International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

A Secure Outsourced Aggregation over Internet of Things Based on Location

I. Bhuvana Priya[1], A. V. Naga Mani[2]
[1]Student, V. S. Lakshmi Women's Degree & P.G. College, Kakinada
[2]Senior lecturer, V. S. Lakshmi Women's Degree & P.G. College, Kakinada

Abstract: Secure outsourced aggregation in the Internet of Things (IoT) can solve the problem that sensing devices are limited in energy and bandwidth by outsourcing data aggregation task to a third-party service provider. Location-based secure outsourced aggregation (LBOA), aggregating data whose location satisfies user's location strategy, is very important in some location-critical scenarios (e.g., smart homes, intelligent transportation, and smart city). Recent work studied secure data aggregation to reduce transmission overhead and network bandwidth by optimizing topology of networks or adopting the cryptographic approach. However, as far as we know, scarcely any work considers the location information of the data source and the privacy protection of the data at the same time in the studies of secure outsourced aggregation. In this paper, we first propose an LBOA scheme LBOA*Max*, which can return the maximum value of sensory data whose location satisfies location strategy by applying one-way chain, order-preserving encryption, and some other cryptographic operation. Then, we proposed scheme LBOA*Top*□*k* and scheme LBOA*Sum*, which can return the largest *k* values of data and the summation value of data based on location, respectively. The security analysis results show that our schemes can satisfy the defined requirements and the experiment results show that our schemes are feasible and efficient for each entity in practice

.

I. INTRODUCTION

IoT i.e. Internet of Things is said to be the self-configured network as it interconnects the particular objects or the things that are present in the network. An object means the item which is present in the real world and capable enough to provide the communication chain [1]. The communication helps in transmission of data in the given paths by taking the help of network. Hence, it is meant to say that the main aim of IoT model is to connect the things in real world. In a simple words, IoT can be defined as the Network of interconnected objects or things. All of the IoT object can be transmittable either physically or virtually and each of these objects are associated with ID.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

IoT has revolutionized the normal lifestyle by providing the convenience for various application and through the research, it has been found out that by the end of 2020, the IoT would hold the market of nearly 1.7 trillion dollar and 50 billion connected things [2]. IoT has several application such as in healthcare [3]–[5] agriculture [6]–[8], defense [9] and others. Wireless IoT is capable of interconnecting the embedded devices and these type of devices are mostly battery oriented, hence, they has limited function, such as, computation, processing and transmission. This phenomena has led the IoT to be used in almost everyplace, some of them includes Ehealthcare, Smart cities [10] and Smart homes [11]. IoT possesses variety of characteristics in various areas, however, everywhere they share similar wireless IoT essence. In general, any application can be named as the inter-connected network, which uses the IoT devices. Things that are interconnected contains variety of data and these data can be anything from being the behavior of user to the private information. In case of such dynamic and distributed environment the IoT services can be a major threat where the data might be compromised and which might affect the end user. This damage can occur in various ways such as data modification, data leaking, data tapping and data destroying.

IoT possesses variety of characteristics in various areas, however, everywhere they share similar wireless IoT essence. In general, any application can be named as the interconnected network that uses the IoT devices. Moreover, IoT devices interconnects variety of multimodal data and these data can be anything from being the behavior of user to the private information. In case of such dynamic and distributed environment the IoT services can be a major threat where the data might be compromised and which might affect the end user. This damage can occur in various ways such as data modification, data leaking, data tapping and data destroying. The Fig. 1, shows the data aggregation technique model. It has several parts such as devices, clusters, aggregator and base station. Here, the device sense the data and sends it to the aggregator where the data aggregation takes place. Later, the aggregated data is sent to base station and through base station, it is sent to cloud storage from there end user can access the data.

1.1 Architectural view of IoT

The Fig.1 shows the complete IoT model, it has four distinctive component such as Sensors, Gateway, Cloud Server and End User [12]. Sensors: Sensors are the small devices, which is used for .sensing the environment sensor can be of multiple type such as temperature, pressure motion detection, proximity and others. Moreover, several sensors can be combined to work just more than sensors, smartphone is one of the best example, and it has several sensors.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

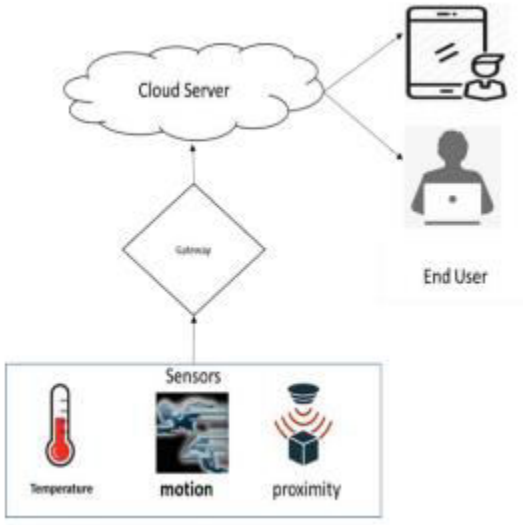

Figure 1 IoT architecture

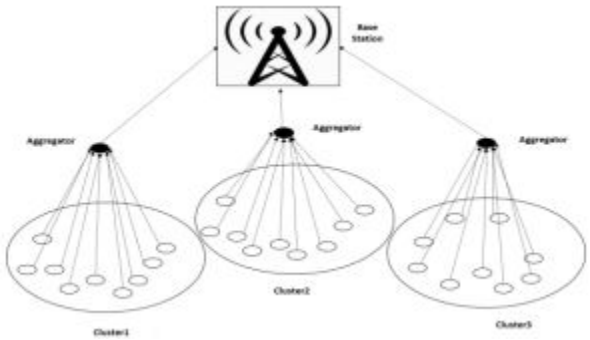

Figure 2 Data Aggregation Model

A Gateway: Once the data is sensed it needs to be stored and it is stored in the cloud, however to, send the data into cloud medium is required and this can be done through the gateway.

B Cloud server: This is one of the important part as the data sensed might be huge, hence cloud platform is used for storing the data.

C End User: Intuitive apps helps the end user for monitor- ing and controlling the devices.

II. LITERATURE SURVEY

As Data Aggregation in IoT has one of the major role to play in processing the data, hence, a lot of research has been done in the past for secure data aggregation. Some of the important methodologies has been surveyed in this research work. The present broadcast protocols that is authenticated [7] need sensors of IoT to verify the data of broadcast with the key revealed by their gateway in upcoming interval of time. This produces an authentication delay, and every single sensor has to store all packets that are unauthenticated within its buffer. Even in scenario where a delay is allowed, there is some limit for the buffer size of IoT devices. However, there is no security for privacy of messages that will be broadcast and no protection design that is proven formally. Privacy protection infrastructure based on interaction, for example, [11], are approaches based for preventing the operations and deactivating the operation that are unauthorized. This privacy protection method utilizes levels of privacy preventing to stop accessing the data, which are sensitive. This protects operations that are unauthorized on IoT data. Solutions of Public Key, for example, as described in system introduced in [9], activate prevention of data for IoT devices. They utilize IoT gateway to gather information from sensors and use encryption accordingly to the information, manage user access and protective transmission algorithms for gaining important privacy and protection needed for data, which are sensitive. Additionally, the interest is getting more to

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

join and help theoretical forensic-by-model as shown in [13]. In the present method of access control that is based on EBA [12], [14], sensors are required to encrypt IoT information with EBA method. User that is having the policies of access control can decrypt the information that is encrypted. Anyways, EBA methods [12] usually generates more computation and are tough to develop in IoT devices and wireless sensors with some range of energy and capacity of computation.

The control method of data access takes help of encryption method of homomorphic offered by cryptosystem of Paillier [4] to make sure the access is privacy protected for IoT information. To use the information, the client needs a secret and public key set (sk, pk) for cryptosystem of Paillier. The key can be possibly controlled and given with CA (Certificate- Authority). To access the information, the client sends a request containing the clients identity, query (along with time window), execution to be done on the information and private, public key set. In our implemented method, the aim is to offer analyzed information to the client without disclosing the actual information to both in between the client and server. The channel of communication between client and access layer of information is considered to be a protective channel and the access layer of information utilizes some kind of access control same. If the clients request clears the sign authentication and fulfills the policies of access control, the access layer of information will execute the Algorithm-1 to fill the corresponding information. Based on CP-EBA, alternative fine-grained method of ac- cess controlling for IoT devices was introduced. This method permits only policies that are based on AND. In [4], author introduces a system, which is based on identity that prevents information of the location of IoT devices while in emergency cases. In this method, every single client interacts with others with the help of VID (Virtual-ID) that is not having any actual data about the client. In this infrastructure, privacy of the client can be prevented very well as they transmit only VIDs to interact, and VID is not specified and cannot be linked to clients. The information of the location will be transmitted to the client only when the authentication is successfully done. In IoT, authenticating identities of the devices are important to stop access that are not authorized to private information of client, and permit the access only for authorized clients. Author introduces a protocol for authentication for IoTs. In the introduced protocol sensors are end nodes, and every node has an exclusive global address for linking via internet. To obtain a session key, cryptograms for PK and SK is assumed for IoT platforms, but they have some issues like cryptograms for SK needs huge memory to hold key chains and cryptograms for PK utilizes more power. Later in the security concern was solved through authentication mechanism i.e. X.509 digital certificates, the digital certificates were capable of encrypting, hashing and then the certificates were created to secure the data. However, the generation of digital certificates is quite complicated. In [7], author introduces an

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

ECC (Elliptic-Curve Cryptosystem) dependent key obtaining approach applicable for IoT platform.

III. EXISTING SYSTEM

Tan and Körpeoglu [7] proposed a power efficient data gathering and aggregation scheme in wireless sensor networks. Rajagopalan and Varshney [8] introduced data aggregation techniques in sensor networks. Chen et al. [9] presented a data aggregation scheme with distributed randomized algorithms. Hekmat and Van Mieghem constructed the shortest path aggregation tree that maximizes network lifetime. Chang and Yen [1] constructed a spanning tree based aggregate routing algorithm, selecting the node that performs the data aggregation operation through the coding tree.

Lee *et al.* [2] presented a construct which use geographical route to balance network traffic, and optimize network lifetime and aggregate data rate through optimization methods. However, these data aggregation schemes are mainly concerned with the issue of energy conservation without focusing on the security of data aggregation.

The security problem of data aggregation [2] began to be studied at home and abroad in recent years, but they mainly focus on safe energy conservation and safe routing at early period. Some work focus on the security of data later. Work in [4], [5] introduced privacy homomorphism technology and proposed data aggregation schemes based on privacy homomorphism. These schemes aggregate encrypted data directly without decryption in order to protect end-to-end privacy of data. Zhu *et al.* [6] proposed a secure data aggregation scheme based on commitment-proof and back testing in order to protect the integrality of data. Chen *et al.* [7] combined homomorphic encryption with bilinear-based signature, and proposed a recoverable data aggregation scheme to ensure data privacy and integrity.

Li *et al.* [8] proposed a privacy preserving data aggregation scheme for mobile edge computing assisted IoT application. However, all of these work only focus on protecting data privacy and integrity but not pay attention to the basic data aggregation query operations such as max, min, count, top-k and so on. Later, some work focus on the basic query operations in secure aggregation. Chan *et al.* proposed a secure data aggregation scheme (SIA) [9].

However, this scheme only supports one aggregator, and it is not applicable to large amounts of data. Then they extended SIA and proposed a secure hierarchical aggregation scheme (SHIA) [3] that supports multiple aggregators. This work only supports limited sets of aggregation functions but not supports aggregation functions such as max and top-k. Nath *et al.* [15] proposed a secure outsourced aggregation scheme which uses one-way chain and related cryptography operations to ensure the security of aggregation. This work supports several aggregation functions

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

such as max, count and top-k, but it doesn't protect the privacy of data.

Disadvantages

- In the existing work, the system leaks guarantee of the confidentiality of the data.
- The existing doesn't provide an effective cryptography techniques.

IV. PROPOSED SYSTEM

The system designs the system model of location-based secure outsourced aggregation in IoT. Then we propose the threat model. Next we propose our design goal. The system model of LBOA defines the participants including location-sensitive devices, user and cloud service provider. The system model also defines the participants' task. The threat model in this study describes the adversarial behaviors including data tampering, cheating, data deleting and so on. The design goal of LBOA in this study presents the requirements such as providing service based on location, achieving location privacy protection, data confidentiality protection and location strategy confidentiality protection.

The system proposes a novel location-based secure outsourced aggregation scheme *LBOAMax* which can return the maximum value under user's location strategy. Then we propose scheme *LBOATop□k* and scheme *LBOASum* which can return the largest *k* values and the summation value under user's location strategy respectively. Our schemes could aggregate data whose location is at specified location correctly. They could also protect the confidentiality of data and the privacy of the location strategy.

The system theoretically analyzes the security of LBOA. The analysis results show that our schemes satisfy our design goal. At the same time, our schemes support much more data aggregation query operations and are much more secure than existing schemes. The system reports experimental evaluations of LBOA. The evaluation results show that our schemes are efficient and feasible in practice.

Advantages

- A location-based secure outsourced aggregation scheme is implemented securely in IoT to realize aggregating data based on devices' location.
- The system is more secured since an achieve secure aggregation based on sensing device's location is implemented.

V. CONCLUSION

In this study, we proposed three novel schemes that can achieve secure outsourced aggregation based on data's location. We proposed LBOAMax to obtain the Max aggregated data first, and then we proposed LBOATop−k and LBOASum to obtain the Top-k and Sum aggregated data respectively. Different from existing

schemes, our schemes could realize secure aggregation based on location and could achieve location privacy protection, data confidentiality protection and location strategy confidentiality protection. Next we analyze the security of our schemes and the analysis results show that our schemes satisfy all the defined requirements. Finally, the experiment results show that our schemes are practical and feasible in IoT.

REFERENCES

[1] H. Xiong, H. Zhang, and J. Sun, ‘‘Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing,’’ IEEE Syst. J., to be published.

[2] J. Zhang, J. Ma, C. Yang, and L. Yang, ‘‘Universally composable secure positioning in the bounded retrieval model,’’ Sci. China Inf. Sci., vol. 58, no. 11, pp. 1–15, 2015.

[3] T. Kwon, J. Lee, and J. Song, ‘‘Location-based pairwise key predistribution for wireless sensor networks,’’ IEEE Trans. Wireless Commun., vol. 8, no. 11, pp. 5436–5442, Nov. 2009.

[4] B. Li, W. Wang, Q. Yin, H. Li, and R. Yang, ‘‘An energy-efficient geographic routing based on cooperative transmission in wireless sensor networks,’’ Sci. China Inf. Sci., vol. 56, no. 7, pp. 1–10, 2013.

[5] A. Boldyreva, N. Chenette, Y. Lee, and A. O’Neill, ‘‘Order-preserving symmetric encryption,’’ in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., Cologne, Germany: Springer, 2009, pp. 224–241.

[6] S. Nath, H. Yu, and H. Chan, ‘‘Secure outsourced aggregation via one-way chains,’’ in Proc. ACM SIGMOD Int. Conf. Manage. Data, Providence, RI, USA, 2009, pp. 31–44.

[7] H. Ö. Tan and I. Körpeoglu, ‘‘Power efficient data gathering and aggregation in wireless sensor networks,’’ ACM SIGMOD Rec., vol. 32, no. 4, pp. 66–71, 2003.

[8] R. Rajagopalan and P. K. Varshney, ‘‘Data-aggregation techniques in sensor networks: A survey,’’ IEEE Commun. Surveys Tuts., vol. 8, no. 4, pp. 48–63, 4th Quart., 2006.

[9] J.-Y. Chen, G. Pandurangan, and D. Xu, ‘‘Robust computation of aggregates in wireless sensor networks: Distributed randomized algorithms and analysis,’’ IEEE Trans. Parallel Distrib. Syst., vol. 17, no. 9, pp. 987–1000, Sep. 2006.

[10] R. Hekmat and P. Van Mieghem, ‘‘Connectivity in wireless ad-hoc networks with a log-normal radio model,’’ Mobile Netw. Appl., vol. 11, no. 3, pp. 351–360, 2006.

[11] C. W. Yu and L. H. Yen, ‘‘Computing subgraph probability of random geometric graphs: Quantitative analyses of wireless ad hoc networks,’’ in Proc. Int. Conf. Formal Techn. Networked Distrib. Syst. Berlin, Germany: Springer, 2005, pp. 458–472.

[12] H. J. Lee, A. Cerpa, and P. Levis, ‘‘Improving wireless simulation through noise modeling,’’ in Proc. ACM 6th Int. Conf. Inf. Process. Sensor Netw., Cambridge, MA, USA, 2007, pp. 21–30.

[13] Y. Yu, V. K. Prasanna, and B. Krishnamachari, ‘‘Energy minimization for real-time data gathering in wireless sensor networks,’’ IEEE Trans. Wireless Commun., vol. 5, no. 11, pp. 3087–3096, Nov. 2006.

[14] T. Jung, X. Mao, X.-Y. Li, S.-J. Tang, W. Gong, and L. Zhang, ‘‘Privacy preserving data aggregation without secure channel: Multivariate polynomial evaluation,’’ in Proc. IEEE INFOCOM, Turin, Italy, Apr. 2013, pp. 2634–2642.

[15] Y.-H. Lin, S.-Y. Chang, and H.-M. Sun, ‘‘CDAMA: Concealed data aggregation scheme for multiple applications in wireless sensor networks,’’ IEEE Trans. Knowl. Data Eng., vol. 3, no. 3, pp. 1471–1483, Jul. 2014.

AUTHORS PROFILE:

A.V.NAGAMANI: Senior lecturer in Dept. of computer Science at V.S.lakshmi Women's degree & pg College, Kakinada since 2011. She has vast experience in handling projects on JAVA and Eclipse.