International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 04 | Apr 2019 www.irjet.net p-ISSN: 2395-0072

Easy to Implement Searchable encryption scheme for Cloud-assisted Wireless Sensor Networks

Mr. Arun Kumar[1], Ms. Anondita Guha [2], Mr. Vishnu A [3], Ms. Sneha Shiju [4]

Mr. Varchas Shishir [5]

[1]*Assistant Professor, CSE Dept. SRM IST, TamilNadu, India,*

[2,3,4,5]*Student, Department of CSE. SRM IST , TamilNadu, India,*

Abstract- *Development of Wireless Sensor networks along with cloud computing's assistance has unparallely driven the flourishment of the Industrial Internet of Things. With the growth in newer technologies ,doors have opened for newer risks in the field of cyber security specially in cloud-assisted WSN's (CWSN) data confidentiality. This problem can be acknowledged in a reassuring manner through Searchable Public-key Encryption. Theoretically it let sensors to send public key cipher texts into cloud and whoever owns these sensors can perform a search of type word and gather data that was intended into the cloud while side by side making sure that data confidentiality is maintained. However when it comes to generating cipher texts and keyword search, all the currently present and substantially secured searchable public key encryption produce extremely higher costs. Therefore, a lightweight searchable public key encryption method (LSPE) is being proposed in this paper along with meaningful security to CWSNs. A great amount of computation based operations are reduced through LSPE which have been take as reference from earlier works. Hence, LSPE provides search based performance nearly similar to some realistic searchable symmetric encryption methods. Along with all this LSPE conserves a healthy amount of time and energy expense of sensors for the production of cipher texts.*

Keywords- CWSNs, cloud computing, LSPE, IoT, Wireless sensor networks.

1. INTRODUCTION

There is rapid emergence in Industrial Internet Of Things(IIOT.) in the fourth industrial revolution . The use of Industrial Internet Of Things mechanisms in manufacturing is IIOT.There are more generic roles in various scenarios of WSNs and correlated cloud computing mechanisms which are one of the most valuable features of IIOT. example : environmental science, agriculture, security defence etc. WSNs job is to create a connection for the sensors to the internet with the use of gateways, bound to the connection that exists in between the WSN along with the Internet, A number of sensors are placed in the auditing place compose a Wireless Sensor Network ,and produce a quantity of sensor data that will be forwarded by gateways. In particular, the growing acquisition of Wireless Sensor Network's or CWSNs is believed to provide few different hurdles in using of energy and data confidentiality.

Sensitive data are in general collected by sensors in CWSNs generally and are then uploaded in to the cloud. Thus making both of the passive as well as the active attackers curious about the mentioned data. It has been shown in multiple researches that cryptography to CWSNs is brought into action in order to protect data confidentiality, along with which multiple cryptographic algorithms are utilized. The CWSNs sensors are proven to be energy-intensive as well as computation power being restricted up to a certain level. Therefore an encryption schema that is supposedly energy efficient for can be presented for secure as well as dynamic Wireless Sensor Networks. Apart from all of this there are a few more encryption methods that have been introduced in CWSNs, such as mixed encryption scheme, authentic encryption scheme, asymmetric encryption scheme and further more. Data confidentiality is supposed to be maintained by a cryptographic technique called searchable encryption (SE) in CWSN. Presently, it is notably intriguing and a tough task to make the search efficiency better than an Searchable Public Encryption leaving out compromising

keywords' semantic security. Theoretically it can be attained through two possible methods first being the idea of lessening the search complexity as in that the resulting complexity becomes lesser compared to the sub linear. The other method is to lessen the computation based operations to a great extent while also making sure of the sub-linear search complexity.

2. EXISTING SYSTEM

Smart metering , military defence, health care, environmental monitoring and agriculture are the various scenarios where a pivotal role is played by WSNs and related cloud mechanisms which are also one of the most valuable features of Industrial Internet Of Things.

The connection between sensors and the internet by the Wireless Sensor Network is done via gateways.A quantity of sensor message which is to be passed through by gateways will be generated by a quantity of sensors present in the auditing area which also contains a Wireless Sensor Network.Data integrity and energy usage are the main terms of the problems faced by the expanding adoption of WSN,s specifically cloud assisted Wireless Sensor Network.Sensitive data that is uploaded to the cloud is usually fetched by the sensors in CWSN's. This is how potential passive attackers are unaware about all this data .

The existing system holds a number of disadvantages as explained below:

We construct an LSPE based on the concepts of SPCHS. Just like XW15 this scheme also creates a star like structure among searchable cipher texts to reach subb-linear search complexity.

- Leaving out immolating semantic security of tokens it becomes a fascinating and chalking task to increase search efficiency of Searchable Public Encryption.Two ways that can be done to achieve this can be bydecreasing the search complexity that the sub-linear complexity is more than resulting complexity or we can reduce the amount of computation intensive.
- The proposed system comes up with the following advantages:
- Generally Energy-Intensive - The existing systems such as the Searchable Symmetric Key Encryption and Searchable Public Key Encryption for CSWN's tend to take up a lot of sensor energy however sensor's for CSWN's are seen to have lower or limited energy forcing cloud to wrap up the search task as quickly as possible thus making the existing systems energy-intensive in general.
- Computing-Power-Limited - As said earlier CSWN sensors hold a limited amount of energy and while the cloud is supposed to finish the search task in that limited amount, the computing power for large data being limited loads high pressure on keyword search system in CSWN's.
- High Energy Consumption - Having to complete keyword search task in a limited amount of time in a vast cloud sensor data it requires the cloud to run fast computing algorithms which in return require lots of energy to work thus making the existing systems highly energy consuming.
- Less Data Confidentiality - Searchable Symmetric Key Encryption requires the exact same key for all the sensors present in it in order to produce a cipher text thus making a compromise in one of the sensor by anyone as a leakage of every sensor data present there.

3. PROPOSED SYSTEM

- Not Energy-Intensive - While the existing systems have been found to be energy intensive in general the proposed Easy to Implement Searchable encryption scheme for CWSN's removed this issue making the system non- energy intensive one.
- Computing-Power Not Limited - The proposed system does not limit the computational power like the currently existing system thus providing the system to perform computational algorithms that require higher power and give better results.
- Less energy consumption - As the proposed system is not energy intensive it allows searchable tasks to be completed at a lower energy consumption rate when compared to the existing systems.

High data confidentiality - The proposed system uses the concept of Searchable Public Key Encryption thus making only the public key a mandatory element to be stored in the sensors while the private key stays with the owner thus not compromising other sensor data on the compromise of a single sensor.

4. SYSTEM REQUIREMENTS

Searchable Encryption is believed to be a dependable technique of cryptography in order to maintain the integrity of data. When SE is pertained into the Cloud based Wireless sensor networks as shown in the above figure, cipher texts that can be searched based on keywords can be produced by the sensors for their information and then transfer it all into cloud.

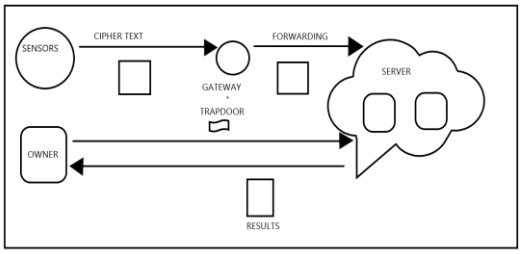

Figure 1- System Architecture For Lspe In Cwsn

In order to get desired information, a search operation for a keyword is performed by the owner in the cloud. All the similar/ matching cipher texts are determined by the cloud and send them as a response to the owner. At last the owner performs decryption over the desired data.

Regarding the security, Searchable Encryption makes sure that either of the eavesdropper or any cloud that is non trusted is not able to learn any information regarding the data present in the sensors in any manner.

Presently, there are two types into which a Searchable Encryption is categorized into. These are SSE and SPE . It is necessary for an SSE to have the exact same symmetric key for every sensor in order to produce in cipher text for an application of CWSN. Thus a compromise in one of the sensors by a foe will lead to the leakage of data from every other sensor too. Luckily, unlike SSE, SPE only makes the storage of public key into every sensor a necessary task. Thus making SPE a more secure mechanism compare to SSE. However it is found that the currently present SPE schemes are not practical for CWSNs when it comes to performance.

Sensors usually are seen to have only a certain amount of energy in CWSNs making it necessary for the cloud to finish a search job as early as it possibly can. Therefore a realistic SPE schema is believed to be largely coherent when comes to producing cipher texts and keyword search. However the SPE schemes re noted to be incompetent to achieve the given goals. The search complexity for the SPE's pioneering work is linear to the total amount of cipher texts.

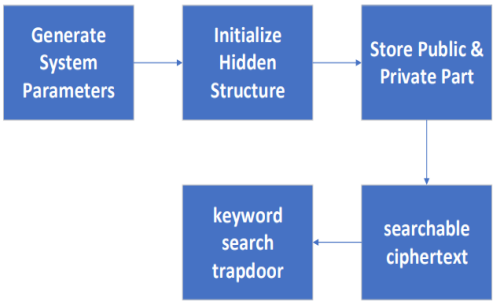

Figure 2- System Architecture Workflow

5. MODULE DESCRIPTION

The proposed LSPE schema is build on the following modules and phases that have been described below as follows: -

5.1 MODULE 1- SETUP PHASE

Setup phase is the phase in which the sensors owner is supposed to select a security related parameter 1k, then running a algorithm PKE1^k of PKE schema in order to show a (Public Key", Searchable Key"). The (Public Key, Public Key") keys are then stored into every sensor after which the owner deploys the above mentioned sensors into the real world for the purpose of collecting data.

5.2 MODULE 2- DATA COLLECTION

The phase of data collection can be explained through the following. Assume that a sensor desires to upload into the cloud all of the data it has collected namely T. For that to happen it performs algorithm Structure (PK) in order to initialize a hidden structure (PUBLIC ,PRIVATE) and then uploads into the cloud the public key. Next it performs extraction of definite keywords from the data we named as T. Assuming that the keywords that were extracted are { X1,… ,Xm }. After this the algorithm Encryption (PK,Xi,

PRIVATE) for i ∈ [1,m] for generating cipher texts that are keyword searchable { C1, ...,Cm }, selecting a randomly chosen symmetric key SK and executing the algorithm Encryption (PKE)(Public Key',SK) in order to show a cipher text C(PKE) and executing the algorithm Encryption (SKE)(SK,T) in order of producing cipher text C(SKE). At the end it finally performs uploading of all the produced cipher texts{C1,..., Cm, C(PKE), C(SKE) }.

5.3 MODULE 3- DATA RETRIEVAL

The data retrieval phase can be explained as the following- Assuming that the sensor's owner wishes to extract data from the cloud for a keyword Ni. It executes the Trapdoor algorithm (SK, Ni) in order to produce the search trapdoor T(Ni) for the keyword Ni later securely uploading the search trapdoor T(Ni) into the cloud. Firstly a search algorithm (Public Key, PUBLIC, T(Ni),C) is performed every hidden structures' public areas in the attempt so that to determine every the similar cipher texts. Next all the determined cipher texts' PKE as well as SKE parts are passed on to the owner by the cloud. At the end the desired data is attained by the owner through decryption of the received PKE along with SKE parts.

This can be explained better through the given example. Assuming that {C1, ..., Cm, C(PKE), C(SKE) } are a set of similar cipher texts, which means that there is a section Ck ∈ {C1, .., Cm} that holds the keyword Ni. The cloud's next task is to pass on the C(PKE) and C(SKE) to the authority. The authority or called (the owner) , then perform decryption of the part C(PKE) with help of the private key it has Searchable Key' in order to improve a symmetric key K, then performing same action to the SKE part C(SKE) using produced SK(K) in order to improve the desired information T.

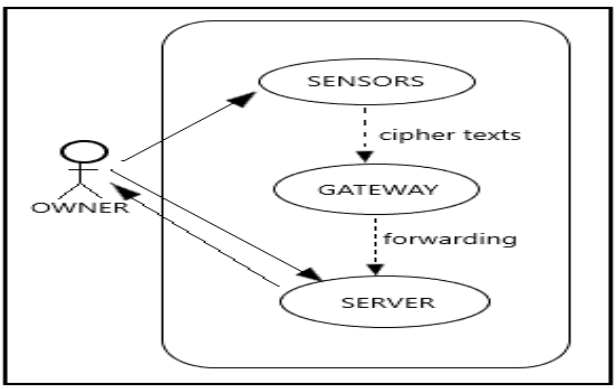

Figure 3- Use Case Diagram

6. SYSTEM REQUIREMENTS

The elements that build the proposed Lightweight searchable public key encryption schema constitutes of - Sensors, gateways and servers that form the base for the Cloud wireless sensor networks. These components are run using 5 SPCHS based on which the proposed algorithm LSPE is being developed. SPCHS defines various different algorithms, which are algorithms Setup,Structure,Encryption, ,Trapdoor,Search.

They are :

ALGORITHM SETUP-

The most important and basic of the 5 algorithms is the Algorithm setup. It generates some kind of system parameters for the remaining algorithms based on the requirements of the security degree. These parameters are majorly made up of 2 parts one master public key and the other one is master private key.

In case of CWSNs, the authority of the sensors implements the Algorithm. All the sensors are then used to accumulate the master public key, whereas the master private key is securely preserved by owner of the sensors.

ALGORITHM STRUCTURE-

Algorithm structure holds responsibility for initializing a secured hidden structure which is later used for the encryption of the algorithm. A hidden structure that has been initialized constituted of two parts- a private and a public part. In case of CWSNs, the sensor implements this algorithms before the 1st time for running the algorithm encryption.

The sensor uploads the public part produced into the cloud while securely storing the private part.

ALGORITHM ENCRYPTION-

The action of generating searchable cipher text of a particular keyword is performed by algorithm Encryption. This cipher text that has been generated holds a hidden relationship with cipher texts that had been previously produced. In case of CWSNs, a sensor implements the algorithm incase it wishes to cipher texts that are searchable through keywords for some gained data. The sensor then uploads the ciphertext produced to the cloud

and in the end updating the private parts of the hidden structure for the upcoming cipher texts.

ALGORITHM TRAPDOOR-

The generation of keyword search trapdoor for a particular keyword is done by Trapdoor algorithm and it is necessary that the master private key is taken as an input into it. In case of CWSNs, a sensor's owner runs this algorithm incase he/she desires to retrieve the particular keywords data present in the sensor and later this trapdoor is sent into the cloud as an authorized keyword search task. As the master private key is only known to the owner, except the owner no one could perform keyword search in cloud.

ALGORITHM SEARCH-

For finding every same cipher text to a particular keyword we use Algorithm search. In case of CWSNs, the clouds performs this algorithm to determine all similar cipher text from the owner upon receiving a keyword search trapdoor.

7. CONCLUSION

An able and easy-to-demonstrate and implement SSE scheme is provided in his paper, it has one round of communication, O(n) times of computations over n documents. Use of hash chaining instead of chain of encryption makes is suitable for lightweight applications. Relative positions and frequency of the word searched cannot be detected, unlike the previous SSE schemes for string search.

Probabilistic trapdoors have been proposed in Searchable Symmetric Key Encryption for String search.Proof of non-adaptive security of our schema against honest-but-curious server is also provided. A new term of search pattern privacy is also introduced, which gives a measure of security against the leakage from trapdoor. It has been proved that the scheme is more secure under search pattern indistinguishably definition. Modifications have been introduced in the scheme so that the, scheme can be made useful against non-passive adversaries at cost of more rounds of communication and memory space. We have validated the scheme against two unique commercial data sets.

REFERENCES

[1] Generating SPE Ciphertext with Hidden Structures for Fast Keyword Search published by Qiahong Wu,Wei Wang,Willy Susilo,Peng Xu,Joseph Domingo Ferrer, Hai Jin and Ferrer.

[2] LSPE for CWSN's published by Shuanghong He,Willy Susil, Hai Jin and Peng Xu.

[3] Data exfiltration from Internet of Things devices: IOS devices as case studies

[4] Everything you need to know about the Industrial Internet of Things

[5] Grand View Research, Industrial IoT Market Size Worth $932.62 Billion By 2025

[6] Evolution of WSN's towards the IOT: A survey.

[7] A domain-based multi cluster SIP solution for mobile Ad Hoc network

[8] A secure cross-domain SIP solution for mobile Ad Hoc network using dynamic clustering

[9] Wireless sensors networks for Internet of Things, pp. 1-6, 2014.

[10] A survey on the privacy preserving data aggregation in wireless sensor networks pp. 162-180, 2015

[11] Deterministic and Efficiently Searchable Encryption