Received: Mar '22
Revised:
Accepted: Mar '22

IMPLEMENTABLE SECURITY ALGORITHMS FOR IOT ENVIRONMENT

Reenu Shukal
Research Scholar, University of Technology, Jaipur

ABSTRACT

Interest in the Internet of Things (IoT) is growing among both professionals and academics. The primary objective of IoT is to unite all elements of society things, people, locations, and processes under a unified infrastructure that can provide us with data and insight into the state of the objects in our environment. Through the "Internet of Things," it is feasible to gain a digital representation of physical things, whether they are living or nonliving. The IoT has already had a profound impact on people's daily lives, and it promises to connect many more aspects of society and objects in the not-too-distant future. To help individuals and businesses overcome the challenges they face every day, the Internet of Things is being used in a number of smart environment and application fields. Both at home and in the workplace, our daily routines are becoming radically different. The ability to use many cryptographic systems means that users may tailor their security to their own needs.

Keywords: Security, Environment, Algorithm, Internet of Thing.

1. INTRODUCTION

The Internet of Things is a new technological era that is only beginning to take shape in our world. In the IoT paradigm, both humans and inanimate items share a network through the web. Internet of Things (IoT) has received a lot of attention in recent years because it provides fantastic opportunities for a wide range of novel uses. It is hoped that the standard of living would improve as a result of this shift in thinking. It has far-reaching effects on fields as diverse as logistics, agriculture, finance, energy savings, preventative maintenance, and business process management. Researchers and businesspeople from all around the world are also very interested in it. As the Internet of Things (IoT) landscape evolves, we are able to save a tonne of money on corporate upgrades and noticeably improve our quality of life. Despite the many researchers working in the topic, there are still many open questions and obstacles to overcome. The study focuses on a critical problem: the lack of protection for data transmitted across the Internet of Things. One of the biggest problems holding the Internet of Things back is security. [1]

Devices in the Internet of Things (IoT) ecosystem, such as embedded systems, mobile devices, actuators, and sensors, are able to exchange and link vast volumes of data as a result of recent technological developments. Here, protecting personal information and keeping sensitive data safe is of paramount importance. As a result, privacy and security have been major topics of study in recent years. There have been hundreds of discussions on potential security measures for the IoT ecosystem recently. It is crucial to explore and create new procedures and strategies by using evolutionary computations due to the large number of criteria and aspects that must be taken into account while dealing with privacy and security concerns. The goal of this Special Issue was to bring together the most up-to-date findings from studies and developments of security and privacy concerns in the Internet of Things (IoT) ecosystem and IoT devices. New techniques for security and privacy solutions, as well as theories and technologies presented to defend IoT-oriented applications from adversarial or malicious assaults, were sought for for this Special Issue. [2]

1.1 Internet of Things

Investigating Mobile Computing, Pervasive Computing, and Wireless Sensor Networks has been going on for over a decade. Currently, mobile ad hoc networks are active but often implemented independently. Despite the fact that they are both branches of Computer Science, coordinated research activities in both fields are exceedingly rare. The Internet of Things (IoT) is an ever-expanding, decentralised network of connected, self-learning devices and sensors that can coordinate their activities, adapt to new conditions, and solve problems autonomously. With the help of IoT, everyday devices, such as smartphones, may share data with one another and the outside world. Today, there is a lot of focus on IoT security due to

the interconnected nature of the devices it connects. [3]

Figure 1: An Internet of Things

2. SECURITY ISSUES IN IOT ENVIRONMENT

Standards, mobility support, traffic characterisation and quality of service, authentication, data integrity, and privacy were identified as problems in the IoT context after examining the aforementioned literature. However, the biggest obstacle to the widespread adoption of IoT is the concern over its safety. The Internet of Things has gained appeal and a wide range of applications due to its "anytime, everywhere connection for anybody" philosophy. Many people worry that their data, their services, and the entire IoT system are at risk due to the prevalence of the same mindset. The confidentiality, integrity, authentication, authorization, availability, and privacy of the whole IoT system must be ensured for it to be considered secure. The primary obstacles to improving security in an IoT setting are depicted in Figure 2. [4]

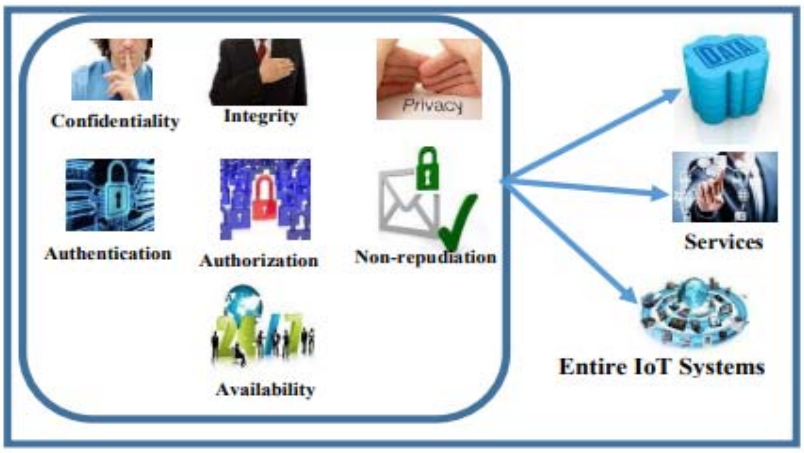

Figure 2: Issues in Security of IoT Data

i. Confidentiality

The system ensures that only authorised parties can view and alter information. Authentication and authorization are two-way processes in an IoT ecosystem, with both users and things receiving credentials. Defining an access control mechanism and an object authentication process are two crucial concepts that must be addressed by any method of ensuring privacy. Concerns about data privacy in an IoT setting also include the need to describe a suitable query language that will enable applications to extract the relevant data from a data stream.[5]

ii. Integrity

In other words, it consists only of truthfulness, honesty, and dependability. In an Internet of Things (IoT) setting, where the number of connected devices and users is expected to grow exponentially, data integrity will be a major concern. The transaction data cannot be tampered

with by an adversary without being detected. Integrity, as defined by Md. Mahmud Hossain et al., is the guarantee that information received has not been tampered with in transit. Unfortunately, tracing the data back to its original source is made extremely difficult by the devices' ambiguous identities. Inconsistencies exist in the deployment of trustworthy hardware and reliable information. In order to keep the data and devices secure in IoT technologies, trusted computing solutions need to be established.

iii. Authentication

In order to ensure that all parties involved in a conversation are who they claim to be, authentication is performed. It is complementary to other concepts such as authenticity, permission, and privacy. Despite the ever-increasing number of internet-connected devices, scalability poses a significant challenge to device authentication. To safely manage the expansion of IoT device numbers, a technique or architecture must be proposed. In order for Internet of Things scenarios to work, strong authentication infrastructures are needed.[6]

iv. Availability

The availability of IoT devices depends on their recoverability and dependability. Due to the decentralised nature of the IoT ecosystem, an unprecedented volume of data is now at everyone's disposal. When connected to the internet, any person or thing can create data and look for a place to put it. Which means that it is possible to secretly follow and monitor anyone. The availability of data and services in an Internet of Things setting requires the creation of an appropriate algorithm.

v. Privacy

Any individual or group has the autonomy to choose how much of its private information to make public. A major problem with privacy will emerge as a result of the Internet of Things. Without the target's knowledge, a large amount of personally identifiable data can be compiled. As things stand, it is difficult to stop the spread of all of this knowledge. users of the IoT system must take responsibility for their own data management. Persons in possession of data have a right to know both who is using it and when. Researchers should provide a standardised privacy framework for the Internet of Things (IoT) and new enforcement methods to allow for scalability in a diverse IoT ecosystem.[7]

3. IOT SECURITY ALGORITHMS

Numerous physical objects in the real world will have internet connections under the IoT paradigm, creating a rich setting for the technology. Information pertaining to chip identification in such a scenario must be encrypted to prevent unauthorised access. The communication in the Internet of Things must be protected by means of confidentiality, integrity, and authentication services. The information gathered by sensor nodes should be secured. Given that sensors might potentially be accessed via the Internet and WSN, additional security measures beyond data encryption, such as firewalls and IDC, are necessary. The Internet of Things faces obstacles from several new factors.[8] These include the sheer number of nodes involved, the limited power of individual nodes, and the one-of-a-kind requirements of their operational environments. That makes it harder to apply a blanket security strategy. To a large extent, cryptography is responsible for security. Its main functions are to provide confidentiality, privacy, authenticity, and the integrity of data. Multiple established protocols exist for ensuring data safety now; examples include DES and AES. Many more gates and strength is lost in these cyphers. Devices connected to the Internet of Things are unable to practically use these cyphers. Embedded systems on a small scale often employ 4-bit/8-bit processors, which have insufficient storage to run even power-hungry programmes. There has been a significant boost to the global computer processor market from eight-bit microcontrollers. These are limited in terms of clock speed, register width, arithmetic capabilities, random access memory (RAM), and read-only memory (ROM/Flash). These limitations on Internet of Things devices have given rise to a new field of study: lightweight cryptography. [9]

3.1 Block Cipher

Block cyphers function by applying a series of operations to a pool of blocks of a certain length. These cyphers all use the same predetermined sized blocks and keys. Encryption, decryption, and key scheduling are three fundamental steps in the field of cryptography. Encryption converts plaintext to ciphertext while decryption restores it to its original form. A set of additional keys derived from the secret master key are made available to the encryption and decryption routines. The processes are iterated over and over until the necessary robustness is achieved. Iterations, often known as

rounds, alter the system state at regular intervals. After exhausting all possible rounds, the ciphertext is obtained. The information is encrypted using the principles of confusion and diffusion in block cyphers. For its operations to be safe, a block cypher must generate a sufficient amount of noise. Disorientation makes it difficult to make the connection between the encryption key and the deciphered message. It is believed that each crucial part will affect every other part of the cypher text in some way. Due to diffusion, a block of cypher text is overly susceptible to statistical attacks, as each bit from the plain text is multiplied across many bits. [10]

There are two major categories of block cyphers, the first being Feistel-based networks and the second being Substitution Permutation Networks. The two major types of Feistel networks are the classical and the generalised. SPN is a collection of related mathematical operations. To generate randomness and spread information throughout a product cypher, Shannon suggested utilising two separate operations: substitution and permutation. Three layers—a replacement layer, a permutation layer, and a key mixing layer compose a single SPN round. Substitution functions and confusion functions give an additional layer of replacement and obscuration. It's often misunderstood as an S-box, and it may be modelled by mapping values into a table. Here, nonlinear operations are performed using either a bit-slice implementation or an S-box. The P-box, a permutation function, provides diffusion. In contrast to SPN cyphers, which employ different techniques for encryption and decryption, the two operations are equivalent in Feistel networks. The Lucifer family of block cyphers was developed by Horst Feistel in the late 1960s, and it employs a pair of symmetric algorithms for both encryption and decryption. Feistel proposed splitting the cipher's state in half and applying a source branch function to each half independently. From this, we may build the second half, or target, of the whole. Before this, there was no shift in the branch at the origin; today, however, that's altered. Feistel networks are comparable to SPNs; however, while SPNs update the entire state in each cycle, Feistel networks only update half of the state. Feistel networks' sluggish propagation of diffusion is because it often requires more iterations than SPNs.[11]

The Lai-Messey design incorporates the best features of both SPNs and Feistel networks. The IDEA cypher is the pioneer in this regard; it combines the two halves of the state and then feeds the result into the F-function. The F-output functions are then applied to both parts of the state. This increases the rate at which the cypher spreads and causes confusion. Lightweight block cyphers SIT and SFN merged SPN and Feistel structure into a single encryption.

Using the key concept of bleaching, the Even Mansour method is presented. For whitening, the key size corresponds to the block size. In the EM method, the n-bit plaintext is encrypted, then XORed with an n-bit key, permuted, and finally XORed with another n-bit key. Since key whitening and permutation are unnecessary in the abridged form of this cypher, it is widely believed that it is trivial to break. The usual implementation of a permutation function makes use of a complex pseudorandom function.[12]

Figure 3: Comparative Use of Various Techniques in Lightweight Block Ciphers

4. IOT CONCEPTS AND ITS ARCHITECTURE

It is believed that the IoT will revolutionise computing and communications in a variety of industries in the near future. Combining "Internet" with "Things," "Internet of Things" (IoT) has become a popular phrase in the contemporary digital environment. Coke machines at Melon University were the first devices programmer-connected to the Internet in the 1980s. The term "Internet of Things" refers to a network that provides a digital representation of physical things, both living and nonliving. Connected sensors on everyday things are brought into the digital realm so that information may be shared about their conditions and context. IoT has a profound impact on everyone's daily lives since it automates the way things communicate across a network. The Internet of Things (IoT) is not a singular technology, but rather the result of the convergence of a variety of emerging technologies. By erecting huge infrastructure worldwide, IoT is improving our quality of life in many ways. In addition to the communication of living beings, the Internet of Things (IoT) has extensive participation from inanimate items. IoT encompasses all components necessary for coordination of worldwide sensor networks.[13]

This comprehensive method dramatically raises data storage needs and network pressures. RFID, Bluetooth, WiFi, ZigBee, Nanotechnology, sensor nodes, GPS-enabled devices, Actuators, Electronic Product Code (EPC), Internet Protocol, and Wireless Sensor Networks are all vital components of the Internet of Things (WSN). For the Internet of Things to function, RFID must be used as its networking backbone. To identify an item, RFID uses radio waves to transmit a unique serial number. It's a good deal since it's trustworthy, efficient, secure, and cheap. The EPC is meant to act as a universal identifier, giving each and every material item a name no matter where it is located in the globe. An RFID tag may store a 64/98-bit code electronically.[14] Objects connected to the Internet of Things use a wide range of technologies in a variety of settings to make the world around them smarter. Because of this, the resulting complicated dynamic system requires a WSN infrastructure that is not tied to any one platform. Such a large-scale sensor network requires data storage, processing power, and analysis capabilities. All IoT ideas are built upon the layered architecture that supports them. The four tiers of the Internet of Things architecture are the perception, network, session, and application layers. To clarify its role in respect to other layers, each one lays forth its functioning. The devices and technologies used in each layer, as well as the services they provide, characterise that layer. Each layer of the IoT architecture has its own set of vulnerabilities that can have a serious effect on the system as a whole. Despite widespread optimism over IoT, the authors of show how critical social services are vulnerable to cyberattacks. IoT design and how its four layers of communication employ different nodes in the IoT network are shown in Figure 4. [15]

Figuer4: IoT Architecture

The perception layer collects ambient data. Perception layer sensors and RFID readers have limited power, compute, and memory, making them less secure. These devices' sensors capture participant data. This layer uses GPS for geographic location tracing. Perception layer nodes promote close-range and local interactions. It records events, collects data, analyses it, and transmits it to the network layer. This tier's threats target sensor-based data collecting. Perception layer security issues abound. RFIDs, sensors, and other embedded intelligence are subject to perception layer assaults. Below are security weaknesses and solutions. Sensor network authentication and privacy concerns include eavesdropping, replay attacks, spoofing, and packet manipulation. If cryptographic systems were more durable, dependable, efficient, and secure, these assaults may be rarer. [16]

5. OPEN SECURITY CHALLENGES IN IOT

Due to the dynamic and pervasive nature of the Internet of Things, there is a wealth of unexplored territory for researchers interested in the topic of IoT security. Simply ensuring scalability is not enough to guarantee a successful implementation and practical usefulness of IoT as the number and variety of connected things continues to increase at an exponential rate. There are still substantial obstacles that must be overcome, such as the introduction of standards, the guaranteeing of Quality of Service, confidentiality, and reliability, the management of massive amounts of data, and the provision of energy efficiency.

The following are some examples of IoT security issues that have not yet been fully addressed: [17]

- heterogeneous device standardisation.
- large-scale usability and adaptability.
- confidentiality.
- security flaws in both software and hardware.
- Devices' physical protections.
- Use of energy and effectiveness.

6. CONCLUSION

When developing a security algorithm for Internet of Things (IoT) devices, it is important to consider the constraints imposed by the devices' limited resources. For instance, to achieve a specific level of security, the size of a block and key are subject to lower bounds in different implementation scenarios. There are still open questions on how to best approach lightweight cryptography methods. Several design factors and tradeoffs for lowering resource requirements are explored here. Customers may align their security needs with the needs of their applications thanks to the wide range of cryptographic technologies supported. Maintaining momentum toward fully realising and securely deploying the IoT requires a reasonable trade-off. The efficiency of the proposed family of lightweight cyphers is measured in a number of ways. On 64-bit platforms, the recommended family cyphers perform worse than any other benchmarked cypher save for RoadRunneR (64/80), but on 32-bit platforms, the suggested cyphers perform better than any similar LBC. All of the suggested family cypher variations have the least flash memory use, with the exception of the version with a 64-bit block size and 96-bit key size.

REFERENCES

1. Dinur, I. (2015). Improved differential cryptanalysis of round-reduced speck. In International Conference on Selected Areas in Cryptography, pp. 147- 164).
2. Al-Dabbagh, S. S. M., Al Shaikhli, I. F. T., AlEnezi, K. A., & Alyaqoup, M. J. (2015). Enhancing Lightweight Block Cipher Algorithm OLBCA through Decreasing Cost Factor. In 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT), pp. 159-164.
3. Jeong, K., Kang, H., Lee, C., Sung, J., Hong, S., & Lim, J. I. (2015). Weakness of lightweight block ciphers mCrypton and LED against biclique cryptanalysis. Peer-to-Peer Networking and Applications, 8(4), 716- 732.
4. Basha, S. N., Jilani, S. A. K., & Arun, M. S. (2016). An intelligent door system using Raspberry Pi and Amazon web services I0T. International Journal of Engineering Trends and Technology (IJETT), 33(2), 84-89.
5. Friansa, K., Haq, I. N., Santi, B. M., Kurniadi, D., Leksono, E., & Yuliarto, B. (2017). Development of battery monitoring system in smart microgrid based on internet of things (IoT). Procedia engineering, 170, 482-487.
6. Ankele, R., Banik, S., Chakraborti, A., List, E., Mendel, F., Sim, S. M., & Wang, G. (2017). Related-key impossible-differential attack on

reduced-round S kinny. In International Conference on Applied Cryptography and Network Security, pp. 208-228.
7. Joshitta, R. S. M., & Arockiam, L. (2018). A novel block cipher for enhancing data security in healthcare internet of things. In Journal of Physics: Conference Series, Vol. 1142, No. 1, p. 012002.
8. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., & Regazzoni, F. (2015). Midori: A block cipher for low energy. In International Conference on the Theory and Application of Cryptology and Information Security, pp. 411-436.
9. Cazorla, M., Marquet, K., & Minier, M. (2018). Survey and benchmark of lightweight block ciphers for wireless sensor networks. In 2013 International Conference on Security and Cryptography (SECRYPT), pp. 1-6. IEEE.
10. Bellare, M., & Kohno, T. (2018). A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In International Conference on the Theory and Applications of Cryptographic Techniques, pp. 491-506.
11. Diehl, W., Farahmand, F., Yalla, P., Kaps, J. P., & Gaj, K. (2017). Comparison of hardware and software implementations of selected lightweight block ciphers. In 2017 27th International Conference on Field Programmable Logic and Applications (FPL), pp. 1-4.
12. Gong, Z., Nikova, S., & Law, Y. W. (2016). KLEIN: a new family of lightweight block ciphers. In International Workshop on Radio Frequency Identification: Security and Privacy Issues, Lecture Notes in Computer Science, 7055, 1-18.
13. Paar, C., Rechberger, C. & Rombouts, P. (2015). PRINCE–a low-latency block cipher for pervasive computing applications. In International Conference on the Theory and Application of Cryptology and Information Security, pp. 208-225.
14. Eun, H., Lee, H., & Oh, H. (2018). Conditional privacy preserving security protocol for NFC applications. IEEE Transactions on Consumer Electronics, 59(1), 153- 160.
15. Gupta, N., Saeed, H., Jha, S., Chahande, M., & Pandey, S. (2017). Study and implementation of IoT based smart healthcare system. In 2017 International Conference on Trends in Electronics and Informatics (ICEI), pp. 541-546.
16. Lim, C. H., & Korkishko, T. (2015). M Crypton–a lightweight block cipher for security of low-cost RFID tags and sensors. In International Workshop on Information Security Applications, pp. 243-258.
17. Ojha, S. K., Kumar, N., & Jain, K. (2019). TWIS–a lightweight block cipher. In International Conference on Information Systems Security, vol. 5905, pp. 280-291.