Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 46 (2025), No. 4-A, pp. 969–977
DOI : 10.47974/JIOS-1824

Enhancing the security of IoT edge computing using quantum cryptographic and cellular automata

Sandeep Kumar Sharma [†]
Vijay Shankar Sharma *
Amit Chauraisa [§]
Department of Computer and Communication Engineering
Manipal University Jaipur
Jaipur 303007
Rajasthan
India

Atul Srivastava [‡]
Department of Computer Science and Engineering
Amity School of Engineering and Technology
Lucknow 201313
Uttar Pradesh
India

Anuradha Pillai [@]
Department of Computer Science and Engineering
Symbiosis Institute of Technology
Pune 412115
Maharashtra
India

Abstract

The IoT edge computing presents a noteworthy capability to provide economy, fast, and secure processing to their systems but the system should integrate with a strong model that can preserve data privacy and secure communication. The proposed research integrates the concepts of cellular automata and quantum cryptography to introduce a model that

[@] *E-mail:* sandeep.sharma@jaipur.manipal.edu
[†] *E-mail:* vijayshankar.sharma@jaipur.manipal.edu (Corresponding Author)
[§] *E-mail:* amit.chaurasia@jaipur.manipal.edu
[‡] *E-mail:* atul.nd2@gmail.com
* *E-mail:* anuradha.pillai@sitpune.edu.in

can remove the loopholes of IoT edge computing-based systems. The cellular automata analyze a two-dimensional grid structure to produce a robust transition function or rule by assessing the nearby neighbors. The Quantum key distribution protocol is used to generate the quantum cryptographic key. The transition function and quantum cryptography key are combined to generate the final cryptographic key of the system. The performance of the proposed integration is measured using the time consumption, computational overhead, and security simulations. The experimented results of the proposed research claim that the combined approach preserved data security and protective communication at high priority.

Subject Classification: *Primary 03B70, Secondary 03D10.*

Keywords: *Cellular automata, Quantum cryptography, Quantum key distribution, IoT edge computing.*

1. Introduction

Cloud-based IoT systems present a vigorous and accessible solution to analyze and manage data produced by IoT Devices. These systems control the computing resources to manage the storage, processing, and data generated by IoT devices. These systems offer a centralized platform where data from numerous IoT devices can be aggregated, analyzed, and managed efficiently. Generally, cloud systems have various benefits for IoT devices i.e., remotely accessible, reduced cost, scalability, etc. Nevertheless, cloud-based systems have significant issues in terms of security, integration, and privacy. To overcome these challenges, IoT edge computing comes with advantages i.e., ensures security, integration, and privacy, and reduces latency, improves scalability, and optimization usage. IoT edge computing is a transformative approach that addresses the challenges of traditional cloud-based IoT systems by bringing computation closer to the data source. With the key benefits of edge computing, many IoT applications exist in the real world i.e., smart cities, industrial IoT, healthcare, automation, etc. [1].

To grasp the difficulties associated with cloud-based Internet of Things computing, the edge-based IoT is very important, but a method or model should collaborate that has advanced cryptographic and reliable computation capabilities is required which can involve enhanced security. The quantum cryptography technique which is based on the idea of quantum physics provides exceptional levels of security with the help of quantum key distribution (QKD) concepts. QKD plays an important role in developing a hypothetically unbreakable encryption key that guarantees safe storage of the data and provides secured communication even when strong challengers. Quantum cryptography works on the principle of quantum superposition, quantum entanglement, and Heisenberg Uncertainty. To encode the information in various quantum conditions, the quantum superposition processes the quantum particles until the entire information is not encoded [2, 3].

Cellular automata (CA) are discrete and abstractive for computational systems in a variety of scientific fields. Cellular automata provide a versatile framework for modeling a wide range of complex systems. Different types of cellular automata, from one-dimensional(1D), two-dimensional(2D), probabilistic, continuous, and CA with memory, all types offer unique capabilities for simulating and analyzing various phenomena. Each type has a specific transition function that defines the state of each cell based on its neighbors and possibly other factors like probabilities or memory [4]. Cellular automata possibly have the flexibility to be employed as a model and could reproduce the behavior of quantum systems in QKD protocols. This CA provides an understanding of how the CA's rules or transition functions may adopt the security and efficiency of the QKD.

Table 1

IoT edge computing-based applications with use cases and security concerns

IoT Edge Computing Applications	Use Cases	Security Concerns
Smart Homes [5]	Home appliances and security systems	Unauthorized access and data breaches are the major concerns
Smart Cities [5]	Traffic signals, road lights, waste management	Data privacy, hacking risk, and DoS attacks
Industrial IoT [6]	Industrial equipment and development	Industrial surveillance, interruption, and vulnerabilities in inheritance systems
Vehicle Automation [9]	Driving and parking assessment	Vehicle data confidentiality, and data protection between vehicle user and external entity.
Healthcare [7]	Remote monitoring of patent and health devices	Device annealing and patent data privacy
Agriculture [8]	Crop and soil fitness monitoring	Remote sensing and integrity issues

2. Literature Survey

The Internet of Things is becoming more popular in smart cities, industrial automation, and healthcare. Securing the substantial amounts of data initiated and managed at the edge becomes crucial as IoT devices grow [10]. Edge computing includes some advantages i.e., low latency and bandwidth consumption with IoT devices while the data processing is performed closer to the data source, but this may have security concerns. In this context, quantum cryptography and cellular automata present intriguing avenues for improving security. To address the security issues with probable solutions associated with IoT edge computing, this study explores existing research and finds the security dumps where some work should occur [11]. Table 1 represents IoT edge computing-based research or applications with use cases and security concerns.

2.1 *Motivation and objective of the research*

The brisk spread of IoT edge computing in various reformed multiple applications by presenting real-time data processing diminished latency and advanced operational efficiency. But this concept causes with it significant security risks. Regardless of their notable allowances, the security concerns motivate the authors to improve the challenges. Due to the security loopholes of IoT edge computing the proposed research was initiated with the following objectives:

- Integrate Cellular automata with quantum key cryptography to introduce a new model to enhance the data security and integrity of IoT edge computing.
- Protect the IoT edge computing systems from the different types of attacks.

3. Integration of CA with quantum cryptography

The Cellular Automata has profound integration flexibility to introduce a new model. The proposed research expenditures the flexibility of the CA with quantum cryptography to generate a secured key for encryption and decryption of the data of an IoT edge computing-based system. Figure 1 depicts the integration approach for secured key generation, communication, and measuring the data privacy and integrity of IoT devices. Cellular Automata can work with one or two-dimensional types of grid data structure, where each grid stores an initial value which is treated as the current state of the automata. A transition state or rule of the CA could be defined by analyzing the nearby grids. The rule examines the current state of the grid and quantum information maintained by the quantum protocol and generates a secured key. The key could be useful to maintain the privacy of IoT edge computing data and communication. Algorithm 1 represents the steps of the key generation and encryption process of the IoT edge computing systems. Algorithm 2 helps to generate a quantum cryptography key using the User's original string and a random string. The original string $\{S_{A1}, S_{A2}, S_{A3}, S_{A4}, S_{A5}, \ldots..,S_{An}\}$ may contain a value of 0 or 1 and the random string $R_A = \{R_{A1}, R_{A2}, R_{A3}, R_{A4}, R_{A5}, \ldots..,R_{An}\}$ and $R_B = \{R_{B1}, R_{B2}, R_{B3}, R_{B4}, R_{B5}, \ldots..,R_{Bn}\}$ contains values H, V, or D. Here H, V, and D represent the horizontal, vertical, and diagonal neighbour values of the grid respectively. The QKD algorithm generates a qubit using the original and random string of the user A as per equation 1. User B generates the original string B_{GS} from the qubit according to equation 2.

$$Qb = \begin{cases} 0 \text{ if } S_{Ai} = 0 \text{ and } R_{Ai} = H \text{ or } V \\ 1 \text{ if } S_{Ai} = 1 \text{ and } R_{Ai} = D \end{cases} \quad (1)$$

$$B_{GS} = \begin{cases} 0 \text{ if } Qb = 0 \\ 1 \text{ if } Qb = 1 \end{cases} \quad (2)$$

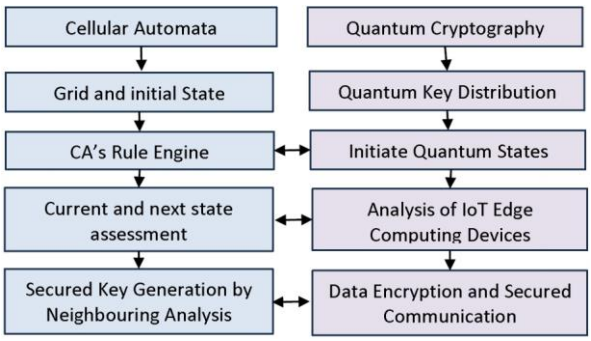

Figure 1
Integration of Cellular Automata and Quantum Cryptography

Algorithm 1: Key Generation and Encryption Process

Step 1: CA grid configuration CA[M][N]
Step 2: CA[M][N] = 0 or 1
Step 3: Transition function definition

$$TF = f(\cup_{i-1,j-1}^{i+1,j+1} CA[i][j])$$

Step 4: Quantum cryptography key generation

$S_A = \{S_{A1}, S_{A2}, S_{A3}, S_{A4}, S_{A5}, \ldots..,S_{An}\}$
$R_A = \{R_{A1}, R_{A2}, R_{A3}, R_{A4}, R_{A5}, \ldots..,R_{An}\}$
$R_B = \{R_{B1}, R_{B2}, R_{B3}, R_{B4}, R_{B5}, \ldots..,R_{Bn}\}$
$S_A \leftarrow$ User A string and $S_A \in (0.1)$
$R_A \leftarrow$ User A random string and $R_A \in (H, V, D)$
$R_B \leftarrow$ User A random string and $R_B \in (H, V, D)$
$Key_{QC} = QKD(S_A, R_A, R_B)$

Step 5: Final secured key generation

$$Key_{Final} = TF\ XOR\ Key_{QC}$$

Step 6: Data encryption $Data_{En} = key_{Final}(Data_{Text})$

Algorithm 2: $QKD(S_A, R_A, R_B)$

Step 1: $n \leftarrow length\ of\ string$
Step 2: // User A process
for i =1 to n
if $S_A[i]$==0 and $R_A[i]$==H or $R_A[i]$==V
Qb[i]=0
if $S_A[i]$==1 and $R_A[i]$== D
Qb[i]=1
Step 3: //User B process
for i =1 to n
if Qb[i]==0 and $R_B[i]$==H or $R_A[i]$==V
S[i]=0
if Qb[i]==1 and $R_B[i]$== D
S[i]=1

4. Experimental Results and Performance Analysis

To perform the experimental results of the proposed research, an experimental setup was initiated with the help of 25 IoT devices and sensors related to the smart city, healthcare, agriculture, and vehicle automation. An edge server has been configured with the devices for communication and data processing. The results of the setup were simulated by considering the following criteria.

- Key generation and distribution time
- Computational overhead
- Encryption and decryption time
- Security level and Attack Simulation

The key generation and distribution time criteria include the time taken by the CA's transition function, quantum cryptography and final key generation, and key distribution process. The computational overhead of the model is measured by including CPU latency, memory, and resource usage cost. The security level of the encrypted data was simulated by applying different types of attacks i.e., eavesdropping, DoS, and man-in-middle attacks. Table 2 represents the average performance measures using time consumption, computational overhead, and security level assessments.

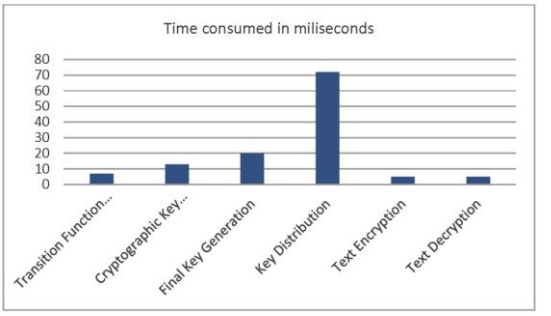

Figure 2

Time consumption assessment while preserving data privacy and communication

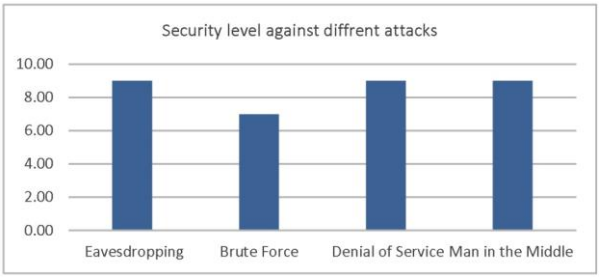

Figure 3

Security level attacks assessment while preserving data privacy and communication

The performance assessment of the combined approach of cellular automata and quantum cryptography to enhance the security of IoT edge computing using time consumption and different security level attacks are depicted in Figures 2 and 3. The results showing the integrated approach for enhancing the security of IoT edge computing systems claim:

- The system realm the data privacy from the unauthorized access.
- Provide secured communication against attacks.
- Maintain the integrity of the systems.

Table 2
Average performance measures using time consumption, computational overhead, and security level assessments

Performance Measures Criteria	Measures Parameters	Units
Average time consumption	Transition Function Definition	7ms
	Cryptographic Key Generation	13ms
	Final Key Generation	20ms
	Key Distribution	72ms
	Text Encryption	5ms
	Text Decryption	5ms
Average Computation Overhead	CPU Latency	213ms
	Memory Usage	23%
	Resource utilization	92.4%
	Energy Consumption	180 mJ
	Processing Speed	$55 * 10^6$ Hz
Security Level and Attacks Simulation	Confrontation to Eavesdropping	High
	Confrontation to Brute Force	Moderate
	Confrontation to Denial of Service	High
	Confrontation to Man in the Middle Attack	High

5. Discussion and Conclusion

This study presents an enhanced model by integrating quantum cryptography and cellular automata concepts to ensure the data privacy of IoT edge computing systems. The proposed integration addresses the challenges of IoT edge computing related to security and privacy. The proposed model has experimented on various IoT devices related to various applications and measured the performance using multiple parameters i.e., time, computation overhead, and security attacks. The results shown in the table express that, the proposed model is fast and protects the data at moderate and high levels.

The proposed method consumes more time while distributing the cryptographic key between the communication parties. The future scope of the study is to reduce the overall time while preserving data privacy.

References

[1] S. K. Sharma and A. Kumar, "A cellular automata approach for extending data privacy and security of edge computing," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 27, no. 2-B, pp. 601–612 (2024), doi: 10.47974/JDMSC-1894.

[2] Z. Yang, M. Zolanvari, and R. Jain, "A survey of important issues in quantum computing and communications," *IEEE Communications Surveys & Tutorials,* vol. 25, no. 2, pp. 1059–1094, Second Quarter (2023), doi: 10.1109/COMST.2023.3254481.

[3] S. Li, Y. Chen, L. Chen, J. Liao, C. Kuang, K. Li, W. Liang, and N. Xiong, "Post-quantum security: Opportunities and challenges," *Sensors,* vol. 23, p. 8744 (2023). [Online]. Available: https://doi.org/10.3390/s23218744.

[4] S. K. Sharma, C. S. Lamba, and V. S. Rathore, "Radius based cellular automata approach for image processing applications," in Proc. 8th Int. Conf. on Computing, Communication and Networking Technologies (ICCCNT), Delhi, India, pp. 1–5 (2017), doi: 10.1109/ICCCNT.2017.8203990.

[5] H. Omrany, K. M. Al-Obaidi, M. Hossain, N. A. M. Alduais, H. S. Al-Duais, and A. Ghaffarianhoseini, "IoT-enabled smart cities: A hybrid systematic analysis of key research areas, challenges, and recommendations for future direction," *Discover Cities*, vol. 1, no. 2 (2024). [Online]. Available: https://doi.org/10.1007/s44327-024-00002-w

[6] O. Peter, A. Pradhan, and C. Mbohwa, "Industrial internet of things (IIoT): Opportunities, challenges, and requirements in manufacturing businesses in emerging economies," Procedia Computer Science, vol. 217(C), pp. 856–865 (2023).

[7] K. H. Almotairi, "Application of internet of things in healthcare domain," *Journal of Umm Al-Qura University for Engineering and Architecture*, vol. 14, pp. 1–12 (2023). [Online]. Available: https://doi.org/10.1007/s43995-022-00008-8.

[8] A. K. Singh, "Smart farming: Applications of IoT in agriculture," in Handbook of Smart Materials, Technologies, and Devices, C. M. Hussain and P. Di Sia, Eds. Cham: Springer (2022). [Online]. Available: https://doi.org/10.1007/978-3-030-84205-5_114.

[9] T. Pradhan and P. Patil, "Quantum cryptography for secure autonomous vehicle networks: A review," in 2024 IEEE Int. Students' Conf.

on *Electrical, Electronics and Computer Science* (SCEECS), Bhopal, India, pp. 1–10 (2024), doi: 10.1109/SCEECS61402.2024.10482142.

[10] J. Li, W. Liang, W. Xu, Z. Xu, Y. Li, and X. Jia, "Service home identification of multiple-source IoT applications in edge computing," *IEEE Transactions on Services Computing*, vol. 16, no. 2, pp. 1417–1430, Mar.–Apr. (2023), doi: 10.1109/TSC.2022.3176576.

[11] T. Aljrees, A. Kumar, K. U. Singh, and T. Singh, "Enhancing IoT security through a green and sustainable federated learning platform: Leveraging efficient encryption and the Quondam signature algorithm," *Sensors*, vol. 23, no. 19, p. 8090 (2023). [Online]. Available: https://doi.org/10.3390/s23198090.

Received October, 2024