Indian Journal of Science and Technology, Vol 10(42), DOI: 10.17485/ijst/2017/v10i42/120341, November 2017
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Privacy Preserving M2M-Iot Environment

P. Devi[1]* and D. Venkata Subramanian[2]

[1]Department of Computer Science and Engineering, Hindustan Institute of Technology and Science, Chennai – 603103, Tamil Nadu, India; devisars@gmail.com
[2]School of Computer Sciences, Hindustan Institute of Technology & Science, Chennai - 603103, Tamil Nadu, India; deancs@hindustanuniv.ac.in

Abstract

Objectives: In IOT environment, an electric grid has security and privacy issues. Security technique in a 24*7-enterprise environment with evaluation of using real time based encryption for security, privacy to achieve IoT security. **Methods/ Statistical Analysis:** Cryptography technique such as Homomorphism Encryption secures the data preventing from unauthorized software or firmware to access data in a known format. Differential Privacy is used to maintain privacy to protect personal information. **Findings:** Securing data readings in real-time is interesting and extremely challenging as all the data and privacy information to be prevented from hacking. **Application/Improvements:** The security measures described can be applied to smart grid, smart meter IOT environment, Machine-to-Machine Environment.

Keywords: Gortis Enhanced Homomorphic Encryption, Industrial Control System, Internet of Things, Machine-Machine

1. Introduction

Machine to Machine (M2M)[1] IOT is a global telecom network of smart, interconnected devices and applications which collaborate heterogeneous data and enabled by various Gateway[1]. Smart grid emphasize digital, bi-directional communication over distributed power generation which involves automatic monitoring and automatic recovery of process or data related to infrastructure of power, water and gas, monitoring resources, calculating demand response. Security plays a major role in distributed environment by low usage of memory, availability of CPU and battery powered devices for effective and efficient utilization of resources. There are 'n' numbers of issues on privacy and security constraints, since every day the adversary keep on break the security by cryptanalysis. When the data is too big, security plays a challenging role for end user to keep the data as secured one. The principle of M2M communications is in recognizable form of Supervisory Control and Data Acquisition (SCADA) systems[2] SCADA is used to monitor the resources. It is expected that millions of IoT devices increase year by year and henceforth the increase in sensors also rapid.

The primary benefits of M2M connecting devices are the ability to maintain devices in the network and to preserve the privacy of connected devices and their owners' details has become an integral part in the communication where the data from the device is transmitted over to a network for specific applications like rectification of faults, etc. Also, the sensitive information about the devices that the details communicate must be preserved to avoid any kind of data breach. Preserving privacy is required for legal/commercial reasons. Cryptography prevents unauthorized users, software or firmware in accessing private data Security in Heterogeneous network model is achieved by introducing Gortis Enhanced Homomorphism Cryptography (GEHC) algorithm and anonymity and Zero-knowledge privacy, etc. In order to maintain privacy and data utility factors intact, sensitive information about the devices that the details communi-

*Author for correspondence

cate must be preserved to avoid any kind of data breach[3] and a new generation privacy techniques is used as part of two-level securities such as Homomorphic Encryption[4–6] has been applied to the device data to encrypt before it is stored in the server. One of the major advantages in using this method is that it allows querying the encrypted data stored to get aggregated results in real time applications. Sometimes, the aggregated result value is small enough in such a way that evens the adversaries. In ICS of 24*7 environments, users of light or heavy bandwidth, use IoT devices for different applications. Data center operations when transferring the data through cloud –based, exhibit security attacks.

In general, the power saving devices should be available on a 24*7 environment to prevent the Industry being put in delicate situations. The attending of fault for each device will take some time and it needs a human intervention to get it back to working condition. Preserving the privacy of some of the connected devices and their owners' details has become an integral part in the communication where the data from the devices is transmitted over to a network for specific applications like rectification of faults, etc. Also, consideringthese prevalent problems, the approach focuses on the proactive way of handling the faults in connected M2M devices thereby preserving the device and its owner's data through secured two-level privacy architecture. Various privacy-preserving methods are available like GEHC cryptography, anonymity and Zero-knowledge privacy[7], etc. In order to maintain privacy and data utility factors intact, we have used new genre of privacy techniques. As part of two-level securities, Homomorphism Encryption[8] has been applied to the device data to encrypt before it is stored in the server. One of the major advantages in using this method is that it allows querying the encrypted data stored to get aggregated results in real time applications. Sometimes, the aggregated result value is small enough in such a way that even the adversaries can interpret the original individual's information using the publicly available auxiliary data. Then the device data from the server is to be shared with the third party, to preserve the privacy, we have applied Differential Privacy[9] on the aggregated result data before it release to third parties for suitable recommendations. These two-level privacy architectures are explained briefly in Section 3. Focuses on new system overview with privacy preserving layers that can easily applied on M2M-IoT background applications as shown in Figure 1. Describe a use case which explains the necessity of proposed architecture for M2M-based applications in future to handle the similar critical situations. M2M server checks the smart meter readings of every department in ICS at regular intervals of time. Whenever the fault is detected, it is immediately report to the end application. The application then authenticates the data, raises a request to external service centers. When the details are shared to network for requesting third party to repair the devices, there is a possibility of data breach can happen[10–12]. To avoid and preserve the individual's privacy, we have introduced two-level privacy architecture where each and every device data is encrypted and stored in the server. Even querying of data is allowed on the server to get aggregated value for other business applications, which also can be secured by generating noise-aggregated output to ensure privacy of individuals. From the proposed setup, it is tough task for anybody to break and get any details from the network.

In this paper, a secured architecture is extended for securing and for privacy preserving the data by means of having Homomorphic Encryption (GEHC method) and Differential Privacy. The Homomorphic encryption secretly computes the cryptanalysis on dynamic data .This work is based on designing a smart meter based Industrial Automation and Control System environment, which meets the above prerequisites, and a data simulation model is experimented by using LABVIEW.

The work is in order such as:

Section 1. Proposed idea based on Industrial Automation and Control System based on smart grid security.
Section 2. Proposed encryption technique and privacy preserving.
Section 3. Overall Technologies used in smart meter, smart grid.
Section 4. Use cases of proposed architecture.
Section 5. Overview of Technologies Used in Smart Meter, Smart Grid.
Section 6. Conclusion.
Section 7. References used in this survey.

2. M2M Architecture

M2M architecture involves various components that are responsible for storing, analyzing and representing the available information of connected devices. Some of the

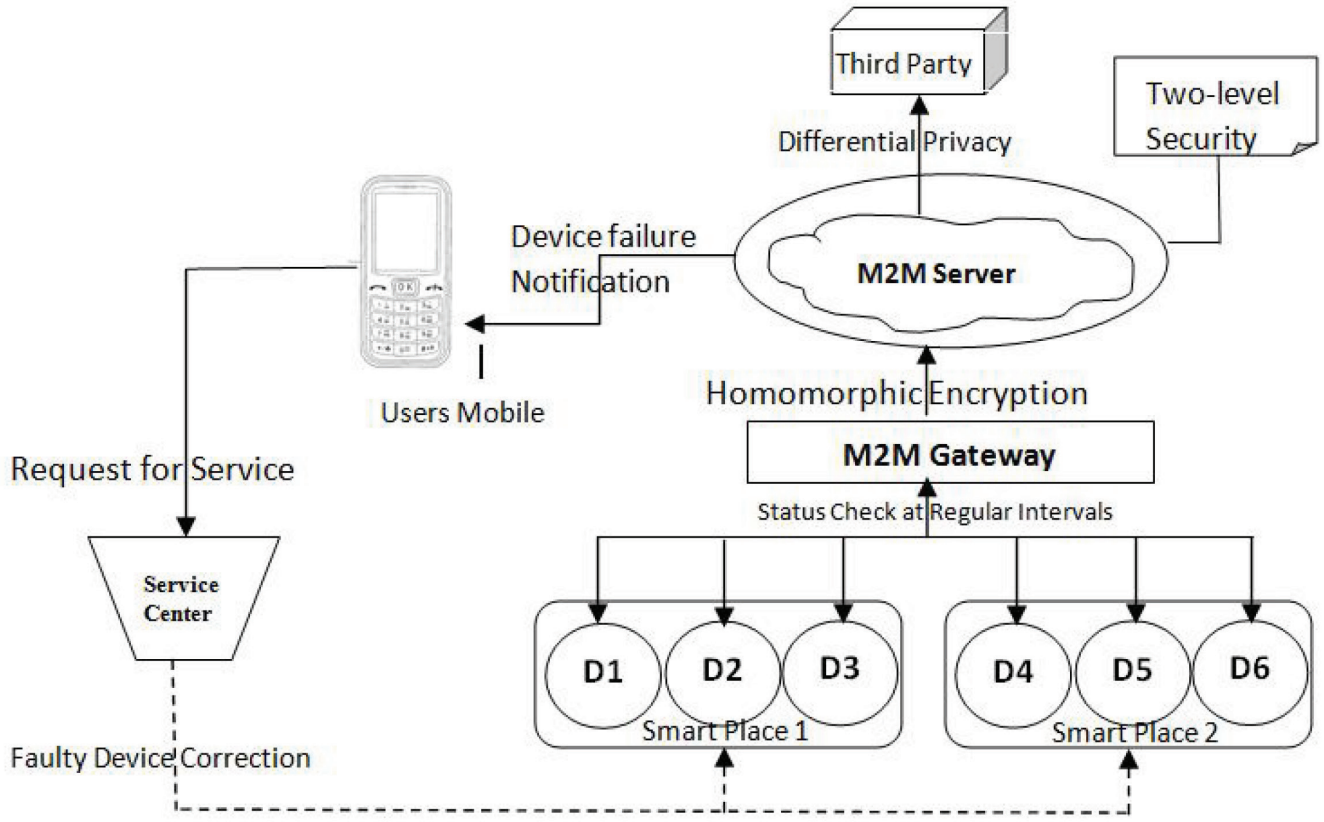

Figure 1. Architecture of M2M ICS Smart Place.

major components involve devices, gateway, server and application. A brief description of the components and how these are used with respect to our approach will be described here.

2.1 Device

These are the components that basically transmit/receive the data based on their events. These are connected through M2M network. Each and every device should have been connected with many proximity sensors that are installed on them, which are responsible for collecting all the events happening on the devices and transmit them over to the closely connected network.

2.2 Gateway

These components receive and analyze the data received from the sensors. They are capable of collecting the data from the sensors installed on the devices and pass them to the servers for further processing. In general, the M2M gateway is the next level in hierarchy that connects the devices within network.

2.3 Server

The server is capable of connecting the gateway with the end user's applications. The server is responsible for the device managements (updates and device configurations) and the data management (collection, storage, analysis of the data obtained from devices). The server communicates the events received from the devices to the applications (applications probably running in end user's handsets) and with the third party tools. The encrypted form of data is stored in the server and a suitable privacy method is applied on the data before communicating with the third party (by communicating with third party, we mean the business enterprises, NGO's, which would use the data for performing device analytics). The full system architecture of the M2M system, which includes an example of smart home environments, is described in Figure 1.

Figure 1, the symbols D1, D2, D3, D4, D5 and D6 are the departments connected in the ICS Smart Place. In the next level, they are connected to the M2M server through M2M gateway. M2M gateways are the multi-service gateways that connect sensors, actuators and devices to the business enterprise. It includes a wide array of secure connectivity solutions through cellular, RF, GSM, Wi-Fi, Bluetooth and ZigBee, Satellite networks[13]. The M2M server is performing like public cloud and it is responsible for communicating the device status with the application running in the user's handset. The M2M server can be installed in any office or company data center and within a few minutes, the devices within the customer's network will be connected and manageable. The two-level privacy is applied on the device data stored in the server in encrypted fashion. The details of two-level security architecture are provided in Section 3. Now, the privacy of individuals should be preserved in a secured way[14]. When a failure in a department say D2 in smart Place is observed by the server, the server communicates the encrypted device status to the application that is running in the end user's handset. The application receives the data and decrypts the data (as described in the next section) with the shared private key and forwards this status to the external service centers if a failure status is observed. The application is a sort of alarm that gets notifications from server. These applications are capable of understanding the messages and schema received from the server and capable of decryption of the messages based on the true identity hand shaken earlier with the server. These could be mapped with value-added utility services that are provided during the time of activation.

To reduce the downtime, service centers/external agencies receive the device name/id, the smart home and the failure reason in case of connected device failure. After the failure correction by the service center technicians, the server again is notified by the working status of the device. This working status is again communicated to the application in the user's handset. This approach reduces manual dependency thereby driving efficiency and profitability and helps in achieving the business profits more efficiently. This approach also helps in the business analytics of the third party tools in aggregated query search from the server for which the differential privacy is used will be explained in next section.

3. Two-level Privacy Architecture

In this paper, organizing two-level privacy architecture is done to preserve the privacy of an individuals and their usage of various devices for various business transactions. The architecture implemented through Gortis Enhanced Homomorphic Cryptography[15] which secures the identity of the devices when sent to user's application and Differential Privacy which secures the aggregated information (whenever it looks predictable) when shared with any third parties. The brief description of the privacy methods used in our approach is described here.

3.1 Gortis Enhanced Homomorphic Cryptography

Homomorphic Encryption (GEHC) schemes support operations on encrypted data which can be applied to real time applications. The gateway analyzes the data from the sensors and the M2M server is responsible for data management. When a third-party queries from the M2M servers, if it is not secure, hackers can breach the data. Hence data stored in the server is encrypted using Gortis Enhanced Homomorphic Encryption algorithm which prevents Indistinguishable Chosen Cipher text Attack (IND-CCA). Any difference in pattern matching, the gateway forward the request to M2M server which, in turn, sends the encrypted details to the user mobile which has a private key for decryption.The System will compute encryption on the data to be secured by following a particular algorithm and the data will be decrypted as and when needed. The decrypted data should match to the original value or data. The decrypted outcome has to be equivalent to the proposed evaluated value if executed on the actual data. For this rationale, the encryption scheme has to recommend a meticulous structure. This research aims to provide a scheme for better performance, security, to minimize processing of CPU cycles, minimizing the energy consumption and memory.

Two large prime numbers 'p' and 'q' are considered with a random number 'r' to create non predictable system. Considering set of apparent text figures Zp and plain text operations (+,-,*,/) such as add/subtract/multiply and diverse multiplication modulo m, where m = pq. Let Zc be cipher text data. Defining the encryption key k = (p,q,m,r) and Encrypt (X) = (X+r*pq) (mod m). Decryption can be organized with secret key k = (p), X = Dk (Y) = C mod p. If p is known, real data can be revealed. However, it is dif-

ficult to break. A computer can feature that number quite fast. There are some tricks, which can break the algorithm by attempting most of probable combinations. Anyone can locate two huge prime numbers p and q that have may be 200 or 400 digits each. Q – The secret key and by multiplying them collectively to build a numeral m = pq, which again is a secret key to encrypt the information. M can be moderately obtained by multiplying p and q. However if anyone be familiar with m, it is fundamentally unfeasible to find p and q. To resolve them, we should factor m and also 'r' which appears to be extremely complicated, as this value will be randomly generated. In general m should be considered at least 1024, if not 2048.

GEHC Formula

The respective formula used for encryption of the data stored in M2M server is given here:

$$\text{Encrypt } (X,m,p,q,r)$$

$Y = (X + r^{*}pq) \pmod m$ Encrypt (x,m,p,r) represents the encryption function of device message m. The cipher text Y is obtained as a result of encryption of message m. The formula for the decryption function Dec (c) is Decrypt (Y,p).

$$X = Y \bmod p$$

3.2 Differential Privacy

Differential Privacy filters the exact queries from stored databases which is static thereby it maximize the accuracy of retrieved data, henceforth it minimize the retrieval of results from complex queries which disturbs the data's in statistical database with sensitive noise[16]. When the third party queries from the M2M server through IoT, though it is encrypted with Homomorphism encryption algorithm[17], it provides the aggregate information as a result. When the aggregate value is too small, it can be linked with other statistical database and privacy may be breached. So as a second level of privacy, differential privacy is applied to the resultant aggregate value before the server replied to the third party and its corresponding formula

$$\Pr[(K(D) \in S] \leq \exp(\epsilon c) \times \Pr[(K(D') \in S]$$

Where $S \subseteq$ Range and privacy factor Ɛ chosen for noise addition. The D and D' characterize the dataset whose query results differ by 1. The addition of noise factor to the distribution is given by,

$$f = \max \| f(D) - f(D') \| 1 \; D,D'$$

4. Usecase of the Proposed Architecture

Figure 1 describes two smart places and six devices. From the figure, it can be evident that how the data is transferred securely and the device's fault (established in an ICS environment) is observed and corrected without human intervention. On a device failure, the device id is sent to the centralized application. Once, the device id is received in encrypted form by the application, the application uses the already registered key to decrypt and find the device details. By applying the GEHC, the device id is obtained and is further reported to external service centers. This method ensures that, the privacy of device with its owner details and no manual intervention in reporting the failure of devices.

Differential privacy basically comes into place when the aggregated device details are queried from server through external agencies. Basically every query is added with a noise factor and privacy is preserved to protect the user's identity and also the device identity. For example, there may be a device which is either too costly or more specific to detect some disease such that it is not used commonly. When the external agencies queries to the server to get the aggregated details about the devices, though the details are encrypted, but the aggregate counts would not be encrypted and it would appear as a very small value such as 1 or 2. In that case, privacy can be breached by using other auxiliary database or statistical database to understand the device and its owner details. To avoid this kind of privacy breach, the aggregated value is added with a noise factor by applying differential privacy method.

5. Technologies

The security plays a vital role in IoT and henceforth many researchers involved in developing a secured architecture and providing privacy to the consumers. Securing

data in static environment or in dynamic Aggregation of data deal with Homomorphic encryption which is an additive Homomorphic Encryption technique (Paillier Cryptosystem) and Zero Knowledge Proof[18,19]. Papers describe the architecture of physical activity monitoring in smart meter, smart grid remote monitoring resp. and gives information about in which circumstances privacy protection is needed .Protocol such as LwIP protocol stack and interface such as MODBUS is used in IoT smart grid environment for effective use of secured data transfer. Many Researchers use communication by ZigBee network[20,21] of IEEE 802.15.4 standard for Smart Grid Applications. By comparing the above, we use Wi-Fi-based WSN[22] which use 802.11 standard and Distributed Energy–efficient Clustering Algorithm (DECC) clustering algorithm is used for AMR data, Homomorphic Encryption of GEHC technique and Zero Knowledge proof and Differential Privacy[23] in our data to maintain security and privacy of data.

6. Conclusion

In M2M, communication over distributed environment, there are lacking of many security measures therefore many security and privacy attacks increase day–by-day which should be identified and rectified since many new business and industries such as education, manufacturing, medical, transportation, governance, industrial, mining etc. are dependent on IoT for their work and progress. The proposed approach basically extends the M2M architecture to minimize the human intervention and preserving the devices with minimum downtime in a two-level secured architecture. The proposed architecture not only preserves the privacy of the device based on Web Semantics such as SPARKQL data storage and its owner's details but also will improve the end user experiences and generate a better satisfaction. The observation to be noted in the literature is: 1. No standardization worldwide. 2. Differ in technologies used in utilities. 3. No standard protocol and 4. Different encryption techniques used previously to secure data. More case studies will be conducted using the proposed architecture to find the feasibility and create the required data structure using ontologies for providing better security mechanisms in smart grid environment.

7. References

1. Erkin Z. Private data aggregation with groups for smart grids in a dynamic setting using CRT. Workshop on Information Forensics and Security; 2015. p. 1–6. Crossref.
2. Qu H, Shang P, Lin X, Sun L. Cryptanalysis of a privacy-preserving smart metering scheme using linkable anonymous credential. IACR; 2015. p. 1–11. PMCid: PMC5466250.
3. Qi J, Yang P. A survey of physical activity monitoring assessment using Internet of Things. 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing; 2015. p. 2353–8. Crossref.
4. Klenze T. Privacy Strategies in Smart Metering. NET; 2014. p. 1–16.
5. Thoma C, Cui T, Franchetti F. Secure multiparty computation based privacy preserving smart metering system. North American Power Symposium (NAPS); 2012. p. 1–6. Crossref.
6. Backes M, Meiser S. Differentially private smart metering with battery recharging. Data Privacy Management and Autonomous Spontaneous Security; 2014. p. 194–212. Crossref.
7. Mohanty S, Panda BN, Paatnik BS. Implementation of Web of Things based smart grid to remotely monitor and control renewable energy resources. IEEE; 2014. p. 1–5.
8. Bedogni L, Trotta A, Felice MD, Bononi L. Machine-to–Machine communication over TV white spaces for smart metering applications. International Conference on Computer Communication and Networks (ICCCN); 2013. p. 1–7. Crossref.
9. Zeadally S, Pathan A, Alcaraz C, Badra M. Towards privacy protection in smart grid. Wireless Personal Communications. 2013; 73(1):23–50. Crossref.
10. Usman A, Shami SH. Evolution of communication technologies for smart grid applications. Renewable and Sustainable Energy Reviews. 2013; 19:191–9. Crossref.
11. Kursawe K, Danezis G, Kohlweiss M. Privacy friendly aggregation for the Smart Grid. Citeseer; 2011. p. 1–17. Crossref.
12. Li F, Luo B, Liu P. Secure information aggregation for smart grids using homomorphic encryption. First IEEE Conference on Smart Grid Communication; 2010. p. 327–32. Crossref.
13. Qu H, Shang P, Lin X, Sun L. Cryptanalysis of a Privacy-Preserving Smart Metering Scheme Using Linkable Anonymous Credential. 2015. p. 1–14.

14. Weber HR. Internet of Things - New security and privacy challenges. Elsevier. 2010; 26:23–30.
15. Gentry C. Fully homomorphic encryption using ideal lattices. Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing (STOC); 2009. p. 169–78. Crossref.
16. DWork C, Roth A. The algorithmic foundations of differential privacy: Automata, language and programming. Lecture Notes in Computer Science. 2014; 9(3-4):211–407.
17. Pinkas B. Cryptographic techniques for privacy-preserving data mining. ACM SIGKDD Explorations Newsletter. 2002; 4(2):12–9. Crossref.
18. Zhang Y, Yu R, Xie S, Yao W, Xiao Y. Home M2M Networks: Architectures, standards, and QoS Improvement. IEEE Communication Magazine. 2011; 49(4):44–52. Crossref.
19. Gehrke J, Lui E, Pass R. Towards privacy for social networks: A zero-knowledge based definition of privacy. Theory of Cryptography – 8th Theory of Cryptography Conference TCC; 2011. p. 1–32. Crossref.
20. Spano E, Niccolini L, Pascoli SD, Iannaccone G. Last-meter smart grid embedded in an Internet of Things platform. IEEE Transactions on Smart Grid. 2015; 6(1):468–76. Crossref.
21. Li L, Xiaoguang H, Jian H, Ketai H. Design of new architecture of AMR system in smart grid. IEEE Conference on Industrial Electronics and Applications (ICIEA); 2011. p. 2025–9. PMid: 21377880.
22. Cha I, Shah Y, Schmidt AU, Leicher A, Meyerstein MV. Trust in M2M Communications. IEEE Vehicular Technology Magazine. 2009; 4(3):6–75. Crossref.
23. Fan L, Xioug X. Real-time aggregate monitoring with differential privacy. Proceeding of the 21st ACM International Conference; 2012. p. 2169–73. Crossref.