A Review of Internet of Things Security Mechanisms

A. Aarthy[1], R.Pradeep[2]
[1]Dept of Computer Science
[2]Assistant Professor, Dept of Electronics and Communication Engineering
[1]Anna University Regional Campus, Coimbatore, India.
[2]Sri Eshwar College of Engineering, Coimbatore, India.

Abstract- *In Internet of things data (IoT) based real time application data can be stored in the Information Centric Network for analysis. It is a major issue that the real time data stored in the cloud can be accessed by unauthorized user. In order to address this issue, there are few security algorithms that transfer the real time data to authorized users. These security algorithms provide an authentication to the user who access the sensor data in the cloud. In this paper a comparative analysis of certain security algorithms used for IoT domain are revealed.*

Keywords- IoT, Security, Information Centric Network, Publisher Algorithm.

I. INTRODUCTION

Internet of Things(IoT) is a current era domain where all of the objects that[1] surround us will be connected to the internet. In the year 2020 it is assumed that about 50 billion devices will be connected to IoT and numerous amount of data will be generated from these devices. IoT data sharing in cloud will produce redundant and bring large latencies. And it has a limitations on giving an available service by IoT. In order to use the IoT services, users are conscious only about the IoT data but they are not concern with where the data are stored. Information Centric networking(ICN) rising technology here the users can retrieve data from nearby store without accessing it from far- away cloud. In account to existing ICNs, Content Centric Network (CCN) and Named Data Network (NDN) is a most effective method, hence we focus the storage CCN and NDN. Compared to IoT design,

ICN based IoT designs have many leading and distinct features in consider security, fast configuration and also reduction in traffic and latency. In future IoT applications and services are supported by ICN so that IoT designs using ICN as Information Centric IoT (ICIoT). ICIoT are used in IoT applications eg: smart cities, smart home data sharing and data collection in IoT. It provides feasible service to user. Security is a major issue where data can be accessed by the unauthorized access of illegal modification and retrieval. It is needed to design a secure IoT data base, where IoT data are securely published and authorized users can retrieve IoT data. Here the sensor and IoT security and authentication, authorization, access control are studied. CP-ABE[8] has few issues as they stored data in the cloud. So as an enhancement a Distributed Publisher driven secure Data sharing for ICIoT, came into an existence. It provides flexible authorization to publisher from users. Attribute manifest (AM) and data manifest (DM) are stored in the Information Centric Internet of Things. The following section in this paper exposes the comparison of few security algorithms based on Bandwidth, Flexibility, Scalability and communication overhead.

II. SECURITYREQUIREMENTS

This section describes about the background ofIoT security systems.

A. IotData

IoT data cannot be modified illegally by the unauthorized attackers, that[16] can be stored at the access points, gateways, routers. It approves correct data sharing between the owner and user.

B. Flexible Authorization

Publisher Publishes the data with the publisher defined policy and helps the user to access the original set of IoT data. Publisher provide the IoT data only to the authorized user based on the accessing rights.

C. Publisher Authentication

To ensure that publisher should provide the original data to the users. It is main target to the publisher that the data should not be illegally modified.

D. User Authentication

It should be guarantee that the requested data is provided by the publishers and it should be the original data free from unauthorized attacks.

III. LITERATURE SURVEY

Due to the issues in IoT security, there are many research work which is ongoing and few security algorithms are discussed in this section.

A. Cipher text Policy Attribute based Encryption (CPABE)

Cryptographic technique was a cipher text policy attribute based method. Here the data has been encrypted the cipher text[12] is identified with the structure and private keys based on attributes. In Key Attribute encryption the, major disadvantage is that the access policies were not created by the encryption. This provided a route to the establishment of Cipher text Policy Attribute Based Encryption which allows the access policies to the encrypted data. The owner who encrypts the data, model the access policy. The use of CP-ABE technique. The data owner is in charge of defining the access policies. This prevents unauthorized access and promotes security. In CP-ABE, revocation is not achieved efficiently. Thus it is not so easy for the data owner to modify the access polices whenever needed.

B. Homomorphic Algorithm

It is an encryption algorithm[13] that provide remarkable computation to encrypted data(cipher text) and gives the encrypted result. This algorithm can solve many issues security and confidentiality. Here encryption and decryption takes place inclient site and provider site and operates on the encrypted data. This can solve risk during the data transferring between client and service provider, it hide plaintext from service provider, provider operates upon cipher text only. Homomorphic encryption performs only the complex mathematical operations on the encrypted data without using the original data. For plaintexts X1 and X2 and corresponding cipher text Y1 and Y2, a Homomorphic encryption scheme permits the computation of X1 Θ X2 from Y1 and Y2 without using P1 Θ P2. The cryptosystem depends upon the operation Θ it can be multiplication or addition.

.

C. Multi Authority Attribute based Encryption

The Multi-Authority Attribute Based Encryption (MA-ABE) is also a[14] cryptographic technique which consists of many authorities to manage the attributes and the distribution of the secret keys. The user who wants to download the information will request the decryption keys from the attribute authority. The attribute key generation is one of the main algorithm in MA-ABE. This algorithm can be run by the authority and the authority will distribute the keys to the users. The appropriate decryption keys can view the information. The algorithms consists of Set up, Attribute Key Generation, Central Key Generation, Encryption, Decryption. This cryptographic scheme handles many number of users. Data confidentiality can be achieved in this type of technique in cloud environment. This cryptographic technique is most suitable for the applications that contains various sectors. This cryptographic scheme contains the advantage like that improves security and reduces key management complexity.

D. Distributed publisher driven algorithm (DPD ICIoT)

The data that are sensed[16] by the sensor using Raspberry-pi are encrypted by using (DPD ICIoT) Algorithm. Where the encrypted data are stored in cloud. Cloud provide the efficient and scalable data storage services with a lower cost. Here the authenticated users with the appropriate key can decrypt the data. In order to retrieve the data user must know the key to decrypt. DSA acts as a key server in order to provide data access rights to users. AM generates the attribute name and store them in the network for the publishers to retrieve for data encryption. AM is issued only by the DSA and stored in network for fast retrievals. DM is used to describe the attributes and data access policies.

It also manages the version of the data. In DPD ICIoT scheme can time between Publishers and users. Without this all users have to search the publishers themselves without any information It also introduces private key to users. Here publisher driven fine grained access control in a distributed caching for ICIoT. We incorporate CP-ABE with ICN,CCN and propose a new DPD-ICIoT for providing secure, and flexible data sharing for ICIoT. We use a key chain mechanism for encryption and encryption. We aim the AM to enable the close copy retrievals of attributes and propose an AASM for updating the attribute.

E. Attribute-Based Encryption(ABE)

Data is shared and stored by the owners on the Internet, the stored[2] data must be encrypted and stored in the internet. The main disadvantage of encrypting data, is that should be selectively shared on the internet. Here a new developed cryptosystem for sharing an encrypted data is known as Key- Policy Attribute-Based Encryption (KP-ABE). In cryptosystem, cipher texts are labeled with sets of attributes and private keys that control cipher texts as a user can decrypt the data. The shared encrypted data supports the private keys Hierarchical Identity- Based Encryption (HIBE).

F. Software-Defined Networking (SDN)

It is a growing new[15] technique for the next generation of network architecture. The control plan and data plan with SDN using dynamic software programs which gives the flexibility to secure, configure and manage the data. In security point of SDN it has the ability to collect information from the devices and allow the program in secured manner. Security solutions are given based on the static firewall programmed by an administrator ie, Intrusion, Detection and prevention system.

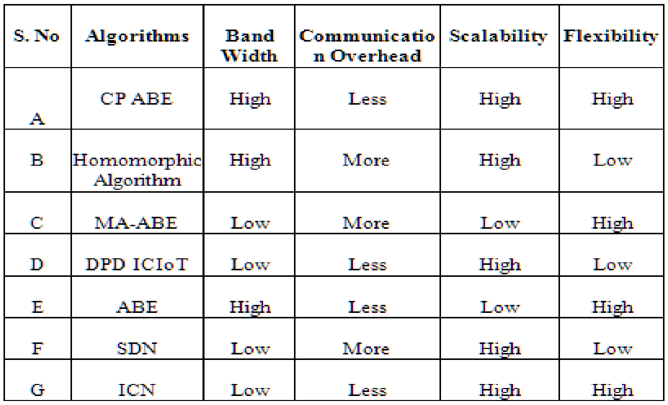
This integrated network program create a platform for IoT. Here the study is focused on the approach to build a network by SDN. A prototype system about 500 devices are predefined on the controller because of this reason a method to control the IP header at the application level has been defeat using opflex with SDN. It provide the better path for objects in the cluster scenario.

G. Information Centric Network(ICN)

There are so many[8] techniques have been planned for IoT platform the physical and digital objects are accessible by different organization and domains, they are based on IP overlay architecture. These inherit the Constraints solution of the current internet, in terms of naming, heterogeneity, mobility and security. Here proposed a new Information-Centric Network (ICN) based IoT middleware to address the challenges of various promising features of ICN. It e elaborate the functions of ICN based IoT middleware by integrating with the two future internet architectures, such as Named-Data Networking and Mobility First. It evaluate the efficiency of service discovery and demonstrate the feasibility of the proposed ICN based IoT middleware. The functions in the proposed system are required with the IoT requirements and protocol and the ICN IoT middleware depend on the IoT protocol.

Table 1

Comparison of IoT Security algorithms



S. No	Algorithms	Band Width	Communication Overhead	Scalability	Flexibility
A	CP ABE	High	Less	High	High
B	Homomorphic Algorithm	High	More	High	Low
C	MA-ABE	Low	More	Low	High
D	DPD ICIoT	Low	Less	High	Low
E	ABE	High	Less	Low	High
F	SDN	Low	More	High	Low
G	ICN	Low	Less	High	High

IV. CONCLUSION

In order to secure data from the illegal modification and unauthorized access. Everyday new techniques are evolving hence fast and secure conventional encryption techniques work with high security rate. This survey paves a way to design and invent a new and fast encryption algorithm compare overcoming the draw backs of existing algorithm. DPD-ICIoT provide a secure and flexible access in IoT. DPD-ICIoT scheme can reduce the bandwidth cost of attribute retrieval compared to existing CP-ABE.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani,M. Mohammadi, M. Aledhari, and M.Ayyash,"Internet of Things: A Survey on Enabling Technologies Protocols and Applications,"IEEE Communications Surveys & Tutorials, issue 99, June2015.

[2] M.AL-Naday, M. Reed, D. Trossen, and K.Yang, "Information Resilience:AN Attribute based Encryption ,"IEEE Network, vol.28, issue 3,pp. 36-42, 2014.

[3] R. Li and H. Asaeda,"A Community-Oriented Route Coordination Using Information Centric Networking Approach," 38th IEEE conf. Local Comput. Netw.(LCN). pp. 793-800,Oct.2013.

[4] M.Amadeo, C.Campolo, A. Molinaro, M,Aledhari, and M.Ayyash. "Multi Source Data Retrieval In IoT via Named Data Networking, " ACM Conference on information-Centeric Networking (ICN 2014), Sept. 2014.

[5] L. Touati, Y. Challal, and A. Bouabdallah, "C-CP-ABE: Cooperative Cipher text Policy Attribute-Based Encryption for the Internet of Things," 2014 International Conference on Advanced Networking Distributed Systems and Applications (INDS).2014.

[6] J. Kumar, and D. Patel,"A Survey on Internet of Things: Security and Privacy Issues," International Journal of Computer Applications, vol. 90. no. 11. 2014.

[7] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K.Fu,"plutus: Scalable Secure File Sharing on Untrusted Storage," USENIX'02, San Fransisco, CA, Dec.2002.

[8] W. Chai, and et. al., "An Information-Centric Communication Infrastructure for Real-Time State Estimation of Active Distribution Networks," IEEE Trans. on Smart Grid, vol. 6, no. 4, pp.2134-2146, July2015.

[9] E. AbdAllah, H. Hassanein, and M. Zulkernine, "A Survey of Security Attacks in Information- Centric Networking," IEEE Communications Surveys & Tutorials, vol. 17, issue 3, pp.1441- 1454, 2015.

[10] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang, and T. Sato, "A Key Management Scheme for Secure

Communications of Information Centric Advanced Metering Infrastructure in Smart Grid," IEEE Trans. on Instrumentation and Measurement, vol. 64, no. 8, pp.2072-2085, Aug.2015.

[11] W. Shang, Q. Ding, A. Marianantoni, J. Burke, and L. Zhang, "Securing Building Management Systems using Named Data Networking," IEEE Network, vol. 28, issue 3, pp.50-56, May2014.

[12] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute Based Encryption," the 28th IEEE Symposium on Security and Privacy, pp. 321-334, Oakland, 2007.

[13] P. Calhoun, J. Loughney, E. Guttman, G.Zorn,
J. Arkko, "Homomorphic Algorithm," RFC 3588, Sept. 2003.

[14] P. Samartini and S. Vimercati, "Multi Authority Attribute based Encryptions," In Foundations of Security Analysis and Design: Tutorial Lectures, LNCS, vol. 2171, p. 137–193, 2001.

[15] SDN-Based Security Framework for the IoT in Distributed Grid Carlos GONZALEZ, Salim Mahamat CHARFADINE, Olivier FLAUZAC and Florent NOLOT University of Reims Champagne- Ardenne.

[16] A Distributed Publisher-Driven Secure Data Sharing Scheme for Information-Centric IoT Ruidong Li, Member, IEEE, Hitoshi Asaeda, Senior Member, IEEE, and Jie Li,Senior Member.