Grenze International Journal of Engineering and Technology, June Issue

IoT Technologies, Security Attacks and their Security Measures under Smart City Framework

Md Shamsul Haque Ansari[1] and Monica Mehrotra[2]
[1-2]Jamia Millia Islamia/Computer Science, New Delhi, India
Email: shamsshamsul@gmail.com, drmehrotra2000@gmail.com

***Abstract*—The idea of developing modern and smart cities is like something which is adaptable by almost majority of the highly aware population if it provides more effective solutions to a wide range of problems usually faced by the societies. The objective behind the development of smart cities should not target to solve all the problems in a particular city but it must provide support to the capability of urban system to handle the variety of challenges. Focus has been diverted to IoT (Internet of Things) in recent years. Various recent technologies are being adapted by the people day by day to improve the communication capabilities. Devices involved under smart city environment are small in size and have the limited capabilities so it is also known as constrained devices. Such devices are prone to be attacked by the attackers as they are connected to the internet. Hence security of such devices and the communication between them plays a major role and obviously the type of supporting technologies which are being used is also important. In this paper authors are focusing on various recent technologies which are being used under smart city environment, various attacks related to smart city environment and putting some light on security measures for the device communication under the same environment.**

***Index Terms*— Smart City, Security, IoT, Smart Technologies, Random Number Generation.**

I. INTRODUCTION

The success of a modern and smart city depends on various components and the recent technologies available in the market which are being adapted by the people to maximize the effectiveness of the resources. With the increase in the number of smartphones in recent years, technology has supported people to get solutions for a majority of their problems and they are able to do their task in more convenient manner. Smart cities widely use Information and Communication Technologies (ICT) to make existing infrastructures more beneficial, efficient and valuable. In other words, a smart city can integrate the functionality of all the major components of infrastructure such as roads, airways, railways, maintenance activities, their monitoring and can help in optimizing the different resources while security issues must be taken into an account in parallel[1][2][3].

In almost every domain IoT is involved and it is providing major support in the process of automation. IoT can provide other benefits for monitoring and optimizing public services like waste management, parking, lighting, surveillance, etc. which are being adapted by the citizens as well as businesses both. Some other favorable applications of IoT includes: i) better management of SCM (Supply chain management), ii) identification of fake products, iii) automated manufacturing, iv) smart homes and their appliances, v) e-government and vi) e-health (monitoring of patients and their records) and many more. Today, the world is adopting emerging technologies

Grenze ID: 01.GIJET.8.2.56

and hence it is surrounded by a variety of smart devices which makes our lives better. These smart devices are preferred by the people because they are small in size and hence portable but having low processing capabilities and have less amount of memory required to perform number of complex operations in terms of security. So, the security mechanism for constrained devices must be designed and implemented. Hence the concept of lightweight cryptography comes into picture[1][4][5][6] .
This paper is organized in the following sections: - Recent IoT technologies which are supporting smart city environment are discussed in Section 2. Various types of attacks are covered in Section 3. Section 4 covers the security challenges in IoT and the suggestive solutions. Section 5 covers the proposed methodology and paper is concluded with the experimental setup and discussion in section 6.

II. IOT TECHNOLOGIES SUPPORTING SMART CITY ENVIRONMENT

As the population is increasing day by day, the number of internet users are also increasing tremendously and the number of smart device users are also increasing accordingly and hence the security of these devices as well as secure communication between them also becomes challenging to implement because such devices communicates with other devices and are controlled through IoT environment[7][8]. Fig. 1 shows different technologies which are associated with IoT.

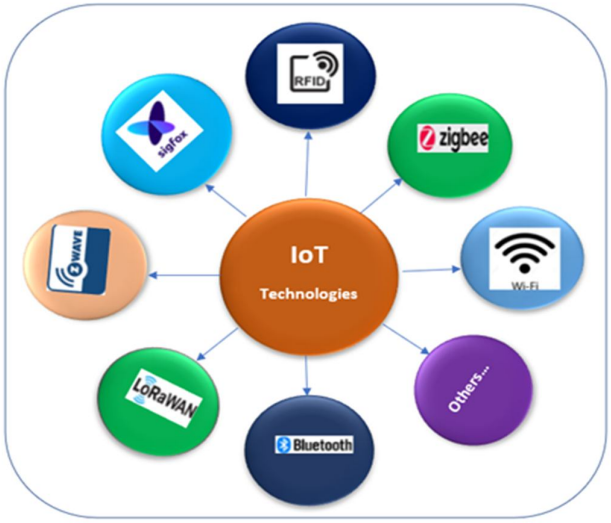

Figure 1: Technologies associated with IoT

Key highlights of the IoT technologies: -
1. **Bluetooth** is a well-known and popular technology for wireless communication with a limited range[9].
2. **Wi-Fi** is a wireless communication which works on limited range[9].
3. **ZigBee** is one of the specifications of IEEE 802.15.4 which is for a collection of protocols related to communication and is used to make personal area network having tiny, minimum power consumption digital radios, like data collection of medical devices, home automation, and other minimum power consumption, low-bandwidth required, designed for small projects which require wireless connection[10].
4. **Z-Wave** is a wireless communication protocol and it uses radio waves to communicate between appliance to appliance. It can also be controlled through the internet and smart gadgets[9].
5. **RFID** is a contactless technology which uses electromagnetic fields and it is used to find the things and track the related information[11].
6. **Sigfox** is a cellular style form of wireless communication which has long range and takes low power[12].
7. **LoRaWAN** is a wireless network protocol that manages communication between end-node devices and the network gateways[12].
IoT devices are low battery powered devices and hence above-mentioned technologies are being used under smart city environment because of its low power consumption and it also provides fast communication among the devices. On the other hand, when the lightweight devices are connected via internet and being controlled through the internet, the chances of lacking in security becomes higher. Fig. 2 shows the comparison of above

technologies in terms of data rate, power consumption and its range. Among other recent technologies, ZigBee is minimum power consumption, low data rate wireless adhoc network[10].

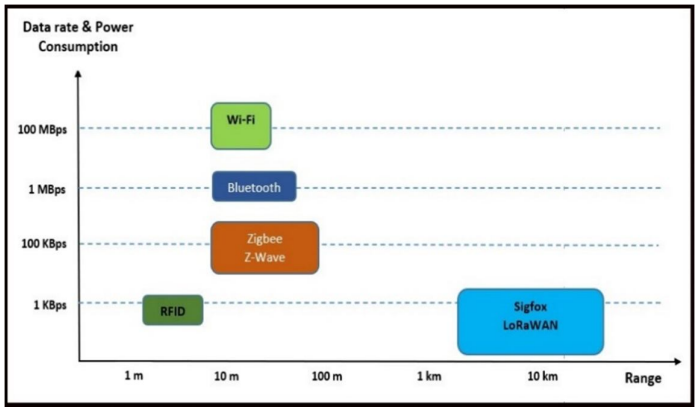

Figure 2: Comparative analysis of IoT technologies in terms of data rate, power consumption and its range

In terms of range and the power consumptions of the IoT technologies, a comparison has been given in Table I.

TABLE I: COMPARATIVE ANALYSIS OF IOT TECHNOLOGIES

S.No.	Technology Name	Range (approx.)	Introduced in the Year	Power Type
1	Bluetooth	10 meters	1994	Low power
2	Wi-Fi	Few Feets-45 meters	1997	Low power
3	Zigbee	10-100 meters	1998	Low power
4	Z-Wave	100 meters	1999	Low power
5	RFID	1-10 meters (short read range)	2002	Low power
6	Sigfox	10 km (urban), 40 km (rural)	2010	Low power
7	LoRaWAN	5 km (urban), 20 km (rural)	2015	Low power

III. ATTACKS ON IOT

A. Denial of Service Attack (DOS)

It is one of the most easy and common attack which is done on IoT systems. It can be seen in various forms but "jamming" is a popular and effective DoS attack. In this attack, attacker floods the network with heavy traffic so that the services are unavailable which are needed by the legitimate users. This attack is also called flood attack. Figure 3 shows that the attacker sends multiple unnecessary requests which increases the load on server also and server becomes down. As a result, when a legitimate user sends the genuine request to the server than the server rejects the request because server state becomes down[13][14].

A. Wormhole

In this type of attack, packets are recorded at some network location and retransmitted to different location through wormhole tunnel. Figure 4 shows that there are two attackers who are in the network and other nodes

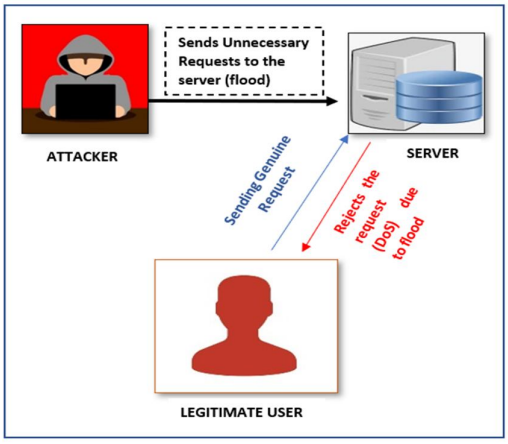

Figure 3: Denial of Service Attack

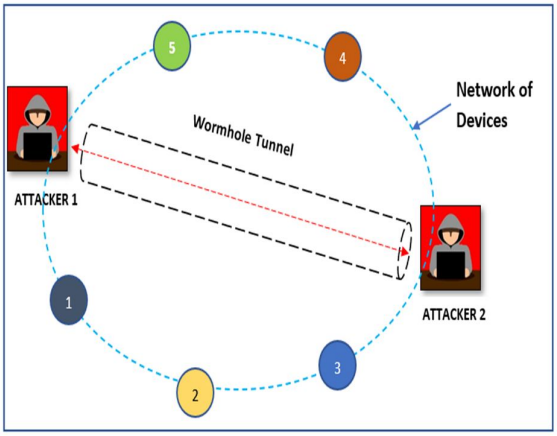

Figure 4: Wormhole Attack

1,2,3,4,5 are non-malicious nodes. Attacker create one tunnel known as wormhole tunnel between both of them, through which they exchange the packets which they receive from other non-malicious nodes and hence they also create network congestion. With this attack, packets do not reach to their destination or they get delayed[15].

C. Eavesdropping

The major objective of the attacker is to listen private communication intentionally to read messages and save them for future purpose. Such information can be utilized against the legitimate users by the intruder. During communication, intruder listens the information passively but the information is not altered. By this attack privacy is prone to be risky. Figure 5 shows the scenario of eavesdropping[15].

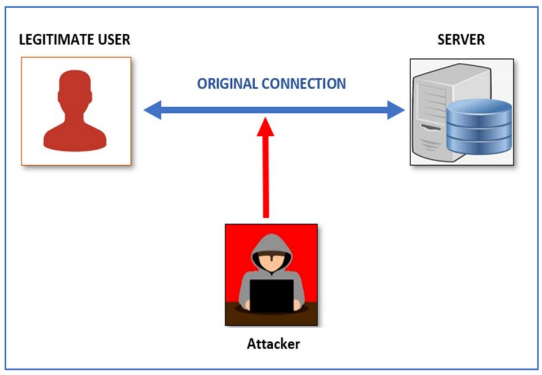

Figure 5: Eavesdropping

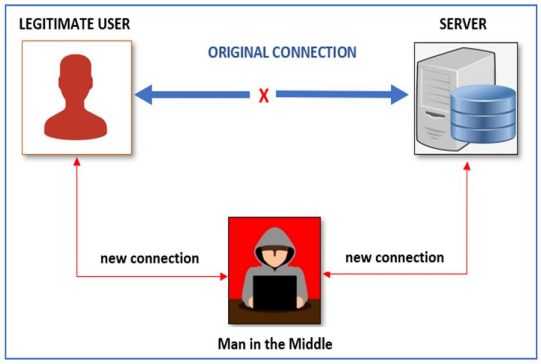

Figure 6: Man-in-the-Middle attack

D. Man-in-the-Middle

This is a type of eavesdropping attack in which attacker interrupt the communication or data transmission and inserts himself in the middle and pretends like a legitimate user and captures the key when these users are exchanging it during communication. Figure 6 shows that the attacker interrupts the communication and captures the data[15].

E. Sinkhole Attack

This attack takes place when a computer system is hacked and the intruder has the control on this system which is also treated as malicious node. This node shares incorrect routing information to its neighboring nodes pretending that it has minimum distance path to the base station which attracts the other nodes. When the traffic flows through this node, message can be altered or even the packets can be dropped. Figure 7 shows that the traffic is passing through the sinkhole[16].

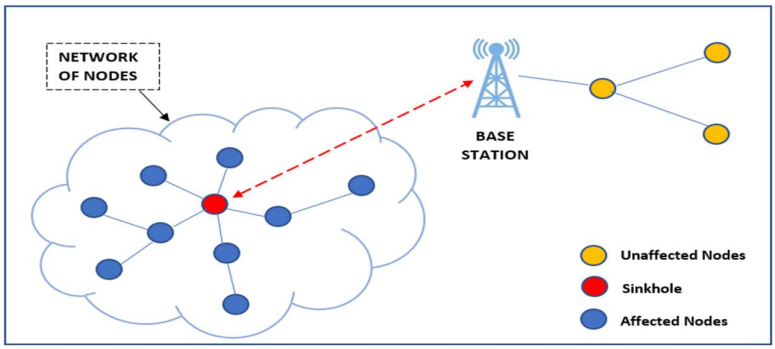

Figure 7: Sinkhole Attack

F. Sybil Attack

It occurs when a computer system is hacked and the hacker captures the identities of different node and acts as them. This hacked computer system will be treated as malicious node. Here malicious node shows multiple identities in the network. For example, a node in voting system can vote several times under WSN (wireless sensor network)[15][17].

G. Side Channel Attack

In this attack, attacker extracts the information related to side channel which consist of power related information, time required to perform various operations, etc. Such information is utilized to identify the encryption key. Side channel attack is a passive attack because it does not change any information. Attacker finds the encryption key with the help of side channel information and therefore it is complex to identify this attack[15].

IV. IoT Security Challenges and Cryptographic Solutions

Secure communication requires some kind mechanism which must be followed by the environment in which communicating devices are going to share their information as they are connected with the internet and prone to be attacked by the malicious users.

A. Conventional Cryptography

Cryptographic approach covers the encryption of data for achieving secure communication. There are two common methods for encryption i:e:- Symmetric and Asymmetric key encryption. Symmetric key encryption uses the same key for encrypting as well as decrypting the data whereas Asymmetric encryption uses two type of keys, public and private key to communicate with sender and receiver. The main drawback of symmetric key encryption is that the distribution of public key among both the parties is cumbersome because if the key goes in wrong hand than the encrypted data is not secure and can be accessed by the malicious person. So, it does not guarantee authentication. Some of the symmetric key algorithms are AES (Advanced Encryption Standard), DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), 3DES, Blowfish (Drop-in replacement for DES or IDEA), RC4 (Rivest Cipher 4), RC5 (Rivest Cipher 5), RC6 (Rivest Cipher 6). All of the above are block ciphers except RC4 which is a stream cipher[18]. The advantage of asymmetric encryption supports all security services and provides safe mechanism for key distribution. Asymmetric key encryption ensures authentication. The major limitation of this method is the large size of key which makes the encryption process slow.

Some of the common algorithms are Ed25519 signing, X25519 key exchange, Ed448 signing, X448 key exchange, Elliptic curve cryptography, RSA, Diffie-Hellman key exchange, DSA, Key Serialization, Asymmetric Utilities, etc.[18]. Figure 8 and Figure 9 shows the process of symmetric key encryption and asymmetric key encryption respectively.

B. Lightweight Cryptography

IoT devices communicate through the internet and therefore, they are available in the public domain and prone to be attacked. Such devices may get affected by various threats and hence it must be kept secured with some kind of strong mechanism. IoT security can be classified in three ways: a) Security and Data Protection b) [19].

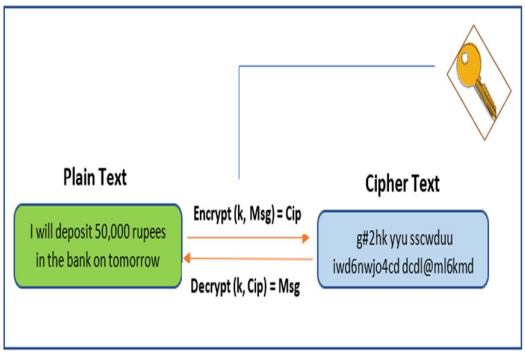

Figure 8: Symmetric Key Encryption

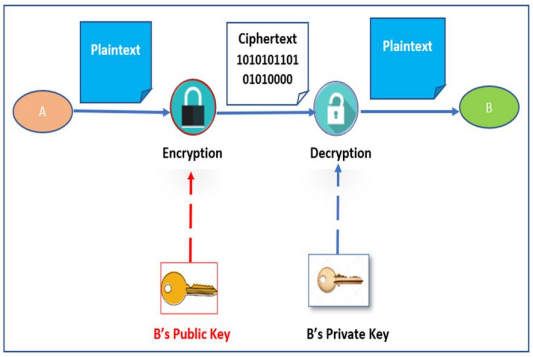

Figure 9: Asymmetric Key Encryption

Authentication and Identity Management c) Privacy. There are various algorithms which are available to provide the security at every level. Every algorithm has its own pros and cons[19].

IoT devices are enabled with wireless technology, having small size, limited storage, low processing power with tiny OS, and small battery. Conventional cryptography requires more processing power and more storge capacity hence it does not suit to the IOT devices as they are constrained devices in nature. Therefore, lightweight cryptography plays a vital role which deals with implementing the security of same level and it is acceptable by such devices. So, NIST has also recommended to prefer lightweight algorithms to provide security for IOT devices[20].

IoT security system is based on lightweight cryptography which covers the security of constrained devices. Designing of lightweight algorithm emphasizes on hardware implementation. Such algorithms are designed by keeping AES as a standard algorithm. AES works on block length of 128 bits with different key sizes of 128, 192, and 256 bits. Another algorithm which is used for security is PRESENT which is one of the ultra-lightweight algorithms used for security purpose with the key size as 80 or 128. RECTANGLE was the improved version of PRESENT. There are various other algorithms which was designed by improving the number of gate count. The total number of logic gates required to run any program is known as gate equivalent and all the algorithms are compared on the basis of it. While designing the lightweight algorithm the objective is always to minimize the gate equivalent[21].

1. Random Number Generator (RNG)

Basically, RNG is used to generate one time password. All the cryptographic encryption method needs some king of key generation method. Such keys play an important role in the whole process of encryption and decryption. A variety of key generation method has been proposed by different researchers. Random numbers generated by any method can be utilized for confidential key generation. They are of two types; one is true random number generator and the another one is pseudo number generator (PRNG). PRNG is software based which generates its output when seeded with some random input bits[22][23][24][25].

2. Hash Function

Hash function can be used to achieve authentication. It is widely used in cryptography. Development of hash calculation is similar as the development of secure key calculation. For IoT devices, lightweight hashing can be designed and if the algorithm takes around 2000 gate equivalent than it will be treated as lightweight[26].

3. Shift Operation

As the devices under smart city environment are low powered and have limited processing capabilities, a different kind of mechanism is required. Researchers found that the computational power required for shift operation is lesser than the power needed by the other operations like right shift, left shift and circular shift. Hence shift operations can be used for implementing lightweight cryptography[27][28].

V. Proposed Methodology

To establish trust between the devices under smart city environment there is a requirement to design a strong mechanism for achieving mutual authentication. Authors are working on such mechanism so that a strong key can be generated for mutual authentication. In this approach a dedicated server will be responsible to generate the keys which will be treated as one time password and it can be used for mutual authentication. It will be

shared by the dedicated server to both the communicating parties and when key matches communication will be initiated else declined. Authors have written the code as per the requirements of NIST (National Institute of Standards and Technology) and it will run on a single dedicated server. NIST provides the Test Suits for checking the randomness of the bit sequence which may be generated by any means. Once these bit sequences are tested for their randomness they can be used as a key for encryption and decryption process. The proposed methodology can be explained with the following steps: -

1. Generate the binary strings as per the required length (all unique combinations of zeros and ones for instance n=3 i: e: - 2^3=8 bit required length).
2. Analyse all the string one by one and calculate the numbers of zeros and number of ones in each (as per the requirement of NIST).
3. Keep the strings which contains equal number of zeros and equal number of ones which can be utilized to generate the key and discard rest of the strings. In our case 62 strings will be generated.
4. Create fixed length blocks of the string and perform block test of NIST. Accept the string which passes the test for equal number of zeros and ones and, discard rest of the strings.
5. Merge all the strings.
6. Break the merged string generated in step 5 in fixed size output
7. This fixed size output can used as a key.

VI. Experimental Setup and Discussion

Authors written the code for the generating the keys in python language as it is a simple language and suitable for the smart city environment. Authors used Spyder as IDE on windows 11 platform with 64-bit operating system and Intel i5-8265U CPU @ 1.60GHz. As per the steps of proposed methodology code is written in python and the randomness of the generated bits has been tested by NIST. Approach to generate the bit sequences is totally software based.

VII. Conclusions

In this paper, author presented various IoT technologies which are being adopted by smart city environment. Authors reviewed different technologies which supports IoT and the types of security threats for the IOT. This paper highlighted many challenges like security of the devices and security for communication between these devices. At the end of this paper authors provided few suitable solutions for implementing the security which can be used under smart city environment where lightweight cryptography is used. Keys generated through the proposed methodology can be utilized for implementing the encryption and decryption processes and it may be covered in the future work.

References

[1] N. Zhang, H. Chen, X. Chen, and J. Chen, "Semantic framework of internet of things for smart cities: Case studies," Sensors (Switzerland), vol. 16, no. 9, 2016, doi: 10.3390/s16091501.

[2] M. S. H. Ansari and M. Mehrotra, "Development of smart cities and its sustainability: A smart city framework," Int. J. Innov. Technol. Explor. Eng., vol. 8, no. 11, 2019, doi: 10.35940/ijitee.K1703.0881119.

[3] A. Meijer and M. P. R. Bolívar, "Governing the smart city: a review of the literature on smart urban governance," Int. Rev. Adm. Sci., vol. 82, no. 2, pp. 392–408, 2016, doi: 10.1177/0020852314564308.

[4] P. Verma, S. K. Sood, and S. Kalra, "Cloud-centric IoT based student healthcare monitoring framework," J. Ambient Intell. Humaniz. Comput., vol. 9, no. 5, pp. 1293–1309, Oct. 2018, doi: 10.1007/s12652-017-0520-6.

[5] B. Sithole, S. Rimer, K. Ouahada, C. Mikeka, and J. Pinifolo, "Smart water leakage detection and metering device," 2016 IST-Africa Conf. IST-Africa 2016, pp. 1–9, 2016, doi: 10.1109/ISTAFRICA.2016.7530612.

[6] S. H. Shah and I. Yaqoob, "A survey: Internet of Things (IOT) technologies, applications and challenges," 2016 4th IEEE Int. Conf. Smart Energy Grid Eng. SEGE 2016, vol. i, pp. 381–385, 2016, doi: 10.1109/SEGE.2016.7589556.

[7] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," IEEE Internet Things J., vol. 1, no. 1, pp. 22–32, Feb. 2014, doi: 10.1109/JIOT.2014.2306328.

[8] L. Da Xu, W. He, and S. Li, "Internet of things in industries: A survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4. IEEE Computer Society, pp. 2233–2243, Nov. 01, 2014, doi: 10.1109/TII.2014.2300753.

[9] "IEEE INTERNET OF THINGS JOURNAL A joint publication of IEEE Sensors Council, IEEE Communications Society, IEEE Computer Society, and IEEE Signal Processing Society CALL FOR PAPERS IEEE Internet of Things Journal Special Issue on Towards Securing Internet of Connected Vehicles from Virtual Vehicle Hijacking," 2019. [Online]. Available: http://iot.ieee.org/journal.

[10] E. Suganya and S. Vijayashaarathi, “Smart vehicle monitoring system for air pollution detection using WSN,” Int. Conf. Commun. Signal Process. ICCSP 2016, pp. 719–722, 2016, doi: 10.1109/ICCSP.2016.7754238.
[11] E. Borgia, “The internet of things vision: Key features, applications and open issues,” Computer Communications, vol. 54. Elsevier B.V., pp. 1–31, Dec. 01, 2014, doi: 10.1016/j.comcom.2014.09.008.
[12] C. Gomez, J. C. Veras, R. Vidal, L. Casals, and J. Paradells, “A sigfox energy consumption model,” Sensors (Switzerland), vol. 19, no. 3, 2019, doi: 10.3390/s19030681.
[13] A. Ebraheim Alsaadi, A. Dhabi, U. Abdallah Tubaishat, and zuacae Abu Dhabi, “Internet of Things: Features, Challenges, and Vulnerabilities,” 2015. [Online]. Available: www.elvedit.com.
[14] M. Husamuddin and M. Qayyum, “Internet of Things: A study on security and privacy threats,” 2017 2nd Int. Conf. Anti-Cyber Crimes, ICACC 2017, pp. 93–97, 2017, doi: 10.1109/Anti-Cybercrime.2017.7905270.
[15] N. Gadkar, “Classifications on IoT Attacks,” vol. 7, no. 07, pp. 436–437, 2018.
[16] Raju and P. Parwekar, “Detection of sinkhole attack in wireless sensor network,” Adv. Intell. Syst. Comput., vol. 381, no. July, pp. 629–636, 2016, doi: 10.1007/978-81-322-2526-3_65.
[17] A. Mosenia and N. K. Jha, “A comprehensive study of security of internet-of-things,” IEEE Trans. Emerg. Top. Comput., vol. 5, no. 4, pp. 586–602, Oct. 2017, doi: 10.1109/TETC.2016.2606384.
[18] L. Gao, L. Zhang, and M. Ma, “Low Cost RFID Security Protocol Based on Rabin Symmetric Encryption Algorithm,” Wirel. Pers. Commun., vol. 96, no. 1, pp. 683–696, Sep. 2017, doi: 10.1007/s11277-017-4196-1.
[19] N. Li, D. Liu, and S. Nepal, “Lightweight Mutual Authentication for IoT and Its Applications,” IEEE Trans. Sustain. Comput., vol. 2, no. 4, pp. 359–370, Jun. 2017, doi: 10.1109/tsusc.2017.2716953.
[20] M. Katagi and S. Moriai, “Lightweight Cryptography for the Internet of Things.” [Online]. Available: http://www.ecrypt.eu.org/stream/.
[21] W. Zhang, Z. Bao, V. Rijmen, and M. Liu, “A New Classification of 4-bit Optimal S-boxes and its Application to PRESENT, RECTANGLE and SPONGENT.”
[22] M. S. Haque Ansari and M. Mehrotra, “Securing M2M communication in smart cities,” 2020 Int. Conf. Emerg. Technol. INCET 2020, 2020, doi: 10.1109/INCET49848.2020.9154158.
[23] Mandal, X. Fan, and G. Gong, “Warbler: A Lightweight Pseudorandom Number Generator for EPC C1 Gen2 Passive RFID Tags,” 2013.
[24] Wu and M. O’Neill, “Ultra-lightweight true random number generators,” Electron. Lett., vol. 46, no. 14, pp. 988–990, Jul. 2010, doi: 10.1049/el.2010.0893.
[25] A. B. Orue Lopez, L. Hernandez Encinas, A. Martin Munoz, and F. Montoya Vitini, “A Lightweight Pseudorandom Number Generator for Securing the Internet of Things,” IEEE Access, vol. 5, pp. 27800–27806, 2017, doi: 10.1109/ACCESS.2017.2774105.
[26] Chakraborti, A. Chattopadhyay, M. Hassan, and M. Nandi, “TriviA and uTriviA: two fast and secure authenticated encryption schemes,” J. Cryptogr. Eng., vol. 8, no. 1, pp. 29–48, Apr. 2018, doi: 10.1007/s13389-016-0137-2.
[27] W. Zhang, S. Liu, S. Wang, B. Yi, and L. Wu, “An Efficient Lightweight RFID Authentication Protocol with Strong Trajectory Privacy Protection,” Wirel. Pers. Commun., vol. 96, no. 1, pp. 1215–1228, Sep. 2017, doi: 10.1007/s11277-017-4232-1.
[28] S. Vigna, “Further scramblings of Marsaglia’s xorshift generators,” J. Comput. Appl. Math., vol. 315, pp. 175–181, May 2017, doi: 10.1016/j.cam.2016.11.006.