

## Research Article

# Securing 5G-IoT Device Connectivity and Coverage Using Boltzmann Machine Keys Generation

Anand Singh Rajawat ,<sup>1</sup> Pradeep Bedi ,<sup>2</sup> S. B. Goyal ,<sup>3</sup> Piyush Kumar Shukla ,<sup>4</sup> Sajjad Shaukat Jamal ,<sup>5</sup> Adel R. Alharbi ,<sup>6</sup> and Amer Aljaedi ,<sup>6</sup>

<sup>1</sup>Department of Computer Science Engineering, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India

<sup>2</sup>Lingaya Vidyapeeth, Haryana, Faridabad, India

<sup>3</sup>City University, Petaling Jaya, Malaysia

<sup>4</sup>Computer Science and Engineering Department, University Institute of Technology,

Rajiv Gandhi Proudyogiki Vishwavidyalaya, (Technological University of Madhya Pradesh), Bhopal 462023, India

<sup>5</sup>Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

<sup>6</sup>College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia

Correspondence should be addressed to S. B. Goyal; [drsbgoyal@gmail.com](mailto:drsbgoyal@gmail.com)

Received 9 July 2021; Accepted 7 September 2021; Published 8 October 2021

Academic Editor: Vijay Kumar

Copyright © 2021 Anand Singh Rajawat et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In terms of growth, effect, and capability, the 5G-enabled Internet of Things (IoT) is incredible. The volume of data distributed and processed by IoT (Internet of Things) systems that trust connectivity and coverage raises some security problems. As IoT technology is directly used in our daily lives, the threats of present cyberspace may grow more prominent globally. Extended network life, coverage, and connectivity are all required for securing IoT-based 5G network devices. As a result of these failures, there are flaws that lead to security breaches. Because purposeful faults can quickly render the entire network dysfunctional, they are more difficult to identify than unexpected failures. Securing IoT-based 5G Network Device Connectivity and Coverage for expending Encryption and Authentication Scheme (EAS) framework is proposed in this study, which uses novel security flaws. In this research, we proposed a Boltzmann machine (BMKG)-based encryption algorithm for securing 5G-enabled IoT device network environment and compared various asymmetric algorithms for key exchange.

## 1. Introduction

Although 5G is still in its initial stages of testing, it has been establishing new standards. Those contribute to a particular set of regulations that apply to the complete international communications system. That is the magnitude of the shift that 5G [1] will bring. In addition, the Internet of Things (IoT) is evolving, and several organizations that use it are starting to plan for 5G. When we expect the incredible advantages that 5G delivers, this is certainly reasonable: providing resources, lower latency, a much more effective process experience, a more frictionless user experience, the capability to change and modify whole networks without impacting activities, and enormous increase in speed.

According to a recent report, researchers are concerned about the impact of 5G on IoT [2] device communication security. They understand that cyber-attacks [3] can have a significant consideration of critical economic activities. The issue here is rooted in the essentials of IoT architecture. Every device connected to the network represents a possible specific target for cybercriminals. Because of the significant number of devices in the system, the big businesses that use IoT architecture do not have a clear picture of the entire network [4]. This is extremely concerning, as a single device's vulnerability might harm the existing network if hackers discover it. Furthermore, as many as 90% of these businesses expect a significant increase in the number of devices in their IoT networks as a result of the current

scenario. Aside from the underlying security issues [5] with IoT, 5G adds to the mix. Criminals and hackers can intercept data as it travels over the network, creating more trouble than we now experience in 4G networks. Considering the shortcomings in 5G and IoT infrastructures, there are ways to ensure security.

Furthermore, companies are coming to realize this and are making the necessary security modifications as a result. IoT security must be addressed early in the design phase rather than after deployment. Following their implementation, it will be more difficult to keep all devices and determine whether they are appropriately protected. It is critical to understand that the Internet of Things (IoT) requires multiple levels of security, covering hardware, software, storage, network, apps, and so on. To secure the security level of the IoT network, every layer must be connected to the others and evaluated accordingly. It is important to keep in mind that IoT security is only as good as its weakest link. That includes the ability for the communication system to be secure; each endpoint and device should be secured. Furthermore, all of those recommendations are taken into interpretation and handled by implementing an acceptable 5G security assurance structure. It is critical to take these future concerns seriously now before they become big problems. The rapid advancement of communication and wireless technologies is creating the foundation for the Internet of Things (IoT), which involves networking a wide range of physical objects. 5G-IoT device applications include smart cities, innovative health, intelligent transportation, automation, and disaster response [6]. As a result of this trend, massive amounts of data are generated. Wireless networks are handling more than 100 times more IP data than wired networks. To meet the demand for new 5G-IoT device services, the fifth generation (5G) of mobile communication will be introduced [3] to offer 1000 times more mobile data volumes, 10–100 times more connectors, data rates per unit area, and five to six times less data latency [7].

Furthermore, to decrease response latency, access network nodes such as base stations, routers, and switches were virtually updated using computing and storage resources. Fog-proximate fog nodes for low-latency 5G-IoT device [8] applications can be cached with service data by integrating Fog computing. Finally, IoT nodes are used to anonymize data and prevent attackers from figuring out how to configure the system an intelligent arbitrary transmitting procedure that applies these Boltzmann machines (BM) methods with Connectivity and Coverage for Exhausting Encryption and Authentication Scheme [9]. Also, this research paper proposes a new asymmetric key encryption and decryption structure for text letters to overcome obtainable protection problems in traditional ciphers [10] by using a Boltzmann machines (BM) design and a key age group device that increases the protection of the classification. The layout of the paper is as follows: Section 2 discusses the related work, Section 3 describes 5G-enabled IoT network and device security, Section 4 proposes methodology, which contains a comprehensive description of encryption and decryption processes, and Section 5 describes the utilization

of the concept and process of Boltzmann machines (BM) work to build a system that predicts whether a user will like or dislike a movie based on previous viewings in our proposed methodology, and the next section describes the notion of restricted BM to contribute in our proposed methodology. Section 6 describes contrastive divergence. Section 7 focuses on the security of IoT device connectivity using the BM machines key. Section 8 proposes the performance criteria and parameters with existing systems. Finally, Section 9 covers the conclusion and future work of the proposed system.

## 2. Related Work

Ni et al. [1] proposed a framework for service-driven authentication that supports 5G-enabled IoT network slicing and fog computing. Shin et al. [11] provided security that is fully validated using BAN-logical and Automated Internet Security Protocols. Shin et al. [12] implemented the system architecture that takes WSN integration and 5G for IoT into account. Based on Shin et al. [13] and system architecture analysis, we propose an authentication, authorization, and key WSN agreement scheme for the 5G-integrated IoT and elliptic cryptography (ECC) basic private protection scheme. Li et al. [14] proposed the Internet of Things system and a node-oriented, secure data transfer algorithm (NOSDT) in the social network. Kim et al.'s [15] proposed protocol has been formally verified as correct by AVISPA and BAN logic. Spinelli et al. [16] concentrated on 5G and network virtualization, as well as the MEC innovative resource deployment's flexibility and migratory abilities. Sufian Hameed et al. [17] have identified, classified, and addressed several security concerns and province initiatives to address these issues in this work. Based on respective optimization goals, Mohammadi, Mehdi et al. [18] examined the efforts that are divided into power consumption optimization, network performance optimization, and QoS optimization. Iraji et al. [19] proposed the latest advancement in M2M communications and the Internet of Things: A Proposed Approach (IoT). Because of the growing expansion in huge IoT threats, Ahmad, Rasheed et al. [20] found that it is critical to design algorithms that incorporate cutting-edge Big Data analytics and machine learning technologies, and determining the correct algorithms and models to identify IoT attacks in real or close to real time requires accuracy and efficiency. El Boudani et al.'s [21] 3D interior navigation in cross smart industries or hugely complicated structures will advantage from the proposed method. In addition, utilising current techniques such as the SVM and KNN approaches in Table 1, it was discovered that the recommended model worked well.

## 3. 5G-Enabled IoT Network and Device Security

The four logical parts of today's telecommunication networks are the radio access network, core network, transport network, and connector network. The control plane is responsible for signaling traffic, the user plane for payload (actual-) traffic, and the managed plane for administrative traffic. Each network component includes three so-called

TABLE 1: Comparative description of the 5G network service attack.

S. no.	Study	Security issue	Description of the attack
1.	Hu et al. (2021)	Denial-of-service (DoS) attacks	The 5G network service and resources will be unavailable for dedicated users due to disruption of services
2.	Alshouili et al. (2021)	Spoofing attacks	Programs are used to classify altering data to receive unfair advantages
3.	Ahmad et al. (2018)	Denial-of-service (DoS) attacks	The 5G network service and resources will be unavailable for dedicated users due to disruption of services
4.	Shaik et al. (2019)	Man-in-the-middle (MitM) attacks	Many resources are used to leak the information between 5G network protocols, servers, or clients
5.	Fang (2021)	Side-channel attack	Important information received from the implementation of 5G technology system

planes, and each of which delivers a different type of traffic. Each of the three planes can be subject to different dangers in terms of network security [22]. Other threats can affect all three domains at once.

The 5G-enabled IoT device security system is made up of the following fundamentals: operators, manufacturers, and other stakeholders develop [23] norms for how global networks interact through standards. This entails evaluating the best ways to protect IoT device networks and people from malicious attacks. Network design and network suppliers design: construct and implement agreed-upon standards for functional network parts and systems that are crucial to the performance and security of the end network product. Network configuration: during the deployment phase, networks are configured for a specific security level, which is essential for setting security settings and further increasing the network's security and resilience—implementation and operation of networks; the operations that allow networks to function. To achieve the appropriate levels of security, the platform's implementation is crucial. 5G is fundamentally different from previous IoT device generations from the user's perspective. In the long run, machine-to-machine (M2M), D2D communication, which 5G enables, is widely predicted to become a strategic discriminator and unique proposition for 5G. 5G networks, among other things, will be critical infrastructure for digitization, automation, and connectivity to machines, robots, and transportation systems. As a result, there is a big amount of money on the line and a wide range of risk tolerance.

### 3.1. 5G-Enabled IoT Device Layer

**3.1.1. Layer of Application Security.** Mobile device users (UEs), as well as vertical industries that produce and employ a variety of applications, are included in the scope of the application security layer. To secure the security of 5G networks and the users and services they support, a multiparty collaboration between MNOs, UE suppliers, application developers, and service providers is required.

Network security multilayered approach: Figure 1 shows the network security multilayered approach. The IoT network device communication typically manages, controls, and operates the network security layer; however, some components may be outsourced to specialized service

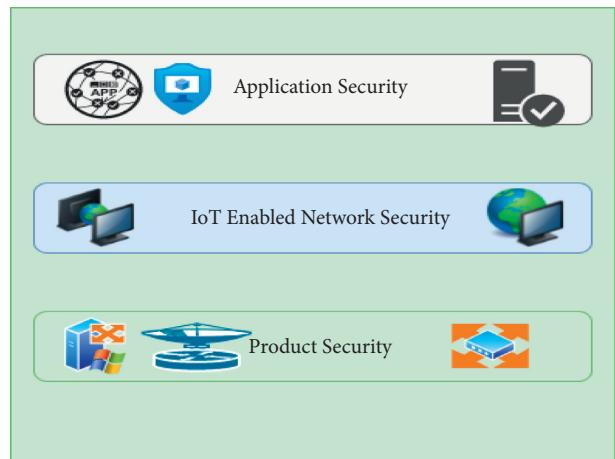


FIGURE 1: 5G-enabled IoT network and device security—a multilayered approach.

providers. IoT network device communication conduct a complete and continual risk assessment during the network design process, considering network components, provided network functionalities, and network architecture to provide effective security threat management. The layer of protection for the product device, such as device providers or network equipment suppliers, is responsible for product security. The security assurance of network elements is a critical technique for determining if network devices and components have been developed and deployed according to defined security standards.

A new era of network security begins with the introduction of encryption in 5G. All data sent across a 5G radio network, for example, a device to a network, are encrypted, integrity-protected, and subject to mutual authentication. The 3GPP and other standardization bodies do not have a standard for how functions are designed and realized. The main purpose of the specifications is to provide compatibility across the many functions required to provide network connectivity. Virtualization and cloud deployments, as a result, are rarely referenced in the specifications. These issues will be addressed throughout the implementation and deployment phases. Malware that infects devices or gets a footing early in a targeted IT system [24] is still frequent. Simultaneously, malware that is anything but simple might

target sophisticated equipment used in telecommunication networks.

#### 4. Proposed Methodology

This research work aims to create a keys generation algorithm in 5G-enabled IoT device communication network that effectively encrypts and decrypts utilizing Boltzmann machines. We developed a more reliable and effective keys generation method [25] that uses deep learning-based BM algorithm. The preliminary results of the delinquent origination are the operative topology and limitations that enable a BM to encrypt and decrypt 2048 binary 8-dimensional vectors successfully. We also train and evaluate the proposed system's robustness by taking into account how sophisticated the braking system will be. To begin, huge random numbers must be generated, the significance of the numbers must be determined, and two enormous numbers must be multiplied. On a modest 32-bit embedded processor, the 2048-bit RSA application will be slow. When multiplying two 2048-bit values, we used the need to use a 64-word multiply operation. The 128-bit symmetric AES key corresponds to the 2048-bit RSA key. The NSA Suite B standard requires a 3072-bit RSA key, equivalent to 256-bit symmetric key encryption.

The RSA elliptical curve shows that computed time increases exponentially as security levels [17] rise. Cryptography is used to solve the discrete logarithm issue. Simply put, finding an elliptical curve with the discrete logarithm of a point is difficult. The real benefit of ECC is that it has a high level of security due to its small key. More temporary keys consume less memory and drastically lower machine requirements. With a 256-bit key and 256-bit primary curve, ECC [26] is comparable to RSA 2048. As part of the overall security solution, key agreements, asymmetric authentication encryption, hash codes, and digital signatures are used to secure 5G-IoT Device Connectivity and Coverage suites. The crucial feature is that RSA is a comprehensive security suite in and of itself, with asymmetric encryption and signatures. Alternatives to RSA are used in one key exchange technique and a different mechanism for signing. The mechanism for generating RSA key pairs has been given.

On the other hand, Diffie–Hellman and RSA require keys to be quite long (2048 bits or more). Curve elliptical Diffie–Hellman algorithm is a Diffie–Hellman method that uses elliptical cryptography. The protocol's proposed goals are as follows.

Mutual authentication: securing 5G-IoT Device Connectivity and Coverage should authenticate one another during the handover process:

- (i) Integrity: any unauthorized entity cannot modify the data transmitted via an open channel
- (ii) Key exchange: the session keys were to be negotiated by both parties without any leakage
- (iii) Privacy: in the exchanged messages, the true identity of 5G-IoT device must not be revealed
- (iv) Defense against: any malignant 5G-IoT device attacks should be dealt with

#### 5. Boltzmann Machines

The Boltzmann machines [27] work and build a system that predicts whether a user will like or dislike a movie based on previous viewings. Even though the types of nodes differ, Boltzmann considers them the same, and all work as one system. The Boltzmann machine receives the training data and adjusts the system that weights accordingly. By teaching us how the system works under normal conditions, Boltzmann machines help us understand abnormalities. The Boltzmann distribution contains different system-based conditions that are responsible for generating other machine states. On increasing the energy, the probability of being in the ground state decreases. Figure 2 shows the working of Boltzmann machines. Therefore, the state level is inversely proportional to the energy level.

Boltzmann machine distribution: we applied BM approach for crypto key generation for distributing the sample formula for crypto key generation.

$$P_i = \frac{e^{(-\epsilon_i/kT)}}{\sum e^{(-\epsilon_j/kT)}},$$

$$P_i = \frac{\phi e^{(-\epsilon_i/kT)}}{\sum e^{(-\epsilon_j/kT)}},$$
(1)

where  $P_i$  represent the probability of a system being in state  $i$ ,  $\epsilon_i$  represent the energy in  $i$ th state,  $T$  is the temperature, and  $k$  is the Boltzmann constant, finally to represent the all possible state  $\sum e^{(-\epsilon_j/kT)}$ .

Update Restricted Boltzmann Machines (RBMs with energy model)

---


$$E(\text{Visible nodes, hidden nodes}) = - \sum a_i \text{Visible nodes}_i - \sum b_j \text{hidden nodes}_j - \sum \sum \text{Visible nodes}_i w_{ij} \text{hidden nodes}_j,$$
(2)


---

$H$ =hidden nodes,  $V$ =visible nodes, and  $a$  and  $v$  represent the content biases.  $P$  (visible nodes, hidden nodes)=probability of presence in a certain state (CS);  $P(v, h) = e^{-E(\text{Visible nodes, hidden nodes})}/Y$ , in which  $Y$  represents all possible states.

We are bringing the RBM close to our film set to contrast divergence. RBM determines features that are essential during the training process. Depending on whether a user liked this film (1), did not like it (0), or did not look at it, the

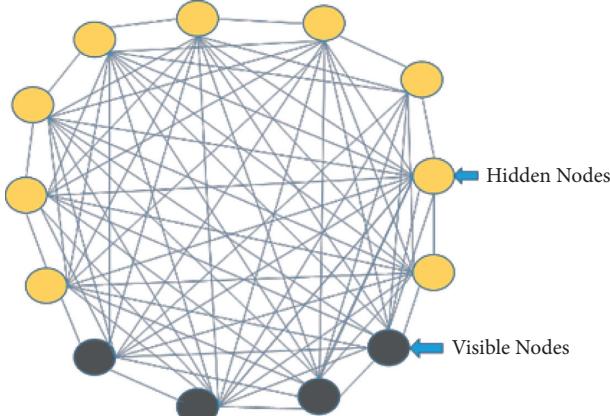


FIGURE 2: Working Boltzmann machines.

training data are either 0 or 1 or missing data (missing data). RBM recognizes key features on its own.

### 5.1. Training to Prediction of Key

- Step 1: train the model with the all the customers' data
- Step 2: during inference time, identify the exact user's training data
- Step 3: analyze the data to find the hidden neuron's activations
- Step 4: calculate the input neuron activations using the hidden neuron values
- Step 5: the changed values of input neurons represent the user's rating

## 6. Contrastive Divergence

Primarily, RBM adjusts its weights as needed. RBM computes [28] the hidden nodes by employing the same weighing method used to reconstruct the input nodes but with a random initial weight assignment. Every hidden node consists of all nodes, and every visible node constructs itself from all of the hidden nodes, and therefore, the input differs, although its weights are the same, from the reconstructed input. The process goes on until the reconstructed entry corresponds to the previous entry. At this stage, the process is expected to converge. All this is called a Gibbs sampling process. Every node is connected to every other node in a complete Boltzmann machine, and the connections are exponentially increasing. That is why we use RBMs. Figure 3 shows the weight of the system and gradient approach. The node connections in RBMs are restricted accordingly—cannot connect hidden nodes and connected, visible nodes, for example, energy function for Boltzmann limited machine.

- (i) Represent the weight of the system and gradient formula applied to a specific system
- (ii)  $D/D_{w_{i,j}} (\log (P(\text{Visible nodes}_0))) = \langle \text{Visible nodes}_{i_0} * \text{Hidden nodes}_{j_0} \rangle$
- (iii)  $\langle \text{Visible nodes}_{i_0} * \text{Hidden nodes}_{j_0} \rangle$  Initial state

- (iv)  $\langle \text{Visible nodes}_{i_\infty} * \text{Hidden nodes}_{j_\infty} \rangle$  Final state
- (v)  $w_{ij}$  represent the weight
- (vi)  $P(\text{Visible nodes}_{i_0})$  represent the probability of the system state

## 7. Securing IoT Device Connectivity

IoT devices establish network connections. Companies should restrict network connections to 5G-IoT devices [29] and only connect with them through firewalls and access control lists; “5G-IoT device will never be able to connect with internal systems in the form of a one-way trust principle, which can limit an attacker’s ability to use it as a jump point to exploit and attack network segments.” While this does not prevent adversaries from attacking systems directly, it limits their ability to move laterally in networks. Businesses can also force 5G-IoT device connections via jump hosts and/or network proxies. “The organization can then inspect network traffic by proxying the connection in a funnelling point before proceeding to and from IoT devices, and more effectively question [traffic],” he explained. Figure 4 shows 5G-IoT Device Coverage using Encryption and Authentication Scheme to determine whether their traffic and payload are suitable for the 5G-IoT device receipt or transmission.

Deep learning has had a significant impact on AI [30] and mechanical learning. Meanwhile, algorithms have been demonstrated to solve certain problems efficiently that are intractable with traditional computers. We show that unlike conventional computing not only reduces the time required to train a profoundly restricted Boltzmann machine but also provides a more rendered and comprehensive framework for profound learning. Our proposed methods can also be used to train multilayer and fully connected models efficiently. We established an unorthodox article to layout a robust and functional asymmetric key cryptography framework as a consequence of on Boltzmann machines. The calibration of a Boltzmann machine neural network is to make it capable of encrypting and decrypting both the unimpaired set and the impaired set. To prove that the system is safe against attacks, a performance study and a theoretical security analysis are being undertaken.

The encryption and decryption processes occur when interchanging information [31]. First, each character of the plain text becomes its representation.

All nine neuron outputs are concealed within a single hidden layer responsible for composing the encrypted version of each eight-bit input set for each input set. Because the activation function of the hidden layer has a range of [0, 1], the outputs of the hidden layer are floating-point values that fall within that range. Finally, each 9-dimensional vector consists of the ciphertext, which forms an array of floating-point with 9 lengths multiplied by the features available that the given data have, as shown in Figure 5

Each floating-point number vector produced in the output layer, 13-dimensional after each block is processed, will be discretized with an application of the threshold function and transformed again. It is important to note that

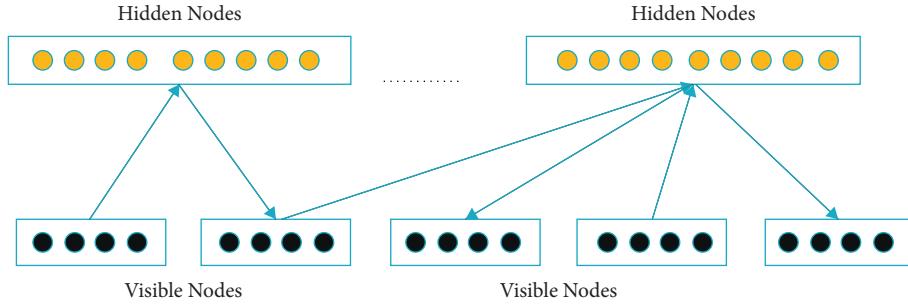


FIGURE 3: Weight of the system and gradient approach.

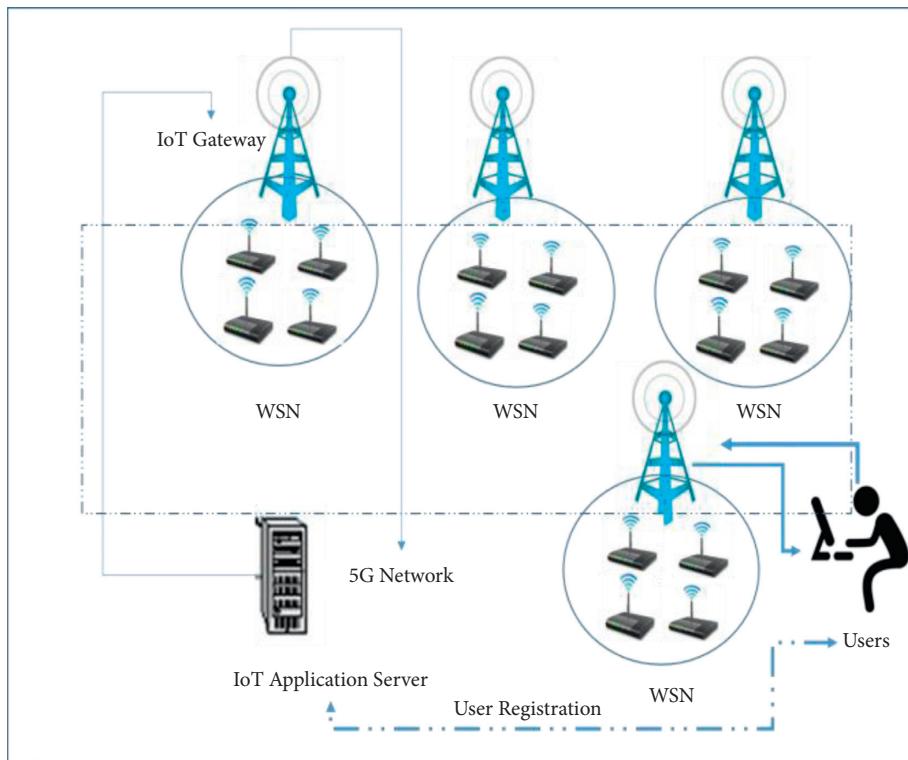


FIGURE 4: 5G-IoT device Coverage using Encryption and Authentication Scheme.

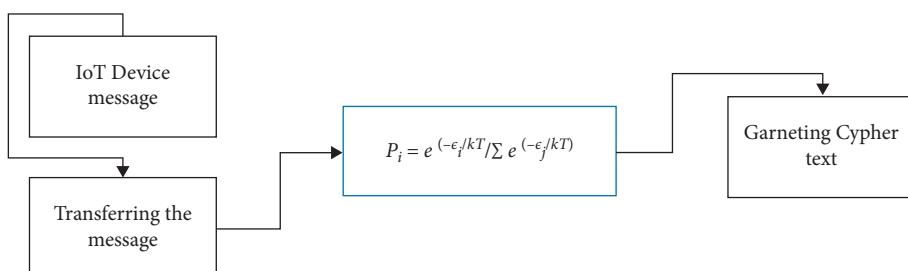


FIGURE 5: Encryption process.

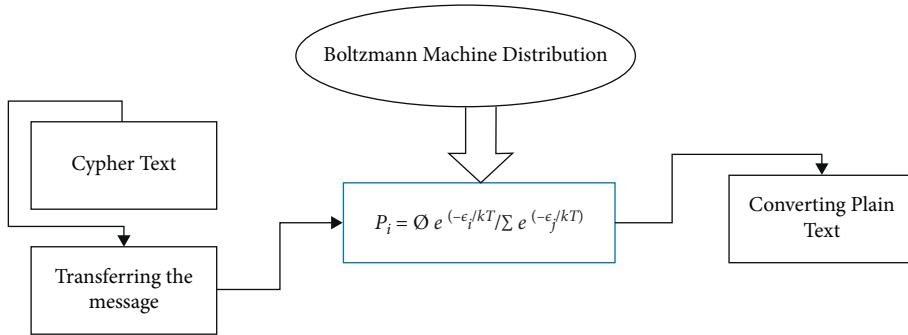


FIGURE 6: Decryption process.

TABLE 2: Evaluation of encryption time with existing study.

Input size	Diffie-Hellman (1024 bits)	RSA (2048 bits)	ECC (256 bits)	Elliptical cryptography (ECDH) (256 bits)	BM keys generation (2048 bits)
800 kB	390	377	288	359	100
6 MB	370	570	599	580	150
12 MB	579	588	688	820	300
40 MB	398	356	288	350	500
100 MB	388	545	592	568	600

this method allows each communication party to encrypt and decrypt data, as shown in Figure 6.

## 8. Performance Evaluation Parameters

It is necessary to have a thorough knowledge of the performance characteristics of a particular algorithm before it can be used in an application. In this work, an analysis of the following metrics is done to compare the proposed system's performance between different cryptographic algorithms.

- (i) Encryption time: the length of time it takes to encrypt data directly impacts the overall system performance. In an ideal situation, the encryption time should be quick enough to ensure speed and responsiveness. Milliseconds are often used to measure time.
- (ii) Decryption time: decryption time is the difference between recovering the plain text from the encrypted text. The time required for decryption is measured in milliseconds in this study. Analysis of security risks parameters: a handful of factors have been developed to build the suggested system's security analysis [27].

That experiment was performed with Linux-5.11.11 and a laptop Core I7, 3.5 GHz; we used the Omnet++ simulator to experiment with different inputs, and the outcomes were associated with various implementations and hardware results. In this manner, an overview of the proposed system's behavior concerning classic algorithms can be obtained—the encryption measurement time. A set of data files was evaluated while the proposed method was running. These files range in size from 800 kB, 6 MB, 12 MB, 40 MB, to 100 BM and are made up of alphanumeric characters. The time elapsed was calculated using Scala functions and compared with the encryption times. The decryption time is

measured. The run-of-the-mill encryption time of the anticipated coordination was matched with the discoveries and performance comparison between cryptographic algorithm and proposed BM. Table 2 shows that the encryption time was measured in milliseconds.

The encryption time [32] was calculated in seconds for this experiment. In this experiment, file size range was tested, and encryption time was calculated in seconds. The second set of studies was done on decryption time, which was measured. The findings were acquired by running the system 10 times compared to the suggested method's average decryption time [33]. Next, the time required for decryption was compared with previously conducted research. The experiment's results were summarized in Table 3. The study found that the suggested approach is marginally faster, whereas standard methods (i.e., ones that do not include biometrics) decode data more quickly than they encrypt it.

Furthermore, the proposed system's performance is comparable with that of traditional systems [34] for files with sizes ranging from 800 kB, 6 MB, 12 MB, 40 MB, to 100 BM. Instead, the proposed system's performance suffers noticeably. As a result, the proposed encryption system's security analysis took hundredths of decimal units into account; furthermore, tenths significantly reduce the proposed system's accuracy [35].

Figure 7 shows the proposed BMKG (Boltzmann machine keys generation) and existing cryptographic technique 5G enabled IoT device. Communication execution time was used to conduct the evaluation.

Improvements were achieved. Figure 8 shows that the execution time to offload data to the cloud of applications running on the network's edge is reduced [36] due to the high availability of resources. We also tested the performance of our distributed BM-based cloud architecture by creating, updating, deleting, and sharing files. We generated

TABLE 3: Evaluation of description time.

Input size	Diffie–Hellman (1024 bits)	RSA (2048 bits)	ECC (256 bits)	Elliptical cryptography (ECDH) (256 bits)	BM keys generation (2048 bits)
800 kB	296	290	199	298	80
6 MB	275	480	470	460	120
12 MB	490	510	599	792	220
40 MB	310	298	198	198	420
100 MB	298	480	489	499	510

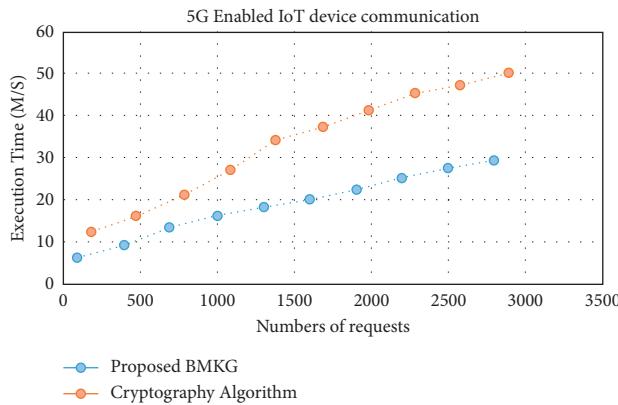


FIGURE 7: Comparative analysis proposed BMKG (Boltzmann machine keys generation) and existing cryptographic algorithm.

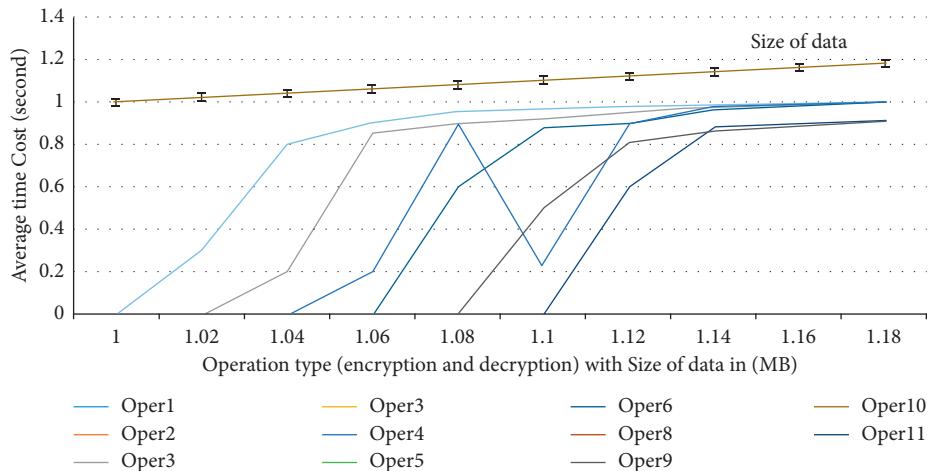


FIGURE 8: Response time and average data retrieval time cost by operation type (encryption and decryption) and data size in megabytes (MB).

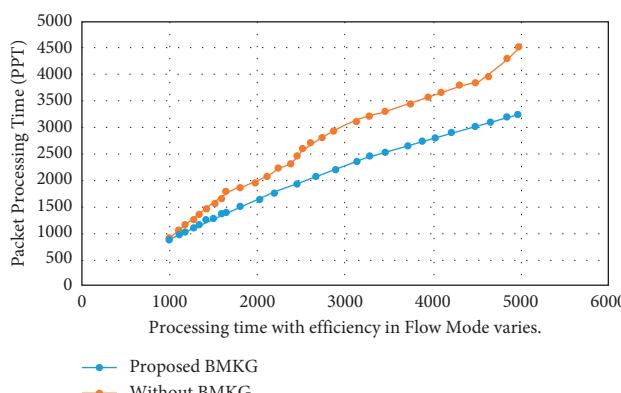


FIGURE 9: Processing efficiency in flow mode varies in comparison with proposed BMKG and without BMKG.

random file names and contents with a file size of up to 4 MB to demonstrate the average response time and data retrieval [37] overhead with various file sizes. The results reveal that the proposed model outperformed the core model while consuming the least number of resources [38]. We calculated the suggested model's attack detection accuracy rate at the fog node using two alternative parameters. In the presence of various traffic and many distinct flaws in the network [39], we examined one parameter and another parameter in the real-time detection of network attacks [40–42].

Figure 9 shows processing efficiency with variation in flow mode, showing that the proposed model maintains a high flow mode flow even at a high packet-in. The operator overhead merely requires the throughput.

## 9. Conclusion and Future Work

In this research, we present a safe and efficient IoT authentication system for 5G network services. This framework provides a privacy-preserving slice selection method that enables 5G-IoT nodes to select appropriate data transmission network slices while concealing user access types. Users can connect to 5G-IoT device servers anonymously and create a secure data channel to retrieve cached data on the local 5G-IoT device, which will be preserved on a remote server. To show that the proposed approach framework is safe and secure, simulation, efficiency, and practicality are used. In the future, we will build network-based secure protocols with efficient access delegation and retransition into 5G networks with authenticated data protection.

## Data Availability

Data are available and will be provided to reviewers as per demand.

## Conflicts of Interest

All authors declare that they do not have any conflicts of interest.

## Acknowledgments

The authors extend their gratitude to the Deanship of scientific research at King Khalid University for funding this work through research group program under grant number. R.G.P. 1/77/42.

## References

- [1] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 3, pp. 644–657, 2018.
- [2] D. Shin, K. Yun, J. Kim, P. V. Astillo, J. Kim, and I. You, "A security protocol for route optimization in DMM-based smart home IoT networks," *IEEE Access*, vol. 7, pp. 142531–142550, 2019.
- [3] S. Shin and T. Kwon, "A privacy-preserving authentication, authorization, and key agreement scheme for wireless sensor networks in 5G-integrated Internet of things," *IEEE Access*, vol. 8, pp. 67555–67571, 2020.
- [4] S. Shin and T. Kwon, "Two-factor authenticated key agreement supporting unlinkability in 5G-integrated wireless sensor networks," *IEEE Access*, vol. 6, pp. 11229–11241, 2018.
- [5] X. Li and J. Wu, "Node-oriented secure data transmission algorithm based on IoT system in social networks," *IEEE Communications Letters*, vol. 24, no. 12, pp. 2898–2902, 2020.
- [6] J. Kim, P. V. Astillo, and I. You, "DMM-SEP: secure and efficient protocol for distributed mobility management based on 5G networks," *IEEE Access*, vol. 8, pp. 76028–76042, 2020.
- [7] B. Bordel, R. Alcarria, T. Robles, and M. S. Iglesias, "Data authentication and anonymization in IoT scenarios and future 5G networks using chaotic digital watermarking," *IEEE Access*, vol. 9, pp. 22378–22398, 2021.
- [8] F. Spinelli and V. Mancuso, "Toward enabled industrial verticals in 5G: a survey on MEC-based approaches to provisioning and flexibility," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 1, pp. 596–630, 2021.
- [9] F. Ullah, M. R. Naeem, L. Mostarda, and S. A. Shah, "Clone detection in 5G-enabled social IoT system using graph semantics and deep learning model," *International Journal of Machine Learning and Cybernetics*, 2021.
- [10] Alani and M. Mohammed, "Applications of machine learning in cryptography: a survey," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, Kuala Lumpur, Malaysia, January 2019.
- [11] B.-H. Kim and J.-Y. Pyun, "ECG identification for personal authentication using LSTM-based deep recurrent neural networks," *Sensors*, vol. 20, no. 11, p. 3069, 2020.
- [12] F. Hu, X. Xu, T. Peng, C. Pu, and L. Li, "A fast pseudo-stochastic sequential cipher generator based on RBMs," *Neural Computing & Applications*, vol. 30, pp. 1277–1287, 2018.
- [13] K. Alshouili and D. P. Agrawal, "Confluence of 4G LTE, 5G, fog, and cloud computing and understanding security issues," in *Fog/Edge Computing for Security, Privacy, and Applications*, Springer, Cham, Switzerland, 2021.
- [14] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G security challenges and solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, 2018.
- [15] A. Shaik, R. Borgaonkar, S. Park, and J. P. Seifert, "New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pp. 221–231, May 2019.
- [16] H. Fang, "Efficient defense against covert and side channel attack on multi-core processor using signal processing techniques," Doctoral Dissertation, The George Washington University, Washington, DC, USA, 2021.
- [17] C. Jothikumar, K. Ramana, V. D. Chakravarthy, and S. Singh, "An efficient routing approach to maximize the lifetime of IoT-based wireless sensor networks in 5G and beyond," *Mobile Information Systems*, vol. 2021, Article ID 9160516, 11 pages, 2021.
- [18] Y. Meng, H. Zhao, Z. Yin, and X. Qi, "IOT medical device-assisted foam dressing in the prevention of pressure sore during operation," *Mathematical Problems in Engineering*, vol. 2021, Article ID 5570533, 11 pages, 2021.
- [19] A. Li and S. Yi, "An indoor positioning algorithm for wearable device using deep learning regression prediction model in IoT applications," *Mathematical Problems in Engineering*, vol. 2020, Article ID 8842784, 7 pages, 2020.

- [20] R. Ahmad and I. Alsmadi, "Machine learning approaches to IoT security: a systematic literature review," *Internet of Things*, vol. 14, Article ID 100365, 2021.
- [21] B. El Boudani, L. Kanaris, A. Kokkinis et al., "Implementing deep learning techniques in 5G IoT networks for 3D indoor positioning: DELTA (DeEp Learning-Based Co-operaTive Architecture)," *Sensors*, vol. 20, no. 19, p. 5495, 2020.
- [22] L. Huang, Y. Deng, and B. Wang, "Flow simulation of suspension bridge cable based on lattice-Boltzmann method," *Mathematical Problems in Engineering*, vol. 2016, Article ID 2537581, 7 pages, 2016.
- [23] Y. Qin, J. Liu, S. Zhao, D. Feng, and W. Feng, "RIPTE: runtime integrity protection based on trusted execution for IoT device," *Security and Communication Networks*, vol. 2020, Article ID 8957641, 14 pages, 2020.
- [24] X. Jia, N. Hu, S. Yin, Y. Zhao, C. Zhang, and X. Cheng, "A2 chain: a blockchain-based decentralized authentication scheme for 5G-enabled IoT," *Mobile Information Systems*, vol. 2020, Article ID 8889192, 19 pages, 2020.
- [25] K. Fan, P. Song, and Y. Yang, "ULMAP: ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G," *Mobile Information Systems*, vol. 2017, Article ID 2349149, 7 pages, 2017.
- [26] Y. Li, D. Y. C. Lie, C. Li, D. Zhao, and C. Fager, RF front-end circuits and architectures for IoT/LTE-A/5G connectivity," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 1438060, 2 pages, 2018.
- [27] Z. Xu, W. Liu, J. Huang, C. Yang, J. Lu, and H. Tan, "Artificial intelligence for securing IoT services in edge computing: a survey," *Security and Communication Networks*, vol. 2020, Article ID 8872586, 13 pages, 2020.
- [28] Y. Shi, J. Lin, G. Xiong, X. Wang, and H. Fan, "Key-insulated undetectable digital signature scheme and solution for secure mobile agents in electronic commerce," *Mobile Information Systems*, vol. 2016, Article ID 4375072, 18 pages, 2016.
- [29] R. Amin, S. K. H. Islam, M. K. Khan, A. Karati, D. Giri, and S. Kumari, "A two-factor RSA-based robust authentication system for multiserver environments," *Security and Communication Networks*, vol. 2017, Article ID 5989151, 15 pages, 2017.
- [30] X. Li, X. Yang, Z. Ding, X. Du, and J. Wen, "ECC design based on uniform design test method and alternating conditional expectation," *Mathematical Problems in Engineering*, vol. 2019, Article ID 9575897, 14 pages, 2019.
- [31] R. K. Kodali and A. Naikoti, "ECDH based security model for IoT using ESP8266," in *Proceedings of the 2016 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCI CCT)*, pp. 629–633, 2016.
- [32] A. K. Saxena, S. Sinha, and P. Shukla, "Design and development of image security technique by using cryptography and steganography: a combine approach," *International Journal of Image, Graphics and Signal Processing*, vol. 4, pp. 13–21, 2018.
- [33] R. Gupta, "Performance analysis of anti-phishing tools and study of classification data mining algorithms for a novel anti-phishing system," *Computer Network and Information Security*, vol. 12, pp. 70–77, 2015.
- [34] R. Bhatt, P. Maheshwary, P. Shukla, P. Shukla, M. Shrivastava, and S. Changlani, "Implementation of fruit fly optimization algorithm (FFOA) to escalate the attacking efficiency of node capture attack in wireless sensor networks (WSN)," *Computer Communications*, vol. 149, pp. 134–145, 2020.
- [35] H. S. Pannu, D. Singh, and A. K. Malhi, "Multi-objective particle swarm optimization-based adaptive neuro-fuzzy inference system for benzene monitoring," *Neural Computing and Applications*, vol. 31, pp. 2195–2205, 2019.
- [36] D. Singh, J. Singh, and A. Chhabra, "High availability of clouds: failover strategies for cloud computing using integrated check pointing algorithms," in *Proceedings of the 2012 International Conference on Communication Systems and Network Technologies*, pp. 698–703, Rajkot, Gujarat India, May 2012.
- [37] D. Singh and V. Kumar, "A comprehensive review of computational dehazing techniques," *Archives of Computational Methods in Engineering*, vol. 26, pp. 1395–1413, 2019.
- [38] M. Gupta, N. Kumar, B. K. Singh, and N. Gupta, "NSGA-III-Based deep-learning model for biomedical search engines," *Mathematical Problems in Engineering*, vol. 2021, Article ID 9935862, 8 pages, 2021.
- [39] A. Dixit, A. Tiwari, and R. K. Gupta, "A model for trend analysis in the online shopping scenario using multilevel hesitation pattern mining," *Mathematical Problems in Engineering*, vol. 2021, Article ID 2828262, 11 pages.
- [40] V. Roy, S. Shukla, P. K. Shukla, and P. Rawat, "Gaussian elimination-based novel canonical correlation analysis method for EEG motion artifact removal," *Journal of Healthcare Engineering*, vol. 2017, p. 11, Article ID 9674712, 2017.
- [41] S. B. Goyal, P. Bedi, J. Kumar, and Ankita, "Realtime accident detection and alarm generation system over IoT," in *Multimedia Technologies in the Internet of Things Environment, Volume 2, Studies in Big Data*, R. Kumar, R. Sharma, and P. K. Pattnaik, Eds., Springer, Singapore, 2022.
- [42] P. Bedi, S. B. Goyal, J. Kumar, and S. Choudhary, "Smart automobile health monitoring system," in *Multimedia Technologies in the Internet of Things Environment, Volume 2, Studies in Big Data*, R. Kumar, R. Sharma, and P. K. Pattnaik, Eds., Springer, Singapore, 2022.