CRYPTOGRAPHY AND SECURITY IN INTERNET OF THINGS

Miss. Medha. M.R

Msc. Computer Science, St.Joseph's college(Autonomous), Irinjalakkuda, Thrissur, Kerala

---***---

Abstract - *The Internet of things (IoT) means connecting different things such as physical devices which are build up with electronics, software , sensors to form a network which helps to collect and exchange data .It is also referred to as Internet of Everything (IoE) as name says it consist of all devices which are web enabled. These devices are called smart devices. While using IoT technologies the human beings play less role in communication and most of the work is done by the smart devices. However in this scenario the requirement of Security plays a vital role for the privacy and trust among the things and users within this system. For the flexible and secured use of this technology we need to introduce some kinds of security methods and this paper is intended to discuss the security issues and provide corresponding security using cryptography for these issues.*

Key Words: **Internet of Things, Cryptography, Lightweight cryptography.**

1. INTRODUCTION

Internet of Things or IoT introduces the mechanism of connecting huge amount of devices and allows communication between them through internet hence the devices become part of the network. This technique minimizes the role of human beings' involvement in such situations. We know that the network is most attractable area today even this area faces lots of security issues such as ethical hacking etc. The devices in IoT have to use only limited amount of resources, bandwidth, and power and storage capability. Because of the need of minimum number of humans' interaction in IoT, it makes the chance of attacks like DoS and also middle attack by man. And also there is a chance to access the device by a third party. When such a situation occurs it leads to a bad network connection and damages the physical devices. Because of these issues the devices and data should make secured in IoT.

The Cryptographic technologies make the study about some issues and implement techniques to overcome them.

2. INTERNET OF THINGS

Definition

The Internet of Things is defined as a network which is a interconnecting of physical devices with some of network concepts to make a overall control among these devices to communicate and share information through sensors and smart objects.

Applications of Internet of Things

There are several different areas become smarter in the real world due to the role of Internet of Things Technique. Some of them are listed below.

- Smart Homes
- Wearable
- Connected Cars
- Industrial Internet
- Smart cities
- IoT in Agricultural
- Smart Retail
- Energy Engagement
- IoT in Healthcare
- IoT in Poultry and Farming

Advantages of IoT

- Encourages communication among devices
- The devices interact without human support
- Monitoring
- Time savings
- Helps transparency in the processes
- Efficient
- Improves the quality of life by providing better management

The use of IoT makes automatic processing among the devices hence it provides better monitoring and management of the percolated devices.

Disadvantages of IoT

- Compatibility
- Complexity
- Privacy/Security
- Safety

The main and important disadvantage is Privacy and security issues this is we discuss in later.

3. Cryptography

Definition

Let's define Cryptography as the process of converting any data into a modified form which cannot identified by any third party. For this security this techniques introduces set of codes. The process of converting the ordinary text into modified or secured form is called Encryption and the reverse process is known as Decryption.

4. Cryptography in IoT

We said that IoT has many advantages it has disadvantages also the main serious problem is Security and privacy because IoT is working based on internet hence there is a huge chance of hacking information by third party over the processing. To solve such issues we use or introduce Cryptographic Techniques in Internet of Things to make the data more secured. We know that there are different encryptions algorithms are used to make data more secured but in the case of IoT there are some problems to inherit these algorithms. The problems are

- Small size of memory
- Limited bandwidth
- Brief execution time
- Short living power consumption
- Need to recharge batteries inconveniently
- No power consumption in some cases

Even with these issues in present an advanced Cryptographic technique is used which is called Light Weight Cryptography.

5. Lightweight Cryptography

In this scheme a set of Identity Based Encryption (IBE) is introduced and is known as fuzzy IBE [1]. It introduces a private key to identify the cipher text in both encryption and decryption if both are close each other. This uses biometric data as key. New ABE scheme allowing the user's private key to be expressed in any accessing formula above attribute[2]. It uses less amount of resource. It uses non-monotonic structure for key policy. We can use any accessing formula to express the key policy. Along with these private keys the unauthorized access can be controlled. When the encrypted data is accessing the structure with possible attributes then the decryption is also possible. The algorithms designed on the basis of ABE scheme are faster. This scheme is also used to decrypt GPSW texts. They analyze the performance of lightweight cryptography algorithm that are used in the application domain of RFID [3]. For the cipher algorithms such as HIGHT, KATAN, TEA, KLEIN code analysis is used. These are also used to evaluate the CPU execution time.Hash functions also used in this techniques.Instead of using a complex hash function in Encryption, XOR manipulation is used for encryption to Provide privacy and faking protection. Security Enhancement is described and demonstrated using Hardware support [9].

Table 1: Existing lightweight cryptography implementations with high computational and less efficiency [4].

Sl no.	Description	Benefits	Issues
1	Fuzzy identity-based encryption, in: Advances in Cryptology[1]	Predefined error to lerance capability	To construct fuzzy IBE schemes that utilize various distance metric between identities is a vital problem
2	Attribute-based encryption with no monotonic access structures[2]	Less expensive, Powerful enough to express the Boolean Access formula.	Less efficient, complex, several challenges may arise for adapting these negation techniques
3	Efficient cipher text policy attribute based encryption with constant-size cipher text and constant computation cost[5]	Cipher text size is efficient , low cost , Scalable, simple. To decentralize the Multi-authority setting, CP-ABE can Be extended.	Constant size cipher text is still challenging, computational cost overhead
4	An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies[6]	Supports complex access policies, high flexibility, low cost, requirement of Bandwidth is reduced.	It does not guarantee attribute collusion resistance.
5	Attribute-based encryption with fast decryption, in: Public-Key Cryptography—PKC[7]	It requires only constant pairing for decryption, key size low	Complexity, time consuming
6	Lightweight Cryptography for the Internet of Things[8]	More efficient for end to-end communication as well as applicable to lower resource Devices. Low power consumption	Quite challenging in terms of popular attacks
7	A lightweight authentication protocol for Internet of Things[9]	Reduces inadequacy, efficient and secure key establishment	Need to establish mutual authentication

Elliptic Curve Cryptography (ECC) uses digital signatures for efficient encrypting and decrypting in access booting. Generation of key serves a vital role in ECC, both in generation of private and the public keys [10].

4. Ethics on existing system

- Denial of services
- Masquerading

- Man in Middle
- Saturation
- Eavesdropping
- Differential

5. Conclusion

This study deals with the concept of IoT and the main problems occur during this technique. The important issue happens while using IoT is privacy or security problem. To overcome these we introduce Cryptographic methods. If we don't focused to solve this issue we don't get any security in transferring information through IoT.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Adv. Cryptology–EUROCRYPT 2005, pp.457–473, 2005.

[2] R. Ostrovsky and B. Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures,"CCS'07, Proc. 14th ACM Conf. Comput. Commun.Secur., no. October, pp. 195–203, 2007

[3] M. Alizadeh, J.Shayan, M. Zamani, and T. Khodadadi, "Code analysis of lightweight encryption algorithms using in RFID systems to improve cipher performance," 2012 IEEE Conf. Open Syst. ICOS 2012,

[4] X. Yao, Z. Chen, and Y. Tian, "A lightweightattribute-based encryption scheme for the Internet of Things," Futur. Gener. Comput. Syst., vol. 49, pp. 104–112, 2015.

[5] P. Junod and A. Karlov, "An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies," Proc. tenth Annu. ACM Work.Digit. rights Manag. - DRM '10, p. 13, 2010

[6] C. Chen, Z. Zhang, and D. Feng, "Efficient ciphertext policy attribute-based encryption with constant-size ciphertext and constant computation-cost," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 6980 LNCS, pp. 84–101, 2011.

[7] S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," Lect. Notes Comput.Sci. (Including Subser. Lect. Notes Artif. Intell. Lect.Notes Bioinformatics), vol. 7778 LNCS, pp. 162–179, 2013.

[8] M. Katagi and S. Moriai, "Lightweight cryptography for the Internet of Things," Sony Corp., pp.7–10, 2008.

[9] J. Y. Lee, W. C. Lin, and Y. H. Huang, "A lightweight authentication protocol for Internet of Things," 2014 Int. Symp. Next-Generation Electron. ISNE 2014, pp. 1–2, 2014.

[10] P. Shruti and R. Chandraleka, "Elliptic Curve Cryptography Security in the Context of Internet of Things," vol. 8, no. 5, pp. 90–93, 2017