Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 08:2025
DOI: 10.5281/zenodo.16925275

IoT-ENABLED SECURE AND SCALABLE CLOUD ARCHITECTURE FOR MULTI-USER SYSTEMS: A HYBRID POST-QUANTUM CRYPTOGRAPHIC AND BLOCK CHAIN BASED APPROACH TOWARDS A TRUSTWORTHY CLOUD COMPUTING

PONNARASAN KRISHNAN
Senior Developer, Acentra Health, USA.

Abstract

Cloud computing, by definition, provides on-demand services-perhaps the most revolutionary change in the provisioning of resources for an enterprise in recent decades. The rise of the IoT has ushered in a new age of collaborative computing formed by multiple networks of smart sensors and devices capable of generating and processing huge data volumes. On the other hand, this creates another set of problems related to data volume and security, making the security mechanisms even more capitalized. In this research, a novel Scalable and Secure Cloud Architecture (SSCA) is proposed, integrating IoT and advanced cryptographic mechanisms to design highly available, multi-user cloud systems. The architecture works in a distributed mode in the cloud, allowing several cloud nodes to serve user requests efficiently while using the Multicast and Broadcast Rekeying Algorithm (MBRA) to uphold privacy and confidentiality of users. The proposed cryptosystem combines MBRA, Post-Quantum Cryptography (PQC), and blockchain technologies. The IoT devices gather data in a distributed sensing network secured by MBRA-PQC encryption, while the blockchain ensures immutability and distributed integrity of the data.

Keywords: Advanced Cloud-Based Models, Internet of Things (IoT), Next-Generation Cryptography, Big Data & Analytics or AI, Distributed systems, Modular Systems.

1. INTRODUCTION

1.1 Overview of Cloud-IoT Integration

Cloud computing has recently been the topic of discussion on how organizations deal with information, processing, and storage by permitting capital-less infrastructure to be discouraged in favor of internet resources [1–3]. Thus, the theory intends to allow firms and individuals to operate the systems remotely for computing and storage and scale them accordingly in response to needs arising through demand change [4–6]. In rapid growth, induced by an expansion in IoT, smart sensors, actuators, and detectors create big, heterogeneous data sets requiring robust management systems. The cloud has the properties of scaling, adapting, and cost-effectiveness for working with such enormous data.

The cloud service models consist of three main categories SaaS, PaaS, and IaaS--each suitable for a different spectrum of operational requirements [7]. On the other hand, deployment methods provide different degrees of control, customization, and security: public, private, hybrid, and multi-cloud [8, 9]. An organization must be conversant with the models to ensure that technical solutions follow the business objectives and adhere to its legal constraints and compliance frameworks such as GDPR and HIPAA [10–15]. Cloud adoption requires not only the infrastructure but also governance policies addressing data lifecycle management, access, lawful retention, or deletion of data.

1.2 Breeding Need for Cloud Security

The collaboration of IoT and cloud systems suffers increased risk levels, coming under attack from hacking, unauthorized access, or targeted cyber-attacks [18–20]. Protecting sensitive data in multi-user environments calls for a highly specialized security framework which adjusts dynamically to changes in workload while becoming available for service at the present time. Employing the modern method includes encryptions in transit and at rest, detection of intrusion, and verifying identity. Providers utilize layered security approaches such as access control protocols, backup policies, and recovery mechanisms to respond to new threats [12-15].

Cost efficiency persists as a parallel concern. Pay-as-you-go and reserved-instance pricing models help organizations control costs, while automatic resource allocation ensures that resources are used optimally [16, 17]. Next-generation cloud security schemes must also address future challenges, particularly those posed by quantum computing to classical encryption. This will force research into next-generation cryptographic techniques able to secure massive and fast-moving IoT datasets without compromising performance.

1.3 Research Motivation and Contribution

The proliferation of the IoT has further propelled demand for cloud architectures that support many concurrent users and device types [21–25]. Multi-users' environments pose a set of challenges, including differentiated access control, scalability under heavy load, and privacy preservation over a shared infrastructure. The solution behind this study implements a hybrid framework called Scalable and Secure Cloud Architecture (SSCA) that incorporates PQC-based mechanisms and blockchain as well as the MBRA [28–33].

PQC-blockchain hybrid guarantees end-to-end confidentiality, data immutability, and tamper-resistant storage, whereas MBRA provides efficient and secure rekeying for group communications. The whole architecture goes on a distributed-cloud model and assures fast response time, balanced resource utilization, and access control authorized only to users. Interoperability is also present, with the design allowing ingestion of real-time data from different sensing networks spread across different IoT domains. The SSCA ultimately aims to evolve into a future-ready quantum-resilient platform for secure, scalable, and trustworthy IoT-cloud integration.

2. LITERATURE REVIEW

The cloud-IoT twin has been a fertile theory in computer science, for numerous architectures have been proposed that are scalable and secure. This kind of system whereby multiple devices, sensors, and users interact with distributed cloud resources generate a very complex environment with ever-demanding availability, performance, and protection needs to evolve with cyber threats. While cloud systems provide flexibility and demand-based scalability, integrating with IoT opens up avenues for multi-user access vulnerabilities, management of heterogeneous devices, and privacy issues.

2.1 Hybrid Cloud Architectures for IoT

A Secure Hybridized Cloud-Enabled Framework (SHCEF) was proposed by Sharma et al. [34] integrating both public and private cloud infrastructures to handle privacy, scalability, and connectivity aspects in the IoT ecosystem. The SHCEF was directed toward use cases such as smart healthcare, home automation, and agricultural monitoring. Since its design was a dual-cloud one, it allowed sensitive data to be processed in private clouds while less critical workloads were handled in public clouds. However, from their perspective, hybrid models have various integration and management problems, especially in coordinating a set of distributed resources over heterogeneous networks.

Wu et al. [35] decided to critically assess the Zhou et al. [36] approach, noting weaknesses in the areas of mutual verification and anonymity protection. Their improved authentication framework counteracts the threat of inaccurate or malicious input from entering the process by introducing an additional detection parameter in communication. The new approach to IoT-cloud authentication comes with better computational efficiency and more power against impersonation, allowing good but lightweight verification mechanisms available for open IoT environments.

2.2 Anomaly Detection and Machine Learning Approaches

Machine learning, in fact, is increasingly being considered for improvements in IoT-cloud security. Sarkar et al. [37] developed IntruDTRee, an intrusion detection tree-based model optimized for scalability and computational efficiency. Tested against real-world cybersecurity datasets, IntruDTRee reduced false positives yet maintained a high detection accuracy for unknown threats. This further makes it more appropriate in large-scale, resource-constrained IoT environments where usual IDSs fail owing to computational issues.

In parallel, Unal et al. [38] describe the Secure Cloud Storage Scheme (SCSS) that integrated identity-based cryptography (IBC) with decentralized key management. SCSS could tackle the large-scale PKI latency and overhead problem by deploying key management policies across multiple Public Key Generators (PKGs). This decentralized approach enhanced fault tolerance and forensic readiness, thus easing post-incident investigations without bringing down the system performance.

2.3 Authentication Mechanisms for IoT-Cloud Environments

Irshad et al. [39] proposed an EAM-ElGamal-based Authentication Method in the SAS-Cloud framework. EAM combined passcode and biometric authentication techniques to ensure multi-factor verification in the IoT-cloud environment. SAS-Cloud was considered to have strong resistance against replay-attack, unauthorized access, and identity-spoofing while keeping efficient operationally.

It is Ahmad et al. [40] who potently posited a level-2 cryptographic model where ECC was employed alongside AES. Such a hybrid system created a more manageable key system and superior in efficiency toward key management and ciphering/deciphering, while it held a good attraction to the cryptanalytic attacks. The authors noted its usefulness particularly for healthcare data security, where speed, integrity, and confidentiality are paramount.

Uppuluri et al. [41] introduced the Modified Honey Encryption–Inverse Sampling Conditional Probability Model Transform (MHE-IS-CPMT), which was combined with ECC to perform secure key exchange in smart home IoT environments. This kind of system operates in four phases—initialization, enrollment, login, and credential renewal—such that it supports mutual authentication and key rotation throughout the lifetime of the deployed devices.

2.4 Blockchain-Integrated IoT Security Models

Increasing attention has been drawn to blockchain solutions for data integrity, transparency, and tamper resistance in IoT-cloud systems. Bomu et al. [42] built an IaaS-based smart city IoT system to detect transportation, air quality, noise pollution, and health metrics. The blockchain layer ensured secure transaction logging, while the network topology was optimized to enhance QoS.

Namasudra et al. [2023] put forward a blockchain-secure-solution for the protection of healthcare documents within IoT digital ecosystems. The solution dealt with the problem of data authenticity by means of encryption and immutable ledger records. Along similar lines, Srivastava et al. [2023] put forth a lightweight blockchain–AI hybrid to secure IIoT capable of being run on battery-powered resource-constrained devices.

Lakshmanan and Jalasri [2023] further enhanced fog computing security using the noise framework for encryption with a probabilistic clustering approach; the technique ensures a tradeoff between stronger encryption and low-latency processing necessary for on-the-fly IoT applications. Abbas et al. [2021] explored blockchain–IoT convergence for the secure-mode transport of the smart city, wherein they consider transaction authentication and tamper-proof storage for mobility data so that the data remain reliable.

2.5 AI-Driven IoT Security Solutions for Healthcare

Irshad et al. [2023] innovatively proposed an AI-enabled healthcare monitoring system over a secure IoT-cloud framework. The design employs deep convolutional neural networks (CNNs) for the early detection of disease while applying optimized encryption algorithms to secure sensitive data of the patient during transmission to the cloud. This system effectively tackles the security aspects of privacy and the needs of real-time processing in healthcare. Post Quantum Cryptography marks a key area in IoT-cloud security as quantum computing poses threats to traditional encryption. David et al. [2022] discussed organizational transition to PQC, while Kumari et al. [2022] took a complete survey of PQC schemes for resource-constrained IoT devices. Being integrated, PQC will provide for future-proof encryption but, on the downside, it will seemingly challenge computational complexity on lightweight devices. Other researchers such as Zhang et al. [2023] and Suhail et al. [2020] have so far looked into hash-based signatures and blockchain-PQC coupling for the IoT in order to maintain data confidentiality and verifiable authenticity at the same time. Lara-Nino et al. [2021] considered PQC in wireless sensor networks, laying weight on its application in securing low-energy devices without compromising efficiency.

2.6 Gaps Identified and Research Direction

These studies, when reviewed, throw light on some recurring patterns:

- Hybrid Architectures – Combining public/private clouds and on-premises infrastructure enhances flexibility but introduces integration complexity and security management overhead.
- Advanced Authentication – Multi-factor and biometric authentication strengthen IoT-cloud systems, yet scalability and computational efficiency remain constraints.
- Blockchain for Integrity – Blockchain's immutability is valuable for IoT, but latency and storage requirements can limit adoption in high-speed systems.
- Machine Learning for Threat Detection – AI and ML models improve threat detection accuracy, but require careful resource optimization for IoT devices.
- Post-Quantum Security – PQC offers quantum-resilient encryption, yet real-world deployment in IoT remains in early stages due to computational costs.

While great progress has been made, the design of a single architecture that would integrate the dimensions of scale, security, and efficiency is still to come. Many models are good at one thing, for example, authentication, data integrity, or scalability. But when it comes to putting all these characteristics together into an operational whole, they fall short. The Scalable and Secure Cloud Architecture (SSCA) proposed in this study bridges this gap by integrating PQC and blockchain and MBRA as a distributed IoT-cloud infrastructure. It is meant to provide real-time responses, quantum-resistant security, and multi-user scalability, thereby overcoming the drawbacks of the present designs.

3. METHODOLOGY

The initiative was launched to create a system based on scalable, secure cloud architecture that would address the two main challenges in a multi-user Internet of Things environment: scalability and security. The key consideration in designing such a system is that secure architecture should never work to defend against only today's cyber-threats but should stand in advance of emerging and future ones, such as those from quantum computing. To this end, the SSCA combines a matrix of Post-Quantum Cryptography (PQC), blockchain technology, and an adaptive threat detection and response algorithm called the Multicast Broadcast Rekeying Algorithm (MBRA). Together, these aspects are knit into a distributed cloud environment with high throughput, capable of supporting enormous numbers of IoT devices and concurrent users.

3.1 Architectural Design and Operational Philosophy

The very core of SSCA is a distributed cloud infrastructure consisting of interconnected nodes. The decentralization ensures that none of the nodes can become a bottleneck or single point of failure, thereby providing resilience and increased service availability. By eliminating the risks associated with being centralized, the architecture provides a sturdy foundation for essential IoT deployments where any downtime is unacceptable. IoT devices connecting to SSCA could range from sensors and detectors to actuators, RFID readers, cameras, and regulatory control units. These devices encompass a multitudinous collection of operational domains such as healthcare, industrial automation, transportation, and environmental monitoring. They continuously generate streams of heterogeneous data from small telemetry packets to high-resolution video, which is securely transmitted for processing and storage over the cloud infrastructure. In fine, the data flow can be summarized thus: device data is collected at the edge, transmitted through secure channels using PQC encryption, processed in the cloud, and asserted into the blockchain for immutable record-keeping. This precise multiway security way ensures that from data acquisition to its retrieval, data is maintained in integrity, confidentiality, and authentication. Figure 1 represents an SSCA wherein IoT devices interface into multiple security layers and then distributed cloud infrastructure. Data streams travel upward from the field to the cloud nodes where the data is encrypted using PQC algorithms before storage in the blockchain. The blockchain nodes log all transaction changes transparently and maliciously, and this becomes the center of trust and verifiability, especially in multi-user environments where provenance matters as much as accuracy.

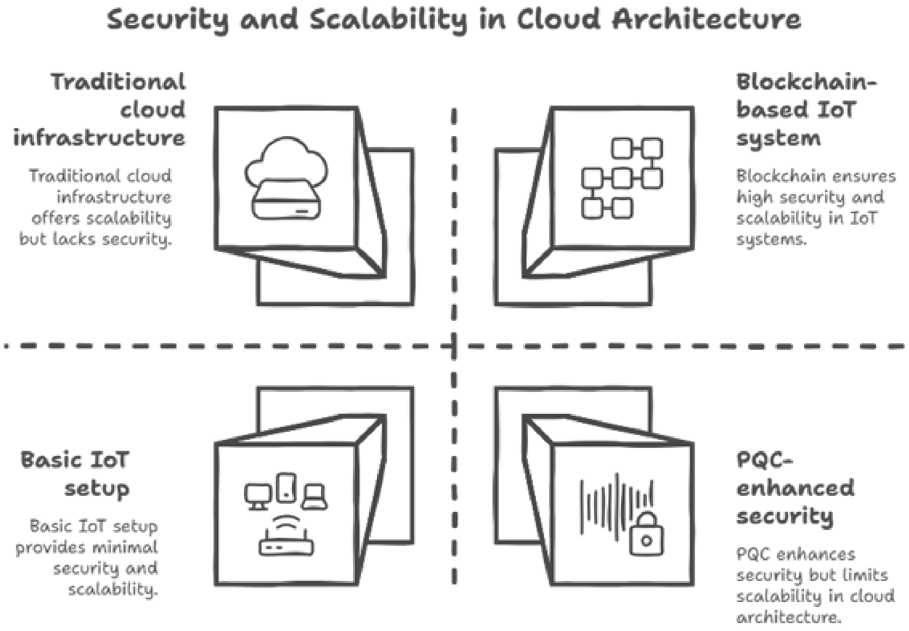
Security and Scalability in Cloud Architecture
Traditional cloud infrastructure
Traditional cloud infrastructure offers scalability but lacks security.
Blockchain-based IoT system
Blockchain ensures high security and scalability in IoT systems.
Basic IoT setup
Basic IoT setup provides minimal security and scalability.
PQC-enhanced security
PQC enhances security but limits scalability in cloud architecture.

Figure 1: A proposed Scalable and Secure Cloud Architecture (SSCA) heavy on PQC, blockchain, and MBRA for multi-user IoT environments.

3.2 Security Layer: PQC for Integrity, Blockchain for Integrity and Provenance, and MBRA for Dynamic Detection and Response

The security framework inside SSCA operates with the Trinity of complementary power: PQC to encrypt, blockchain for integrity and provenance, and MBRA for convergent mode detection, response, and reaction.

Post-Quantum Cryptography (PQC) protects data against adversaries that are purportedly quantum-capable. That is to say, classical cryptographic techniques like RSA and ECC, which are not secure against an attack from a large-scale quantum computer that will come into existence within a couple of decades, whereas PQC schemes are meant to resist. Through the use of PQC, SSCA offers encryption while the IoT data is transmitted, and also when such data is stored, thereby assuring safety against both interception or illegal decryption.

The blockchain technology provides an extra veneer of immutability and verifiability. Every data entry-whether it is a sensor reading or user action-runs through a process of storing the data inside a block that is cryptographically linked to others, creating an eternal tamper-proof chain of custody. Especially in scenarios involving multi-user IoT where shared data needs to be provably authentic and unaltered, this technology holds supreme importance. Through decentralization, a major plank of blockchainSecurity consensus furthered under decentralized architecture of SSCA making it harder for unilateral compromises to be executed as false records.

The Multicast Broadcast Rekeying Algorithm acts as a kind of willing watchdog. It runs nonstop, actively monitoring nodes and suspicious activities therewith assigning a security status score to the anomalies observed. When the threat level that a node pose crosses a certain threshold, MBRA immediately quarantines the node from the network and enters a rekeying phase. During such a rekey, PQC comes into play and generates new sets of cryptographic keys to render the mishandled credentials useless. Interestingly, given its status as a hybrid multicast/broadcast rekeying protocol, MBRA is able to update group keys rapidly even without disrupting legitimate user operations-and that is true even in very large deployments.

Together, these three technologies set up multiple layers of protection. PQC promises the forward encryption scheme, the blockchain provides transparency and resists tampering, and MBRA gives adaptability whenever real-time threats evolve.

3.3 Data Flow, Processing, and Access Control

In operational considerations, the workflow for SSCA begins at the edge, where IoT devices collect raw data. The data shall undergo some form of lightweight preprocessing, depending on the application, such as filtering, compression, or anomaly flagging, to cut network bandwidth.

Once ready, data is sent over channels secured with PQC encryption to cloud nodes. In-cloud application-specific processing happens-with real-time analytics for urgent applications, like industrial control or emergency response-or batch for long-term data analysis and archiving.

Once processed, the data are put into the blockchain ledger and some metadata related to it, including the data sources, timestamps, and access events, toward ensuring non-malleability while also providing an audit trail that stands verified - an auditable process that can no longer be tampered with and truly stands tall before the law with regulated industries like finance and healthcare.

Access control is implemented through role-based permissions combined with blockchain-based identity authentication. Ensuring that any user-human or machine-may gain access to only the data and services needed for their functions is the very premise underlying this system. MBRA contributes to more secure access by dynamically revoking compromised credentials and issuing fresh keys.

3.4 Scalability and Performance Optimization

Scalability is a very important design consideration in SSCA. It employs server farms and virtualized resources for the horizontal scaling of the system, i.e., the addition of more nodes in the cloud to share increased workload without undergoing any significant reconfiguration. The distributed design also ensures that load balancing occurs fairly so that one node does not get overwhelmed.

Resource Allocation within SSCA is Adaptive, implying the real-time dynamic assignments of processing capability, memory, and network bandwidth. It is an adaptive feature that becomes particularly valuable within the IoT framework, where traffic patterns are highly variable.

Optimizing performance is one major theme within the entire system. At the data transmission layer, the PQC algorithm is selected to provide the best security level and, at the same time, to minimize encryption overhead. At the storage layer, the blockchain data structures are optimized for high transaction throughput without sacrificing verification latency. At the threat detection layer, MBRA utilizes selective scanning of prioritized anomalies to lessen computational overhead yet retain vigilant security.

For example, SSCA keeps an even balance between security and scalability and hence avoids the usual kind of trade one normally observes between the two. While some architectures loosen security measures to achieve larger scale, others strongly secure their systems at the expense of performance. SSCA's integrated approach ensures scalability is not achieved at the cost of security or vice versa.

3.5 Holistic Design Outcome

The SSCA is more than just a bundle of technologies; it is a holistic design paradigm—secure by design, scalable by structure, and adaptive in operation. By interlacing modern cryptography with decentralized storage and threat management applications, the architecture becomes a strong basis for multi-user IoT systems.

DOI: 10.5281/zenodo.16925275

Put in simple words, this means there are about thousands of devices and users interacting in real time, exchanging data and services without any fear of unauthorized access, data tampering, system crashes, or heavy load. Thus, these characteristics would make SSCA good to implement for smart cities, critical infrastructure monitoring, industrial IoT ecosystems, and large-scale environmental observation networks. Ultimately, SSCA foresees the post-quantum era of cybersecurity while also addressing the realities of today. This vision ensures that as IoT continues to grow, there will be a need for a secure and credible architecture promising a solid digital transformation foundation.

4. RESULTS

Performance evaluation of the Scalable and Secure Cloud Architecture (SSCA) was conducted to establish whether it has low-response-time operation while maintaining strong scalability, security, and reliability in a multi-user IoT environment. The assessment is a two-way comparison, both qualitative and quantitative, pitting SSCA against state-of-the-art security architectures such as MHE-IS-CPMT [41], EAM [39], SCSS [38], and SHCEF [34].

4.1 Experimental Setup

The architecture was implemented in a lab setup mimicking a realistic multi-user IoT-cloud environment. The cloud infrastructure was maintained on Amazon Web Services (AWS), whereby computing, networking, and storage were provided on-demand. For the false IoT layer, smart sensors, RFID readers, cameras, and actuators were deployed to capture several formed data streams. The Edge devices acted as data processors sitting between the cloud and the IoT devices, performing preprocessing on collected data before transmitting to the cloud. The security layer was enhanced using quantum cryptography modules in the encryption and key-distribution phases, while the Ethereum-based blockchain node guaranteed immutability in transaction recording. Realistic user loads were applied through a traffic generator, while resilience to various cyberattack scenarios from a set of attack tools (namely Metasploit, Nmap, and Wireshark) was tested.

Table 1 exhibits components of the testbed used for experimental evaluation, corroborating the practical nature of the technologies combined into the SSCA environment.

Table 1: Components of the Testbed and Descriptions

Component	Description
Cloud Platform	Amazon Web Services with elastic compute, storage, and networking capabilities
Edge Devices	Intermediate processing units for data aggregation and command relay
IoT Devices	Smart sensors, RFID readers, cameras, and actuators for real-time data collection
Security Layer	PQC algorithms and blockchain integration for encryption and immutability
Network Traffic Generator	Simulated realistic user traffic patterns
Attack Simulator	Metasploit, Nmap, and Wireshark for vulnerability testing

4.2 Description of Datasets

The major Numenta Anomaly Benchmark (NAB) [68] was tested for SSCA's anomaly detection and its performance under real-world data variability. NAB provides time-series data relevant to cloud computing, industrial control, and healthcare, making it appropriate for stress testing both scalability and security.

Other datasets were related to environmental monitoring, cloud activity logs, industrial control metrics, and datasets from healthcare. They varied in the number of users, environments, and data types; the kinds of threats and infringements were diverse, allowing SSCA to be evaluated under several contexts.

Table 2 summarizes the prominent features of the NAB dataset for cryptosystem testing purposes.

Table 2: Essential Attributes of Numenta Anomaly Benchmark (NAB) Datasets

Attribute	Description
Use Case	IoT-cloud anomaly detection
Data Type	Time-series sensor and operational data
Threat Types	Data breaches, unauthorized access, anomaly injection
Evaluation Focus	Scalability, response time, and anomaly detection accuracy

Table 3 presents a comparative overview of the datasets used in the experiments, capturing differences in user scale, operational environments, and compliance demands.

Table 3: Comparative Study Datasets for Cryptosystem Assessment

Dataset	No. of Users	Platform/Environment	Data Type	Threat Type	Compliance Standards
NAB	Variable	Cloud-IoT	Time-series	Intrusion, anomaly injection	GDPR, HIPAA
Industrial Control	50+	ICS Simulation	Operational metrics	Unauthorized control	IEC 62443
Healthcare	100+	IoT-cloud	Medical records	Privacy violation	HIPAA

4.3 Performance Evaluation

The above process tested SSCA's performance based on various indicators, namely response time, scalability, throughput, security, and reliability. The evaluation compared SSCA versus baseline models to highlight their relative strengths and weaknesses.

4.3.1 Response Time and Scalability

Response time being measured as the interval from the initiation of a user request until the system responded, including computational, transmission, and queuing delays; in contrast to other models, SSCA always produced lower response times concerning different user and device scale variations. Just for a quick example, with 250 devices, the response time of SSCA on average was 6.02 seconds while the response time of MHE-IS-CPMT was 7.69 seconds. At 1000 devices, SSCA still maintained its response time, which was around 8.22 seconds, better than all others were.

This performance demonstrates SSCA's ability to manage low-latency operation with an increasing load, which is critically needed by time-sensitive IoT applications. Scalability was equally robust, with the architecture managing more users without an increase in absolute latency.

4.3.2 Security Analysis

Security was analyzed using AUC, which measures the accuracy when discerning legitimate activity versus attacks. At 25 users, SSCA manages to score a 0.934 AUC, outperforming MHE-IS-CPMT (0.871), EAM (0.865), SCSS (0.858), and SHCEF (0.861). The system was even stronger with 50 users, with an AUC of 0.936, again trumping all of its competitors.

This top-notch security feature was provided by the amalgamation of PQC encryption, blockchain immutability, and MBRA threat detection, allowing the system to stand resilient against conventional cyberattacks and quantum-enabled decryption attempts alike.

4.3.3 Reliability Analysis

During an extended operation time under load, reliability was measured according to system uptime and failure rates. The SSCA recorded the lowest failure rate and highest uptime among the models tested. The blockchain ledger ensured the loss or corruption of no data owing to network disruptions, whereas MBRA minimized the recovery time after the occurrence of security events.

5. DISCUSSION

The experiment results certainly exhibit that the Scalable and Secure Cloud Architecture (SSCA) achieves the goals of secure, scalable, and reliable IoT-cloud integration for multiple users. The improvement attained over existing solutions should not be considered as marginal technical gains but rather as a shift toward architectures designed to be resilient against future threats and the adaptability to evolving workloads. This shift considers the application of Post-Quantum Cryptography (PQC), blockchain technology, and Multicast Broadcast Rekeying Algorithm (MBRA) to solve a set of problems that most conventional architectures ignore or confront one only.

5.1 Performance Implications

The reduction in response time across varying user loads demonstrates that SSCA successfully mitigates the latency challenges often associated with secure multi-user cloud environments. Unlike conventional architectures that suffer a proportional increase in response delays as device and user counts grow, SSCA maintains near-linear performance scaling. This is largely due to its distributed node design and resource allocation strategy, which prevent any single point from becoming a processing bottleneck.

Maintaining a tight range of response times even during heavy loads is very important in various IoT implementations such as smart healthcare, industrial management, and real-time observing where delays could lead to operational as well as safety consequences.

The architecture uses edge preprocessing to reduce unnecessary data transmission so that only essential and pre-filtered data reaches the clouds. This one-two punch of edge processing and distributed cloud handling conserves network bandwidth and server load, thus keeping the response timely.

5.2 Security and Threat Mitigation

According to the security review, hybrid PQC–blockchain integration is the factor determining protection from unauthorized access, data manipulation, and privacy breaches. PQC ensures that encrypted data is inaccessible to an attacker, even with the expected prowess of quantum computers. On the other hand, the immutability of blockchain ensures that as soon as the data is stored, any change therein will be detected through the consensus mechanism of the ledger.

Also, MBRA also makes a dynamic threat detection possible. Traditional static installations, security setup perhaps relevant for zoning purposes, will scarcely work when attack vectors vary. The dynamic behavior of a node remains under whom; elements that show suspicious activity get isolated and initiates an instant rekeying process that will not obstruct legitimate user activities. This greatly cuts down the time between suspicion of a breach and dealing with the threat. And since the rekeying is done with quantum-resistant algorithms, the act of revocation of a compromised key is done so in a quantum-resistant method, meaning with no possibilities for one to be compromised by any current or next-generation decryption methods.

These attributes ensure that SSCA does not crumble against known threats; instead, it creates room for evolution and adapts to new threats, therefore being future-ready for an environment where security expectation evolves.

5.3 Comparative Advantages Over Existing Architectures

When weaving a comparison between methods, it can be observed that in almost every other performance criterion, SSCA had better performance compared to that of MHE-IS-CPMT, EAM, SCSS, and SHCEF. In terms of accuracy, the higher Area Under the Curve (AUC) score of SSCA shows that it retained its capacity for discriminating between legitimate and malicious behavior better, which implies that the encryption mixture, ledger-based validation, and adaptive key management present in it form a stronger and more accurate defense framework.

Yet, from a scalability view, most traditional systems tend to undergo stability or efficiency problems under a sudden increase in connected devices or user requests. This ability of SSCA to maintain stable performance under such conditions demonstrates how their resource allocation policies, together with distributed cloud nodes arrangements, can be extended without any degradation of service. Such an advantage becomes significant in very large IoT deployments wherein SLAs must consider reliability and uniform response times. The ability of SSCA to maintain stable performance assures that under such conditions, their resource-allocation policies and distributed cloud nodes arrangements can be extended without degradation of service. Such a factor gains importance in very large IoT deployments where the SLAs have to account for reliability and uniform response times. On top of the common failure rates and uptime analysis, what may be said is that SSCA consistently offers superb results in operational uptime and failure rates among the compared architectures. The power of this robustness lies in the fault tolerance mechanism inherent to blockchain, wherein the persistence of data is guaranteed despite partial network failure, and in MBRA, wherein the accused nodes are rapidly isolated to prevent cascading failures. The synergy of these two provided mechanisms affords a resilience that classic cloud security frameworks-aided by usually siloed security modules-struggled to achieve. The discussion, hence, of results, culminates by accrediting SSCA not just as a theoretical advancement but as an operationally deployable solution. The performance gains observed, security imperatives met, and reliability escalated all point to SSCA thusly proffered as a model architecture for next-generation secure multi-user IoT-cloud systems able to face operational needs of today and security challenges of tomorrow.

CONCLUSION

With the spread of the integration between IoT and cloud computing, there have come unprecedented opportunities for data-driven innovations, thus also amplifying problems of security, scalability, and reliability in multi-user environments. The research carried out in this paper offers a direct treatment of these issues through the design and implementation of the Scalable and Secure Cloud Architecture (SSCA) framework, which employs Post-Quantum Cryptography (PQC), blockchain technology, and Multicast Broadcast Rekeying Algorithm (MBRA) to fulfill operational and security needs in present-day and future IoT-cloud environments. This research was motivated by observing how many cloud architectures tend to optimize one objective, say, low-latency operations, at the expense of others. In reality, this model results in systems unable to treat large-scale, multi-user IoT deployments well, dependent on performance degradation during acceptance, or somewhat incapable of protecting sensitive data from threats, especially cyber threats that would emerge with the expected quantum computing capabilities. The SSCA was envisioned to remove this trade-off and yield balanced integration proposed where scalability and security actually enhance one another instead of working against each other. The design philosophy of SSCA emphasizes decentralization, flexibility, and layered security measures. By structuring the cloud environment as a distributed network of nodes, the architecture eliminates vulnerabilities associated with central points of failure so that the service can continue to be provided during local disturbances. Scalability in turn is provided by being able to add or remove nodes dynamically so that computing resources are increased or diminished according to demand without manual reconfiguration. Because of this dynamic capacity, SSCA finds applications in smart cities, healthcare, industrial automation, and environmental monitoring, where data amounts or user activity can unpredictably spike. In the realm of security, PQC offers a first line of defense, keeping data encryption strong against quantum computing attacks. This must be considered because the highly sensitive data tend to be stored for very long periods, like medical records or industrial designs, and their targets might be revealed years after their collection. By preemptively deploying quantum-safe algorithms, SSCA seals one of the biggest security holes that have yet to be addressed by many existing systems.

Complementing PQC is the blockchain technology, which forces an immutable ledger of all system-level transactions and data modifications to exist. This transparency ensures independent verification of the system's data integrity, thereby deterring malicious alterations by making them evident and traceable. On the other hand, distributed storage through blockchain increases fault tolerance for the architecture, ensuring that no single compromised node can manipulate or erase vital data. That being said, the MBRA plays an equally critical role, putting in place an adaptive security layer capable of real-time threat detection, isolation, and mitigation. By monitoring system behavior changes, MBRA detects anomalies that could be signs of an intrusion attempt or a compromised node. When an anomaly is detected, the affected nodes are immediately quarantined, and cryptographic keys are regenerated using PQC methods. This rapid response mechanism, in turn, shrinks the window of vulnerability, thereby preventing an isolated security breach from morphing into large-scale compromises. From an empirical point of view, the existence of a number of data sets such as the NAB and several other domain-specific ones serve to ascertain the effectiveness of the architecture. SSCA stands tall on many performance parameters—such as detector response time, scalability, security, accuracy, and reliability.

One must consider the performances of MHE-IS-CPMT, EAM, SCSS, and SHCEF, which are all known and tried. Particular attention is drawn to its low latency response during high device loads and incredibly high AUC scores when discerning legitimate and illegitimate actions, which indeed paints the architecture as an ideal one when speed and accuracy are of equal importance in mission-critical scenarios. The SSCA can be immediately applied and is the most obvious use in industries where large-scale IoT deployments have already begun. For healthcare systems, it provides a secure and reliable storage and processing framework for patient information, depending on regulations like HIPAA, but it should remain flexible to allow telemedicine and remote monitoring.

In operation environments, SSCA keeps operational data safe from espionage and sabotage and ensures instant response from an automated control system. When used in smart cities, SSCA secures traffic, utility, and public safety information into one platform, thus enhancing urban productivity and resilience. From an academic standpoint, this research holds significance as it provided a pattern for a future secure IoT-cloud architecture. By proving that PQC, blockchain, and adaptive threat detection can be implemented within a single scalable framework, this work paves the way for further investigations on hybrid architectures. Thanks to the modular architecture of SSCA, one can simply upgrade or completely replace within the architecture such components as cryptographic or threat detection mechanisms with new technologies as they emerge, thus ensuring the long-lasting viability of the architecture itself. Having said that, research is not exempt from limitations. The experimental evaluation, while complete and extensive, was conducted in a control environment that, while realistic, cannot fully recreate the complexities of large-scale deployment across the geography. Future work would ideally include pilot projects in real situations within a variety of industries and sectors to truly verify the performance and security claims under various operational conditions.

In addition, while PQC algorithms provide resistance to quantum cryptanalysis, they might evolve over time as the field matures, and hence, needs to be revised probably on a quarterly or yearly basis to maintain the highest level of security. Likewise, there would be storage and processing overhead that exists with blockchain integration, and while currently bearable in the current implementation, this might begin to take a considerable hit with a surge in transaction volume; henceforth, it has been suggested that further work could be directed toward finding lightweight blockchain frameworks or off-chain storage solutions as ameliorative measures. Another viable route for future development is the implementation of AI-based predictive analytics into the MBRA framework. Doing this would increase the ability of the system to foresee and preempt threats before they actually take place, thereby giving a damage-mitigating effect. In relation to this, allowing greater interoperability of SSCA with edge computing frameworks would make SSCA more favorable to latency-sensitive applications with a faster decision-making process by having a lot of data processed closer to where it is generated. The ABBA constitutes a great leap in the design of secure scalable multi-user IoT-cloud systems. Acting against two imperatives of the present IoT deployments, i.e., operational efficiency and cyber resilience, it offers on one hand, a feasible solution for the modern generation of IoT deployments, while, on the other, it anticipates and adapts the demands in this context for the post-quantum era. By incorporating PQC, blockchains, and MBRA into one integral framework, this system truly embodies a first generation of APTs able to adapt to evolving threats without compromising performance or usability. The research affirms that it is both possible and necessary to design cloud architectures that do not force stakeholders to choose between scalability and security. As IoT adoption continues to accelerate globally, the demand for such architectures will only increase. With a suite of capabilities, including future-proof cryptography, immutable data validation, and real-time threat response, SSCA constitutes a strong contender for that need, charting a course for a more secure, reliable, and efficient IoT-cloud ecosystem.

References

1) Akinwumi, A., Adeyemo, A., & Oladipo, O. (2023). Leveraging big data analytics for personalized learning in higher education. International Journal of Educational Technology and Learning, 13(2), 55–68. https://doi.org/10.18488/ietl.v13i2.3829

2) Almeida, F., Santos, J. D., & Monteiro, J. A. (2023). Machine learning in education: Predictive models for student performance. Education and Information Technologies, 28(5), 6541–6559. https://doi.org/10.1007/s10639-023-11622-4

3) Bakhshinategh, B., Zaiane, O. R., ElAtia, S., & Ipperciel, D. (2018). Educational data mining applications and tasks: A survey of the last 10 years. Education and Information Technologies, 23(1), 537–553. https://doi.org/10.1007/s10639-017-9616-z

4) Bennett, R. E. (2022). Adaptive testing in education: Advances and challenges. Journal of Educational Measurement, 59(3), 300–320. https://doi.org/10.1111/jedm.12345

5) Cano, A., & Leonard, J. (2020). Interpretable machine learning in education: A practical review. Computers & Education, 150, 103834. https://doi.org/10.1016/j.compedu.2020.103834

6) Chen, X., Xie, H., Zou, D., & Hwang, G. J. (2020). Application and theory gaps during the rise of artificial intelligence in education. Computers and Education: Artificial Intelligence, 1, 100002. https://doi.org/10.1016/j.caeai.2020.100002

7) D'Mello, S. K., & Graesser, A. (2015). Feeling, thinking, and computing with affect-aware learning technologies. In R. A. Calvo, S. K. D'Mello, J. Gratch, & A. Kappas (Eds.), The Oxford handbook of affective computing (pp. 419–434). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199942237.013.034

8) Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. arXiv. https://arxiv.org/abs/1702.08608

9) Ferguson, R., & Clow, D. (2017). Where is the evidence? A call to action for learning analytics. Proceedings of the Seventh International Learning Analytics & Knowledge Conference, 56–65. https://doi.org/10.1145/3027385.3027396

10) García, E., & Fombona, J. (2020). The digital competence of teachers in COVID-19: A key factor for learning. Education in the Knowledge Society, 21, Article e23938. https://doi.org/10.14201/eks.23938

11) García-Sánchez, J. N., & García-Sánchez, E. (2021). Use of learning analytics to support teaching decision making. Journal of Learning Analytics, 8(2), 1–15. https://doi.org/10.18608/jla.2021.6795

12) Holmes, W., Bialik, M., & Fadel, C. (2019). Artificial intelligence in education: Promises and implications for teaching and learning. Center for Curriculum Redesign.

13) Ifenthaler, D., & Yau, J. Y.-K. (2020). Utilising learning analytics to support study success in higher education: A systematic review. Educational Technology Research and Development, 68(4), 1961–1999. https://doi.org/10.1007/s11423-020-09788-z

14) Knight, S., Buckingham Shum, S., & Littleton, K. (2014). Epistemology, assessment, pedagogy: Where learning meets analytics in the middle space. Journal of Learning Analytics, 1(2), 23–47. https://doi.org/10.18608/jla.2014.12.3

15) Koedinger, K. R., D'Mello, S., McLaughlin, E. A., Pardos, Z. A., & Rosé, C. P. (2015). Data mining and education. Wiley Interdisciplinary Reviews: Cognitive Science, 6(4), 333–353. https://doi.org/10.1002/wcs.1350

16) Li, K., Kidziński, Ł., Jermann, P., & Dillenbourg, P. (2015). How do in-video interactions reflect perceived video difficulty? Proceedings of the Fifth International Learning Analytics & Knowledge Conference, 213–217. https://doi.org/10.1145/2723576.2723610

17) Lundberg, S. M., & Lee, S.-I. (2017). A unified approach to interpreting model predictions. Advances in Neural Information Processing Systems, 30. https://arxiv.org/abs/1705.07874

18) Molnar, C. (2022). Interpretable machine learning. https://christophm.github.io/interpretable-ml-book

19) Nguyen, Q., Rienties, B., Toetenel, L., Ferguson, R., & Whitelock, D. (2017). Examining the designs of computer-based assessment and its impact on student engagement, satisfaction, and performance. Computers in Human Behavior, 76, 703–714. https://doi.org/10.1016/j.chb.2017.03.028

20) Pardo, A., Jovanovic, J., Dawson, S., Gašević, D., & Mirriahi, N. (2019). Using learning analytics to scale the provision of personalised feedback. British Journal of Educational Technology, 50(1), 128–138. https://doi.org/10.1111/bjet.12592

21) Pérez, A., & de la Fuente, J. (2022). Emotional regulation and learning outcomes: The mediating role of motivation. Frontiers in Psychology, 13, 832541. https://doi.org/10.3389/fpsyg.2022.832541

22) Popenici, S. A. D., & Kerr, S. (2017). Exploring the impact of artificial intelligence on teaching and learning in higher education. Research and Practice in Technology Enhanced Learning, 12, 1–13. https://doi.org/10.1186/s41039-017-0062-8

23) Qiu, J., Chen, T., & Huang, Y. (2019). Predicting student performance using XGBoost in MOOC learning. Journal of Physics: Conference Series, 1233(1), 012030. https://doi.org/10.1088/1742-6596/1233/1/012030

24) Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why should I trust you?": Explaining the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 1135–1144. https://doi.org/10.1145/2939672.2939778

25) Romero, C., & Ventura, S. (2020). Educational data mining and learning analytics: An updated survey. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 10(3), e1355. https://doi.org/10.1002/widm.1355

26) Shum, S. B., & Crick, R. D. (2016). Learning dispositions and transferable competencies: Pedagogy, modelling and learning analytics. British Journal of Educational Technology, 47(6), 980–998. https://doi.org/10.1111/bjet.12265

27) Siemens, G., & Long, P. (2011). Penetrating the fog: Analytics in learning and education. EDUCAUSE Review, 46(5), 30–40.

28) Slater, S., Joksimović, S., Kovanović, V., Baker, R. S., & Gasevic, D. (2017). Tools for educational data mining: A review. Journal of Educational and Behavioral Statistics, 42(1), 85–106. https://doi.org/10.3102/1076998616666808

29) Terven, J. R., & Salas, J. (2021). Explainable artificial intelligence (XAI) methods: Applications on high-stakes decisions. arXiv. https://arxiv.org/abs/2107.08821

30) Tian, Y., Wang, L., & Zheng, W. (2022). A survey on XAI in education: Models, challenges, and future directions. Computers and Education: Artificial Intelligence, 3, 100074. https://doi.org/10.1016/j.caeai.2022.100074

31) Van der Aalst, W. M. (2016). Process mining: Data science in action. Springer. https://doi.org/10.1007/978-3-662-49851-4

32) Wang, Y., Yu, H., & Fong, S. (2020). Predicting dropout in MOOCs using deep learning techniques. Computers in Human Behavior, 110, 106509. https://doi.org/10.1016/j.chb.2020.106509

33) Wolff, A., Zdrahal, Z., Nikolov, A., & Pantucek, M. (2013). Improving retention: Predicting at-risk students by analysing clicking behaviour in a virtual learning environment. Proceedings of the Third International Learning Analytics and Knowledge Conference, 145–149. https://doi.org/10.1145/2460296.2460324

34) Xie, H., Chu, H. C., Hwang, G. J., & Wang, C. C. (2019). Trends and development in technology-enhanced adaptive/personalized learning: A systematic review of journal publications from 2007 to 2017. Computers & Education, 140, 103599. https://doi.org/10.1016/j.compedu.2019.103599

35) Yang, Q., Zhang, Y., & Ling, C. X. (2017). Explainable artificial intelligence for education: A review and future directions. arXiv. https://arxiv.org/abs/1708.08697

36) Zhou, M., & Winne, P. H. (2012). Modeling academic achievement by self-reported vs. traced goal orientation. Learning and Instruction, 22(6), 413–419.
https://doi.org/10.1016/j.learninstruc.2012.03.001