International Journal of Research in Engineering, Science and Management
Volume-3, Issue-11, November-2020
https://www.ijresm.com | ISSN (Online): 2581-5792

Data Security Using Time Based Publisher Encryption Algorithm

A. Aarthy[1], R. Pradeep[2*]
[1]*Department of Computer Science Engineering, Anna University Regional Campus, Coimbatore, India*
[2]*Assistant Professor, Department of Electronics and Communication Engineering, Sri Eshwar College of Engineering, Coimbatore, India*
*Corresponding author: pradeepkrishna005@gmail.com

***Abstract*: In Internet of things security and privacy are the main issues for IoT data, in which data can be hoard anywhere in the network for easy retrievals. In order to provide flexible data authorization to the users, Cipher Text Policy Attribute Based Encryption and Distributed Publisher Driven IC IoT are incorporated and proposed Time Based Publisher Driven Algorithm to make available of pristine data access to users, where it enable only authorized users to retrieve IoT data. Time Based Publisher Driven Algorithm introduces DSA to deal services between users and publishers, other than the registered users no one can access data in the cloud server. According to performance Evaluation Encryption and Decryption time is fast and security is high when compared with existing systems.**

***Keywords*: Cipher text attribute based encryption, Information centric network, Internet of Things, Publisher algorithm, Security.**

1. Introduction

Internet of Things is the emergence of a variety of communications solutions targeted at specific application domains. It is predicted that 50 billion devices will be connected through IoT by 2020 and vast amount of data will be generated from those devices [4]. Internet of things (IoT) is the inter connection of physical objects or things implanted with electronics, sensors, actuator, software and internet connectivity which enables these objects to collect and exchange the real time data. IoT endorse object to be sensed and controlled remotely across subsisting network infrastructure, engendering opening for more direct integration between the substantial world and computer predicated systems and resulting in ameliorated efficiency, precision and monetary benefit. It has many services across the cyber world and in many case they are data centric in which the data were amassed, sensed, stored and shared to the target group of entity and person [11]. Thereby the users will be mainly fixated on the data and information rather than to communicate. IoT systems lead to real time data communication and storage through wired or wireless communication. The data sensed should be securely sent to cloud data base through internet connections. IoT frame work requires security mechanisms in two directions one while sending the data to the cloud storage and other to publish the data to the target user from the information centre. Hence security is one of the major issues in IoT based systems. The vision of IoT becomes true only when primary security threats are eradicated while sending the data to the data centre and also sharing the data to distributed authorized user. The three main requirements to enable IoT security are (AAA) authentication, authorization and access control [2]. Traditional way on IoT network security is not adequate to provide high level of AAA. Hence the need of novel security mechanisms for IoT system becomes mandatory to implement an accomplished IoT world. In this paper, we contributed to provide a better solution to meet out the security requirements of IoT based systems.

Al-Fuqaha [3] et al presented that constrained application protocol COAP aims to enable the contrivances with low potency, calculation and communication that can utilized for the restful interactions. COAP can be sub divided into layers, the messaging sub-layer and the request or replication sub-layer. The messaging sub-layer detects duplications and provides reliable communication over the UDP convey layer. It does not have an error instauration mechanism. The request or replication sub-layer withal handles REST communications. COAP has four types of messages: confirmable, non-confirmable, reset and cognizance. Reliability of COAP is mainly depends on confirmable and non-confirmable messages.

Xiaokang Xiong, [19] used Computing Bilinear Pairing on sensor platforms has become a paramount research topic in cryptography to Wireless Sensor Networks (WSNs). Anterior works have provided benchmarks for the pairing of sensors. It may be a consummate pairing predicated cryptographic scheme requires a bilinear pairing operation. Here the first planarity functional pairing-predicated cryptographic library for WSNs was utilized. The library is expeditious and lightweight, with an adscititious of one identity-predicated encryption scheme and additionally proposed several incipient algorithms and techniques, and shows that they significantly amend the haste and reduces the recollection utilization of the library. The performance results of implementing the three pairing-predicated cryptographic schemes that pairing predicated cryptosystems are feasible.

Ruidong [18] proposed that in order to secure a wireless sensor and actuator network (WSAN). In cyber physical systems, trust management quandary of nodes and stimulate nodes to cooperate each other. This subsisting system is divided into reputation frame work and trust frame work but still it has so many quandaries, in order to solve that quandary, they proposed a hybrid trust management framework (HTMF) to construct the trust environment of WSANs.

Lo-Yao Yen, [17] et al that Internet of Things (IoT) contrivances for medical accommodation and pervasive Personal Health Information(PHI) systems play consequential roles in the Health environment. A cloud predicated promising approach privacy and information security. Here proposed a cloud predicated fine grained health information access control for lightweight IoT contrivances. Only symmetric cryptography is required for IoT contrivances, such as wireless body sensors. A variant of cipher text-policy attribute-predicated encryption, used to fortify fine-grained access control, efficient dynamic data auditing, batch auditing, and attribute revocation. The proposed scheme additionally defines and handles the cloud where the accommodation providers can avail each other evade data loss. Ruidong-list [16] proposed in Information-Centric Internet of Things (ICIoT), IoT data can be stored throughout a network for close data copy retrievals. Such a distributed data caching situation, poses a dare to flexible sanction in the network. To address this challenge, Cipher text Policy Attribute-Predicated Encryption (CP-ABE) has been identified as a promising approach. Though it is subsisting CP-ABE scheme, publishers need to retrieve attributes from a central server for encrypting data, which leads to high communication overhead. In order to solve this quandary, with CP-ABE scheme and proposed a novel Distributed Publisher driven secure Data sharing for ICIoT (DPD-ICIoT) to enable only sanctioned users to retrieve IoT data from distributed cache. In DPDICIoT, incipiently introduced Attribute Manifest (AM) is stored in the network, through which publishers can retrieve the attributes from nearby copy holders in lieu of a centralized attribute server. And withal, a key chain mechanism is utilized for efficient cryptographic operations, and an Automatic Attribute Self Update Mechanism (AASM) is proposed to enable expeditious updates of attributes without querying centralized servers.

In all the above mentioned research work, the issue of problems facing in security is resolved with certain limitations like complexity, efficiency, safety and reliability. In this paper, we propose a Time based publisher driven algorithm that is the hybrid algorithm. It involves the features of CP-ABE & DPD-ICIOT algorithms to provide the solution for access policies, encryption / decryption and security mechanisms. In CP-ABE a particular user can access data based on the attribute value. DPD-ICIOT scheme introduce attribute manifest in the network through which publishers can retrieve attributes from nearby copy holders instead of a centralized attribute server.

2. System Description

A. *Time based publisher driven algorithm*

In order to provide security for IoT data, we incorporate CP-ABE and DPD-ICIOT and propose the Time Based Publisher Driven Algorithm to make available of pristine data access to users. In CP-ABE as well in the DPD-ICIOT IoT data can be encrypted and decrypted without considering about where the data are cached. The users cannot be predefined in ICIOT and also IoT data can be used at the time of publishing. Without considering about the unauthorized access encrypted data can be stored anywhere in the network. And also the existing scheme in order to encrypt the data publishers need to retrieve attributes from the centralized servers.

In Time Based Publisher Driven Algorithm as in existing scheme DPD-ICIOT introduces DSA to deal services between publishers and users. As same as CP-ABE scheme to provide data access rights to users. The introduced DSA acts as a key server and also provide attribute extraction to the particular users. Information Centric Networking (ICN) is a forthcoming new technology that helps the users to access data from close caches instead of data access from far-away servers. Here both DSA and ICN approach unite to provide efficient, flexible data and security among IoT data, publishers and users. In CP-ABE and DPD-ICIOT approach only from the centralized server attributes are stored and retrieved. But in Time Based Publisher Driven Algorithm attributes values are registered in publishers and it verified by DSa.

1) *Architecture Diagram*

The proposed system architecture diagram for Time Based Publisher Driven Algorithm is shown in figure 1. Publishers provide data access rights to users from DSA. Here CP-ABE scheme is used for generation of attribute for users and also flexible data access based on their attributes. We detailed below the architecture diagram with the following layers,

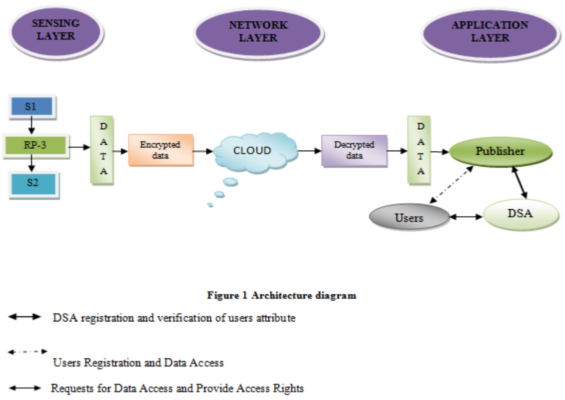
SENSING LAYER
NETWORK LAYER
APPLICATION LAYER
S1
RP-3
S2
DATA
Encrypted data
CLOUD
Decrypted data
DATA
Publisher
Users
DSA
Figure 1 Architecture diagram
DSA registration and verification of users attribute
Users Registration and Data Access
Requests for Data Access and Provide Access Rights

Fig. 1. Architecture diagram

Sensing Layer: IoT devices are equipped sensors that are Raspberry pi 3 is connected with sensors s1 and s2 where s1 is temperature sensor DS18B20 and gas sensor MQ2. Sensors are the devices that help in interact with the physical environment.

The data collected by the sensor has to be stored and processed. The storage and processing of data can be done in a server. The processed data is sent to the server and the communication between IoT devices is mainly wireless.

Network Layer: Networking make possible IoT devices to communicate with other device these are the services are in the cloud. Communication is innermost to internet of things. This layer provides the path for network communication and data is transferred in the form of packets. Data that are sensed from the sensing layer is encrypted and stored in the cloud server. One of the best ways to protect data in cloud is Encryption in order to protect data from the cloud as well to store data, Encryption and Decryption is done through Time Based Publisher Driven Algorithm for security.

Application Layer: The Application Layer enables the user, that is human or software, to access the network. It also provides the file transfer, access and management (FTAM). In application layer there are three systems that are Publisher, DSA and Users.

Publisher: The entity who publishes IoT data for a set of users. IoT is an extension of publishing and to generate the information about users and add DSA. It consists of user and Data Sharing Authority registration. In order to access the data, the particular user has to register their necessary details in the publisher sector.

Data Sharing Authority: DSA were added by publisher. Users will request for data access to DSA. After the verification of users in publisher DSA provide data access rights to users based on their attribute value.

Users: One who retrieves data from the server? Here not all the user can retrieve data. Only the register user can retrieve IoT data.

3. Proposed Time Based Publisher driven Algorithm

Time based encryption consists of three fundamentals scheme: Setup, Encrypt and Decrypt.

Setup: It takes the input and output of parameters. It chooses the random odd numbers 'N', V asensed value, T(s) is sensed time in seconds and the function is F_e (V, T).

Encrypt F_e (V, T): The encryption Algorithm encrypts a sensed value (V). It first chooses 'N' i.e. random odd prime numbers. These polynomials are chosen in the following way, starting from the sensed value (V) & next to 'N', where function of Encryption is denoted as F_e.

Let,
R is the Random odd Prime numbers
T(s) Time in seconds
$N = \{2, 3, 5, 7, 11,13,17,19, 23, 29...\}$
$N =\{x / x € R\}$
$F_e (V, T(s))$
$$\text{Cipher Text (CT)} = (V + N * T(s)) / T(s) \quad (1)$$

Decrypt F_d (CT, D): The decryption algorithm takes cipher text (CT), Time in seconds T(s) as inputs and perform the decryption function in order to find the value (V). In the following way decryption takes place.

$$F_d (CT, T^*(s))$$
$$CT * T = V + N * T(s)$$
$$CT * T(s) – N * T(s) = V \quad (2)$$

4. Discussion

In this section we present a Time and security based performance analysis of our proposed system.

A. Encryption Time

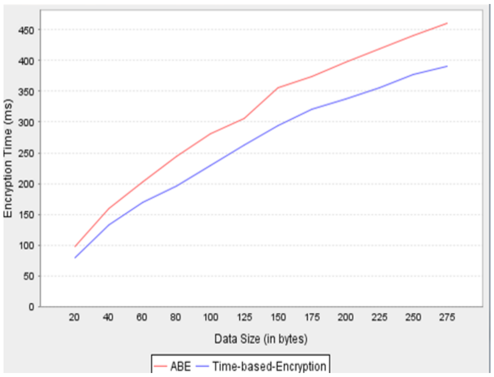

Fig. 2. Comparison of DPD ICIoT and time based encryption based on encryption time

B. Decryption Time

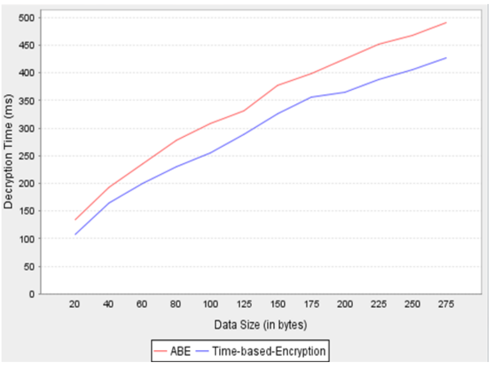

Fig. 3. Comparison of DPD ICIoT and time based encryption based on decryption time

C. Confidence level analysis

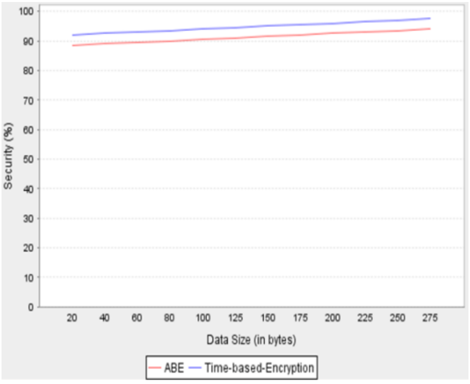

Fig. 4. Comparison of DPD ICIoT and time based encryption on security basis

5. Conclusion

This paper presented a novel time based publisher driven algorithm for secure and flexible data access in Internet of Things that incorporates the qualities of both CP-ABE and DPD-ICIoT. In CP-ABE and DPD-ICIOT approach only from the centralized server attributes are stored and retrieved. But in Time Based Publisher Driven Algorithm attributes values are registered in publishers and it verified by DSA. Data Sharing Authority provides the data access privilege only to the registered users. In addition, system evaluations have been done, which illustrate that Time Based Publisher Driven Algorithm can reduce encryption / decryption time and security is also high when compared with existing systems. There are number of issues to be addressed in security of IoT data sharing. In future to secure IoT data such as trust based security is needed to advance this paper a set further.

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies Protocols and Applications,” IEEE Communications Surveys & Tutorials, no. 99, June 2015.

[2] M. AL-Naday, M. Reed, D. Trossen, and K. Yang, “Information Resilience: AN Attribute based Encryption,” IEEE Network, vol. 28, no. 3, pp. 36-42, 2014.

[3] R. Li and H. Asaeda, “A Community-Oriented Route Coordination Using Information Centric Networking Approach,” 38th IEEE conf. Local Comput. Netw. (LCN). pp. 793-800, Oct.2013.

[4] M. Amadeo, C. Campolo, A. Molinaro, M, Aledhari, and M. Ayyash. “Multi Source Data Retrieval in IoT via Named Data Networking,” ACM Conference on information-Centeric Networking (ICN 2014), Sept. 2014.

[5] L. Touati, Y. Challal, and A. Bouabdallah, “C-CP-ABE: Cooperative Cipher Text Policy Attribute-Based Encryption for the Internet of Things,” 2014 International Conference on Advanced Networking Distributed Systems and Applications (INDS), 2014.

[6] J. Kumar, and D. Patel, “A Survey on Internet of Things: Security and Privacy Issues,” International Journal of Computer Applications, vol. 90. no. 11. 2014.

[7] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, “plutus: Scalable Secure File Sharing on Untrusted Storage,” USENIX’02, San Fransisco, CA, Dec. 2002.

[8] W. Chai, and et. al., “An Information-Centric Communication Infrastructure for Real-Time State Estimation of Active Distribution Networks,” IEEE Trans. on Smart Grid, vol. 6, no. 4, pp. 2134-2146, July 2015.

[9] E. AbdAllah, H. Hassanein, and M. Zulkernine, “A Survey of Security Attacks in Information-Centric Networking,” IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1441-1454, 2015.

[10] K. Yu, M. Arifuzzaman, Z. Wen, D. Zhang, and T. Sato, “A Key Management Scheme for Secure Communications of Information Centric Advanced Metering Infrastructure in Smart Grid,” IEEE Trans. on Instrumentation and Measurement, vol. 64, no. 8, pp. 2072-2085, Aug. 2015.

[11] W. Shang, Q. Ding, A. Marianantoni, J. Burke, and L. Zhang, “Securing Building Management Systems using Named Data Networking,” IEEE Network, vol. 28, no. 3, pp. 50-56, May 2014.

[12] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-Policy Attribute Based Encryption,” the 28th IEEE Symposium on Security and Privacy, pp. 321-334, Oakland, 2007.

[13] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, “Homomorphic Algorithm,” RFC 3588, Sept. 2003.

[14] P. Samartini and S. Vimercati, “Multi Authority Attribute based Encryptions,” In Foundations of Security Analysis and Design: Tutorial Lectures, LNCS, vol. 2171, pp. 137–193, 2001.

[15] Carlos Gonzalez, Salim Mahamat Charfadine, Olivier Flauzac and Florent Nolot, “SDN-Based Security Framework for the IoT in Distributed Grid University of Reims Champagne-Ardenne.

[16] R. Li, H. Asaeda and J. Li, "A Distributed Publisher-Driven Secure Data Sharing Scheme for Information-Centric IoT," in IEEE Internet of Things Journal, vol. 4, no. 3, pp. 791-803, June 2017.

[17] L. Yeh, P. Chiang, Y. Tsai and J. Huang, "Cloud-Based Fine-Grained Health Information Access Control Framework for Lightweight IoT Devices with Dynamic Auditing and Attribute Revocation," in IEEE Transactions on Cloud Computing, vol. 6, no. 2, pp. 532-544, 1 April-June 2018.

[18] R. Li, J. Li, and H. Asaseda, “A Hybrid Trust Management Framework for Wireless Sensor and Actuator Networks in Cyber-Physical Systems,” IEICE Trans. on Information and Systems), vol. E97-D, no. 10, pp. 2586-2596, October, 2014.

[19] X. Xiong, D. S. Wong, and X. Deng, “Tiny Pairing: A Fast and Lightweight Pairing-based Cryptographic Library for Wireless Sensor Networks,” IEEE Wireless Communications & Networking Conference (IEEE WCNC10), Sydney, Australia, April 2010.