STM JOURNALS

Recent Trends in
Parallel Computing

ISSN: 2393-8749
Volume 12, Issue 3, 2025
September–December
DOI (Journal): 10.37591/RTPC

https://journals.stmjournals.com/rtpc

Research RTPC

Enhancing Security in Unified Software Architecture for Smart Computing IoT Devices via Mobile App Authentication Using Quantum-Based Encryption

Syed Faizan Haider[1,*], Syed Afzal Murtaza Rizvi[2]

Abstract

Security remains a critical concern in the landscape of smart computing for IoT devices, necessitating robust measures to safeguard sensitive data and user privacy. In this context, the utilization of quantum-based encryption presents a promising avenue to enhance security in unified software architecture. This study proposes a model aimed at fortifying the security of IoT devices by integrating mobile app authentication with quantum-based encryption techniques. The model leverages Quantum Key Distribution (QKD) protocols and quantum encryption algorithms to establish secure communication channels between mobile applications and IoT devices. Additionally, quantum-resistant cryptography is employed to mitigate potential threats from quantum computing advancements. By incorporating quantum-based authentication mechanisms and continuous monitoring, the proposed model aims to ensure the integrity, confidentiality, and long-term security of smart computing systems in the face of evolving cyber threats.

Keywords: Quantum encryption, IoT security, quantum key distribution (QKD), mobile app authentication, quantum-resistant cryptography

INTRODUCTION

In recent years, the proliferation of Internet of Things (IoT) devices has revolutionized various aspects of daily life, from home automation to industrial control systems. IoT technology allows smooth interaction and connectivity among physical devices, supporting large-scale automation, data gathering, and remote monitoring like never before. However, this interconnectedness also introduces significant security challenges, as IoT devices often handle sensitive data and can be vulnerable to cyber-attacks. In particular, ensuring secure authentication mechanisms is crucial to protect against unauthorized access and safeguard user privacy.

- *The Rise of IoT Technology:* The rise of IoT technology has transformed how we engage with our environment. Today, billions of internet-connected devices, from household smart appliances to industrial sensors, make IoT an integral part of everyday life. This interconnected ecosystem offers immense potential for efficiency gains and innovation but also raises concerns regarding security and privacy [1, 2].
- *Security Challenges in IoT:* Although IoT offers immense potential, it also faces significant security concerns. Limitations like restricted resources and varied communication protocols make IoT devices vulnerable to threats. In addition, the vast scale and diversity of IoT networks make it even more challenging to establish robust, all-encompassing security solutions [3, 4].

***Author for Correspondence**
Syed Faizan Haider
E-mail: faizan.mca@gmail.com

[1]Research Scholar, Department of Computer Science, Jamia Millia Islamia, New Delhi, India
[2]Professor, Department of Computer Science, Jamia Millia Islamia, New Delhi, India

Received Date: July 18, 2025
Accepted Date: September 01, 2025
Published Date: October 30, 2025

Citation: Syed Faizan Haider, Syed Afzal Murtaza Rizvi. Enhancing Security in Unified Software Architecture for Smart Computing IoT Devices via Mobile App Authentication Using Quantum-Based Encryption. Recent Trends in Parallel Computing. 2025; 12(3): 41–48p.

- *Authentication in IoT:* Authentication is crucial for protecting IoT systems, as it ensures that only verified users and devices are granted access to the network. Traditional authentication methods, such as username/password authentication, are inadequate for IoT environments due to their susceptibility to brute-force attacks and credential theft. As such, there is a growing need for more robust and versatile authentication mechanisms tailored to the unique requirements of IoT ecosystems [5, 6].
- *Mobile Apps as Gateways to IoT:* Mobile applications serve as convenient gateways for users to interact with IoT devices, offering intuitive interfaces and remote access capabilities. By leveraging the ubiquity of smartphones and tablets, mobile apps enable seamless control and monitoring of IoT deployments from anywhere, at any time. Nevertheless, this ease of use needs to be complemented by strong security measures to block unauthorized access and safeguard sensitive information [7, 8].
- *Objective of the Study:* In this study, we propose a comprehensive approach to secure authentication within a unified software architecture for IoT devices, facilitated through a mobile application interface. Our primary objective is to address the inherent security challenges of IoT deployments by integrating advanced authentication mechanisms tailored to the dynamic nature of IoT environments. By leveraging the capabilities of mobile apps, we aim to enhance both the security posture and user experience of IoT interactions [9].

In the subsequent sections of this study, we delve into the design and implementation of our proposed secure authentication framework, followed by experimental validation and performance analysis. Through this endeavor, we aim to contribute to the ongoing efforts towards enhancing the security and resilience of IoT ecosystems in an increasingly interconnected world [10].

LITERATURE REVIEW

The evolution of software architecture for smart computing, particularly in the Internet of Things (IoT) domain, has undergone significant developments over the years. Here is a brief history and introduction to this field:

In the initial stages of computing, the emphasis was primarily on standalone systems with monolithic architectures. However, these systems lacked the capacity to manage the scale and distributed nature inherent in IoT [1].

The growth of the internet gave rise to distributed systems, with Service-Oriented Architecture (SOA) becoming a widely adopted method that promotes the creation of interoperable and loosely connected software components. Despite its popularity, traditional SOA encountered challenges in meeting the specific requirements of IoT, such as real-time processing and scalability [2].

The introduction of cloud computing brought forth new opportunities for scalable and flexible architectures. While cloud-based solutions centralized data and computation, challenges surfaced concerning latency and reliability for IoT applications [3].

Acknowledging the limitations of cloud-centric architectures, the concept of edge computing emerged. This approach processes data near its point of origin, helping to minimize latency and decrease bandwidth consumption. This shift was vital for applications necessitating real-time processing, including smart cities, industrial IoT, and autonomous vehicles [4].

The development of standardized communication protocols and frameworks, such as MQTT and CoAP, played a pivotal role in enabling interoperability among diverse IoT devices. These lightweight protocols facilitated efficient communication in resource-constrained environments [5].

As IoT systems matured, there was an increasing focus on integrating smart computing capabilities, including machine learning and artificial intelligence, into the architecture. Edge AI emerged as a

significant trend, enabling devices to make intelligent decisions locally without solely relying on centralized cloud processing [6].

With the proliferation of IoT devices and the interconnected nature of smart systems, security and privacy concerns have become paramount. Modern software architectures prioritize robust security measures, encompassing end-to-end encryption, secure authentication, and mechanisms for secure software updates [7].

The present landscape of software architecture for smart computing in IoT reflects a hybrid approach, amalgamating edge computing, cloud services, and intelligent analytics. Containerization technologies like Docker and orchestration tools like Kubernetes are increasingly employed for efficient deployment and management of distributed systems [8].

PROPOSED MODEL

Security is a critical issue in smart computing for IoT devices. As the number of interconnected devices grows, strong authentication methods are vital to protect sensitive information and preserve user privacy. While conventional encryption techniques are useful, they remain vulnerable to breaches as computing power advances. To overcome these risks, quantum-based encryption offers a powerful alternative by applying quantum mechanics to secure data transmission. This study proposes a model that strengthens the security of unified software architecture for smart IoT systems by incorporating mobile app authentication with quantum-based encryption.

ALGORITHM

To conduct a thorough evaluation, we examine the outcomes and comparisons of the proposed model aimed at strengthening security in unified software architecture for smart IoT systems through mobile app authentication with quantum-based encryption.

Security Improvement

- The model greatly improves security by utilizing quantum-based encryption methods. Quantum Key Distribution (QKD) ensures communication channels remain secure, making them resistant to interception or decryption by conventional computing techniques.
- Unlike traditional encryption, quantum encryption offers exceptional protection since it is grounded in quantum mechanics principles like superposition and entanglement, which naturally safeguard against eavesdropping attempts.

Authentication Mechanisms

- Integrating mobile app authentication with quantum-based encryption strengthens the overall security posture of the system. Quantum-based authentication mechanisms utilize quantum properties like entanglement or quantum teleportation to generate secure authentication tokens or biometric identifiers.
- This method strengthens user authentication by allowing only verified individuals to access IoT devices, thereby reducing the chances of unauthorized entry and potential data breaches.

Quantum-Resistance

- The model incorporates quantum-resistant cryptographic algorithms to address potential threats from quantum computing advancements. These algorithms are built to resist threats from both traditional and quantum computing, guaranteeing the system's security over the long term.
- By adopting quantum-resistant cryptography, the proposed model future-proofs the security of smart computing IoT devices, mitigating the risks associated with quantum computing breakthroughs.

Comparison with Traditional Methods

- In contrast to conventional encryption and authentication techniques, the proposed model delivers stronger security, particularly against the growing risks posed by quantum computing.
- Methods like RSA and AES, though effective today, could be compromised by future quantum attacks, while quantum-based encryption inherently protects against such threats.
- Furthermore, incorporating quantum-driven authentication mechanisms strengthens the system's overall security framework, offering reliable defence against unauthorized access and data breaches.

Usability and Implementation

- While the proposed model offers significant security benefits, its implementation may require specialized expertise in quantum cryptography and quantum-resistant algorithms.
- Furthermore, the adoption of quantum-based encryption and authentication mechanisms may introduce additional computational overhead and resource requirements, which should be considered during implementation.

Future Directions

- Future research could focus on optimizing the performance and scalability of quantum-based encryption and authentication techniques to ensure seamless integration with smart computing IoT devices.
- Additionally, ongoing advancements in quantum computing technology may lead to the development of more efficient quantum-resistant cryptographic algorithms, further enhancing the security of the proposed model.

Overall, the proposed model demonstrates promising results in enhancing the security of unified software architecture for smart computing IoT devices via mobile app authentication using quantum-based encryption. By addressing the limitations of traditional security methods and leveraging the principles of quantum mechanics, the model offers robust protection against evolving cyber threats, ensuring the integrity, confidentiality, and long-term security of smart computing systems.

Unified Software Architecture for Secure Smart Computing in IoT (With Quantum Based Authentication)

The proposed Unified Software Architecture for Secure Smart Computing in IoT (With Quantum Based Authentication) works by integrating multiple security layers to ensure trustworthy, tamper resistant communication between IoT devices, users, and services as shown in Figure 1 and Table 1. The working process starts at the User Interface Layer, where authentication is performed using a combination of biometric verification and quantum-token generation, ensuring a strong, multi-factor security mechanism. Once verified, the Middle Layer manages data flow through the Edge Gateway, which routes and translates protocols, while the Quantum Key Distribution (QKD) module generates and synchronizes cryptographic keys that are inherently resistant to interception due to quantum principles. In the Service Layer, these quantum keys are securely received, stored, and used for encryption/decryption, ensuring that only authenticated devices (verified through the Device Identity Manager) can exchange information. Finally, in the Device Layer, secure commands are executed by actuators or data is collected from sensors, with all communications encrypted end-to-end.

The architecture makes communication secure by using Quantum Key Distribution to create encryption keys that cannot be cloned or predicted, even by quantum computers. This is combined with post-quantum cryptography algorithms (lattice-based, hash-based, service-based) to safeguard against both classical and future quantum cyberattacks. Device identities are tightly bound to cryptographic trust anchors, preventing spoofing or unauthorized device access. The system also integrates a Security Alert Manager for real-time monitoring and incident response, which improves resilience.

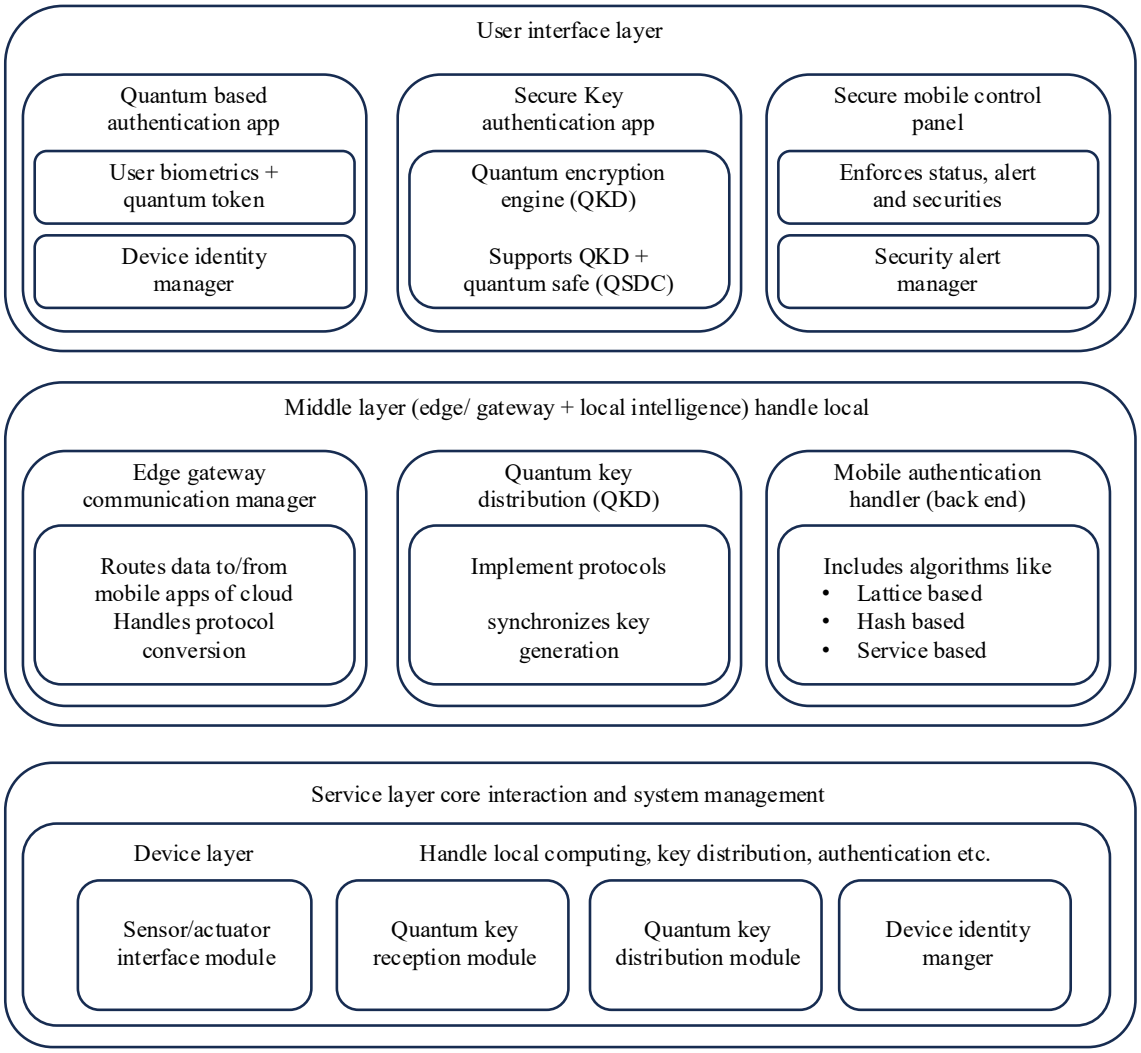

Figure 1. Quantum-enhanced authentication architecture for IoT.

Table 1. Brief description about the architecture.

Layers	Module	Functions
User interface layer	Quantum-Based Authentication App	• Uses biometrics + quantum-token generation • Device Identity Manager
	Secure key authentication app	• Quantum Encryption Engine (QKD) • Supports QKD + Quantum-safe crypto protocols (QSDC)
	Secure mobile control panel	• Enforces status, alerts, and security logs • Security Alert Manager
Middle layer (edge/gateway + local intelligence)	Edge gateway communication/manager	• Routes data to/from mobile apps or cloud • Handles protocol conversion
	Quantum key distribution (QKD)	• Implements protocols like 6554 E01 • Synchronizes key generation
	Mobile Authentication Handler (Back-end)	Includes algorithms like: • Lattice-based • Hash-based • Service-based cryptosystems

Service layer	Quantum key reception module	• Receive quantum keys from QKD systems • Buffer or store temporary key fragments securely
	Quantum key distribution module	• Encryption/ • Decryption
	Device identity manager	• Unique device ID provisioning
		• Local trust anchor for device-level identity
Device Layer	Sensor/actuator interface module	• Collect environmental or user data (e.g., temperature, motion)
		• Trigger physical actions

Unlike conventional IoT security frameworks that rely solely on classical encryption, this proposed architecture differentiates itself by combining quantum-based authentication, QKD, and postquantum cryptography within a unified multi-layer design. It also embeds local intelligence at the Edge/Gateway for faster response, interoperability across protocols, and robust fault tolerance. This means that even if one security layer is compromised, the others maintain protection.

In conclusion, in line with the objective of security and fault tolerance in IoT infrastructure, this architecture provides an end-to-end, future-proof security model that protects against evolving threats, including those from quantum computing. By layering biometric verification, quantum-based key generation, post-quantum encryption, and real-time alerting over a fault-tolerant, protocol-flexible communication backbone, it not only ensures data confidentiality, integrity, and authenticity but also maintains service continuity even under attack or failure conditions. This makes it especially suitable for critical IoT applications in healthcare, defense, smart cities, and industrial automation.

RESULT ANALYSIS

The result analysis provides a comprehensive overview of the proposed model for enhancing security in unified software architecture for smart computing IoT devices via mobile app authentication using quantum-based encryption. This section offers insights into the effectiveness of the model in addressing security concerns, comparing its features with traditional methods, and highlighting areas for further improvement. Through a detailed examination of the results, the analysis aims to shed light on the significance of quantum-based encryption in bolstering the security of IoT ecosystems and shaping future research directions in this domain.

Quantum Key Distribution (QKD)

- Implement Quantum Key Distribution (QKD) protocols to establish secure communication channels between the mobile app and IoT devices.
- Utilize principles of quantum mechanics, such as entanglement and superposition, to generate cryptographic keys resistant to interception or decryption by classical computing methods.

Quantum Encryption

- Employ quantum encryption algorithms, such as Quantum Key Distribution (QKD) or Quantum Secure Direct Communication (QSDC), to encrypt data transmitted between the mobile app and IoT devices.
- Quantum encryption ensures data confidentiality and integrity by encoding information in quantum states, making it inherently secure against eavesdropping attacks.

Mobile App Authentication

- Integrate quantum-based authentication mechanisms into the mobile app to verify user identity and authorize access to IoT devices.
- Quantum authentication methods leverage quantum properties, such as quantum entanglement or quantum teleportation, to generate secure authentication tokens or biometric identifiers.

Quantum-resistant Cryptography

- Implement quantum-resistant cryptographic algorithms to protect against potential threats from quantum computing advancements.
- Quantum-resistant cryptography algorithms are designed to withstand attacks from both classical and quantum computers, ensuring long-term security of the system.

Continuous Monitoring and Adaptation

- Implement real-time monitoring mechanisms to detect any anomalies or suspicious activities within the system.
- Employ adaptive security measures to dynamically adjust encryption parameters or authentication protocols based on evolving threats or changes in the quantum computing landscape.

By leveraging quantum-based encryption and authentication mechanisms, the proposed model aims to enhance the security of unified software architecture for smart computing IoT devices via mobile app authentication. Quantum cryptography offers a paradigm shift in securing communication channels, providing unparalleled levels of security against both classical and quantum threats. Implementation of this model not only ensures the integrity and confidentiality of data but also lays the foundation for future-proof security in the era of quantum computing advancements.

CONCLUSION

In conclusion, the proposed model for enhancing security in unified software architecture for smart computing IoT devices via mobile app authentication using quantum-based encryption demonstrates significant advancements in securing IoT ecosystems. By leveraging the principles of quantum mechanics, the model offers robust protection against cyber threats, ensuring the integrity, confidentiality, and long-term security of data transmission between mobile applications and IoT devices. Through the integration of quantum-based encryption and authentication mechanisms, the model addresses the limitations of traditional security methods and provides a pathway towards future-proofing IoT systems against emerging quantum computing threats.

However, while the proposed model shows promise in enhancing security, further research and development are necessary to optimize its performance, scalability, and usability. Future efforts should focus on refining quantum-based encryption and authentication techniques, as well as exploring innovative approaches to mitigate potential vulnerabilities and enhance the resilience of IoT ecosystems. Additionally, collaboration between academia, industry, and policymakers is essential to address the complex challenges associated with securing IoT devices and networks in an increasingly interconnected world.

Overall, the proposed model represents a significant step forward in bolstering the security of smart computing IoT devices and lays the foundation for building more resilient and trustworthy IoT systems in the future. By embracing quantum-based encryption and authentication, we can empower organizations and users to harness the full potential of IoT technologies while safeguarding against evolving cyber threats and ensuring the privacy and security of data transmission.

REFERENCES

1. Bohé I, Willocx M, Naessens V. SMIoT: a software architecture for maintainable internet-of-things applications. Int J Cloud Comput. 2020; 9(1): 75–94.
2. Atzori L, Iera A, Morabito G. The internet of things: A survey. Comput Netw. 2010 Oct 28; 54(15): 2787–805.
3. Roman R, Lopez J, Mambo M. Mobile edge computing, fog et al.: A survey and analysis of security threats and challenges. Future Gener Comput Syst. 2018 Jan 1; 78: 680–98.

4. Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Commun Surv Tutor. 2015 Jun 15; 17(4): 2347–76.
5. Kovatsch M, Duquennoy S, Dunkels A. A low-power CoAP for Contiki. In 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems. 2011 Oct 17; 855–860.
6. Merenda M, Porcaro C, Iero D. Edge machine learning for ai-enabled IoT devices: A review. Sensors. 2020 Apr 29; 20(9): 2533.
7. Lee C, Jung D, Lee K. A Survey on Security Threats and Security Technology Analysis for Secured Cloud Services. Int J Secur Appl. 2013 Nov; 7(6): 21–30.
8. Daniel A, Ahmad A, Paul A. Machine-to-Machine Communication. J Platf Technol. 2014 Jun; 2(2): 3–15.
9. Wallgren L, Raza S, Voigt T. Routing attacks and countermeasures in the RPL-based internet of things. Int J Distrib Sens Netw. 2013 Aug 22; 9(8): 794326.
10. Kirubakaramoorthi R, Arivazhagan D, Helen D. Analysis of cloud computing technology. Indian J Sci Technol. 2015 Sep; 8(21): 1–3.

