European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 08, Issue 02 , 2021

IOT-ENABLED INFRASTRUCTURE PRIVACY PRESERVATION IN BIG DATA

[1]K. Ashokkumar,[2]S.K.B. Sangeetha,[3]S. Gayathri,[4]K. Kamala,[5]S. DivyaKeerthi

[1]Assistant Professor ,[2]Assistant Professor (Sr.G), [3,4,5]UG Scholar,
[1,2,3,4,5]Department of Computer Science and Engineering,
[1] Miriam Navajee Munoth Jain Engineering College, Chennai
[2]SRM Institute of Science and Technology, Chennai.
[3,4,5]Rajalakshmi Engineering college , Chennai.

Abstract : The growth in internet of items (IoT) use in big data is exponential, and a large number of these devices are expected to be monitored in various domains for different applications. Therefore, high traffic volumes and safety standards and procedures must be managed by the servers. Although many mechanisms are in place to protect the data transmitted, they are not enough to satisfy the data requirements. This work therefore aims to enhance the security and privacy of IoT communications among big data through the implementation of server privacy and the development of unique signatures using device attributes.These features may be constant depending on the user, but when the device communicates, identity changes to protect privacy. To allocate IDs based on the IoT device attributes, a special server called the Attribute Management System (AMS) is used. Depending on data type and transfer length, three different algorithms are used. This latest, secure IoT device design communication offers safe big data confidentiality.

1.INTRODUCTION

The Internet of Things (IoT) is a series of interconnected computing devices with specific UIDs and the ability to transfer data through a network without the need for contact between people and computers. The enterprise use of the IoT in big data can be divided into two segments: industrial-specific services such as sensors in a manufacturing plant or real-time healthcare monitoring systems and IoT equipment which can be employed in any industry such as smart air conditioning or security systems.However, several security issues remain to be resolved in order to meet IoT's maximum potential Abdul Qawy et al.[2015]. IT security problems, forms of encryption, attribute based encryption, and the purpose of this work are the main objective of this work.

A broad range is also divided into consumer, commercial, infrastructures and industrial applications.One of these IoT technologies is the definition and devices of Smart Home Systems (SHS) consisting of Internet based tools, home automation systems and efficient energy information systems. Furthermore, a further significant accomplishment of IoT in big data is the Smart Health Sensing system (SHSS). SHSS comprises lightweight, intelligent instruments and healthcare services. Such software can be used both indoors and outdoors to test and track various health and wellness issues or the amount of calories in the fitness centre, etc Sheik dawood et al.[2018].

In addition, vehicles with pre-installed sensing devices that can detect the upcoming heavy traffic congestion on the map will be implemented and can suggest another low traffic congested lane. Therefore in different fields of life and technology IoT has a lot to bring in big data. We may conclude that IoT provides tremendous potential for both technological advancement and human enhancement in the big data field Kumar et al.[2019]. IoT networks' handling big data rising complexity also increases the security problems faced by those networks. Due to the large number of devices connecting to the Internet along with the huge data generated by those devices, the challenge of IoT networks is due. IoT assaults in big data are likely because computers are a convenient target for IoT network intrusion. Hackers will gain control and conduct malicious activities once they are infected and target other devices close to the node. IoT computers have no virus or malware detection software. This is a natural product of the low memory and low power architecture of these devices Monsi zadeh et al.[2018]; Shaik et al.[2019].

When an IoT based big data system is breached, the attacker may also secure the routing and forwarding of the computer. Appealers may also access confidential data besides targeting many other devices in the network. This absence of confidentiality, integrity and information protection in IoT will disturb the widespread adoption of this technology. The discussion thus far shows that the problem of securing IoT devices is greatly exacerbated by the resource constraints, and that IoT networks cannot easy incorporate attack prevention and privacy solutions used on traditional networks Sufian Hameed et al.[2019].The algorithms have been chosen among many other literary cryptographic algorithms. The choice was made to choose algorithms designed to be light on resource-restricted platforms with relatively few storage and processing resources, but at the same time providing the minimum necessary security level Geovandro et al.[2017]; Jurcut et al.[2019].

The encryption feature allows the sender to encrypt the message without a public key certificate. In certain cases, the solution to the issue is that data can be encrypted without certificates with a public key. User A can, for example, send an encrypted message to receiver B without PKI or if the receiver is not linked at switch. The data owner, the user and the third party, the Trusted Hub, gets the details. The role of the trusted centre is to get the key to encrypt and decrypt data holders. A complete collection of predefined characteristics creates the master and the public keys. When it adds a user with a new device attribute, it adds the attribute to the list and re-constructs open and master keys.The data owner encrypts them along with the public key and some attributes. The data the user can decipher using his own private key is obtained. This main is a consumer-friendly hub. It then checks the correspondence between the private key attributes of the user and the encrypted data attributes. If a default threshold d exceeds the number of matched attributes, the user may use a private key to decrypt the data. Unable to decrypt the files, otherwise Suo et al.[2012];Mohammed et al.[2017];Perwaj et al.[2019].

This work seeks to enhance big data protection on IoT devices through a new technique for encryption. The aims of the study are:

- In order to recognise the security problems of the big data based IoT network, a better trustworthy network can be created.
- The weaknesses in current encryption techniques to establish a secure encryption technique should be established.
- Transfer of data in encrypted format using IoT system attributes.

Section 2 provides a design of attribute based encryption. Section 4 explains the assessment of the proposed problem and the study of the outcome shown by graphical representation. Section 4 concludes the work.

2. DESIGN OF ATTRIBUTE BASED ENCRYPTION

ABE is an asymmetrical encryption in which a number of attributes depend on the user's Secret Key (CK) and Chip Text (CT) (e.g. service, postal code, classification, etc.). ABE is among the fine grained access control algorithms not supported by other symmetrical and asymmetrical encryption schemes.A sender with a set of descriptive attributes in key policy attribute (KP-ABE) is the sender that defines the ciphertext, while a trusted user attribute authority provides a protocol with a privacy key (also called the access structure) specifying what sort of ciphertext the key is to decrypt.When a sender encrypts a message with a ciphertext attribute-based encryption (CP-ABE), it describes a certain access policy in terms a ciphertext attribute access structure which specifies the kind of recipients which can retrieve the ciphertext. Users have a set of attributes and obtain the hidden keys of the attribute authority. Such a customer can decrypt a chip text if its characteristics comply with the chip-related access policy. The CP-ABE method therefore has a conceptual resemblance to the traditional approach to position-based access control Muthswamy et al.[2016].

2.1 Attribute based Encryption on IoT

The Big Data Technology business, trade, medicine, banking, the State, etc., is centralised and expanded. Generally, a large amount of data is generated every day in the industrial production sector which includes business data from IT systems, IOT computer data and other data from related platforms. Big data is used not only to improve the efficiency of the organisation but above all for the transformation of the production process and business model for a manufacturing company. The centre for smart production and industrial IoT is Industrial Big Data, which gives Industry 4.0 the most favourable support for growth.

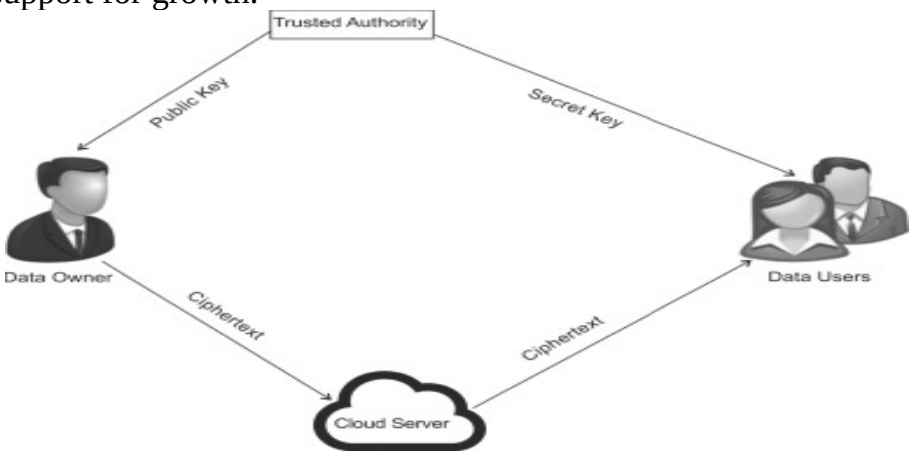

Figure 1.ABE on Cloud Computing

Illustration 1. Represents the design of cloud-based ABE implementation. IoT is a cloud computing platform that allows user-friendly, easy and on-demand access to the Internet through a common pool (i.e. networks, servers, storage, software and services) of personalised computing resources which are easy to distribute and distributed with minimal intervention in the administration and service provider. There are two main types of cloud infrastructure: public cloud and private cloud. In order to make use of public clouds that are usually semi-trusted, that is, genuine and yet curious, the data owners have to pass their data to corporate cloud providers.This ensures that cloud providers will try to dig into outsourced data from users, as much of the cloud information as possible, but in general, they will be frank with the protocol.

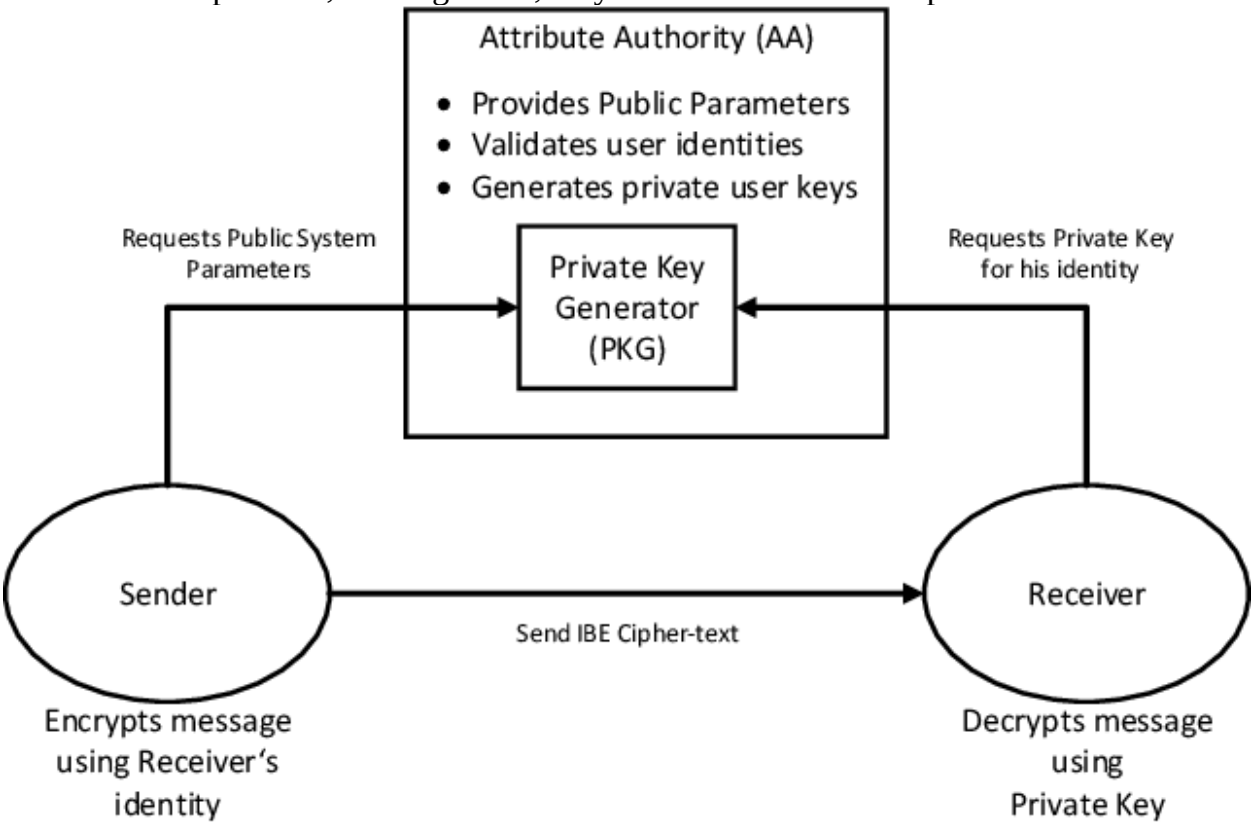

Figure 2. Architecture of ABE on IoT Devices

Illustration 2. Displays the ABE-based IoT basic data flow. Present approach management approaches rely on the assumption that the server is in the trusted domain of the data owners, thereby enabling the enforcement of access policies against authenticated users through an omniscient reference controller. This theory does not usually extend to the cloud computing context, however, and thus such approaches are not applicable. It needs a decentralised, flexible and versatile approach to managing cloud access without relying solely on cloud service providers.

2.2 Secure Encryption mechanism for IoT

Implementation of a contact server and the ABE server for customer support is fast and straightforward emulation. You can quickly switch to any IoT network in this architecture.

The actual implementation will contain 2 servers.

1. Command/Communication Interfacing Server
2. AMS (Attribute Management Server)

The command/communication Interfacing server acts as the provider of resources or data for IoT applications, which stands as IoT endpoints in our implementation. It is also connected to all customers. The client also connects to the AMS in order to receive secure and anonymous encryption keys. The Client originally provides its AMS attribute and AMS creates keys for each client and his identity according to its attribute. When an AMS is sent for a customer request, it sends the ID to AMS and will obtain a private key to decrypt the application.This preserves the true identity of the client and simultaneously maintains the protection of the server. The only condition is to comply both with the terms of the AMS and with the respective functions on the contact / command Server.

3.PERFORMANCE ANALYSIS

3.1 Performance perspectives

In order to verify the encryption/decryption speed of an algorithm, the comparison takes place with the execution of several encryption settings for different data block sizes. This work provides a comparison of results across the four most popular encryption algorithms: ECC; AES; RSA; Hummingbird. ECC is the latest type of encoding that offers greater protection for Elliptic Curve Cryptography. Compared with RSA and DSA, the ECC of 256bit is equivalent to the 3072bit RSA key. It is also suitable for smartphones and tablets to use less computing resources, fast and stable communication.

The AES encryption algorithm specifies a number of transformations on data stored in an array. The first step of the cypher is to add the data to an array; subsequently a number of encryption rounds repeat the cypher transformations. The key length specifies the number of rounds, for the 128-bit keys with 10 rounds, for the 192-bit keys 12 rounds and for the 256-bit key with the 14 round algorithm. Both RSA and AES algorithms are used between these algorithms. The lightweight, sophisticated algorithms used in this study are ordered by Hummingbird, AES, RSA, and ECC algorithms.

Count of Priority

Figure 3. shows the count of priority among the priority values HIGH, KEY, LOW and MODERATE.

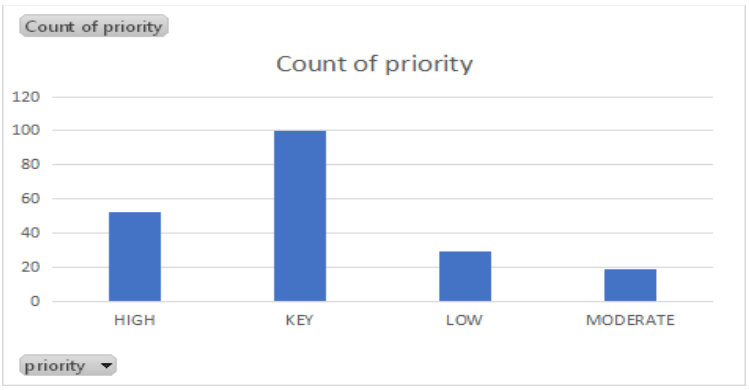

Figure 3. Count of Priority

Sum of What by priority

Figure 4. depicts the Some of what by priority among the priority values HIGH, KEY, LOW and MODERATE.

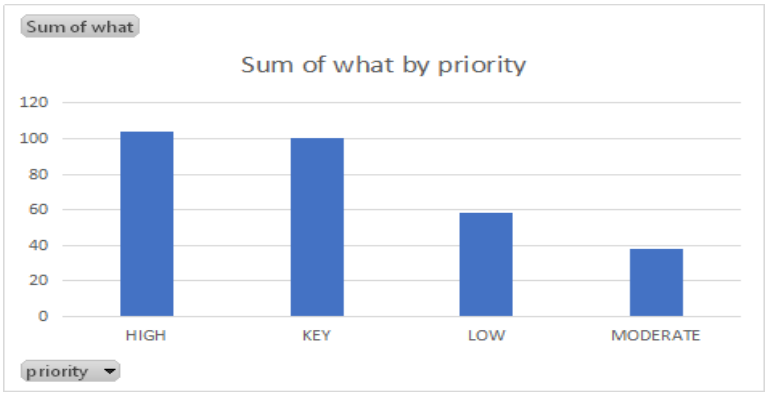

Figure 4.Some of What by priority

Sum of total time by priority

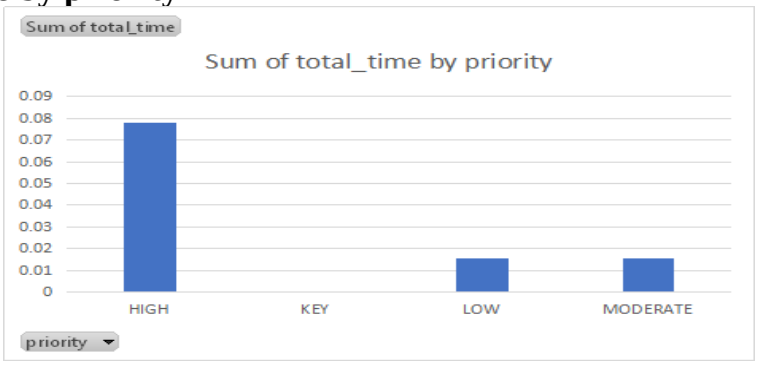

Figure 5. Sum of Total time by priority

Total time

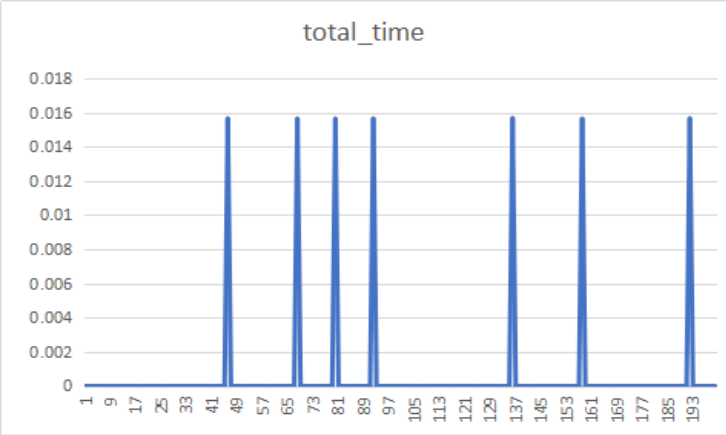

Figure 6. Total-time requirement

Several tests are performed to ensure accuracy in the results and that comparison of the different algorithms is fair. Our review gives a simple summary of the overall performance of the above listed metrics, and an alert of selected safety levels and attributes. In general, when the security level increases relative to the number of attribute values, there is a higher performance penalty. The number of attributes to be considered must be decreased by 10 times an average for better protection (i.e. 80 to 128 bits).Our results are an excellent guide for researchers and designers of new security technologies, based on the ABE. This mixture of platforms, levels and attributes is a notable insight in this parallel-space. We consider that future research ought to concentrate on enhancing ABE performance, both through careful selection of attributes and optimization of cryptography libraries.

4. CONCLUSION

With the exponential growth of Internet technology, the Internet of Things (IoT) is gaining popularity. In 2020, it will have around 30 billion smartphones that will significantly boost the quality of life. The amount of device connections rises as data is increasingly being transmitted between different devices. Data created by intelligent IoT devices, such as intelligent watches, intelligent home devices and other applications, are vulnerable to security and privacy threats. The users of the app are also entitled to track and preserve data accessibility.This contributes to many problems, including protection of data and privacy. Encryption techniques are used by the devices to boost security, but problems such as machine complexity and performance lead to problems of confidence. Attribute-based encryption is an encryption variant widely used in various applications for the control of fine grained data access. This kind of encryption is important for the prior setting of the policy for ciphertext during encryption.This improves the encryption process and makes it a lightweight algorithm that fits lightweight IoT devices. An improved attribute-based encryption algorithm is required to improve security for IoT devices. In this study the goal is to improve the safety of IoT devices by improving the encryption algorithm based on the attributes.

REFERENCES

1. Geovandro C. C. F. Pereira, Renan C. A. Alves 2017.Performance Evaluation of Cryptographic Algorithms over IoT Platforms and Operating Systems, Security and Privacy in Emerging Wireless Networks, Hindawi.
2. Jurcut, Anca & Ranaweera, Pasika & Xu, Lina. (2019). Introduction to IoT Security. 10.1002/9781119527978.ch2.
3. Kumar, S., Tiwari, P. & Zymbler, M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data 6, 111 (2019).
4. Mohammed, Husamuddin & Qayyum, Mohammed. (2017). Internet of Things :A Study on Security and Privacy Threats. 10.1109/Anti-Cybercrime.2017.7905270.
5. Muthuswamy, Sujithra & Ganapathi, Padmavathi. (2016). IOT Security Challenges and Issues – An Overview.
6. Monshizadeh, Mehrnoosh & Khatri, Vikramajeet. (2018). IoT Security. 10.1002/9781119293071.ch11.
7. Perwej, Dr. Yusuf & Parwej, Dr. Firoj & M., Mumdouh & Akhtar, Nikhat. (2019). The Internet-of-Things (IoT) Security : A Technological Perspective and Review. Volume 5. Page 462-482. 10.32628/CSEIT195193.
8. Shaikh, Eman & Mohiuddin, Iman & Manzoor, Ayisha. (2019). Internet of Things (IoT): Security and Privacy Threats. 1-6. 10.1109/CAIS.2019.8769539.
9. M, Sheik dawood. (2018). Review on Applications of Internet of Things (IoT).
10. Sufian Hameed, Faraz Idris Khan & Bilal Hameed (2019): Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review, Journal of Computer Networks and Communications.
11. Suo, Hui & Wan, Jiafu & Zou, Caifeng & Liu, Jianqi. (2012). Security in the Internet of Things: A Review. Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012. 3. 10.1109/ICCSEE.2012.373.