5g Network Security For Iot Implementation

***Dr. Deepika Pathak, *Pratik Shah**
Dr. APJ Abdul Kalam University, Indore
Research Scholar

Abstract:
Internet of Things (IoT) 5G-enabled growth, influence and capabilities are astounding in comparison to previous generations. Using IoT (Internet of Things) technologies that rely on connectivity and coverage poses several security issues. The dangers of cyberspace may become more obvious as IoT technology becomes more commonplace in our daily lives. Secure IoT-based 5G network devices demand an extended network life, wide coverage, and constant connectivity. It is because of these mistakes that security holes are discovered. Identifying deliberate faults is more harder to do than identifying accidental failures since they might soon cause the entire network to fail. Using novel security weaknesses, a new approach to securing IoT-based 5G network device connectivity and coverage has been offered in this study. A Boltzmann machine (BMKG)-based encryption method was suggested and compared to several asymmetric techniques for key exchange in this study.
Keywords: security, 5g network, IoT, attacks.
DOI: 10.24297/j.cims.2023.23

1. Introduction

5G mobile technology, the fifth generation, is a fundamental pillar to satisfy demand for new services and massive deployment, with this increasing security risks and problems of vulnerability and attacks in various network layers becoming more apparent. 5G mobile technology is a key pillar for IoT development in recent years. Security frameworks for the 5G-IoT network are still being developed and tested. Encryption reduces attacks on devices; the IoT architecture based on layers on models and security features is able to identify possible attacks; and, the analysis of the network layer proposes solutions for the IoT industry's challenges.

Since the introduction of the GSM system, encryption has been a major part of mobile communication. As a 2G mobile communication technology, GSM is commonly referred to as GSM. Every year, as technology and generational shifts bring new transmission capabilities and speeds to mobile communications. In today's world, 5G is the preferred method of mobile communication. It is necessary to include security procedures into 5G due to the large number of

people using it, so that the client can benefit from secure data transmission. This technology has received a lot of attention and investment, and there are many more to come.

2. Literature Review

Ijaz Ahmad (2019) The development of the Fifth Generation (5G) wireless networks is gaining momentum to connect almost all aspects of life through the network with much higher speed, very low latency and ubiquitous connectivity. Due to its crucial role in our lives, the network must secure its users, components, and services. The security threat landscape of 5G has grown enormously due to the unprecedented increase in types of services and in the number of devices. Therefore, security solutions if not developed yet must be envisioned already to cope with diverse threats on various services, novel technologies, and increased user information accessible by the network. This article outlines the 5G network threat landscape, the security vulnerabilities in the new technological concepts that will be adopted by 5G, and provides either solutions to those threats or future directions to cope with those security challenges. We also provide a brief outline of the post-5G cellular technologies and their security vulnerabilities which is referred to as Future Generations (XG) in this paper. In brief, this article highlights the present and future security challenges in wireless networks, mainly in 5G, and future directions to secure wireless networks beyond 5G.

Shancang Li (2018) The existing 4G networks have been widely used in the Internet of Things (IoT) and is continuously evolving to match the needs of the future Internet of Things (IoT) applications. The 5G networks are expected to massive expand today' s IoT that can boost cellular operationgs, IoT security, and network challenges and driving the Internet future to the edge. The existing IoT solutions are facing a number of challenges such as large number of conneciton of nodes, security, and new standards. This paper reviews the current research state-of-the-art of 5G IoT, key enabling technologies, and main research trends and challenges in 5G IoT

1R.Vignesh (2017) This paper confers a survey and an investigates of the current status and analysis of Internet of things (IoT) security. The IoT structure pursue to append anyone with anything, anywhere. As against to the fixed Internet, in addition to humans, an IoT fastens a large number of machines, resource-coerced devices and sensors using different wired and wireless networks. An IoT normally has a three imaginary layers consisting of realization, Network, and Application layers. This paper narrates security problems within and across these layers. Many

security ideas that should be implemented at each layer are also furnished. Previous work specific to enforcing security for each IoT layer and matching countermeasures are also reviewed. Finally, the paper presents future orientations for acquiring the IoT.

Mohamed Kamal Yassin (2017) The enhancement of environmental connection of things through the internet is based on the efficiency of the cellular network and how much it can serve massive amount of devices. The roll of previous cellular networks in the Internet of Things (IoT) trend serves a small number of devices with limited data rates, insufficient delay and large percentage of packet loss. In this research the aim is to measure the efficiency of a real test of an IoT environment using 3G and 4G cellular network sequentially, and also testing the same network in a simulative environment and compare the outputs to the real test outputs measuring the accuracy of the simulation, then also to examine a 5G network based on the millimeter wave (mmWave) and directional antennas, from this point we can analyze the efficiency of the 5G network based on the accuracy of the simulation. Bottom line, we have achieved an overall enhancement percentage of the throughput 84% and lessened delay by 80%, but, the number of packets lost was larger due to blockage that faces the mmWave signal.

3. Methodology

Using Boltzmann machines, this research attempts to design a key generation technique for 5G-enabled IoT device communication networks. Using deep learning-based BM algorithm, we have devised a more reliable and effective way of key creation. BMs can successfully encrypt and decrypt 2048 binary 8-dimensional vectors using the operative topology and restrictions of the delinquent origination. Additionally, we train and evaluate the proposed system's robustness by taking into account how sophisticated the brake system will be. Starting with big random numbers created, significance is determined, and then two massive numbers are compounded. The 2048-bit RSA programme on a 32-bit embedded CPU will be slow. It was necessary for us to employ a 64-word multiply operation when multiplying two 2048-bit numbers. The 2048-bit RSA key is equivalent to the 128-bit symmetric AES key. In order to comply with the NSA Suite B standard, you'll need an RSA key length of 3072 bits, which is equal to 256 bits of symmetric encryption.

If you increase the level of security, the amount of time it takes to compute increases exponentially. The discrete logarithm problem can be solved via cryptography. It is difficult to find an elliptical curve with the discrete logarithm of a point. Because of its short key, ECC's

primary benefit is its high level of security. Machine needs are greatly reduced by using more temporary keys. ECC is comparable to RSA 2048 with a 256-bit key and 256-bit primary curve. Securing 5G-IoT Device Connectivity and Coverage is made possible via key agreements, asymmetric authentication encryption, hash codes, and digital signatures. The most important aspect of RSA is that it is a complete security suite in and of itself, comprising asymmetric encryption and digital signatures. When it comes to exchanging keys, one method uses RSA, whereas when it comes to signing, another method does not. RSA key pair generation has been explained. Diffie–Hellman and RSA, on the other hand, necessitate extremely long keys (2048 bits or more). It's a curve elliptical Diffie–Hellman algorithm that employs elliptical cryptography. The protocol aims to accomplish the following.

Security of 5G-IoT Device Connectivity and Coverage should be secured by mutual authentication:

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

ANALYSIS

IoT devices connect to the internet. "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 utilise it as a jump point to exploit and attack network segments," according to a report from the CERT/CC. Despite the fact that this does not prohibit adversaries from directly attacking systems, it reduces their capacity to move laterally through networks. Businesses can also use jump hosts and/or network proxies to force 5G-IoT device connectivity. For example, the business could analyse network communication before it goes through IoT devices, and more effectively question him. 5G-IoT Device Coverage Using Encryption and Authentication Scheme in Figure 1 displays the traffic and payload suited for 5G-IoT device receipt or transmission.

Artificial intelligence and mechanical learning have benefited greatly from deep learning. Algorithms, on the other hand, have been shown to be able to solve some intractable computer problems. It is shown that unlike conventional computing, a severely constrained Boltzmann machine may be trained in significantly less time and with a more rendered and extensive

foundation. It is possible to train multilayer and fully connected models using our proposed methods. Boltzmann machines were the inspiration for an unconventional paper on a robust and functional asymmetric key cryptography system. Boltzmann neural networks must be calibrated so that they can decrypt and decrypt both the unimpaired and impaired datasets. A performance study and a theoretical security analysis are being conducted to establish that the system is safe from attacks.

Data exchange necessitates the use of encryption and decryption. The first step is to convert each character of the original text into an image.

The encrypted form of each eight-bit input set is composed from a single hidden layer that conceals all nine neuron outputs. For example, because a hidden layer activation function has a specific range, the hidden layer outputs all fall inside that range. A floating point array of 9 lengths, multiplied by the features of the provided data, generates the ciphertext, which is displayed in Figure 2 as a 9-dimensional vector.

Thirteen dimensional floating-point numeric vectors will be discretized and converted using the threshold function after each block is processed. Important to remember is that

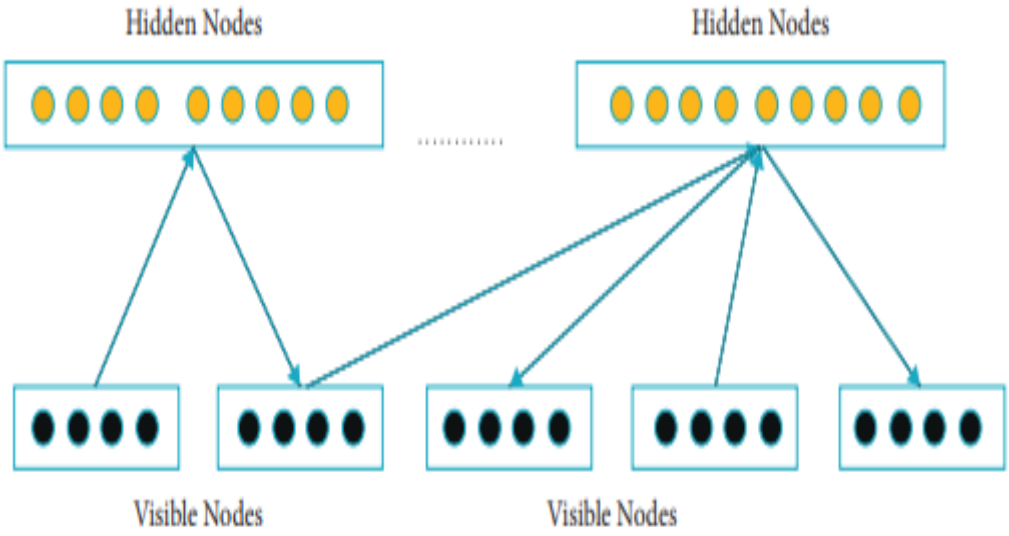

Figure 1 Weight of the system and gradient approach.

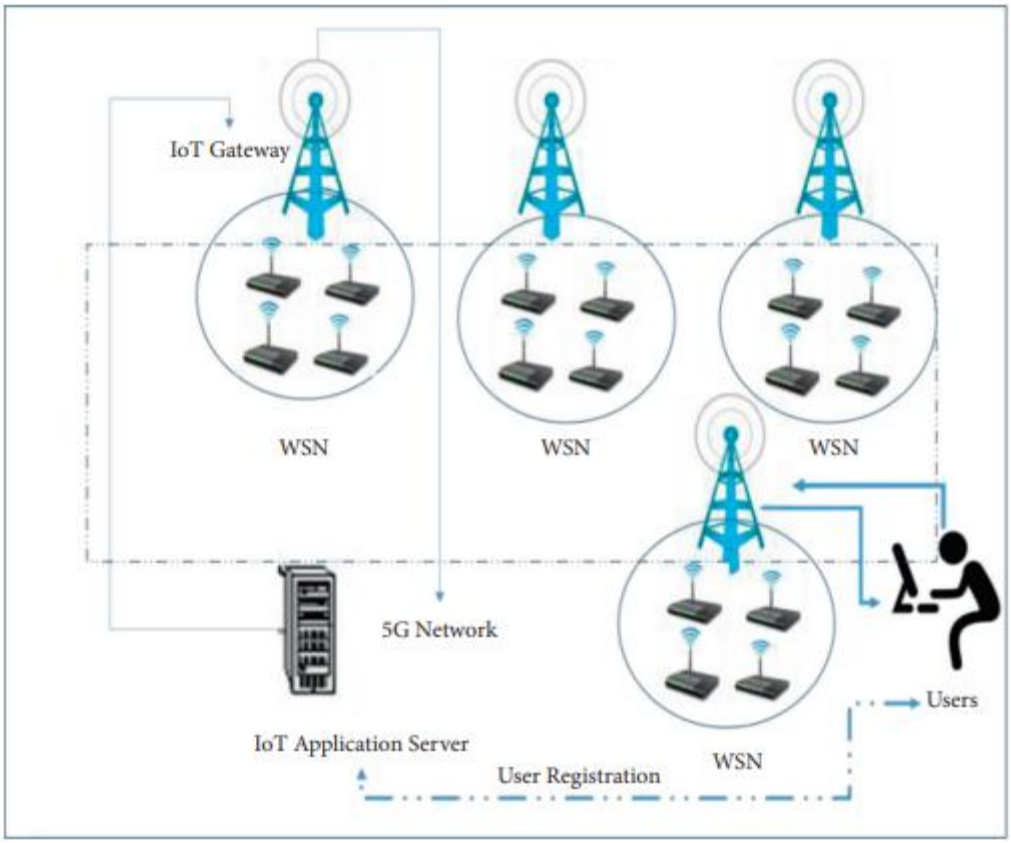

Figure 2 5G-IoT device Coverage using Encryption and Authentication Scheme

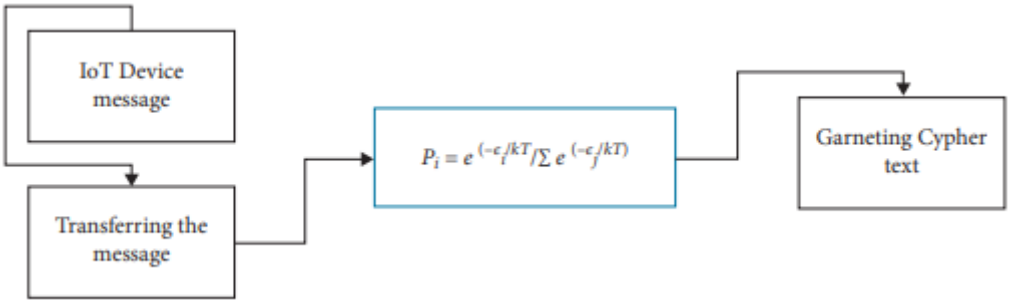

Figure 3 Encryption process.

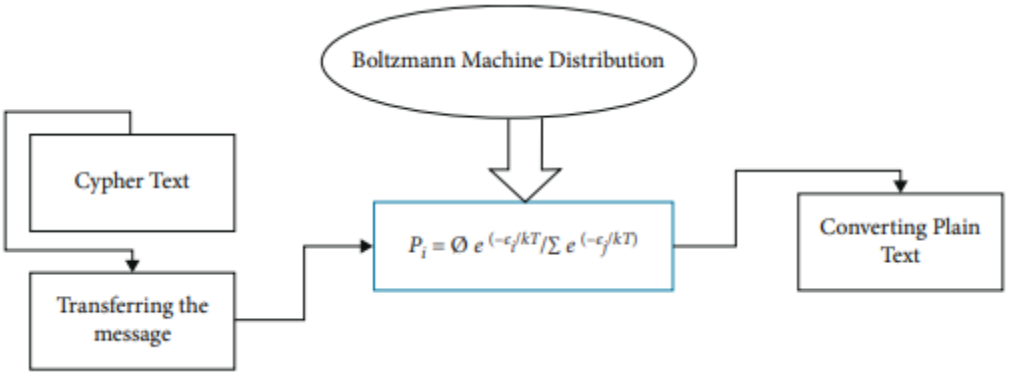

Figure 4 Decryption process.

Table 1 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

As demonstrated in Figure 4, this technology allows both parties to a connection to encrypt and decode data.

Before an algorithm can be employed in an application, it is vital to have a complete understanding of its performance characteristics. A comparison of the suggested system's performance based on the following metrics is carried out in this work.

- A system's total performance is directly affected by the time it takes to encrypt data. In a perfect world, the encryption time should be fast enough to assure responsiveness and speed of operation. Time is frequently measured in milliseconds.
- Decryption time: this is the amount of time it takes to decrypt the encrypted text from the original text. In this study, the amount of time it takes to decrypt a message is measured in milliseconds. According to the proposed system's security analysis, there are a few parameters to consider.

A laptop Core I7 3.5 GHz and Linux-5.11.11 were utilised in this experiment; Omnet was used to test various inputs and the results were associated with various implementations and hardware results. Encryption measurement time can be produced as an overview of the proposed system's behaviour with respect to traditional methods in this manner In order to test out the proposed strategy, a collection of data files were examined. All of these files are alphanumeric, and they range in size from 800 kB to 100 BM. Time was determined using Scala functions and compared to the encryption times, which were then compared to each other. Decryption times are recorded. The projected encryption time was matched with the findings and performance comparisons between the suggested BM and the cryptographic technique. Milliseconds were used to measure the time it took to encrypt.

Table 2 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

There was progress made. By modifying, removing, and sharing files, we were able to test the performance of our distributed cloud architecture. We used random file names and contents with a file size of up to 4 MB to show the average response time and data retrieval overhead for varied file sizes.

According to the results, the proposed model excelled and consumed the least resources compared to the core model in terms of performance. In order to evaluate the proposed model's attack detection accuracy, we used two different parameters. In the face of a wide range of traffic and several defects in the network, we tested one parameter and another in the detection of network attacks in real time.

4. Conclusion

A secure and effective IoT authentication solution for 5G network services is presented in this study. Allows 5G-IoT nodes to identify appropriate data transmission network slices while concealing user access types using this privacy-preserving slice selection mechanism. A secure data channel can be established between a 5G-IoT device and a remote server, allowing users to access data stored locally on the 5G-IoT device that has been saved. Simulation, efficiency, and practicality are used to demonstrate the safety and security of the proposed approach framework. A network-based secure protocol with fast access delegation and retransition to 5G networks with authenticated data protection will be developed in the future

Reference

1. J. Ni, X. Lin, and X. S. Shen, "Efficient and secure serviceoriented authentication supporting network slicing for 5Genabled 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. R.Vignesh, (2017) Security on Internet of Things (IOT) with Challenges and Countermeasures, IJEDR | Volume 5, Issue 1
4. Nam Tuan Le, (2016), Survey of Promising Technologies for 5G Networks, Hindawi Publishing Corporation Mobile Information Systems Volume 2016, Article ID 2676589, 25 pages
5. Mohamed Kamal Yassin, (2017), Enhancing the IoT Efficiency Using Millimeter Wave in 5G Simulation Environment and its Comparison with Real 3G and 4G Environment, SBN: 978-1-63248-131-3
6. Shancang Li, (2018), 5G Internet of Things: A Survey
7. R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 165-172, 2014.
8. M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," Int'l Journal of Critical Infrastructure Protection, vol. 5, 86-97, 2012.
9. Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in Applied Mechanics and Materials, 1430-1432, 2014
10. J.-Y. Lee, W.-C.Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in Int'l Symposium on Next-Generation Electronics (ISNE), 1-2, 2014.