International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Securable Identity Based Encryption Technique by Generating Key in Wireless Sensor Network

S. Sushmitha[1], V. Devi[2]
[1]M.E (CSE), NPRCET, Dindigul, Tamil Nadu, India-624401
[2]Department of CSE, NPRCET, Dindigul, Tamil Nadu, India-624401

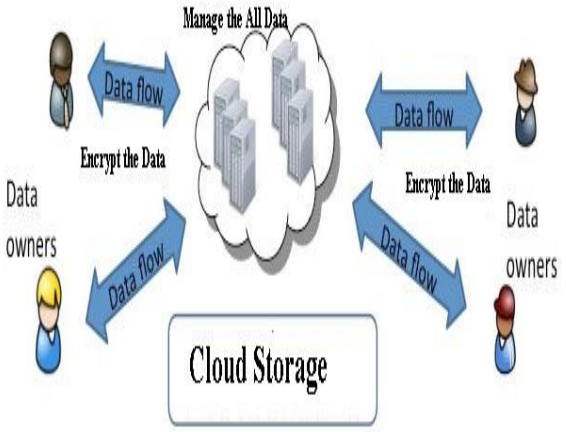
Abstract*—Managing secure and efficient big data aggregation methods are very enticing in the field of wireless sensor networks research. In real settings, the wireless sensor networks have been broadly applied, such as objective tracking and environment remote monitoring. In this paper ID-Based Aggregate Signature Scheme in an ID-based cryptography, the user's public key is easily generated from this user's for unique existence information. Combining the highlights of aggregate signature strategy and ID-based cryptography, we give an ID-based aggregate signature. Information can be easily concede by a vast of attacks, such as information interception and data tampering. It mainly focus on data integrity protection by give an identity-based aggregate signature scheme and also generating a key with a designated verifier for wireless sensor networks. The advantage of aggregate signatures, our scheme not only can keep data integrity, but also can reduce transmission and storage cost for wireless sensor networks.*

***Keywords*—** *Data integration, data tampering, bandwidth and storage cost.*

I. INTRODUCTION

Wireless sensor networks (WSNs), with a large number of cheap, small and highly constrained sensor nodes sense the physical world, has very broad application prospects both in military and civilian usage, including military target tracking and surveillance, animal habitats monitoring, biomedical health monitoring, critical facilities tracking. It can be used in some hazard environments, such as in nuclear power plants. Due to them, remarkable advantages, comprehensive attention has been de-voted to WSNs, and a number of schemes have been sensor nodes are usually resource-limited and power-constrained, they always suffer from the restricted storage and processing resources. Therefore, different from 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 is considered as a Holy Grail to reduce energy consumption for WSNs. However, the technique still has the inherent security problems, such as eavesdropping, reply attacks, data forge and data tampering, etc. Hence, designing a secure and efficient data aggregation method is very significant for WSNs. In an ID-based cryptography, the user's public key is easily generated from this user's any unique identity information.

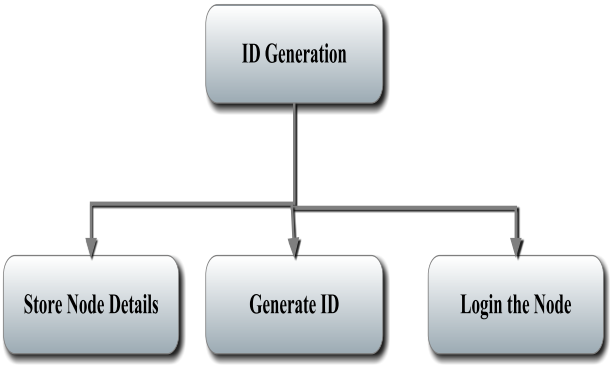
II. ARCHITECTURAL DIAGRAM



III. MODULE DESCRIPTION

ID Generation

In this module ID generation, is based on the node details. Nodes are storing the details and Server check the node details. After checking Server generate the ID for the node. Node login based on that Server generate the ID.

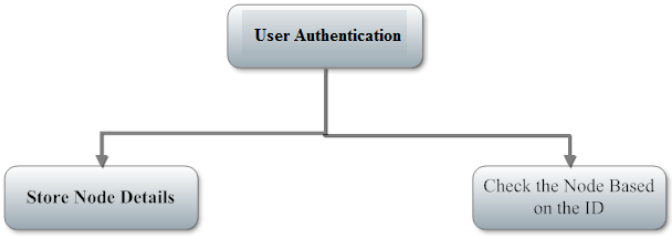


User Authentication

In this module User Authentication, Store the Node Details and Generate the ID for the user. Node login to the Network Server check the node based on the ID Aggregation. After checking Node Details sent to the Server.

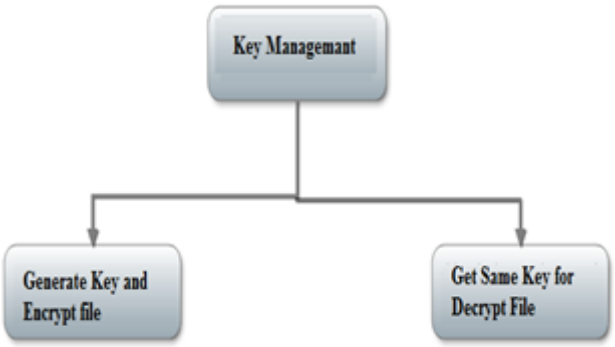
S. Sushmitha and V. Devi, "Securable identity based encryption technique by generating key in wireless sensor network," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 1, pp. 198-199, 2017.

International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024



Key Management

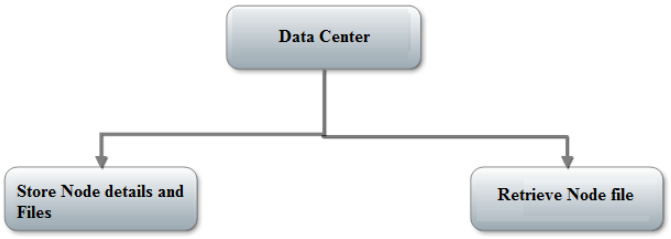
In this section key management is based on the server, that network server generate the key for the file. That key used



to encrypt the file and stored to server. If user want to download the file server verify the user and a file, key to the authenticated user. After receiving the file user decrypt the file.

Data Center

In this module Data Center storage of the all node files. Data center Store the user sending files and Retrieve the user requested file. Data Center Store the file based on user, because it's very easy to find the data from the large data scale.



IV. CONCLUSION

Due to the limited resources of sensor nodes in terms of computation, memory and battery power, secure and energy-save data aggregation methods should be designed in WSNs to reduce the energy cost of data collection, data processing and data transmission. In this paper, we present an ID-based aggregate signature scheme for WSNs, which can compress many signatures generated by sensor nodes into a short one, and also generating the key for providing security to the user information. it can helps to reduce the communication and storage cost. Moreover, we have proved that our IBAS scheme is secure in random oracle model based on the CDH assumption, and we also have proved that our aggregate signature can resist coalition attacks, that is to say the aggregate signature is valid if and only if every single signature used in the aggregation is valid. In our future work, we will focus on designing more efficient data aggregation schemes.

REFERENCES

[1] E. Hargittai, "Is Bigger Always Better? Potential Biases of Big Data Derived from Social Network Sites," 2015.
[2] 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," 2015.
[3] H. Li, D. Liu, Y. Dai, and T. Luan, "Engineering Searchable Encryption of Mobile Cloud Networks: When QoE Meets QoP," 2015.
[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," 2014
[5] H. Li, R. Lu, L. Zhou, B. Yang, X. Shen, "An Efficient Merkle Tree Based Authentication Scheme for Smart Grid," 2014
[6] I. Paik, T. Tanaka, H. Ohashi and W. Chen, "Big Data Infrastructure for Active Situation Awareness on Social Network Services," 2013.
[7] Z. Fu, X. Sun, Q. Liu, L. Zhou, J. Shu, "Achieving Efficient Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Sup-porting Parallel Computing," 2015.

S. Sushmitha and V. Devi, "Securable identity based encryption technique by generating key in wireless sensor network," *International Research Journal of Advanced Engineering and Science*, Volume 2, Issue 1, pp. 198-199, 2017.