Crypto Mechanism to Provide Secure to the IOT Data

Mrs. Chethana C

Assistant professor, CSE Dept. of BMSIT&M, Avalahalli, Yelahanka, Bengalore-64

Abstract - *Internet of things and cloud computing are two different technologies which are the important components of future internet. The merging of these two technologies is called IOT. The large amount of data could be collected in the cloud by various IOT applications. In this research we are going to propose the model which provides security to the IOT data in the Cloud.*

***Key Words*: Cloud, Decryption, Encryption, IoT, Secure**

1. INTRODUCTION

Internet of things (IOT) is defined as network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external states or the external environment. Internet of things is a one of the emerging new technology.

It allows unbounded connectivity of various devices at any time, at any place. It allows the organizations and third parties to collect and analyze the data about various information. It also allows making use of different technologies to manage the data [1].

Internet of things and cloud computing are two different technologies which are the important components of future internet [2]. The merging of these two technologies is called IOT.

Cloud platform allows third parties to develop IOT plugins so that any devices to be connected to the cloud. This type of service model enables to meet complex requirements such as timeliness, scalability, security, easy configurability and flexibility. The union of IOT resources into cloud introduces new resource management.

The various applications used in cloud IoT are: Healthcare, Smart cities and communities, Smart home and smart metering, Video surveillance, Automotive and smart mobility, Smart energy and smart grid, Smart logistics, Environmental monitoring.

The sensitive data (Example in an health monitoring applications data such as, heart rate, location, step-count, etc.) of the user may be intruded by the outside world. Therefore approaches to preserve the privacy of the data in the cloud are very important.

The security for database needs a separate consideration in addition to traditional cytological security. Especially, since various attacks such as inference attack, query execution attack or known-plaintext attack are possible according to the nature of database.

2. LITERATURE SURVEY

There are various encryption and decryption algorithm few of which are, homomorphic encryption scheme, encrypted query processing, order preserving encryption etc

Drawbacks in existing systems are as follows

- Leakage of information.
- May not applicable for IOT
- frequency and order based inference attacks cannot be avoided
- Attacker can learn the occurance of data item
- Expensive

Zheli Liu, et al. [4] proposed, "New order preserving encryption model for outsourced databases in cloud environments". Order-preserving encryption (OPE) is a common encryption scheme which ensures that the order of plaintexts remains in the ciphertexts. It is appealing because systems can perform order operations on ciphertexts in the same way as on plaintexts: for example, a database server can build an index, perform SQL range queries, and sort encrypted data, all in the same way as for plaintext data.

The proposed OPE model can be implemented by any programming language, and users can define their split methods and encrypt function. The disadvantage of this algorithm is it does not provide the nonlinear encrypt function and also it does not prevent frequency based inference attacks.

Seny kamar, [5] proposed, "Encrypted search". One common way to store IoT data is in structured databases, such as SQL databases. In an encrypted query processing system, a plaintext SQL query is transformed to an encrypted query, such that the cloud cannot learn about the values in the query. The query is then executed over encrypted data and the encrypted result is sent back to the user. The disadvantage of this algorithm leads to leaking information.

In CryptDB [6], the cloud can perform traditional database queries over encrypted data and reply with the encrypted result. To achieve this, CryptDB relies on a trusted proxy which intercepts the communication and applies en-decryption transparent to the user. CryptDB is designed with web applications in mind and is not suitable for IoT application scenarios, mainly because: (i) it employs cryptographic schemes that are prohibitively expensive for

constrained IoT devices and (ii) it relies on a trusted proxy, which has access to the encryption keys and plaintext information.

H. Shafagh et. al, Talos: Encrypted Query Processing for the IoT [7], in this paper, authors present Talos1, an IoT data protection system which securely stores encrypted IoT data on the Cloud database, while allowing for efficient database query processing over the encrypted data. In their design, they move away from CryptDB's focus on web applications only. Instead, they have a secure end to end system that stores encrypted data from IoT devices on a cloud database, where data protection is executed at the data source.

Craig Gentry et.al, proposes an "Homomorphic Evaluation of the AES Circuit" [8]. Research on fully homomorphic cryptosystems has made significant advancements in the recent years, and been able to show that arbitrary computations on encrypted values are implementable. However, the involved computations are yet prohibitively high even for full-fledged devices and by far infeasible for resource constrained devices. The computations involved are presently prohibitively expensive even for full-fledged devices and highly infeasible for resource-limited devices. It is, however, with regards to IoT resources, computationally intensive and results into a large ciphertext size of 256 Byte, given a key size of 1024 bit.

"Inference Attacks on Property-Preserving Encrypted Databases", proposed by M. Naveed et al [9], showed how simple attack techniques can be used to disclose encrypted medical data in the OPE and Deterministic encryption schemes. The attack schemes require access to auxiliary information, such as range of data and distribution of it, which is seemingly simple to retrieve for certain application scenarios. The disadvantage of this is techniques such as frequency attack can be used to learn about encrypted data.

3. OBJECTIVE OF THE PROPOSED RESEARCH

The Objective is to:

- Provide an efficient encryption and decryption algorithm for the IoT data stored in the cloud.
- To provide a secure end to end connection between IOT device and cloud. A secure end to end connection between Cloud and User.

4. PROBLEM IDENTIFICATION AND DEFINITION

The Internet of Things (IoT), one of the fastest growing trends in computing. IoT may have significant impact on individuals' privacy. IoT devices of any type contribute to the enormous amount of data stored on corporate clouds. The challenges due to the ecosystem of IoT applications require a more careful system design with regard to resource constraints. It remains an important open research problem to design and prove secure and practical encrypted data processing schemes for the IoT domain. Limitations on IoT devices are their resource constraints. IoT devices are inherently limited with regards to energy, memory, CPU, and bandwidth.

The traditional cryptographic algorithms applied to the database cannot overcome the various attacks like inference attack, query execution attack. The proposed work is to provide a safety encryption and decryption algorithm to secure IoT data on to cloud.

5. PROPOSED WORK AND METHODOLOGY

The proposed system crypto mechanism to provide secures to the Iot data in the cloud. The IoT data stored in database have to be secured from various attacks. Therefore encryption mechanism suitable for database environment is required.

Hence, the proposed work will emphasize on enhancing the resource utilization by providing security features for the data.

The proposed system consists of the following modules

- Authenticity module:
- Data Intake module
- Encryption module
- Manager Module
- Decryption Module

Authenticity module: To address Network-based Attacks between the IoT device (sensing and actuator) and the Cloud, cloud and the user , Iot and user , a direct HTTPS [10] connection is used. This allows The Internet of Things (IoT), one of the fastest growing trends in computing. IoT may have significant impact on individuals' privacy. IoT devices of any type contribute to the enormous amount of data stored on corporate clouds.

The challenges due to the ecosystem of IoT applications require a more careful system design with regard to resource constraints. It remains an important open research problem to design and prove secure and practical encrypted data processing schemes for the IoT domain. Limitations on IoT devices are their resource constraints. IoT devices are inherently limited with regards to energy, memory, CPU, and bandwidth.

The traditional cryptographic algorithms applied to the database cannot overcome the various attacks like inference attack, query execution attack. The proposed work is to provide a safety encryption and decryption algorithm to secure IoT data on to cloud. Providing confidentiality,

integrity protection, and authenticity of the data consisting of two steps

- Handshaking
- Key Generation for communication

1. **Data Intake and encrypt module**: This module reads the data from the data sensing IOT device at front end, and apply encrypt scheme [11] to store in the cloud database. Encryption of read data using protocol consists of preprocessing and transformation. The transformation process will apply HMAC recursively.

2. **Decryption Module**: Consisting of decryption scheme [11] Inverse transformation and post processing to get Plaint text of the encrypted data present in the cloud data base. This module will be deploying at data back end IOT device.

3. **Manager Module**: This comes with the security module, which will enable the administrators to control the data access and data sharing among the other users of the organization.

4. **User module**: Secure connection between user and cloud will be established. Then the user is allowed to search for the data. The encrypted data from the cloud will be decryptedbby the decryption module and plain data will be displayed on to the user application.

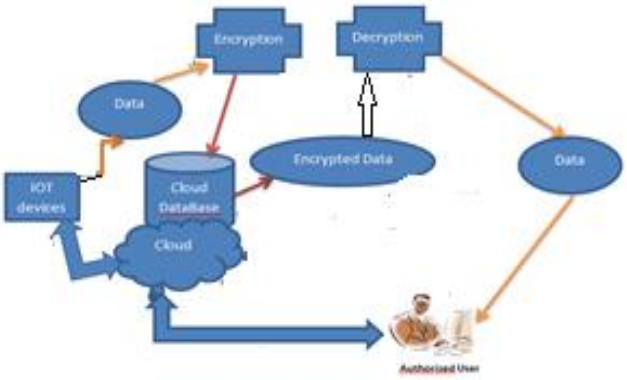

Fig1. Proposed IoT Model to seure IOT data.

The various steps of our IOT model shown in Fig2 is expained below.

First step is to establish secure connection between Iot Device and Cloud. Accessed IoT data wll be encrypted before storing data on to the cloud database. Then next step is to establisg secure connection between Cloud and User. Once the secure connection is established between user and the cloud, he is allowed to search for data. The user, and gets the encrypted data from the cloud database. The encrypted data will be decrypted to get plain text. The plain text will be displayed at user application.

6. CONCLUSION

The sensitive data in the database needs to be secured from various attacks, or accessing from unauthorized persons. The various attacks such as inference attack, query execution attack or known-plaintext attack are possible according to the nature of database; an encryption mechanism suitable for database environment is required.

Therefore we can make use of a better algorithm that can carry out range search without exposing the order. We also propose to build a formal model to verify and validate the outcome of the research work, measuring of various factors like energy memory consumption, time usage for encryption and decryption.

REFERENCES

[1] X. Caron, R.Bosua,S. B. Maynard,A. Ahmed, "The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective", elsevier ,Science Direct, Pp.No 4-5, 2016.

[2] Botta, W. D. Donato, V.Persico,A.Prescape, "Integration of Cloud computing and Internet of Things: A survey", Elsevier, Future Generation Computer Systems, Vol 56, Pp.No 684–700, 2016.

[3] H. Shafagh, "Towards computing over Encrypted Data in IoT Systems", ACM, XRDS- WINT ER, Vol.22(2), Pp.No 48-52,2015, DOI: 10.1145/2845157.

[4] Z.Liu, X. Chen,J. Yang, C.Jia, I.You, "New order preserving encryption model for outsourced databases in cloud environments", Elsvier, Journal of Network and Computer Applications, Vol 59, Pp.No 198-207, 2016.

[5] B. S.Kamara," Encrypted Search", ACM, XRDS-Spring, Vol. 21(3), Pp. No 30-34, DOI:10.1145/2730908.

[6] R. A. Popa, C. M. S. Redfield, N. Zeldovich,H. Balakrishnan, "CryptDB: Protecting Confidentiality with Encrypted Query Processing", ACM, 978-1-4503-0977,2 Pp.No 1-16,2011.

[7] H.Shafagh, A. Hithnawi, S. Duquennoy, W.Hu," Talos: Encrypted query Processing for the Internet of Things", ACM, 978-1-4503-3631, 2015, http://dx.doi.org/10.1145/2809695. 2809723.

[8] C.Gentry, S,Halevi, N. P. Smart, "Homomorphic Evaluation of the AES Circuit", In Proceedings of Advances in Cryptology (CRYPTO '12). ACM, New York, 2012.

[9] M.Naveed, S. Kamara, C. V. wright, "Inference Attacks on Property-Preserving Encrypted Databases, In Proceedings of the 22nd ACM SIGSAC, Conference on Computer and Communications Security (CCS'15), New York, 2015, DOI: http://dx.doi.org/10.1145 /2810103.2813651.

[10] K.Gaurav, P. Goyal, V. Agrawal, S.L. Rao," IoT Transaction Security", 5th International Conference on the Internet of Things (IoT), 2015.

[11] D. Lee, N. Park, "Security Enhancement Scheme supporting range queries on encrypted DB for Secure e-Navigation Era", International Journal of Security and Its Applications, vol.10 (2) Pp. No 141-150,2016, http://dx.doi.org/10.14257/ijsia.2016.10.2.13