2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) 978-1-7281-4142-8/20/$31.00 ©2020 IEEE 10.1109/ic-ETITE47903.2020.175

Enabling authenticity and integrity with Information Hiding for secure communication in Internet of Things

Jebin Bose S
ME Computer Science and Engineering
Noorul Islam Centre for Higher Education
Kumaracoil, India
jebinboses@gmail.com

Julia Punitha Malar Dhas
Associate Professor/ Dept of Computer Science and Engineering
Noorul Islam Centre for Higher Education
Kumaracoil, India
julaps118@gmail.com

Sybi Cynthia
Assistant Professor/ Dept of Computer Science and Engineering
Saveetha School of Engineering
Saveetha Institute of Medical and Technical Sciences
Chennai, India
sybi.cynthia@gmail.com

Abstract— **Internet of Things (IoT) enhances the global connectivity to all the remote sensing devices. It enables the connectivity of communication and processing the real-time data that has been collected from an enormous number of connected sensing devices. There is an increase in the IoT technology that leads to various malicious attacks. It is more important to overcome the malicious attacks, mainly to stop attackers or intruders from taking all the control of devices. Ensuring the safety and accuracy of the sensing devices is a serious task. It is very much important to enabling the authenticity and integrity to obtain the safety of the devices. Dynamic tree chaining, Geometric star chaining and Onion encryption are the three solutions that has been proposed in this project for in order to enable authenticity and integrity with information hiding for secure communication. The simulation results are driven displays that the proposed system is very stable and much better than other existing solution in means of security, space and time.**

Keywords— Data retrieval, Onion encryption, Hash chaining, Information hiding, Signature verification, authentication

I. INTRODUCTION

Internet of things becoming more familiar in recent years as it can connect and make smart of any devices through the internet. This article demonstrates the overall aspects and challenges in the internet of things as it can connect any devices. Identities and virtual personalities having things that operate by connecting all the smart devices [1-3]. Internet and Things are the two classifiers that can be split from the term IoT. Frequently used TCP/IP has not been properly analyzed in the IoT [2-4]. Around us, around the world, there are enormous amounts of Smart devices that have been connected with the internet. The evolution of sensors, RFID based sensors connected with the Internet brings us the Internet of Things. Collection of data's can be carried out by the smart devices that are connected with the Internet [5]. The difficult task of Ubiquitous computing has become easier due to the computation and speed of the computer [6]. The data that are collected and stored are to be secured [8]. Nowadays IoT has been developing everywhere around the globe. But there are various security flaws behind this IoT.

To maintain IoT security, various IoT techniques and strategies have been proposed. Moreover, along with the development of IoT, its security measures have also to be upgraded. The development of IoT is developing at an enormous speed that upgrades the static internet to future internet. This revolution in IoT and the Internet will completely change the people's way, their work, and their life. Consider and imagine every object in the human's hand is connected through the internet from the wallet to watch as it can easily be monitored if it gets stolen.

These sensing data somehow has to be stored in the cloud or some other storage environment. Ensuring its authenticity, integrity and security of the data is a difficult task [15-17]. Sometimes these data can be interrupted, modified or can be altered and stolen by the intruders [18]. Without security, authenticity, and integrity the data cannot be used later for medical purposes or some other important decision-making purposes. As it may result in the loss of human life or some other economic failure. So ensuring authenticity and integrity is a major important task.

The main aim of is to ensure the drawbacks that relates with the security, its authentication issue and to obtain upgradable security solutions. Here this paper also examines IoT data communication with Dynamic tree chaining, Geometric star chaining, and Onion encryption as it provides reliable and uninterrupted secure communication.

II. RELATED WORKS

Nowadays everywhere in the field of computer security, the Digital signature is used to ensure the data security, data integrity and data authenticity. But there are no proper systems that enables the proper security that have been specified below.

978-1-7281-4142-8/$31.00 ©2020 IEEE

The Public-key cryptography are much slower when compared to symmetric key. [10]. Using Hash chaining [9] O(m) to O(1) the buffer space complexity will be reduced. Here only first message is signed in hash chaining signature scheme. Moreover, due to partial data retrieval when some events are dropped, hash chaining fails.

Some of the other methods relevant to the point stated above are discussed below:

A new technique has been proposed by Challa et al. [7]. ElGamal type elliptic curve cryptography (ECC) scheme has been used here and in the IoT network, it provides authentication among communicating entities. More computation cost is required.

Wazid et al. [11] proposed a three-factor authentication that is a new secure lightweight scheme called as user authenticated key management protocol (UAKMP). The user personal biometrics of user , smart card of user and password are the three factors used in UAKMP. Only cryptographic hash function has been used as it is very efficient and also uses symmetric encryption and decryption. More computation cost and more Verification time have been required in this technique.

A new lightweight RFID mutual authentication scheme has been proposed by Fan W. Jiang et al. [13] that have used in a medical context. Useful can be processed by RFID tags in the system. High communication cost and is required in this technique.

The Dancing Signals (TDS) a new protocol for mobile devices have been proposed by Xi1 et al. [14]. Among all the legitimate devices the channel state information (CSI)has been used to be the common secret. The main drawback is the high error rate and man in middle attack.

III. DESIGN GOALS

A. System Model

In the cloud based data service system there are four entities the IoT devices, the cloud server, the sensing data, and the data applications that are to be considered in this work that has been shown in Fig. 1. Resource-constraint devices are IoT devices in which the sensing data's has been generated. These may be in limited memory, may have less power resources, and lesser computation. Data storage to the clients and data access to the data applications has been offered by the Cloud Server. All those cloud servers are third party servers. The software systems indicates the Data applications in which the request has been generated for the sensing data's in order to examine the verification or validation process. Important data can be fetched by the application in order to make appropriate decisions. The Trusted entities are the IoT devices and the data applications in our system model. Through coordinators, in the cloud server all the IoT devices can sense and upload the data. The generated sensing data using IoT devices are signed and encrypted over the outsourced data in order to enable authenticity and information hiding in remote data integrity. In remote data integrity, by data applications the information hiding and the authenticity has to be verified, in order to prevent data corruption by transmission failures, intruders, transmission failures.

B. Data Model

The event data and time series data and are the IoT sensing data [23]. For every fixed time period, by each device it generates a time series data such as 1 second. Used in order to monitor tasks that may be a temperature reports or other health reports. Event data are generated such as human appearing in a smart camera.

C. Threat Model and Security Definitions

The data applications and outsourced data are stored and managed by cloud server in our model. Moreover, cloud storage is not trusty as it can provide irrelevant results to the applications. The main objective is to provide that the cloud provides accurate results to the applications.

In this work, some of the below security threatens has to be considered.

1) Data corruption: The outsourced data is corrupted in this. It may provide the result wrongly. The adversaries may be the outside attackers.

2) Incorrect results : In the cloud it does not process the complete input, rather it enhances a simultaneous partial output as it enables a incorrect results.

D. Design Objectives

In order to obtain the IoT devices to verify the authenticity and integrity for secure communication is the ultimate goal. In case of device compromises it enhances the use of the private key. In order to boost the secure communication special hardware are not provided[24].

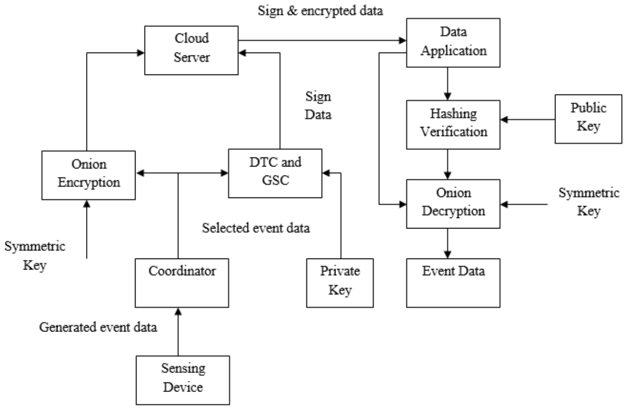

Fig. 1. Representation of proposed system

IV. VERIFIABLE COMPUTATION FOR PROPOSED MODEL

The unstoppable growth of IoT requires cloud in order to store the sensing data. It it very necessary to check with the cost related issues. But the DTC, GSC and Onion encryption enhances the low cost process.

A. Sampling Protocol Design

The coordinator is the new entity introduced by the sampling protocol in the network model. Software is one of the coordinators that resides among cloud and sensing devices. In server or the hub of IoT a coordinator can be installed. It enhances communication among all the sensing devices and temporarily buffers the IoT data sample.

In the coordinator and sensing device there will be two algorithms that have been used.

Algorithm 1: In Round *j* SP at Sensing Device *k*

```
For each event $e$ do
i ← $\min\{x \in N : h(e) \geq 2^{-x-1}\}$;
$l_i^k$ ← $l_i^k$ +1;
if $i \geq j$ then
Forward $e$ to the coordinator;
else
Discard $e$;
end
end
```

1) Sensing Device: Initially it first computes numeric interval {Si} after receiving a new event e, that h(e) falls in, where the uniform random hashing function is h(·) and $\forall x : 0 \leq h(x) \leq 1$. Let l^k_i be a local counter for S_i at device k. Own local counters has been managed by the coordinator and the sensor. In order to audit the coordinator, the local counters are used when $h(e) \in S_i$. Event e will be forwarded to the coordinator by the device, if $i \geq j$, which implies $h(e) \leq 2^{-j}$. Then sensing device signs both counters and sampled events that are maintains at the end of each epoch. The pseudo-code for the sensing device sampling protocol is Algorithm 1.

2) Coordinator: All the queues $\{Q^k_i\}$ has been maintained by the coordinator, that may corresponds to one numerical interval in {Si}. The coordinator first computes i when receiving an event e, so h(e) ∈ Si, that is to be carried out by comparison of i and j. Event e is discarded, in the case of i< j , else it will be buffered at queue Q^k_i that will be followed by updating both the counter associated with global counter g and the numerical interval Si. Now, all event queues that are associated with Si will be discarded, when the value of the global counter g exceeds the budget limit B, the global counter will be updated and sampling protocol processes with the next round j ← j + 1. The newest round j will be promoted by the coordinator. B + 1 events all the time will be buffered by the coordinator that has been evident. The pseudo-code is the Algorithm 2 for the coordinator part.

Algorithm 2 : In Round *j* SP at the Coordinator

```
For each *event e* do
i ← $\min\{x \in N : h(e) \geq 2^{-x-1}\}$;
k ← e.source;
if $\geq$j then
$Q_i^k$ .add(e);
$l_i'$ ← $l_i'$ +1;
g ← g+1;
while g>B do
Discard queues { $\forall k$^,$Q_i^k$^};
g ← g- $_j'$
j ← j+1;
Broadcast $j$ to all sensing devices;
end
else
Discard e ;
end
end
```

B. Signature Schemes

In order to validate and verify data integrity and data authenticity, the digital signature is widely used. Moreover, no existing schemes provide better security. In this paper, two new signature schemes are used.

1) Dynamic Tree Chaining (DTC): A new technique that is determined to be the tree chaining. It represents the binary authentication tree that the digest of each event id one of its leaf node. the internal node value will be computed to be the hash of its two children. The parent of D1, D2 is D12, so D12 = H(D1 || D2), hence message digest function is termed as H(·). So, D14 = H(D12 || D34), D18 = H(D14 || D58). Hence all the roots will be summarized. With epochID the block digest is appended. In order to create block signature it is then signed by the private key.

$D'_3 = H(e_3)$ will be computed by the receiver, that is in order of $D'_{34} = H(D'_3 \,||\, D_4)$, $D'_{14} = H(D_{12} \,||\, D'_{34})$, $D'_{18} = H(D'_{14} \,||\, H_{48})$. If decrypted block signature equal D'_{18}, event e_3 is verified.

2) Geometric Star Chaining (GSC): This technique is one of the more secured way of communication technique. It is somewhat more secured when compared with the other existing systems. Events are in geometric distribution. Here successful numerical integer has been defined {Si} hence Si {x ∈ R : 2−i−1 < x ≤ 2−i , i ∈ N. In {Si} the sensing device computes the numeric interval after receiving a new event e.

Identify that the event in the same block cannot be retrieved back. For one message block one digest has been computed.

C. Onion Encryption and Decryption

It is a data structure. Here, Encryption holds promise in addressing all these avenues of attack. Onion encryption protects and hides sensing data from IoT device to cloud storage. Fig. 2 mentions these onions have different layers each encrypted by using same key to reduce computational cost. At the end of each epoch, the encryption of sampled events is computed in a layered way with the symmetric key of Ks.

The encrypted onion part is generated by

$$m = O_{Ks}\ (e) \qquad (1)$$

The encrypted onion part is updated by

$$\text{Cipher text, } C= O_{Ks}\ (m) \qquad (2)$$

For decryption, removes one by one layer on the top of the encrypted onion by using same symmetric key of Ks, and continues the full data reached.

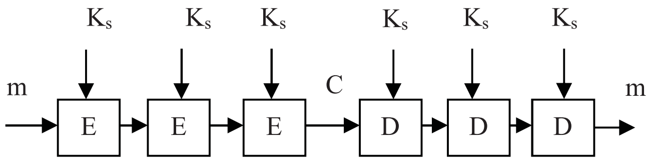

Fig. 2. Onion Encryption model

D. Data Retrieval

For most IoT applications, the sampled data are clear and easy [19]. For some fraction of events some intimation has been obtained from the cloud. The secured verifiable authenticity, integrity and security is provided by the GSC.

At first the data application notices the maximum number of events to be received. Next it sends it to the cloud storage. The sampling protocol will be compatible to the GSC and DTC. GSC is a normal cost efficient security process. Some modifications are to be required in DTC. As both enhances its security measures.

V. PERFORMANCE ANALYSIS

In this simulation, fix the budget limit to 100 events in this micro-scale experiment. The two lines in Fig. 5 represent the number of events sent to the coordinator by all the 7 sensing devices and monitored at all sensing devices, respectively. The two lines vary against time in one day. Initially, the number of events is the same for the two lines. It is worth mentioning that the total number of events sent to the coordinator grows slower with the time, which is a desirable property since the communication cost stays low even if much more events are monitored. This simulation experiment, to some extent, validates the theoretical analysis on the communication cost in which the communication cost only grows logarithmically.

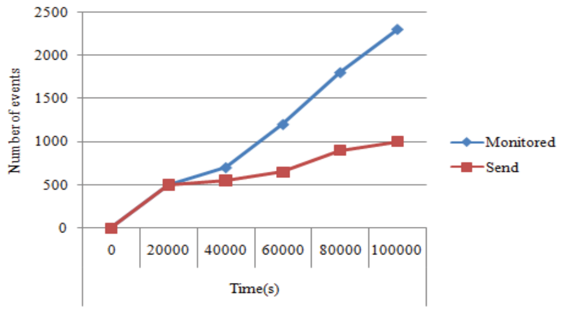

Fig. 3. One-day micro-scale exp

Next, process on how many events recides on the cloud. Mention the different storage of data in the cloud. Fig. 6 mentions that it uses 75% in avarage. Here the sampling protocol get worked correctly.

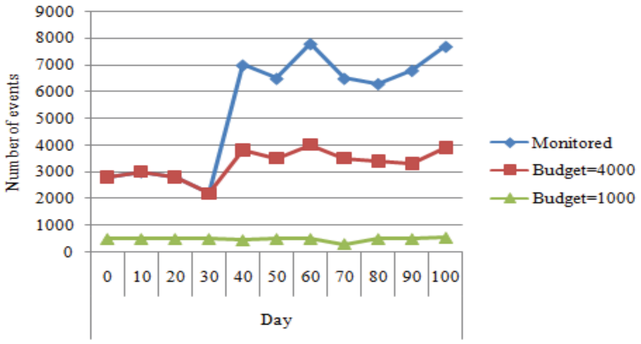

Fig. 4. Events saved in the cloud

The overall comparison of the performance of the verifyer and the signer in DTC and the GSC is analysed in Fig. 7. Here GSC runs at the very maximum speed.

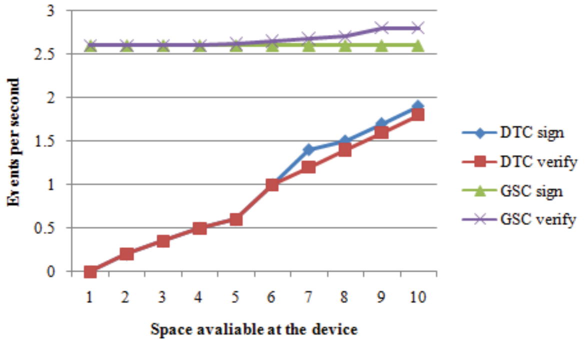

Fig. 5. Throughput comparison

VI. CONCLUSION

Here the practical problem of outsourcing the outsourced cloud data has been examined. To fulfill the requirements, enhancement in the security, authenticity and integrity has been proposed and examines that the existing solution does not provides security to the mark. Besides, the information hiding in remote data integrity is still able to be efficiently executed using onion encryption. Also, our scheme meets the requirements in order to sample the data from all the IoT devices and the data to be stored in the cloud. The performance evaluation prove and shows that proposed scheme is more secure and is efficient.

References

[1] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), “The Internet of Things,” Springer, 2010. ISBN: 978-1-4419-1673-0.J.

[2] L. Atzori, A. Iera and G. Morabito, “The Internet of Things: A survey,” Computer Networks (2010), doi:10.1016/ j.comnet.2010.05.010

[3] J. A. Stankovic, “Research Directions for the Internet of Things,” IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3-9, 2014.

[4] D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010.

[5] G. Tripathi, D. Singh, "EOI: Entity of Interest Based Network Fusion for Future Internet Services", ICHIT2011, September 23-25,2011, Daejeon, Korea.© Springer-Verlag Berlin Heidelberg, CCIS, vol. 206, pp. 39–45, 2011

[6] Hall, D. L., Llinas, J., “Handbook of Multisensor Data Fusion,” CRC Press, (2001).

[7] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy, E. J. Yoon, and K. Y. Yoo, “Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications,” IEEE Access, vol. 5, pp. 3028– 3043, 2017.

[8] T. Song, R. Li, B. Mei, J. Yu, X. Xing, and X. Cheng, “A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes,” IEEE Internet of Things Journal, 2017, DOI: 10.1109/JIOT.2017.2707489.

[9] R. Gennaro and P. Rohatgi. 1997. How to sign digital streams. In Crypto.

[10] K. Piotrowski, P. Langendoerfer, and S. Peter. 2006. How public key cryptography influences wireless sensor node lifetime. In Proc of ACM SASN.

[11] M. Wazid, A. Kumar, and V. Odelu, “Design of Secure User Authenticated Key Management Protocol for Generic IoT Networks,” IEEE Internet of Things Journal, 2018.

[12] S. Yamakawa, Y. Cui, K. Kobara, and H. Imai, “Lightweight Broadcast Authentication Protocols Reconsidered,” in IEEE Wireless Communications and Networking Conference, Budapest, Hungary, April 2009, pp. 1–6.

[13] K. Fan W. Jiang, and Y. Yang, “Lightweight RFID Protocol for Medical Privacy Protection in IoT,” IEEE Trans. on Ind.. Infor..., Apr. 2018, pp. 1656 - 1665.

[14] W. Xi1, C. Qian, and J. Han1, “Instant and Robust Authentication and Key Agreement among Mobile Devices,” in Proc. ACM SIGSAC Conf. on Comp. and Comm. Sec...., Oct. 2016, pp. 616-627.

[15] D. He and S. Zeadally, “An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment using Elliptic Curve Cryptography,” IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72–83, Feb 2015

[16] Y. Zhang, L. Duan, and J. L. Chen, “Event-driven SOA for IoT services,” in Proc. IEEE Int. Conf. Services Comput., Jul. 2014, pp. 629–636.

[17] G. Wang et al., “Towards replay-resilient RFID authentication,” in Proc. 24th Annu. Int. Conf. Mobile Comput. Netw., Nov. 2018, pp. 395–399.

[18] W. Xi et al., “Instant and robust authentication and key agreement among mobile devices,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2016, pp. 616–627.

[19] Sampling For Big Data. Accessed: Aug. 2014. [Online]. Available: https://www.kdd.org/kdd2014/tutorials /t10 part1.pptx

[20] I. B. Damgård, “A design principle for hash functions,” in Proc. CRYPTO, 1989, pp. 416–427.

[21] R. C. Merkle, “A digital signature based on a conventional encryption function,” in Proc. CRYPTO, 1987, pp. 369–378.

[22] C. K. Wong and S. S. Lam, “Digital signatures for flows and multicasts,” in Proc. 6th Int. Conf. Netw. Protocols, Oct. 1998, pp. 198–209

[23] Y. Zhang, L. Duan, and J. L. Chen, “Event-driven SOA for IoT services,” in Proc. IEEE Int. Conf. Services Comput., Jul. 2014, pp. 629–636.

[24] G. Wang et al., “Towards replay-resilient RFID authentication,” in Proc.24th Annu. Int. Conf. Mobile Comput. Netw., Nov. 2018,