Privacy Awareness Protocol for M2M Communication in IOT

Apurva R. Wattamwar[1], Dr. P. N. Mahalle[2]
Department of Computer Engineering,
Smt. Kashibai Navale College of Engineering, Savitribai Phule, Pune University, Pune, India

Abstract - Internet of Things (IoT) winds up optional piece of regular day to day existence and could come upon a risk if security isn't considered before arrangement of communication. Verification and access control in IoT is similarly critical to set up secure correspondence between machines. When two machines start communication then data send from sender to receiver and vice versa, this traveling of data from one to another is not secure it may consists of man in middle, replay and denial of service attacks. This paper presents information about convention utilizing ECC (Elliptic curve Cryptography) along with ElGamal cryptography, which secure against the attacks.

Here it partitions a Record into pieces and encodes given document section, and repeats the divided information over the cloud/server hubs. Every one of the hubs stores just a solitary section of a specific information document that guarantees that even if there should arise an occurrence of an effective attack; no important data is get to the attacker. So finally data is get secure from above mentioned attack. This paper gives general idea about how proposed system works and store fragment of file to protect data from attacks.

Keywords - Attribute-based encryption, Cloud storage, Privacy protection, Decryption, Large universe, Full security.

I. INTRODUCTION

In this paper proposed a novel end-to-end data integrity Cloud-assisted cyber-physical systems (Cloud-CPSs; also known as cyber-physical cloud systems) have broad applications, ranging from healthcare, to smart electricity grid, smart cities, battlefields, military, and so on. In such systems, client devices (e.g., Android and iOS devices, or resource constrained devices such as sensors) can be used to access the relevant services (e.g., in the context of a smart electricity grid, it may include utility usage data analyzed and stored in the cloud) from/via the cloud/server. However, client devices generally have less computing capabilities and hence, are unlikely to have adequate security (technical) measures in comparison to the conventional personal computers (PCs).

From the existing work survey, like this here deduce the both security and performance are critical for the next generation large-scale systems, such as clouds. Therefore, in this project, the collective approach is the issue of security and performance as a secure data replication problem. It presents Division and Replication of Data in the Cloud for Optimal Performance and Security that judicially fragments user files into pieces and replicates them at strategic locations within the cloud.

The division of a record into fragments is finished supported a given user standards such that the individual fragments don't incorporate any good sized statistics. every of the cloud nodes (here technology use the time period node to represent computing, garage, bodily, and virtual machines) carries a wonderful fragment to boom the information security. In a a hit assault(attack) on a single node need to not display the places of different fragments at periods inside the cloud/server. To maintain an attacker unsure about the places of the report fragments and to in addition enhance the security, here it pick out the nodes in a way that they are no longer adjoining and are at certain distance from each different. The node separation is ensured via suggested that of the T-coloring Method.

II. MOTIVATION

The extent of security required for devices varies dramatically depending upon the function of the device. rather than asking if the device is secure, it ought to be asking if the communication channel is going to be secure enough or no longer.

Cloud-assisted cyber-physical systems (Cloud-CPSs; also called cyber-bodily cloud systems) have extensive programs, starting from healthcare to smart power grid to clever towns to battlefields to army, and so on. In such structures, gadgets (e.g., Android and iOS gadgets, or aid restrained devices which includes sensors) may be used to access the applicable offerings (e.g., in the context of a smart electricity grid, it can consist of application usage records analyzed and stored within the cloud) from/through the cloud. but, client devices typically have much less computing talents and consequently, are not going to have good enough security (technical) measures in evaluation to the conventional personal computers (desktops). So the file cryptographic storage is an effective method to prevent private data from being stolen or tampered. Data integrity is also maintain if attack is performed for tempered data then it should detect and prevent. By which we can able to perform secure communication between two or more devices.

III. OBJECTIVES

a. Provide proper and secure key exchange algorithm.

b. Maintain privacy of message and end connection devices.

IV. REVIEW OF LITERATURE

Paper [1] presents Multi-client accessible encryption scheme, scheme, which has various points of interest over the known methodologies. The related model and security prerequisites are likewise planned. It further talks about to expand given plan in a few different ways in order to accomplish different search abilities.

In propose paper [2] a secure data access scheme dependent on character based encryption and bio metric validation for distributed computing. System describe the security worry of distributed computing and after that propose a coordinated integrated data access scheme for distributed cloud computing, the strategy of the proposed conspire incorporate parameter setup, key appropriation, include layout creation, cloud information processing and secure data access control.

The paper third proposes an identity based data storage scheme where the two questions from the intra-space and between areas are considered an agreement assaults can be stood up to. Moreover, the entrance authorization can be controlled by the proprietor autonomously [3].

Fourth paper, focuses on the critical issue of identity revocation, System bring re-appropriating calculation into IBE and propose a revocable plan in which the disavowal activities are appointed to CSP. With the guide of KU-CSP, the proposed plan is full-highlighted: It accomplishes steady proficiency for both calculation at PKG and private key size at client;

i). User needs not to contact with PKG amid key-refresh, at the end of the day, PKG is permitted to be disconnected in the wake of sending the denial rundown to KU-CSP;

ii). No secure channel or client confirmation is required amid key-refresh among client and KU-CSP [4].

Here in paper [6] document partitions into pieces, and repeat the divided information over the cloud hubs. Every one of the hubs stores just a solitary section of a specific information record that guarantees that even if there should be an occurrence of an effective assault, no important data is uncovered to the aggressor. Besides, the hubs putting away the pieces are isolated with certain separation by methods for diagram T-shading to preclude an aggressor of speculating the areas of the sections. Idea of T-shading chart for part position just as calculation for section arrangement has been alluded from this paper. Document is divided put away on different hubs. [6]

Seventh paper shows the protocol is based on an ECC-based double trapdoor chameleon hashing. Through informal security analysis, given paper shows that how protocol is secure against key exposure problem and provides integrity and authenticity assurances [7].

Eighth paper present, this paper presents Identity establishment and capability based access control (IECAC) convention utilizing ECC (Elliptical Curve Cryptography) for IoT alongside convention assessment, which ensure against the Man in middle, replay and denial of service attacks. The convention assessment by utilizing security convention confirmation apparatus demonstrates that IECAC is secure against mentioned attacks. [13].

Paper ninth presents two constructions of Fuzzy IBE schemes. Our constructions can be as an Identity-Based Encryption of a message under several attributes that compose a (fuzzy) identity. Our IBE schemes are both error-tolerant and secure against collusion attacks. Additionally, our basic construction does not use random oracles. System proves the security of our schemes under the Selective-ID security model [14].

Tenth paper presents a key which is common and shared among the different users. Here in proposed method the presenters use ECC key cryptography for encrypt and decrypt data. Then utilization of self-affirmed open key in the proposed convention defeats the declaration the executives issue so as to verify general society key, just as expels the private key escrow issue. [15].

V. OPEN ISSUES

1. In the cloud/server, for achieving access control and keeping data confidential, the data owners could adopt attribute-based encryption to encrypt the stored data.

Users with restricted computing power do square measure but a lot of possible to delegate the mask of the decoding task to the cloud servers to cut back the computing value. As a result, attribute-based encryption with delegation emerges.

2. Still, there are caveats and questions remaining in the previous relevant works. For instance, during the delegation, the cloud/servers could tamper or replace the delegated cipher text and respond a forged computing result with malicious intent.

3. They may also cheat the eligible users by responding them that they are ineligible for the purpose of cost saving. Furthermore, during the encryption, the access policies may not be flexible enough as well.

VI. GAP ANALYSIS

In below Table 2 shows that the proposed system key is uses the key having small size that generated from ECC. The algorithm used is Diffie-Hellman key exchange for key exchange. The Diffie-Hellman key exchange method allows two parties and that have no idea of each other to establish a shared secret key on an insecure channel. The system allow user to authenticated users only. While login time authentication must be done. Access policy is performed by circuit-cipher text .That helps to access only authenticated accessible files. File is fragmented and stored on multiple nodes. Man-in -middle at- tack is removed because this system uses ECC-Diffie-Hellman key exchange for key exchange. Replay attack is handled by fragmentation and replication in proposed system.

Table 1: Security Parameter's Handled By Proposed System.

Number	Parameter	Proposed system	Existing system of Security
1	Use of ECC key size[7]	Yes	No
2	Use of key ex-change[13]	Yes	No
3	Access control to access file[7]	Yes	No
4	Integrity checking[5]	Yes	Yes
5	Authentication	Yes	Yes
6	Access policy[12]	Yes	No
7	Distributed nature[15]	Yes	No
8	Resist to Man in middle attack[14]	Yes	No
9	Resist to Replay attack[14]	Yes	No

VII. PROPOSED WORK

In given Figure 1 shows the architectural flow of proposed system. Here user request browser and browser accept its request, then through browser file is get uploaded while uploading of file it will bet encrypted through defined policy attribute. This files integrity and user's authentication is checked via server then file is uploaded on cloud/server. When user wants the uploaded file again then cloud/server check the integrity of user. After user gets verified then file is accessible to end user but here file is given in encrypted format. To decrypt this file user needs to get intended key from authenticated user after getting key user decrypt the file by using sender key plus self key. Then original content of file will be downloaded by the user.

In proposed system owner will get data that file will allocate to users according to users position location and experience. Owner distributor will assign the file to user by generating access policies by considering user attributes like date and time stamp after entering encryption key then file will be divided into fragments and store the fragment and its replica on server/cloud. When Authenticated user login then he will get the file with which his policy attribute matches. Then he can request for the file key and download the file after entering secrete key. Third party auditor will check data integrity of stored fragment that means placed fragment content is changed or not if changed then integrity checker will inform to owner about that file. Then integrity checker will replace tempered fragment with original fragment and provide security to the file.

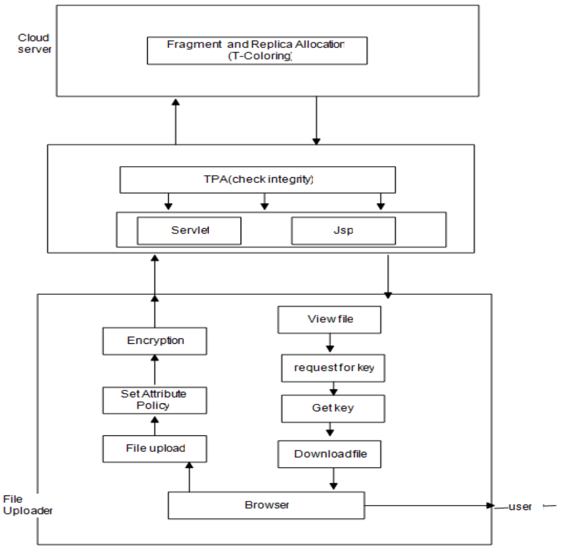


Figure 1: System Architecture

A. Mathematical model:

i). Notations

1. NN_ik -Nearest neighbor of S_i holding O_k
2. O_k - kth fragment of file
3. O_k -Size of O_k
4. W_{ik}- Aggregate write cost of W_{ik}
5. R_{ik}- Aggregate read cost of R_{ik}
6. S_i-Size of S_i
7. r^i -Number of reads for O_k from S_i
8. w^i -Number of writes for O_k from S_i

ii). Equation

Fragment=Size of file/No. of fragments --- (1)

The total read time of O_k by S_i from NN_ik is denoted by R_{ik} and is given by:

$R^i \Rightarrow r^i$ (i, NN_ik) ---- (2)

The total read time of O_k by S_i from NN_ik is denoted by R_{ik} and is given by:

$R^i \Rightarrow r^i$ (i, NN_ik) ---- (3)

iii). Algorithm

1. **Elliptic curve cryptography (ECC) -** ECC is relies on sets of numbers that are related to the mathematical objects called elliptic curves. There are rules for adding and computing multiples of those numbers, even as these are just as there are for numbers modulo p.

ECC includes a variant of many cryptographic schemes that were initially designed for modular numbers such as ElGamal encryption and Digital Signature Algorithm.

Here ECC is used for the purpose of key generation. So we have to create public and private keys to exchange it with another user. So keys are generated as flows:

- Select a number**'d'** within the range of n. where **'d'** is private key.
- Now generate the public key **(Y)**
- y1 ⇒d*p and y2=q1 mod p , where p is point on curve.
- Now Y =y1+y2

2. ECC-DH Algorithm - ECDH is a variation of the Diffie-Hellman calculation for elliptic curve. It is really a key-agreement convention, in excess of an encryption calculation. In proposed system it is used for exchanging of generated keys.

Step 1: Generate passing ECDH key pair
Step 2: Exchange the public keys.
Step 3: Perform key agreement.
Step 4: Take out the shared secret and derive keys for further processing.

3. EL-Gamal Algorithm - The ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffe-Hellman key exchange. ElGamal depends on the one way function the first public key system proposed by Diffe and Hellman requires association of both sides to compute a common private key. Those problems if the cryptosystem should be applied to communication system wherever either side aren't able to move in reasonable time due to deferrals in transmission or inaccessibility of the receiving party. It means that the proposed scheme defined by Diffe and Hellman is not a general purpose encryption algorithm as it can only provide secure secret key exchange. Thus it presents a challenge for the cryptologists to design and provide a general purpose encryption algorithm that satisfies the public key encryption standards.

Encryption: Given a message m such that "$0 \leq m < p$", any user "B" can encrypt "m" as follows: "Y" is public key and "d" is private key

Pick the integer "$k \in \{1...p-2\}$" uniformly at random.

Two cipher texts will be generated let it be **C1** and **C2.**

$$\mathbf{C1 = Y^k \bmod p} \quad (2)$$

$$\mathbf{C2 = m \times Y^k \ (\bmod p)} \quad (3)$$

C1 and C2 will be sending.

Decryption: Now for get back the message 'm' that was send to us,

$$\mathbf{m = [C2 \times (C1^{d-1})] \bmod p}$$

M is the original message that is send.

VIII. SECURITY ANALYSIS

A. DOS Attack for Login - The attack is avoided in proposed system at the time login failed of person when three time fail to enter the password that extend visitors of system at that time machine will send mail to owner of account that your account is trying to access by another unauthorized person.

B. Replay attack - In proposed machine, if fragment of file is modified then file might be checked by higher auditor and update that facts with duplicate of created unique fragment. So tempering of information is identified in addition to save you from going on attack.

IX. RESULT AND DISCUSSION

Table 2: demonstrated the execution time required for encryption and decryption of proposed algorithm

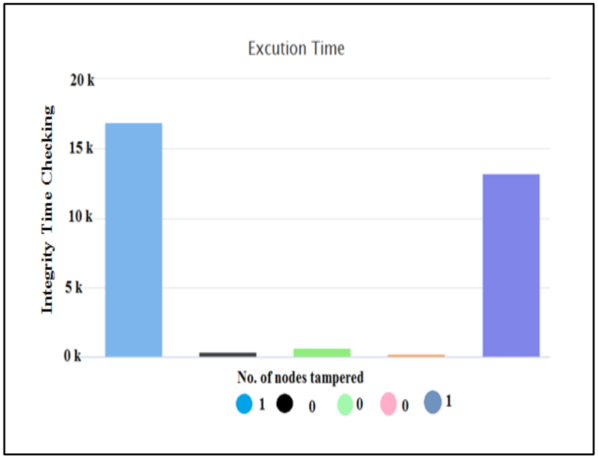
Sr.	Scheme	Time in Mili Sec
1	Encryption	4.340
2	Decryption	1.156

In above graph, it shows the time require for encryption of inserted file by user. It gives time in mili second. it also include time of node creation of file after file is get encrypted.

File is always generate in fragments format and it is generated by size of file divided by number of fragments have to be generated of file.

Here less time required because In proposed system key sharing mechanism is used ECC for key generation and ELGAMAL for encryption and decryption and to exchange the key ECDH mechanism are used. ECC is used for ease of key management. For the same level of security, very short keys are required, thus it takes less time than other method.

Graph 1 - Integrity checking and recovery time of files and recovery in mili seconds



Above graph shows on X-axis No. of fragment tempered and On Y-axis Time to check integrity of each file (ms).The graph is get by TPA After checking each file integrity. After checking integrity tempered nodes fragment is replaced by replica of that fragment here attack is detected and prevented so user can get original file that is uploaded by owner.

X. CONCLUSIONS AND FUTURE SCOPE

This paper proposed a novel end-to-end data integrity protocol to protect data aggregation against message tampering. Protocol is based on an ECC-based. Through informal security analysis, it show that how proposed protocol is secure for provides integrity and authenticity assurances improved ECC EIGamal algorithm can product meets conditions key in a short time. And in the same security level achieve by, ECC key pair which is much shorter than the other cryptosystems. So proposed algorithm can use small resource and little time delay to achieve high security.

In future system will be applicable in it industry for particular department. Data will store on multi -cloud storage. So it is intend to implement a prototype of the proposed protocol so that we can evaluate its practicability in a real- world setting.

XI. REFERENCES

[1]. Yang, Yanjiang, Haibing Lu, and Jian Weng. "Multi- user private keyword search for cloud computing." Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on. IEEE, 2011

[2]. Cheng, Hongbing, et al. "Identity based encryption and biometric authentication scheme for secure data access in cloud computing." Chinese Journal of Electronics 21.2 (2012): 254-259.

[3]. Han, Jinguang, Willy Susilo, and Yi Mu. "Identity-based data storage in cloud computing." Future Generation Computer Systems 29.3 (2013): 673-681.

[4]. Li, Jin, et al. "1Identity-based Encryption with Outsourced Revocation in Cloud Computing." (2015).

[5]. Hur, Junbeom, and Dong Kun Noh. "Attribute-based access control with efficient revocation in data outsourcing systems." IEEE Transactions on Parallel and Distributed Systems 22.7 (2011): 1214-1221.

[6]. Ali, Mazhar, et al. "Drops: Division and replication of data in cloud for optimal performance and security." IEEE Transactions on Cloud computing 6.2 (2018): 303-315.

[7]. Chameleon: A Blind Double Trapdoor Hash Function for Securing AMI Data Aggregation Heng Chuan Tan, Kelvin Lim, Sye Loong Keoh, Zhaohui Tang*, David Leong, Chin Sean Sum. 2018 IEEE.

[8]. Tan, Heng Chuan, et al. "Chameleon: A blind double trapdoor hash function for securing AMI data aggregation." 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE, 2018.

[9]. Somkunwar, Rachna, et al. "SECURE DYNAMIC FRAGMENT AND REPLICA ALLOCATION OF DATA WITH OPTIMAL PERFORMANCE AND SECURITY IN CLOUD."

[10]. Quanlu Zhang, Shenglong Li, Zhenhua Li, Yuanjian Xing, Zhi Yang, and Yafei DaiCHARM: A Cost-efficient Multi-cloud Data Hosting Scheme with High Availability .2015

[11]. Kaufman, Lori M. "Data security in the world of cloud computing." IEEE Security & Privacy 7.4 (2009).

[12]. Boru, Dejene, et al. "Energy-efficient data replication in cloud computing datacenters." Cluster computing 18.1 (2015): 385-402.

[13]. Mahalle Parikshit, et al. "Identity establishment and capability based access control (IECAC) scheme for Internet of Things." WPMC. 2012.

[14]. Sahai, Amit, and Brent Waters. "Fuzzy identity-based encryption." Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2005.

[15]. Gupta, Shalini, Abhimanyu Kumar, and Nitin Kumar. "Design of ECC based authenticated group key agreement protocol using self-certified public keys." 2018 4th International Conference on Recent Advances in Information Technology (RAIT). IEEE, 2018.

[16]. Lai, Junzuo, Robert H. Deng, and Yingjiu Li. "Expressive CP-ABE with partially hidden access structures." Proceedings of the 7th ACM symposium on information, computer and communications security. ACM, 2012.