. By combining PQC and MBRA with blockchain methodology, the hybridized cryptosystem provides a strong foundation for secure communication, data storage, and access control in the cloud system. It ensures the confidentiality of sensitive information during transmission and safeguards against potential attacks,

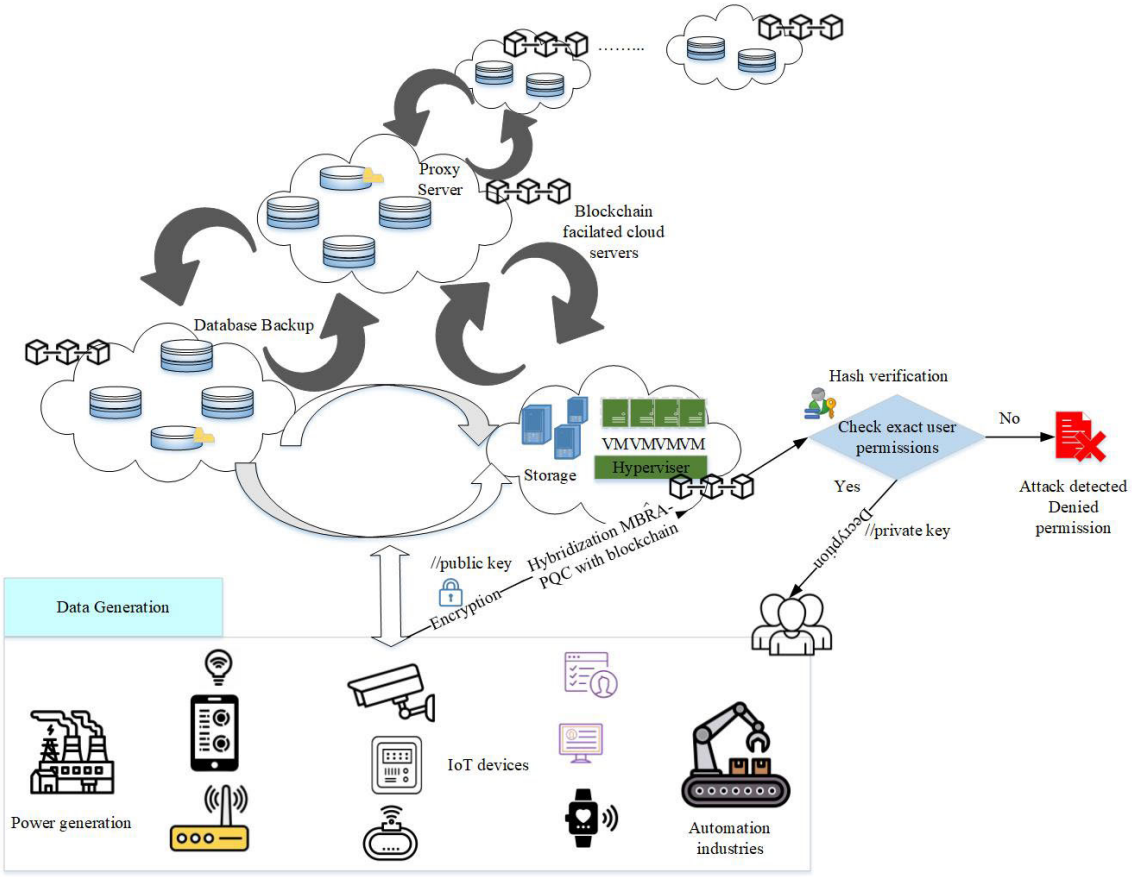


**FIGURE 2.** A Visual representation illustrating the Proposed Scalable and Secure Architecture for Multi-User Systems, outlining the attacks and the corresponding preventive mechanisms of the proposed SSCA.

offering a high level of protection for the system and the data it handles [53]. The subsequent section delves into the comprehensive mechanism and formulation of the MBRA for potential threat detection.

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

The strategy recommended in this context draws inspiration from the battle royale algorithm (BRA) video game subgenre. The foundational concept behind BRA involves a randomized population uniformly distributed across the issue space. In this scenario, each individual (referred to as a soldier/player) targets the nearest soldier to them, much like firing a weapon. Command-position soldiers thus affect their closest neighbors, leading to a dynamic cascade of interactions. With each encounter inflicting damage, a soldier gains damage levels. Moreover, injured soldiers strive to relocate swiftly, aiming to approach adversaries from novel vantage points. The injured soldier's movement trajectory is directed towards a location positioned midway between its present coordinates and the best position achieved so far (the elite player), emphasizing strategic exploitation. This function finds application within the realm of PQC for attack detection and mitigation. The mathematical representation of this interaction is approximated by Eq. (1).

$$x_{s.i} = x_{s.i} + rand(x_{best.i} - x_{s.i}) \tag{1}$$

where *rand* represents a randomly generated number uniformly distributed in the range [0,1], and $x_{s.i}$ denotes the parameter with the least favorable location in the *ath* dimension. If the parameter with the poorest location can influence its adversary in the subsequent iteration, $x_{i.s}$ will also be reset to zero. Here, $x_{i.s}$ signifies the lowest level of the *ith* parameter, and its interaction is expressed as $x_{i.s} + 1$. If a parameter's damage level surpasses a predefined threshold, denoted as 3, the parameter is considered to have reached a critical state. At this juncture, the parameter is reinitialized at random within the potential problem space, while its harm level, $x_{i.s}$, is reset to 0. This mechanism encourages further exploration and curtails premature convergence. Subsequent to being "killed," a soldier reenters the problematic zone as stipulated by Eq. (2).

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

The range for the $i^{th}$ dimension of the problem space is defined by the lower and upper limits denoted as $Lb_i$ and $Ub_i$,

respectively. Furthermore, with each iteration $\Delta$, the feasible search area of the problem contracts towards the optimal solution. Initially, $\Delta$ is determined as $\Delta = \log_{10}(H_k)$, and subsequently, $\Delta$ is updated as $\Delta = \Delta + \text{round}(\frac{\Delta}{2})$. Here, $H_k$ represents the maximum number of iterations. This interplay effectively balances exploration and exploitation. Consequently, the adjustment of the lower bound and upper bound is modeled by the Eq. (3) and Eq. (4).

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

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

The achieved optimal position is represented by $x_{best.i}$, while the standard deviation of total transmission in the $i^{th}$ dimension is denoted as $\sigma$. Consequently, if $Lb_i$ exceeds the initial lower/upper bound $Lb_a$, the range of $Lb_i/Ub_i$ is set to $Lb_i/Ub_i$. The best attack and key for PQC discovered in each iteration are retained and treated as special, thus emphasizing the concept of elitism. The computational cost of the proposed approach is influenced by the problem's dimensions, along with the population size and the maximum number of iterations. Given that every response necessitates a comparison with each other response to compute its Euclidean distance, the computational complexity for all solutions is $O(v^2)$. Therefore, the quantity of iterations, denoted as $t$, dictates the computational complexity of MBRA, resulting in $O(v^3)$.

### C. THE HYBRIDIZATION MECHANISM OF MBRA-PQC AND BLOCKCHAIN SYSTEM

In this section, we leverage the advantages of MBRA-PQC and blockchain technology to enhance the PQC algorithm [54] for transactions and data stored within the blockchain, while also exploring the identification of the optimal key using MBRA. The objective is to seamlessly integrate blockchain with an enhanced MBRA approach, and establish a cohesive linkage with PQC systems. In the pursuit of developing and integrating the hybrid MBRA-PQC with Blockchain system, we prioritize the refinement of IoT-based cloud systems. This involves the careful adjustment and modification of corresponding equations within these systems to achieve a seamless and cohesive framework.

Within our study, we have meticulously examined an IoT-based cloud system designed to accommodate a diverse array of users. In this context, we have harnessed the sophisticated encryption process provided by MBRA-PQC to establish robust and secure channels of communication between IoT devices and the cloud servers. Consider a scenario wherein a multitude of $n$ IoT devices are present, each denoted as $D_1, D_2, D_3, \ldots, D_n$, alongside a dedicated cloud server, designated as $\mathcal{C}$. Every individual IoT device is assigned a unique identifier, represented as $Z_i$, and autonomously generates an individualized symmetric key, denoted as $k_i$. This specific key, $k_i$, plays a pivotal role in encrypting data before its transmission to the designated cloud server $\mathcal{C}$. As a preemptive security measure, prior to transmitting any sensitive information to the cloud server, the symmetric key $k_i$ undergoes a meticulous encryption process utilizing the robust PQC method. Notably, the intricate task of estimating optimal keys finds its foundation in the MBRA methodology. The comprehensive security protocol unfolds through a sequence of meticulously orchestrated steps:

#### 1) THE KEY GENERATION PROCESS OF MBRA

Key generation is a crucial process in cryptography that involves creating a pair of keys: a publicly accessible key and a confidential (private) key [55]. These keys are generated through a secure mechanism aligned with specific cryptographic algorithms. The public key, as the name implies, plays a vital role in encryption processes by being openly shared among users, enabling anyone possessing the public key to securely encrypt data. In contrast, the private key must remain confidential and be known only to the intended recipient. This private key is used for decrypting encrypted data, ensuring that only authorized individuals can access the original information. The key generation process typically involves random or pseudorandom number generation techniques. Additionally, key generation might include key derivation functions, deriving keys from a primary key for an added layer of security. Therefore, it is important to highlight that the strength and randomness of the generated keys significantly influence the overall security of cryptographic systems [55].

Each entity, represented as $D_n$, generates a public-private key pair for PQC using the MBRA method. The public key, denoted as $k_{PQC_i}$, is shared openly, while the private key, designated as $k_{(PQC_i)^{-1}}$, remains undisclosed. This key pair plays a pivotal role in securely encrypting and decrypting sensitive information within a post-quantum computing environment.

#### 2) DATA REPRESENTATION

The data intended for encryption is usually converted into a numerical representation, often a vector or bit sequence. This transformation enables the data to undergo mathematical operations, facilitating processing and manipulation throughout the encryption process [56], [57].

#### 3) PUBLIC KEY MATRICES

During the encryption process, numerical vectors derived from the data are augmented using public key matrices. These matrices are generated in the key generation phase and are designed to be publicly accessible [58]. The format and properties of these matrices are dictated by the specific encryption algorithm employed, with the application of MBRA methodology further influencing their characteristics.

#### 4) QUANTUM ENCRYPTION

The encryption process encompasses multiple steps aimed at ensuring the secure transformation of information into an encrypted form [59]. Encrypting the symmetric key $k_i$

involves leveraging the PQC public key $k_{PQC_i}$, which triggers the generation of a ciphertext, labeled as $x_i$, through the encryption function $Y_E(k_i, k_{PQC_i})$. This resultant ciphertext $x_i$ represents the encrypted rendition of the symmetric key $k_i$, thereby ensuring its confidentiality throughout transmission or storage.

#### 5) VECTOR AUGMENTATION

The numerical vector acquired through the data representation step is subsequently enriched using the public key matrices. This enrichment entails mathematical operations, which can encompass matrix multiplication or modular arithmetic, contingent on the chosen encryption algorithm. The objective of this stage is to metamorphose the initial vector into an encrypted vector, housing the encrypted depiction of the information.

#### 6) ENCRYPTION VECTOR

The outcome of the vector augmentation process yields the encrypted vector, which encompasses the altered and encrypted rendition of the original data [60]. It is noteworthy that the encrypted vector generally possesses a larger size compared to the original vector, owing to the supplementary information integrated during the augmentation procedure.

#### 7) CONFIDENTIALITY AND SECURITY

The encrypted vector, derived from augmentation by harnessing the optimal public key matrices of MBRA, confers confidentiality and security to the information. The lack of possession of the corresponding private key renders the computational reversal of the encryption process and retrieval of the original data from the encrypted vector infeasible.

Once the cloud server gains access to the initial symmetric key $k_i$, it can effectively employ this key for both encryption and decryption of the data transmitted by the IoT device. This mechanism ensures the safeguarding of sensitive information as it traverses from the IoT device to the cloud server. In the context of a multi-user IoT-based cloud system, the MBRA-PQC encryption procedure can be succinctly represented through Algorithm 1, which delineates the specific steps and operations integral to the encryption process.

**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, $\kappa_i$ signifies the symmetric key, $\kappa_{OPQC_i}$ represents the optimal PQC public key obtained through MBRA, $\kappa_{OPQC_i^{-1}}$ denotes the corresponding optimal PQC private key, $x_i$ denotes the ciphertext, and $\zeta_i$ refers to supplementary data transmitted from the IoT device to the cloud server.

#### 8) HASH VERIFICATION

A blockchain is a distributed, immutable electronic ledger that can reliably and transparently document transactions without a single point of failure as it relies on several computations [51]. The encrypted data are stored in the blocks of the blockchain system. The hash value of $\beta_i$ on a blockchain is computed using a cryptographic hash function (denoted as $\mathcal{H}$) that ensures its integrity and security [61]. This hash function takes an input consisting of the data of $\beta_i$ concatenated with a nonce value $\eta_i$, selected by users to meet specific requirements. The resulting hash value is a fixed-length string of bits that uniquely identifies $\beta_i$ on the blockchain, including the currently active one [62]. To meet certain criteria, such as having a specified number of trailing zeros, users engage in a computationally intensive and risky mining process [63]. The challenge lies in finding a nonce value $\eta_i$ that, when combined with the data of $\beta_i$, produces a hash value satisfying the desired conditions.Miners compete with each other to discover a valid nonce, employing significant computational power and resources. The mining process can be time-consuming and requires substantial computational effort due to the difficulty of finding a suitable nonce. The first miner to find a nonce value that fulfills the criteria is rewarded for their mining contribution. The utilization of the hash function and the nonce value ensures the immutability of the blockchain. Modifying any data in a previous block would require recalculating the hash values for subsequent blocks, making it computationally infeasible and preserving the integrity of the blockchain.

Let $\mathcal{H}(\beta_{i-1})$ be the hash value of the previous block, $\beta_i$. Let $P_i$ be the plaintext data to be stored in the current block. Let $f(\Upsilon_E)$ be the optimal MBRA-PQC encryption function, with $\kappa_{OPQC_i}$ as the optimal PQC public key. Let $\eta_i$ be a randomized nonce value. Then, the hash value of the current block, $\beta_i$, can be computed as shown in Eq. (5)

$$\beta_i = \mathcal{H}\left[\eta_i \| (\beta_{i-1}) \| P_i \| f(\Upsilon_E(\eta_i, k_{OPQC_i}))\right] \tag{5}$$

In the equation above, $\|$ denotes concatenation. The hash value of the previous block, the plaintext data, and the result of the MBRA-PQC encryption function applied to the nonce value and the optimal PQC public key are combined using concatenation. The resulting concatenated string is then passed through the cryptographic hash function $\mathcal{H}$ to obtain the hash value of the current block, $\beta_i$.

The consensus and mining process in the hybrid MBRA-PQC with Blockchain system involves solving a complex mathematical puzzle to add a new $\beta_i$ to the blockchain. Let $Sc$ represent the current state of the blockchain, and let $N$ be the set of nodes in the network. To add a new block $\beta_i$ to the blockchain, a node (miner) must find a nonce value $\eta_i$ such that the hash value of the current block $\mathcal{H}(i)$ satisfies specific criteria, such as having a

certain number of leading zeros. This can be mathematically represented as Eq.(6)

$$\mathcal{H}(\beta_i) = \mathcal{H}\big(\eta_i \| x_i \| N\big) \tag{6}$$

In the given context, $\|$ represents concatenation, and $x_i$ represents the MBRA-PQC based encrypted data to be added to $\beta_i$. The miner is required to iterate through different values of $\eta_i$ until they find a nonce that results in a suitable $\mathcal{H}$ value. Once a nonce is found that satisfies the desired criteria, the miner broadcasts the new $\beta_i$ to the network for verification. Verification involves checking that the nonce value $\eta_i$ of the previous block $\beta_{i-1}$ in the blockchain matches the value stored in the state $S_c(\beta_i)$, and also validating that the nonce value used to generate the current block $\beta_i$'s hash value is valid, as shown in Eq.(7)

$$\mathcal{H}(\beta_i - 1) = \mathcal{H}\big[\eta_{i-1} \| N \| x_i\big] \tag{7}$$

In Eq.(7), $\beta_{i-1}$ represents the previous block in the blockchain. In addition to verifying the nonce value and the hash criteria, nodes in the network also validate the optimal PQC encryption process $f(\Upsilon_E)$ used to encrypt the data in block $\beta_i$ and ensure that the PQC public key $\kappa_{OPQC_i}$ used is trusted. This can be mathematically represented as Eq.(8)

$$P_i = d(x_i, \kappa_{OPQC_i^{-1}}) \tag{8}$$

Once the new block is verified, it is appended to the blockchain, and the network achieves consensus on the updated state of the blockchain. The security of the hybrid MBRA-PQC-based Blockchain system relies on the computational complexity of the mathematical problems encountered in the consensus and mining process, which are considered difficult for both classical and quantum computers. Furthermore, the hash value of the block is calculated by following the steps outlined in Algorithm 2.

The security of the hybrid MBRA-PQC with Blockchain system relies on the computational complexity of the mathematical problems inherent in both the MBRA-based PQC encryption process and the blockchain consensus mechanism. These problems are designed to be challenging for both classical and quantum computers.

#### 9) QUANTUM DECRYPTION

The decryption process involves utilizing the confidential (private) key to decrypt the encrypted data and recover the original information [64], [65]. To decrypt the ciphertext $x_i$, the cloud server requires access to the MBRA-PQC private key $k_{(PQC_i)^{-1}}$ associated with the device $D_n$. Using this private key, the cloud server performs decryption by applying the decryption function $d = x_i, k_{(PQC_i)^{-1}}$. This process yields the original symmetric key $k_i$, which was used to encrypt the data. By obtaining the original symmetric key, the cloud server can effectively access and retrieve the encrypted information. The decryption flow is provided in Algorithm 3. Whenever the cloud server possesses authorization to the original symmetric key $k_i$, it can utilize this key to generate ciphertext and recover the original data sent by the IoT device. This process ensures that the data exchanged between the IoT devices and the cloud server remains secure and inaccessible to unauthorized parties. By employing the symmetric key, the cloud server can encrypt and decrypt data reliably, safeguarding the confidentiality and integrity of the transmitted information.

## IV. RESULT DISCUSSION

In this section, we present an elaborate comparative study of the proposed SSCA. This innovative approach is developed through the synergistic hybridization of MBRA, PQC, and blockchain, aimed at augmenting data transmission within cloud-based IoT networks. To facilitate a comprehensive comparative analysis, the subsequent sections delve into the discussion of the experimental environment setup, followed by a detailed dataset description and an exposition of the features employed. Subsequently, we offer both visual and quantitative comparative studies that juxtapose the proposed SSCA against a range of established state-of-the-art security methodologies. This integrated presentation aims to provide a holistic assessment of the novel SSCA in relation to existing approaches.

### A. EXPERIMENTAL SETUP

Table 1 outlines the components of the testbed utilized in the experimental setup, essential for creating a realistic environment to evaluate the proposed system. The Cloud Platform, based on AWS, offers scalable storage, networking, and processing power. Edge Devices act as intermediaries, enabling data collection, analytics, and communication between IoT devices and the cloud. IoT Devices, including smart sensors, Radio Frequency Identification (RFID) readers, cameras, and actuators, are deployed to gather data and enable remote control. Quantum Cryptography ensures secure data transfer through encryption and key distribution. The Blockchain System tracks and verifies transactions using a distributed and tamper-proof ledger system like Ethereum. A Network Traffic Generator simulates realistic network applications and usage patterns. Finally, an Attack Simulator tests the defenses against simulated attacks using tools like Metasploit, Nmap, and Wireshark. These components collectively create a comprehensive and representative testbed for the evaluation of the proposed system's performance and effectiveness in a practical setting.

### B. DATASETS DESCRIPTION

Table 2 [66] and Table 3 provides an overview of the datasets used in the experimental setup, covering diverse use cases Numenta Anomaly Benchmark (NAB) [67], cloud computing, cloud security, industrial control systems, and healthcare. The NAB dataset is valuable for evaluating the performance of multi-user systems in terms of scalability and security. It enables practical assessments of system capabilities, such as handling large datasets, detecting anomalies efficiently, and ensuring robust privacy protection. Table 2 summarizes

**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 $H$

**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*

the Essential Attributes of NAB Datasets for Cryptosystem Assessment, which providing acceptable value ranges to assess the effectiveness of a cryptosystem. The NAB [67] dataset to evaluate the effectiveness of our proposed security model against various crucial threat criteria in the Cloud with IoT platforms. The NAB dataset is a compilation of real-world datasets specifically designed for evaluating streaming methods in anomaly detection using the NAB as benchmarking cryptosystems. The NAB dataset serves as a valuable resource for assessing the performance of anomaly detection algorithms, particularly in multi-user settings that involve numerous IoT devices. This enables us to assess the performance, accuracy, and robustness of our algorithm under various scenarios and validate its effectiveness in real-world settings. the other cloud computing, cloud security, industrial control systems, and healthcare dataset includes specific attributes like the number of users, platform/environment, data types, threat types, and compliance standards in Table 3. These datasets facilitate the evaluation of different scenarios and allow for the assessment of proposed solutions in real-world contexts.

### C. PERFORMANCE EVALUATION CRITERIA

Performance analysis is a crucial aspect of this research, aiming to evaluate the effectiveness and efficiency of each strategy employed. By examining the outcomes, valuable insights can be gained, leading to further investigations and advancements in the field. To assess the success of the proposed SSCA model, a comparative analysis is conducted, comparing its results with existing works such as MHE-IS-CPMT [40], ElGamal-based Authentication Method(EAM) [38], SCSS [37], and Secure hybridized Cloud-Enabled Framework (SHCEF) [34]. Moreover, the suggested architecture is evaluated based on various performance indicators, including response time, scalability, throughput, security, and dependability (reliability). These indicators serve as criteria to assess the effectiveness and suitability of the proposed architecture in meeting the desired objectives. Applying the above criteria the proposed architecture is validated in the following.

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

| 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 |

#### 1) RESPONSE TIME AND SCALABILITY

The number of users is a key factor in assessing the scalability of the architecture, while the response time reflects the performance aspect. Evaluating the response time across different user counts allows us to gauge the system's ability to handle increased loads while maintaining quick response times. This is crucial for ensuring the usability and effectiveness of the architecture in real-world scenarios. Additional factors such as the number of devices, transactions, or requests can also be considered on the X-axis, depending on the specific use case and system requirements. However, it is important to note that the calculation of response time may vary depending on the specific context and metrics being measured and can be calculated as shown in Eq. (9).

$$\tau = \alpha + \beta + \gamma + q \tag{9}$$

In the above equation, the processing time ($\alpha$) refers to the duration required for executing computations and cryptographic procedures involved in processing a transaction or request. The transmission time ($\beta$) encompasses any delays caused by network factors such as latency, available resources, and congestion. The queuing time (q) represents the duration spent in a queue before a transaction or request is completed. Lastly, the waiting time ($\gamma$) indicates the time taken by the system to respond or acknowledge a request. Together, these components contribute to the overall response time of the system.

Figure 3(a) illustrates the evaluation results of various models, including MHE-IS-CPMT, EAM, SCSS, SHCEF, and SSCA, based on the number of users and their average response time. The number of users serves as a measure of the architecture's scalability, indicating its capability to handle larger user loads while maintaining satisfactory performance levels. On the other hand, the response time measures the duration taken by the system to respond to user requests, directly influencing the system's usability and effectiveness in practical scenarios.

The findings from the evaluation reveal a consistent trend across all models, where the average response time exhibits an upward trajectory as the number of users rises. This suggests that increased user load negatively impacts the performance of all models, leading to a degradation in response time. However, it is important to note that the extent of this impact differs among the evaluated models, indicating variations in their ability to handle higher user loads and maintain optimal performance. Further analysis is required to understand the specific strengths and limitations of each model concerning scalability and response time. The evaluation results demonstrate that SSCA exhibits a significantly lower average response time compared to the other models. This finding suggests that SSCA is more effective in handling increased user load while maintaining fast response times. As a result, SSCA demonstrates better scalability and performance characteristics compared to the other models. The superior performance of SSCA in terms of response time highlights its ability to efficiently process user requests and deliver timely responses, making it a promising solution for real-world scenarios with high user loads.

**TABLE 2.** Essential attributes of numenta anomaly benchmark (NAB) [67] datasets for cryptosystem assessment.

| 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. |

By examining the results depicted in Figure 3(b), it is evident that the response time of each model exhibits an increase as the number of devices increases. However, there are variations in the performance of different models when handling increased device loads. For instance, the MHE-IS-CPMT model demonstrates a response time of 7.69 seconds when dealing with 250 devices, which subsequently increases to 9.19 seconds when managing 1000 devices. Similarly, the SSCA model shows a response time of 6.02 seconds for 250 devices, which rises to 8.22 seconds when accommodating 1000 devices. In this context, the number of devices serves as an indicator of the architecture's scalability, while the response time and scalability factors represent the performance aspects of the architecture. Overall, the evaluation results demonstrate that the SSCA model exhibits superior performance in terms of response time compared to the other models across all numbers of devices. The consistently lower average response time of the SSCA model indicates its enhanced scalability and superior performance under high device loads. These findings highlight the effectiveness and efficiency of the SSCA model in handling increased device loads and maintaining fast response times, positioning it as a highly scalable and performant solution.

The results depicted in Figure 3(c) illustrate the performance of different models (MHE-IS-CPMT, EAM, SCSS, SHCEF, and SSCA) concerning the number of transactions and their corresponding response times. The number of transactions serves as an indicator of the system's workload or throughput, while the response time represents the duration it takes for the system to respond to each transaction. As anticipated, the findings demonstrate that as the number of transactions increases, the response time also increases for all models, indicating the impact of workload on system performance. Notably, the SSCA model consistently exhibits lower response times compared to the other models across all transaction values. This suggests that the SSCA model is more adept at handling increased workload while maintaining faster response times in comparison to the alternative models. These results underscore the superior performance and scalability of the SSCA model in handling higher transaction volumes effectively.

### 2) SECURITY

The evaluation of a system's security involves assessing its vulnerabilities and determining the effectiveness of the implemented security measures in mitigating potential threats.

**TABLE 3.** The datasets and their attributes for the experimental setting.

| Dataset Name | Attributes | Possible Values or Range |
|---|---|---|
| No. of Users | - | 100 |
| Cloud Computing Use Case Attributes | Cloud Platform | AWS |
| | Edge Platform | Raspberry Pi |
| | Network Environment | IoT, Industrial Control Systems, Smart Buildings, Medical Devices |
| | Data Types | Network Traffic, Log Data, System Images |
| | Threat Types | Malware, Phishing, Insider Threat, DDoS |
| Cloud Security Use Case Attributes | Cloud Platform | AWS |
| | Security Controls | Access Controls (0-1), Network Security (0-1), Encryption (0-1), Logging and Monitoring (0-1) |
| | Compliance Standards | NIST Cybersecurity Framework |
| | Data Types | Network Traffic, Log Data, System Images |
| | Threat Types | Malware, Phishing, Insider Threat, DDoS |
| Industrial Control Systems Use Case Dataset | Industrial Control Systems | SCADA |
| | Network Environment | Power Grid, Water Treatment, Manufacturing, Oil and Gas |
| | Data Types | Network Traffic, Log Data, System Images |
| | Threat Types | Malware, Insider Threat, Physical Access, Supply Chain |
| Healthcare Use Case Dataset [67] | Healthcare Environment | Hospitals, Clinics, Medical Devices |
| | Compliance Standards | HIPAA, HITECH |
| | Data Types | Network Traffic, Log Data, System Images |
| | Threat Types | Malware, Insider Threat, Physical Access, Supply Chain |

Key elements such as cryptographic key management, the use of cryptographic techniques, and secure communication protocols play a crucial role in ensuring the system's security. Equation (10) presents a computational formula that can be utilized to measure the level of protection provided by each model against possible vulnerabilities. By applying this equation, one can quantitatively evaluate and compare the security effectiveness of different models.

$$\Phi = \left[x \times P[\cdots] \times y\right] + \sum_{t=0}^{N}(\delta) \tag{10}$$

where $P\left[\cdots\right]$ represents the probability of security events occurring, $x$ represents the severity of the security events, $y$ represents the susceptibility of the system to be exploited and cause a security event, and $\delta$ represents the total duration required to detect and respond to a security breach. This equation provides a comprehensive framework for assessing the security level of a system by considering the likelihood, severity, susceptibility, and response time associated with potential security events. By evaluating these factors, one can gain insights into the effectiveness of the security measures and identify areas for improvement in the system's security.

The results presented in Figure 4 (a) to 4 (d) demonstrate the comparative security performance of the proposed SSCA model and existing models (MHE-IS-CPMT, EAM, SCSS, and SHCEF) at varying user levels. The AUC (Area Under the Curve) values are utilized as a metric to assess the security of the system, with higher values indicating better security performance. The X-axis represents the vulnerability rate, while the Y-axis represents the degree of protection.

The observed AUC values consistently indicate that the SSCA model outperforms the existing models in terms of security performance across all user levels. At each user level, the AUC value for SSCA is higher than that of MHE-IS-CPMT, EAM, SCSS, and SHCEF. This suggests that the proposed SSCA model provides better protection against security threats compared to the existing models. For instance, at the 25-user level, the AUC value for SSCA is 0.934, while the AUC values for MHE-IS-CPMT, EAM, SCSS, and SHCEF are 0.871, 0.865, 0.858, and 0.861, respectively. Similarly, at the 50-user level, the AUC value for SSCA is 0.936, whereas the AUC values for the other models are 0.884, 0.843, 0.821, and 0.782, respectively.

Furthermore, as the number of users increases, the AUC values for all models also increase, indicating improved security performance. However, the SSCA model consistently exhibits higher AUC values compared to the existing models across different user levels. For instance, at the 100 user level, the AUC value for SSCA is 0.935, while the AUC values for MHE-IS-CPMT, EAM, SCSS, and SHCEF are 0.892, 0.801, 0.822, and 0.834, respectively.

### 3) RELIABILITY

The term "reliability" refers to the ability of a system to consistently perform its intended tasks over time. In the context of information security, "dependability" is a measure

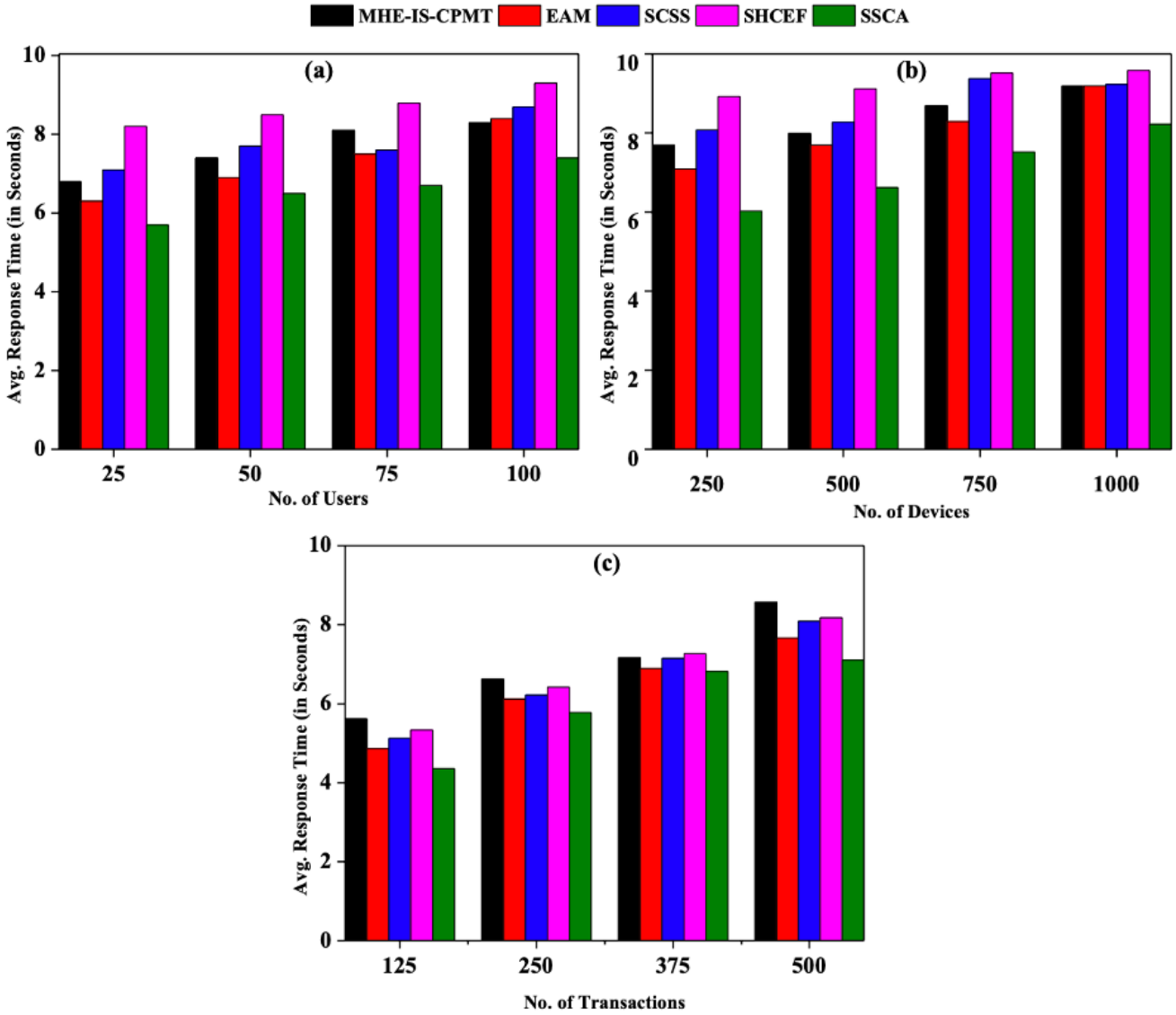


**FIGURE 3.** (a) Average value of ($\tau$) Vs Number of Users, (b) Average value of ($\tau$) Vs Number of Devices, and (c) Average value of ($\tau$)Vs Number of Transaction.

of reliability and is often expressed as a percentage representing the amount of downtime experienced by the system due to security incidents or attacks. Thus, reliability is the rate at which a system continues to function normally without malfunction over time. The following equation (11) computation can be used to calculate the dependability.

$$R_t = e^{[FU]]} \tag{11}$$

where the various factors such as the $R_t$ is the reliability at time $t$, $F$ is the failure rate and $U$ is the uptime duration of system. The failure rate represents the average number of breakdowns expected to occur during a specified time interval, typically measured in failures per unit of time (e.g., failures per hour). By dividing the total number of system failures by the total operational time of the system, we can estimate the frequency at which failures occur due to attack consequences, as expressed by Eq. (12).

$$\phi = \frac{\varphi}{\xi} \tag{12}$$

where, $\phi$ denotes the frequency of system failures due to attack consequences, $\varphi$ signifies the number of system failures due to attack consequences, and $\xi$ indicates the total duration of system uptime.

We evaluate the reliability ($R$) and the incidence of system failures due to attack consequences ($\phi$) for different values of system uptime ($U$) by plotting a graph with the duration of system uptime on the y-axis and the rate of system failures due to attack consequences on the x-axis. This allows us to assess the system's reliability over time.

Figure 5 compares the reliability measures of 10 events between the existing models MHE-IS-CPMT, EAM, SCSS,

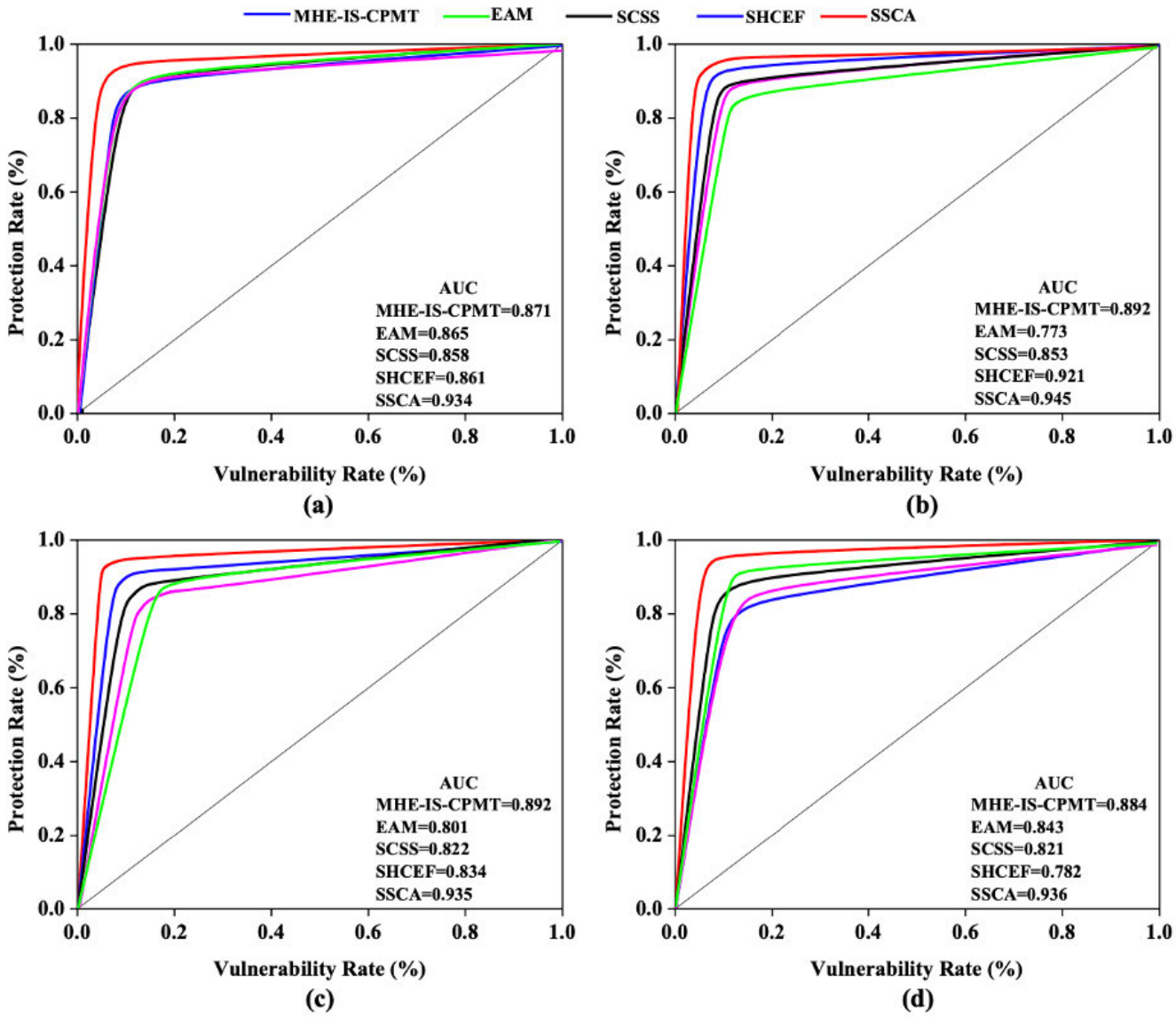


**FIGURE 4.** A comparison of the security utilizing the Area under the curve(AUC). (a) AUC at 25 User Level, (b) AUC at 50 User Level, (c) AUC at 75 User Level, and (d) AUC at 100 User Level.

SHCEF, and the proposed SSCA. In this comparison, the model with the lowest percentage on the X-axis and the highest percentage on the Y-axis is considered the most reliable. The results show that the proposed SSCA exhibits a lower percentage on the X-axis and a higher percentage on the Y-axis compared to the other models. This indicates that the proposed SSCA outperforms the others in terms of achieving optimal reliability. It demonstrates greater resilience to attacks and faster recovery from system failures caused by attacks, leading to fewer instances of downtime.

Moreover, the proposed method is compared with the state-of-the-art methods used in this research are summarized in Table 4.

The comparison shows that the proposed method has achieved the finest performance in terms of high reliability with the secured performance, very less response time and high prediction rate, less overall execution, and very less complexity over the earlier methods. In Sharma et al. [34] work, the consequences show that the reliability is moderate, response time is more and high complexity, these lead to poor security and hackers can easily gather the user's data. similarly, Sarker et al. [21], Wu et al. [35], Irshad and Chaudhry [38], Uppuluri and Lakshmeeswari [40], Sharma et al. [42], Jalasri and Lakshmanan [44] research methods also gained moderate and very less level of reliability performance. The Unal et al. [37], Ahmad et al. [39], Selvarajan et al. [43] research methods have attained high-reliability performance. However, the other significant metrics failed to improve in secured transmissions like high response and execution time with less prediction rate. Yet, the proposed method has achieved reliable performance in overall works due to its effective threat detection and

**TABLE 4.** A comparative study of the proposed SSCA with the cutting-edge security approaches.

| 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. [21] | IntruDTRee | Moderate | 8.05 | 0.812 | 82 | Low |
| Unal et al. [37] | SCSS | High | 7.8 | 0.821 | 75 | Moderate |
| Irshad et al. [38] | EAM | Low | 7.65 | 0.785 | 82 | Moderate |
| Ahmad et al. [39] | KAS-ECC | High | 8.2 | 0.86 | 76 | High |
| Uppuluri et al. [40] | MHE-IS-CPMT | Low | 7.5 | 0.75 | 72 | High |
| Bommu et al [41] | IaaS | Very low | 7.4 | 0.84 | 86 | Moderate |
| Sharma et al [42] | PA | low | 9.5 | 0.79 | 89 | High |
| Selvarajan et al [43] | COSNN-AILBSM | High | 8.94 | 0.895 | 91 | Moderate |
| Jalasri et al [44] | Clustering-noise protocol framework | Low | 7.91 | 0.75 | 85 | High |
| Proposed | SSCA | Very low | 3.85 | 0.975 | 94.5 | Very low |

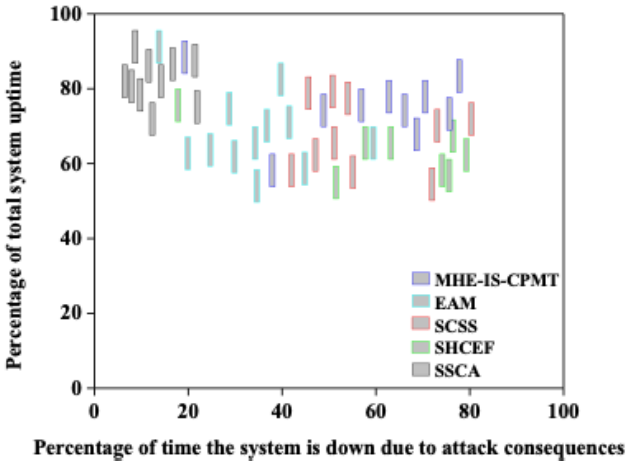


**FIGURE 5.** A comparison of the reliability of the proposed SSCA against the MHE-IS-CPMT, EAM, and SCSS, approaches.

optimal security function. The developed model used the best keys generated by MBRA for PQC encryption and decryption function as well as the blockchain-based hash verification function is applied. Thus, the authorized person is only able to gather and decrypt the data for their use. This method is validated with commonly used real-world data. However, more analysis is needed to show the function of our proposed approach in different scenarios.

## V. CONCLUSION AND FUTURE DIRECTION

In this paper, we introduced the Scalable and Secure Cloud Architecture, a novel IoT-enabled cloud architecture that effectively addressed the multifaceted challenges encompassing scalability, security, and data management within the realm of cloud computing. The proposed architecture combines decentralized cloud nodes, robust MBRA & PQC encryption algorithms, and blockchain technology to ensure efficient handling of user requests, privacy of user information, and secure storage of confidential data. The architecture was specifically designed and rigorously tested to effectively handle large data sets and high-demand scenarios. The evaluation results distinctly showcased the superiority of the proposed SSCA over existing approaches, including MHE-IS-CPMT, EAM, SCSS, and SHCEF, across various performance metrics encompassing response time, scalability, and enhanced security. Specifically, when examining the response times for 250 and 1000 devices, the MHE-IS-CPMT model exhibited response times of 7.69 and 9.19 seconds, whereas the proposed SSCA model displayed significantly improved response times of 6.02 and 8.22 seconds, respectively. This translates to a noteworthy response time enhancement of 1.67 and 0.97 seconds in favor of the SSCA compared to MHE-IS-CPMT. Furthermore, at the 25-user level, the normalized AUC value for SSCA reached 0.934, while the normalized AUC values for MHE-IS-CPMT, EAM, SCSS, and SHCEF were 0.871, 0.865, 0.858, and 0.861, respectively. Correspondingly, at the 50-user level, SSCA achieved a normalized AUC value of 0.936, while the normalized AUC values for MHE-IS-CPMT, EAM, SCSS, and SHCEF were 0.884, 0.843, 0.821, and 0.782. These results imply that SSCA outperformed other models, improving AUC values by 6.30%, 6.90%, 7.60%, and 7.30% for the 25-user level, and 5.20%, 9.30%, 11.50%, and 15.40% for the 50-user level when compared to MHE-IS-CPMT, EAM, SCSS, and SHCEF models, respectively.

However, it is worth noting that while the proposed SSCA has been evaluated with sufficient datasets, further assessments over larger datasets and the incorporation of auto-scaling features would contribute to gauging the architecture's scalability. This future direction aims to test

SSCA's capacity to manage even more extensive datasets and support increasingly complex programs. Thus, prospective enhancements to SSCA will involve integrating auto-scaling functionalities alongside security algorithms, and rigorous testing across a diverse range of datasets and user profiles to ensure the provision of reliable, secure, and scalable cloud services.

## ACKNOWLEDGMENT

The authors are thankful to the Deanship of Scientific Research at Najran University for funding this work, under the Distinguish Research Funding Program grant code (NU/DRP/SERC/12/11).

## REFERENCES

[1] A. Gutierrez, E. Boukrami, and R. Lumsden, "Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the U.K.," *J. Enterprise Inf. Manage.*, vol. 28, no. 6, pp. 788–807, Oct. 2015.

[2] A. Benlian, W. J. Kettinger, A. Sunyaev, and T. J. Winkler, "Special section: The transformative value of cloud computing: A decoupling, platformization, and recombination theoretical framework," *J. Manage. Inf. Syst.*, vol. 35, no. 3, pp. 719–739, Jul. 2018.

[3] X. Luo, S. Zhang, and E. Litvinov, "Practical design and implementation of cloud computing for power system planning studies," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2301–2311, Mar. 2019.

[4] S. A. El-Seoud, H. F. El-Sofany, M. Abdelfattah, and R. Mohamed, "Big data and cloud computing: Trends and challenges," *Int. J. Interact. Mobile Technol.*, vol. 11, no. 2, pp. 1–19, 2017.

[5] K. K. Patel, S. M. Patel, and P. Scholar, "Internet of Things-IoT: Definition, characteristics, architecture, enabling technologies, application & future challenges," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 1–10, 2016.

[6] S. N. Shirazi, A. Gouglidis, A. Farshad, and D. Hutchison, "The extended cloud: Review and analysis of mobile edge computing and fog from a security and resilience perspective," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2586–2595, Nov. 2017.

[7] B. H. Krishna, S. Kiran, G. Murali, and R. P. K. Reddy, "Security issues in service model of cloud computing environment," *Proc. Comput. Sci.*, vol. 87, pp. 246–251, Jan. 2016.

[8] D. Zeginis, F. D'Andria, S. Bocconi, J. G. Cruz, O. C. Martin, P. Gouvas, G. Ledakis, and K. A. Tarabanis, "A user-centric multi-PaaS application management solution for hybrid multi-cloud scenarios," *Scalable Comput., Pract. Exp.*, vol. 14, no. 1, pp. 17–32, Apr. 2013.

[9] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud computing: Security issues and research challenges," *Int. J. Comput. Sci. Inf. Technol. Secur.*, vol. 1, no. 2, pp. 136–146, 2011.

[10] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quart.*, vol. 34, no. 3, pp. 523–548, 2010.

[11] R. F. Smallwood, *Information Governance: Concepts, Strategies, and Best Practices*. Hoboken, NJ, USA: Wiley, 2019.

[12] S. Asadi, M. Nilashi, A. R. C. Husin, and E. Yadegaridehkordi, "Customers perspectives on adoption of cloud computing in banking sector," *Inf. Technol. Manage.*, vol. 18, no. 4, pp. 305–330, Dec. 2017.

[13] S. Achar, "Cloud computing security for multi-cloud service providers: Controls and techniques in our modern threat landscape," *Int. J. Comput. Syst. Eng.*, vol. 16, no. 9, pp. 379–384, 2022.

[14] S. M. Shah and R. A. Khan, "Secondary use of electronic health record: Opportunities and challenges," *IEEE Access*, vol. 8, pp. 136947–136965, 2020.

[15] J. J. M. Seddon and W. L. Currie, "Cloud computing and trans-border health data: Unpacking U.S. and EU healthcare regulation and compliance," *Health Policy Technol.*, vol. 2, no. 4, pp. 229–241, Dec. 2013.

[16] Y. Zhao, R. N. Calheiros, A. V. Vasilakos, J. Bailey, and R. 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*. San Diego, CA, USA: Springer, Jun. 2019, pp. 26–47.

[17] F.-K. Wang and W. He, "Service strategies of small cloud service providers: A case study of a small cloud service provider and its clients in Taiwan," *Int. J. Inf. Manage.*, vol. 34, no. 3, pp. 406–415, Jun. 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 Comput.*, vol. 22, no. S4, pp. 9737–9753, Jul. 2019.

[19] A. K. M. B. Haque, B. Bhushan, and G. Dhiman, "Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends," *Expert Syst.*, vol. 39, no. 5, Jun. 2022, Art. no. e12753.

[20] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Inf. Syst.*, vol. 48, pp. 132–150, Mar. 2015.

[21] I. H. Sarker, Y. B. Abushark, F. Alsolami, and A. I. Khan, "IntruDTree: A machine learning based cyber security intrusion detection model," *Symmetry*, vol. 12, no. 5, p. 754, May 2020.

[22] O. Yousuf and R. N. Mir, "A survey on the Internet of Things security: State-of-art, architecture, issues and countermeasures," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 292–323, Jun. 2019.

[23] A. K. Pandey, A. I. Khan, Y. B. Abushark, M. M. Alam, A. Agrawal, R. Kumar, and R. A. Khan, "Key issues in healthcare data integrity: Analysis and recommendations," *IEEE Access*, vol. 8, pp. 40612–40628, 2020.

[24] S. Gusmeroli, S. Piccione, and D. Rotondi, "A capability-based security approach to manage access control in the Internet of Things," *Math. Comput. Model.*, vol. 58, nos. 5–6, pp. 1189–1205, Sep. 2013.

[25] K. Chard, S. Tuecke, and I. Foster, "Efficient and secure transfer, synchronization, and sharing of big data," *IEEE Cloud Comput.*, vol. 1, no. 3, pp. 46–55, Sep. 2014.

[26] A. Rahman, M. J. Islam, S. S. Band, G. Muhammad, K. Hasan, and P. Tiwari, "Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT," *Digit. Commun. Netw.*, vol. 9, no. 2, pp. 411–421, Apr. 2023.

[27] G. Kuldeep and Q. Zhang, "Multi-class privacy-preserving cloud computing based on compressive sensing for IoT," *J. Inf. Secur. Appl.*, vol. 66, May 2022, Art. no. 103139.

[28] L. Malina, L. Popelova, P. Dzurenda, J. Hajny, and Z. Martinasek, "On feasibility of post-quantum cryptography on small devices," *IFAC-PapersOnLine*, vol. 51, no. 6, pp. 462–467, 2018.

[29] F. Zhang, H. Wang, L. Zhou, D. Xu, and L. Liu, "A blockchain-based security and trust mechanism for AI-enabled IIoT systems," *Future Gener. Comput. Syst.*, vol. 146, pp. 78–85, Sep. 2023.

[30] T. Nouioua and A. H. Belbachir, "The quantum computer for accelerating image processing and strengthening the security of information systems," *Chin. J. Phys.*, vol. 81, pp. 104–124, Feb. 2023.

[31] A. E. Azzaoui, P. K. Sharma, and J. H. Park, "Blockchain-based delegated quantum cloud architecture for medical big data security," *J. Netw. Comput. Appl.*, vol. 198, Feb. 2022, Art. no. 103304.

[32] S. Suhail, R. Hussain, A. Khan, and C. S. Hong, "On the role of hash-based signatures in quantum-safe Internet of Things: Current solutions and future directions," *IEEE Internet Things J.*, vol. 8, no. 1, pp. 1–17, Jan. 2021.

[33] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013.

[34] A. Sharma, T. Goyal, E. S. Pilli, A. P. Mazumdar, M. C. Govil, and R. C. Joshi, "A secure hybrid cloud enabled architecture for Internet of Things," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, Dec. 2015, pp. 357–362.

[35] H.-L. Wu, C.-C. Chang, Y.-Z. Zheng, L.-S. Chen, and C.-C. Chen, "A secure IoT-based authentication system in cloud computing environment," *Sensors*, vol. 20, no. 19, p. 5604, Sep. 2020.

[36] L. Zhou, X. Li, K.-H. Yeh, C. Su, and W. Chiu, "Lightweight IoT-based authentication scheme in cloud computing circumstance," *Future Gener. Comput. Syst.*, vol. 91, pp. 244–251, Feb. 2019.

[37] D. Unal, A. Al-Ali, F. O. Catak, and M. Hammoudeh, "A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption," *Future Gener. Comput. Syst.*, vol. 125, pp. 433–445, Dec. 2021.

[38] A. Irshad and S. A. Chaudhry, "Comment on 'ElGamal cryptosystem-based secure authentication system for cloud-based IoT applications,'" *IET Netw.*, vol. 10, no. 5, pp. 244–245, Sep. 2021.

[39] S. Ahmad, S. Mehfuz, and J. Beg, "Hybrid cryptographic approach to enhance the mode of key management system in cloud environment," *J. Supercomput.*, vol. 79, no. 7, pp. 7377–7413, May 2023.

[40] S. Uppuluri and G. Lakshmeeswari, "Secure user authentication and key agreement scheme for IoT device access control based smart home communications," *Wireless Netw.*, vol. 29, no. 3, pp. 1333–1354, Apr. 2023.

[41] S. Bommu, M. A. Kumar, K. Babburu, N. Srikanth, L. N. Thalluri, G. V. Ganesh, A. Gopalan, P. K. Mallapati, K. Guha, H. R. Mohammad, and S. S. Kiran, "Smart city IoT system network level routing analysis and blockchain security based implementation," *J. Electr. Eng. Technol.*, vol. 18, no. 2, pp. 1351–1368, Mar. 2023.

[42] P. Sharma, S. Namasudra, R. G. Crespo, J. Parra-Fuente, and M. C. Trivedi, "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," *Inf. Sci.*, vol. 629, pp. 703–718, Jun. 2023.

[43] S. Selvarajan, G. Srivastava, A. O. Khadidos, A. O. Khadidos, M. Baza, A. Alshehri, and J. C.-W. Lin, "An artificial intelligence lightweight blockchain security model for security and privacy in IIoT systems," *J. Cloud Comput.*, vol. 12, no. 1, p. 38, Mar. 2023.

[44] M. Jalasri and L. Lakshmanan, "Managing data security in fog computing in IoT devices using noise framework encryption with power probabilistic clustering algorithm," *Cluster Comput.*, vol. 26, no. 1, pp. 823–836, Feb. 2023.

[45] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy, and A. A. A. El-Latif, "Convergence of blockchain and IoT for secure transportation systems in smart cities," *Secur. Commun. Netw.*, vol. 2021, pp. 1–13, Apr. 2021.

[46] R. R. Irshad, S. Hussain, S. S. Sohail, A. S. Zamani, D. Ø. Madsen, A. A. Alattab, A. A. A. Ahmed, K. A. A. Norain, and O. A. S. 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*, vol. 23, no. 6, p. 2932, Mar. 2023.

[47] R. R. Irshad, S. Hussain, I. Hussain, I. Ahmad, A. Yousif, I. M. Alwayle, A. A. Alattab, K. M. Alalayah, J. G. Breslin, M. M. Badr, and J. J. P. C. Rodrigues, "An intelligent buffalo-based secure edge-enabled computing platform for heterogeneous IoT network in smart cities," *IEEE Access*, vol. 11, pp. 69282–69294, 2023.

[48] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, and R. Hansen, "Transitioning organizations to post-quantum cryptography," *Nature*, vol. 605, no. 7909, pp. 237–243, May 2022.

[49] O. Alkadi, N. Moustafa, B. Turnbull, and K. R. Choo, "A deep blockchain framework-enabled collaborative intrusion detection for protecting IoT and cloud networks," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9463–9472, Jun. 2021.

[50] A. Ali, M. F. Pasha, J. Ali, O. H. Fang, M. Masud, A. D. Jurcut, and M. A. Alzain, "Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography," *Sensors*, vol. 22, no. 2, p. 528, Jan. 2022.

[51] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Comput. Appl.*, vol. 34, pp. 11475–11490, Jul. 2022.

[52] S. Kumari, M. Singh, R. Singh, and H. Tewari, "Post-quantum cryptography techniques for secure communication in resource-constrained Internet of Things devices: A comprehensive survey," *Softw., Pract. Exp.*, vol. 52, no. 10, pp. 2047–2076, Oct. 2022.

[53] U. Khalil, M. Uddin, O. A. Malik, and S. Hussain, "A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions," *IEEE Access*, vol. 10, pp. 76805–76823, 2022.

[54] C. A. Lara-Nino, M. Morales-Sandoval, and A. Diaz-Perez, "Post-quantum cryptography on wireless sensor networks: Challenges and opportunities," in *Integration of WSNs Into Internet of Things*. Boca Raton, FL, USA: CRC Press, 2021, pp. 81–99.

[55] I. Memon, M. R. Mohammed, R. Akhtar, H. Memon, M. H. Memon, and R. A. Shaikh, "Design and implementation to authentication over a GSM system using certificate-less public key cryptography (CL-PKC)," *Wireless Pers. Commun.*, vol. 79, no. 1, pp. 661–686, Nov. 2014.

[56] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[57] R. R. Irshad, S. S. Sohail, S. Hussain, D. Ø. Madsen, M. A. Ahmed, A. A. Alattab, O. A. S. Alsaiari, K. A. A. Norain, and A. A. A. Ahmed, "A multi-objective bee foraging learning-based particle swarm optimization algorithm for enhancing the security of healthcare data in cloud system," *IEEE Access*, early access, Apr. 10, 2023, doi: 10.1109/ACCESS.2023.3265954.

[58] L. Kong, L. He, X.-Y. Liu, Y. Gu, M.-Y. Wu, and X. Liu, "Privacy-preserving compressive sensing for crowdsensing based trajectory recovery," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst.*, Jun. 2015, pp. 31–40.

[59] M. E. Saleh, A. A. Aly, and F. A. Omara, "Data security using cryptography and steganography techniques," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 6, pp. 1–8, 2016.

[60] G. Kanda and K. Ryoo, "Vedic multiplier-based international data encryption algorithm crypto-core for efficient hardware multiphase encryption design," *Webology*, vol. 19, no. 1, pp. 4581–4596, Jan. 2022.

[61] B. Gipp, N. Meuschke, and A. Gernandt, "Decentralized trusted timestamping using the crypto currency Bitcoin," 2015, *arXiv:1502.04015*.

[62] H. Cho, "ASIC-resistance of multi-hash proof-of-work mechanisms for blockchain consensus protocols," *IEEE Access*, vol. 6, pp. 66210–66222, 2018.

[63] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 2, p. 162, Jan. 2018.

[64] P. Geetha, V. S. Jayanthi, and A. N. Jayanthi, "Optimal visual cryptographic scheme with multiple share creation for multimedia applications," *Comput. Secur.*, vol. 78, pp. 301–320, Sep. 2018.

[65] R. R. Irshad, S. Hussain, I. Hussain, A. A. Alattab, A. Yousif, O. A. S. Alsaiari, and E. I. I. Ibrahim, "A novel artificial spider monkey based random forest hybrid framework for monitoring and predictive diagnoses of patients healthcare," *IEEE Access*, vol. 11, pp. 77880–77894, 2023.

[66] N. Albishry, R. AlGhamdi, A. Almalawi, A. I. Khan, P. R. Kshirsagar, and B. D. Bejena, "An attribute extraction for automated malware attack classification and detection using soft computing techniques," *Comput. Intell. Neurosci.*, vol. 2022, Apr. 2022, Art. no. e5061059.

[67] Numenta. *Numenta Anomaly Benchmark*. Accessed: May 10, 2023. [Online]. Available: https://www.numenta.com/resources/htm/numenta-anomoly-benchmark/

**REYAZUR RASHID IRSHAD** received the B.Sc. degree from Aligarh Muslim University, Aligarh, India, in 2000, and the master's degree in computer application from Indira Gandhi University, New Delhi, India, in 2010. He is currently pursuing the Ph.D. degree with JJT University, Rajasthan. He is a Lecturer with the Department of Computer Science, Najran University, Saudi Arabia. He has published many articles in reputed journals and has attended some conferences. His research interest includes web-based applications.

**SHAHID HUSSAIN** received the B.S. degree in mathematics and the M.Sc. degree in computer science from the University of Peshawar, in 2002 and 2005, respectively, and the M.S. and Ph.D. (Hons.) degrees in computer engineering from Jeonbuk National University, South Korea, in 2016 and 2020, respectively. He was a Postdoctoral Researcher with the Gwangju Institute of Science and Technology (GIST), South Korea, in 2020, and the University of Galway (UoG), Ireland, from 2020 to 2022. He is currently a Senior Postdoctoral Researcher with the Innovative Value Institute (IVI), School of Business, National University of Ireland Maynooth (NUIM), Ireland. His research interests include smart grids, energy management, electric vehicles, smart grid infrastructure, optimization algorithms, micro-grid operations, distributed energy resources, peer-to-peer energy trading, and machine learning in medical applications (e.g., prediction and risk analysis of osteoporosis) using fuzzy logic, game theory, ontology, AI, and blockchain approaches and technologies. He achieved the Jeonbuk National University Presidential Award for academic excellence during his Ph.D. studies.

**IHTISHAM HUSSAIN** is currently pursuing the B.S. degree in computer science with Abdul Wali Khan University Mardan, Khyber Pakhtunkhwa, Pakistan. He has participated in several coding competitions, hackathons, internships, and projects. Besides his academic interests, he is a Devoted Programmer and a Technology Enthusiast, continuously investigating new tools and approaches to enhance his coding talents. His research interests include artificial intelligence and machine learning applications in a variety of fields, such as bioinformatics, energy, and business.

**JAMAL ABDUL NASIR** received the Ph.D. degree from the Computer Science Department, Syed Babar Ali School of Science and Engineering (LUMS), Lahore, Pakistan. He was an Assistant Professor with the Department of Computer Science and Software Engineering, International Islamic University, Islamabad, Pakistan. He is currently an Assistant Professor with the School of Computer Science, University of Galway, Ireland. His research interests include text categorization and clustering, text summarization, sentiment analysis, lexical expansions using contextualization, uplift modeling in bioinformatics, data mining, and machine-learning algorithms and applications.

**ASIM ZEB** received the B.Sc. and M.Sc. degrees in computer science from the University of Peshawar (UOP), Pakistan, in 2002 and 2005, respectively, and the Ph.D. degree in computer science from the University of Technology Malaysia, in 2016. From 2014 to 2015, he was a Research Fellow with the Nagoya Institute of Technology, Japan. From February 2016 to April 2019, he was an Assistant Professor with the Qurtuba University of Science and IT. Since May 2019, he has been an Assistant Professor with the Department of Computer Science, Abbottabad University of Science and Technology, Pakistan. His research interests include self-organized networks, network architectures and protocols, and supervised machine-learning techniques. From 2013 to 2014, he received the MJIIT-Malaysia Scholarship and JASSO-Japan Scholarship from 2014 to 2015.

**KHALED M. ALALAYAH** received the B.Sc. and M.Sc. degrees in computer science from the University of Technology, Baghdad, Iraq, in 1999 and 2003, respectively, and the Ph.D. degree from Menoufia University, Egypt, in 2011. He is currently an Assistant Professor with the Department of Computer Science, Najran University, Saudi Arabia. He is also an Assistant Professor with Ibb University, Yemen. He has published many articles in reputed journals and conferences. His research interests include information security, data mining, image processing, and neural networks.

**AHMED ABDU ALATTAB** received the B.Sc. degree in computer science from the University of Baghdad, Baghdad, Iraq, in 1997, the M.Sc. degree in computer science from the University of Technology, Baghdad, in 2002, and the Ph.D. degree in computer science-artificial intelligence from the University of Malaya, Kuala Lumpur, Malaysia, in 2013. He is currently an Assistant Professor with the Department of Computer Science, Najran University, Saudi Arabia. He is also an Assistant Professor with Thamar University, Yemen. He has published many articles in reputed journals and conferences. His research interests include artificial intelligence image processing, image retrieval, image classification, object recognition, deep learning, natural language processing, computer vision, and neural networks.

**ADIL YOUSIF** received the B.Sc. and M.Sc. degrees from the University of Khartoum, Sudan, and the Ph.D. degree from the University of Technology in Malaysia (UTM). He is currently an Associate Professor with the College of Arts and Sciences Sharourah, Najran University, Saudi Arabia. He is also the Principal Investigator of several research projects in artificial intelligence and emerging technologies. His research interests include computer networks, cloud computing, artificial intelligence, and optimization techniques.

**IBRAHIM M. ALWAYLE** received the B.Sc. degree in mathematics from San'aa University, Yemen, in 1999, and the M.Sc. and Ph.D. degrees in computer science from Al Mansurah University, Egypt, in 2004 and 2008, respectively. He is an Assistant Professor with the Department of Computer Science, Najran University, Saudi Arabia. He is permanently an Assistant Professor with Amran University, Yemen. His research focuses on pattern recognition, image processing, and AI.