International Research Journal of Computer Science (IRJCS)
Issue 05, Volume 4 (May 2017) SPECIAL ISSUE
ISSN: 2393-9842
www.irjcs.com

ID-Based Aggregate Signature Scheme for Wireless Sensor Networks Using Secure and Efficient Data Transmission

[1]Noor Basha, [2]Kavya N, [3]Manjushree K, [4]Arogyasheela A, [5]Bhavana T,

[1]Asst Professor, [2,3,4,5]UG Students
[1,2,3,4,5]Department of CSE,
Vemana Institute of Technology, Bangalore-34, India

Abstract: ***Data Aggregation is an important topic and a suitable technique in reducing the energy consumption of sensors nodes in wireless sensor networks (WSN's) for affording secure and efficient big data aggregation. The wireless sensor networks have been broadly applied, such as target tracking and environment remote monitoring. However, data can be easily compromised by a vast of attacks, such as data interception and tampering of data. Data integrity protection is proposed, gives an identity-based aggregate signature scheme for wireless sensor networks with a designated verifier. The aggregate signature scheme keeps data integrity, can reduce bandwidth and storage cost. Furthermore, the security of the scheme is effectively presented based on the computation of Diffie-Hellman random oracle model.***

Keywords: ***Big Data, Wireless Sensor Network, Id-based Cryptography, Data Aggregation, Aggregate Signature, Data Integrity, Coalition Attack, Verifier, Encryption, Decryption, Elliptic Curve Cryptography, Data Privacy.***

I. INTRODUCTION

In big data era, [5] wireless sensor nodes is demanding technique and large collection of distributed sensors nodes called sensor devices, which are capable of sensing information like environmental conditions, and collect data from domain areas and sending the data. The emerging new services, like social network, cloud computing and internet of things produced by the digital universe is in stunning speed. Big data are gathered by omnipresent wireless sensor networks, aerial sensory technologies, software logs, information-sensing mobile devices, microphones, cameras, etc.

One of the most highly anticipated key contributions to big data is wireless sensor networks for future developments in networks. Wireless sensor networks (WSNs), with a large number of cheap, small and highly constrained sensor nodes sense the physical world, has wide range of applications both in military and civilian usage, including military sensing and target tracking, environmental monitoring, animal habitats monitoring, disaster management, biomedical health monitoring, critical facilities tracking. It can be used in some hazard environments, like in nuclear power plants. Due to the rewardable advantages, comprehensive attention has been provided to WSNs, and lots of schemes have been proposed. In WSNs, they always suffer from the restricted storage and processing of resources, since the sensor nodes usually consists of limited resources and constrained-power. Therefore, compare to traditional networks, WSNs have their inherent resource constraints and design limitations, such as low bandwidth, short communication range, limited amount of energy, and limited processing and storage in every sensor node. Data aggregation technique reduces energy consumption for WSNs and hence considered as the Holy Grail. Aggregator is a special sensor node provided which has the ability to communication and calculation. Data center used for computing power and storage which process original data collected by sensors and can provide that information to the customers. However, the technique still has the security problems, such as eavesdropping, reply attacks, data forge and data tampering, etc. Hence, designing a secure and efficient data aggregation technique is very practical and significant for WSNs.

II. SYSTEM ARCHITECTURE

In Wireless sensor networks using secure and efficient transmission of data in identity based aggregate signature scheme consists of four main sub divisions.

There are namely: Key Generator, Sensor nodes, Cluster Head, Base Station.

A. WORKING

Sensor nodes, if they want to transmit messages, first they want to register with key server, for this case we make use of key generator to generate unique keys like public and private keys using Elliptic Curve Cryptography (ECC). The same procedure repeats for cluster head and even for base station.

Sensors in order to send the messages to the cluster head they make use of public key of base station and its own private key to generate a shared key for encrypting the message. This encrypted message is sent to the cluster head, where cluster head will aggregate the message and produces the aggregate data and signature for it and sends to the base station. In base station in order to decrypt the message sent form the cluster head it make use of public key of the sensor and using its own private key it generates a shared key which will decrypt the sent messages. If the decrypted message is same as the encrypted messages then we can say that the matching is successful.

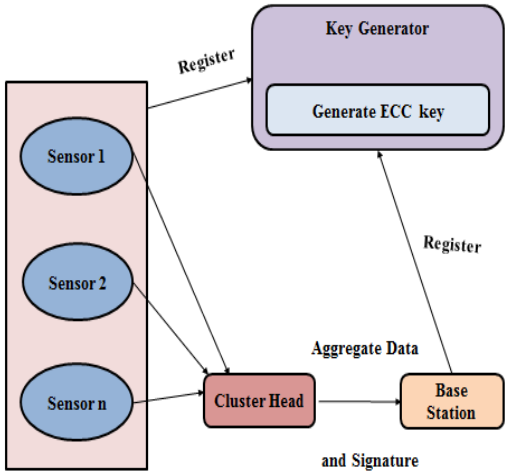

Fig 1: System Architecture

III. LITERATURE SURVEY

A. Enabled Fine-Grained Multi-Keyword Search Supporting Classified Sub-Directories Over Encrypted Cloud Data

In this paper, [1] using cloud computing, individuals can store their data on remote servers and allow them to access to public users by means of the cloud servers. Although outsourced data are likely to contain sensitive privacy information, they are typically encrypted before updated to the cloud. However significantly it limits the usability of outsourced data due to the difficulty of searching over the encrypted data. Here, we overcome this problem by developing the fine-grained multi-keyword search technique over encrypted cloud data. It consists of various folds.

- *Firstly, introduction of the relevance scores and preference factors upon keywords enables the precise keyword search and personalized user experience.*
- *Secondly, development of a practical and very efficient multi-keyword search scheme that supports complicated logic search which is a mixture of "AND", "OR" and "NO" operations of keywords.*
- *Thirdly, employing the classified sub-dictionary techniques to achieve better efficiency on index building, trapdoor generating and query.*
- *Lastly, analyzing the security of the proposed schemes in terms of confidentiality of documents, privacy protection of index and trapdoor, and unlinkability of trapdoor. The security analysis and experimental results demonstration proves that the proposed schemes can achieve the same security level as the existing ones and high performance in terms of functionality, query complexity and efficiency.*

B. An Efficient Privacy-Preserving Outsourced Computation Over Public Data

In this paper, [2] a new efficient privacy-preserving outsourced computation framework over public data, called EPOC is used, which allows a user to outsource the computation of a function over multi-dimensional public data to the cloud when it is preserving the privacy of its function and its output. Accordingly, EPOC has three divisions to overcome the different levels of privacy protection and performance.

- *Firstly, a new cryptosystem called Switchable Homomorphic Encryption with Partially Decryption (SHED) is used as the core cryptographic primitive for EPOC.*
- *Secondly, two coding techniques, called message pre-coding technique and message extending and coding technique are used for messages encrypted under a composite group.*
- *Lastly, a Secure Exponent Calculation Protocol with Public Base (SEPB), which serves as the core sub-protocol in EPOC.*

Complete analysis of the security shows that the proposed EPOC overcomes and achieves its goal of outsourcing computation of a private function over public data without any kind of privacy leakage to unauthorized parties and unauthorized accesses. EPOC is also very efficient in both computation and communications due to performance and extension.

C. Efficient And Privacy-Preserving Outsourced Calculation Of Rational Numbers

In this paper, [3] a framework for efficient and privacy-preserving outsourced calculation of rational numbers, called as POCR is used, which a user can securely outsource the storing and processing of rational numbers to a cloud server without any compromise in the security of the original data and the computed results.

- *Here, we make use of a Paillier cryptosystem with threshold decryption (PCTD), which is the core cryptographic primitive, used to reduce the private key exposure risk.*
- *However, we make use of the toolkits that are required in preserving the privacy of calculation of integers and rational numbers to ensure that commonly used outsourced operations can be handled.*
- *Further, proved that the proposed POCR achieves the goal of secured integer and rational number calculations without resulting in privacy leakage to unauthorized parties, even demonstrating the utility and the efficiency using simulations.*

D. EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid

In this paper, [4] we make use of a adaptive key evolution using the demand response scheme to preserve the privacy of smart grid. Smart grid used here is the next generation of power grid that is emerged recently. It has various features, like distributed energy control, robust to load fluctuations, and close user-grid interaction. A demand response can maintain supply-demand balance and reduce users' electricity bills for smart grid. Accordingly, it is also very important in smart grid to preserve user privacy issues and cyber security.

- *An efficient privacy-preserving demand response (EPPDR) scheme which is used to achieve privacy-preserving demand aggregation and efficient response by making use of a technique called as homomorphic encrption.*
- *Futher, an adaptive key evolution technique is used to make sure that the users' session keys to be forward secure.*
- *Complete analysis of security indicates that EPPDR achieves privacy-preservation of electricity demand, forward secrecy of users' session keys, and evolution of users' private keys.*
- *Finally, comparing with its existing systems it also achieves forward security, and even it has got better efficiency with regards to computation and communication and it can also control the key evolution adaptively to balance between the communication efficiency and security level to check its tradeoff.*

IV.DATA FLOW DIAGRAMS

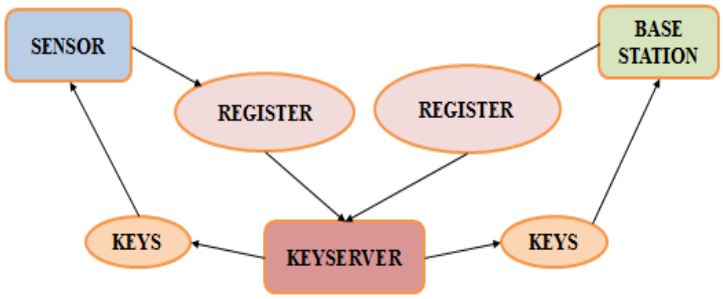

Fig 2: Dataflow diagram for level 1

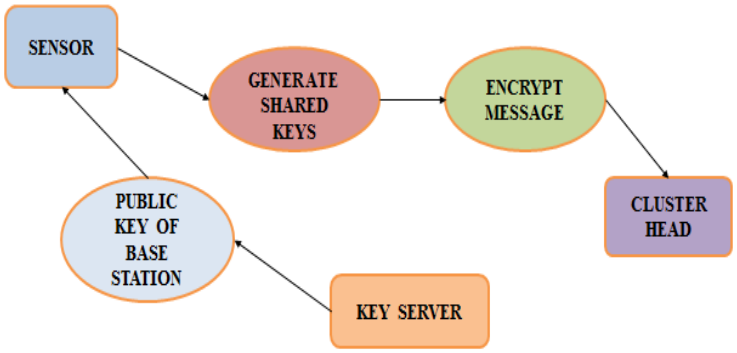

Fig 3: Dataflow diagram for level 2

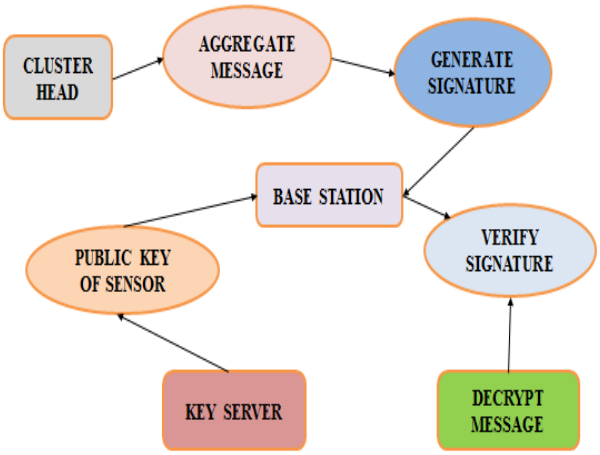

Fig 4: Dataflow diagram for level 3

V. PROBLEM DEFINITION

In an ID-based signature (IBS) system, verification algorithm only involves the signature pair, some public parameters and the identity information of signer, without using an additional certificate. Data tampering, eavesdropping, reply attacks, data forge can be arrised during data transfer. The aggregate signature's validity can be equivalent to the validity of every signature which is used to generate the aggregate signature. The aggregate signature is validity if and only if each individual signer really signed its original message, respectively.

VI. EXISTING SYSTEM

A. IDENTITY-BASED (ID-BASED) CRYPTOGRAPHY SCHEME

- *Introduced by Shamir [7] and they worked on it and proved that, the ID-based cryptography which makes easy for the key management problem by elimination of public key certificates.*
- *The private key generator (PKG), which is used generates and issues privately the corresponding private keys for all users using a master secret key which is known as the trusted third party.*
- *The user's public key is easily generated from this user's any unique identification information in ID-based cryptography, which is assumed that they are publicly known.*
- *Therefore, in existing scheme of ID-based Signature (IBS), we made use of the verification algorithm which only involves some public parameters, signature pair and the identity information of the person signed (signer), which doesnot make use of any additional certificates.*

B. AGGREGATE SIGNATURE SCHEME

- *The aggregate signature scheme was priorly introduced by Boneh et al., [8] which can compress the multiple signatures generated by different users on different messages into a single short message called as aggregate signature in the existing scheme.*
- *It was proved that the aggregated signature is valid if and only if the validity can be same as the validity of every signature which is used to generate the aggregate signature. It means that the aggregate signature is valid if and only if each individual signer really signed its original message.*
- *Hence, reducing storage cost and bandwidth are done by aggregation, and can be used as decisive building block like data aggregation for WSNs, securing border gateway protocols and large scale electronic voting system, etc.*

VII. PROPOSED SYSTEM

A. IDENTITY-BASED AGGREGATE SIGNATURE SCHEME

- *In cluster based method in WSN's [6] [9] combining the highlights of aggregate signature and ID-based cryptography, an ID-based aggregate signature (IBAS) scheme is proposed.*
- *The security model has the capacity to launch any coalition attacks in adversary. We can say the attack is successful, if an adversary can make use of some single signatures including invalid ones to generate a valid aggregate signature.*
- *System model in the proposed system consists of three major components known as data center, aggregator and sensor nodes which are in large numbers. Aggregator works as a cluster head, can produce the aggregate signature and send it to the data center with the messages generated by the sensor nodes.*
- *Although the game is between a challenger and adversary, security model for ID-based aggregate signature technique is introduced. And aggregation algorithm needs to overcome all kinds of coalition attacks that occur.*

- *It includes a designated verifier and proposed technique composes of six probabilistic polynomial time (PPT) algorithms: Setup, Key Generation, Signing, Verification, Aggregation and AggVerification.*
- *The detailed complete security analysis is based on the computational Diffie-Hellman assumption in random oracle model. The proof indicates that ID-based aggregate signature for wireless sensor networks can assure the integrity of the data and reduces the communication and storage cost of the system provided.*

ADVANTAGE

- *The major advantage of ID-based aggregate signature is it reduces band width and storage cost.*
- *It also protects the integrity of data.*

VIII.IMPLEMENTATION

THERE ARE 4 MODULES USED, NAMELY;

- KEY GENERATOR
- SENSOR NODE
- CLUSTER HEAD (AGGREGATOR)
- BASE STATION (DATA CENTER)

A. KEY GENERATOR

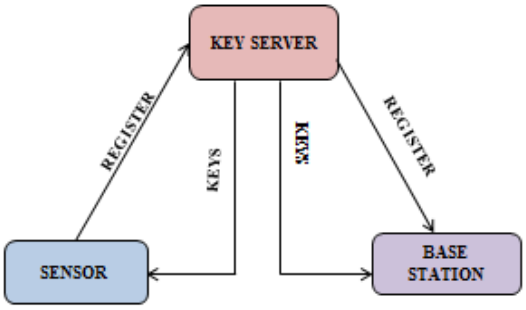

Fig 5: Block diagram for Key generation

- *Private key generator is a key server which generates unique public and private keys for base station and sensor nodes.*
- *Private key generator uses Elliptic Curve Cryptography algorithm to generate keys.*
- *It also shares public keys of sensor and base station.*

B. SENSOR NODE

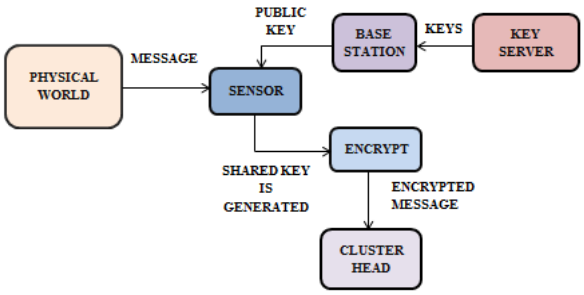

Fig 6: Block diagram for Sensor Node

- *Sensor node has limited resources in terms of computation, memory and battery power. We assume that the PKG generates private key S for each sensor node ID.*
- *When sensor node is deployed, it is embedded with param, SID. Every sensor node ID can use its private key SID to sign messages collecting from the physical world.*
- *In our system, each sensor node belongs to one cluster, sends encrypted messages to their aggregator, and the messages will finally be sent to data center via aggregator.*

C. CLUSTER HEAD (AGGREGATOR)

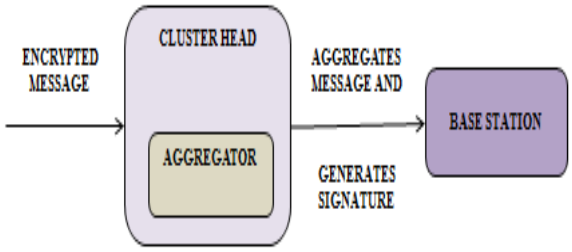

Fig 7: Block diagram for Cluster Head

- *Aggregator is a special sensor node with certain ability to calculation and communication range.*
- *It can sign messages collecting from the physical world, can get the data center's public key (PK) from public channel, can generate the aggregate signature and can send the aggregate signature to the data center.*
- *We assume that the PKG generates the system parameters param, aggregator's private key SID center corresponding to its identifier information ID, then embeds (param, SID) in aggregator when it is deployed.*

D. BASE STATION (DATA CENTER)

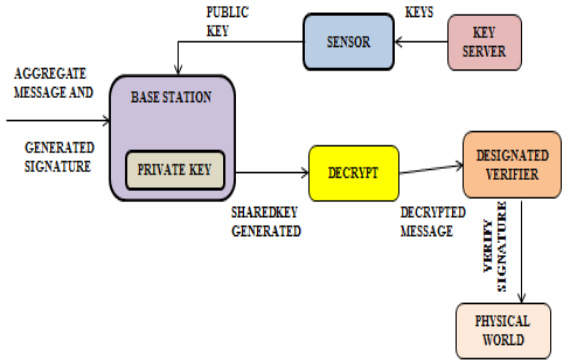

Fig 8: Block diagram for Base Station

- *Data center has a strong computing power and storage space.*
- *It can process all original big data collected by sensor nodes belong to the data center.*
- *It can also provide the data information to consumers.*
- *At the beginning, every data center (as the designated verifier in our IBAS scheme) will receive its public-secret key PK center.*

IX.CONCLUSION

We introduce a novel coalition attack scenario against number of existing PPT algorithms. Moreover, we propose an improvement for ID-Based Aggregate Signature Scheme by providing an initial approximation of trustworthiness of sensor nodes which makes the data not only coalition free, but also more secure and efficient. We make use of Elliptic Curve Cryptography (ECC) and Diffie-Hellman Assumption for the process. In future works we will investigate whether our approach can protect against compromised aggregators to provide privacy over the data transmitted. We also planned to improvement our approach in deployed sensor network.

REFERENCES

[1]. H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou and X. Shen, "Enabling Fine grained Multi-keyword Search Supporting Classified Sub-dictionaries over Encrypted Cloud Data," *IEEE Transactions on Dependable and Secure Computing,* DOI10.1109/TDSC.2015.2406704, 2015.

[2]. X. Liu, B. Qin, R. Deng, Y. Li, "An Efficient Privacy-Preserving Outsourced Computation over Public Data," *IEEE Transactions on Services Computing,* 2015, doi: 10.1109/TSC.2015.2511008.2327-4662 (c) 2016 IEEE. IEEE Internet of Things Journal IEEE INTERNET OF THINGS JOURNAL, VOL. NO: 8

[3]. X. Liu, R. Choo, R. Deng, R. Lu, "Efficient and privacy-preserving outsourced calculation of rational numbers," *IEEE Transactions on Dependable and Secure Computing*, 2016, doi: 10.1109/TDSC.2016.2536601.
[4]. H. Li, X. Lin, H. Yang, X. Liang, R. Lu, and X. Shen, "EPPDR: An Efficient Privacy-Preserving Demand Response Scheme with Adaptive Key Evolution in Smart Grid," *IEEE Transactions on Parallel and Distributed Systems,* vol. 25, no.8, pp. 2053-2064, 2014.
[5]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102-114, 2002.
[6]. G. Gentry and Z. Ramzan, "Identity-based aggregate signatures," *in Proc. Public Key Cryptography*, LNCS vol. 3958, pp. 257-273, 2006.
[7]. A. Shamir, "Identity-based cryptosystems and signature schemes," *in Proc .CRYPTO 1984,* Santa Barbara, California, USA, August 19-22, Springer-Verlag, Berlin LNCS, vol. 196, pp. 47-53, 1984.
[8]. D. Boneh, C. Gentry, B. Lynn and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps", *in Proc. Eurocrypt 2003,* Warsaw, Poland. LNCS, pp. 416-432, 2003.
[9]. J. Xu, Z. Zhang and D. Feng, "ID-Based Aggregate Signatures from Bilinear Pairings," *in Proc. 4th International Conference, CANS 2005*,LNCS vol. 3810, Springer-Veralg, pp. 110-119, 2005.

