International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

SECURED DATA AGGREGATION FOR WIRELESS SENSOR NETWORK USING SYMMETRIC ALGORITHM

Amal B[1], Ashwini H Shetty[2], Nandu Nithyanandan[3]

[1,2,3] *Student, Dept. of Computer Science Engineering, Srinivas School of Engineering, Karnataka, India*

Abstract - *Wireless sensor networks(WSNs) have a wide range of applications towards monitoring and tracking. Since communication of data between nodes consumes the huge amount of energy, sensor nodes are assumed to be unsecured. Therefore, data aggregation is suitable technique to reduce the amount of energy consumption in wireless sensor networks. Data aggregation is the compiling of information from databases with intent to prepare combined datasets for data processing. The main security issues in data aggregation are the integrity of data and confidentiality. In this paper, we propose an efficient way of securing data, by giving an id based signature scheme for wireless sensor networks along with the verifier. This scheme not only reduces storage cost but also provides secured data integrity. The security of this approach is presented based on the computations of advanced encryption algorithm. This improved version of id-based aggregation scheme provides trustworthiness for clients. In future, this approach provides high-security for data by deploying a private cloud for an organization.*

Keywords: Wireless sensor network, Identity-based aggregate signature, Data aggregation, Encryption, Decryption, Data integrity

1.INTRODUCTION

Wireless sensor network has a substantial number of highly contrived, cheap sensor nodes, which can sense the real world. It refers to a group of spatially distributed and dedicated sensors for monitoring and recording the physical conditions of the environment like temperature, level of pollution, wind speed, sound, humidity and so on. It has a wide range of applications both in the military and civilian usage, including military sensing and target tracking, environmental monitoring, animal habitats monitoring, disaster management, biomedical health monitoring, critical facilities tracking. Data from the wireless sensor network are collected and stored in the central location. WSNs always suffer from storage, processing of resources and constrained power. It also consumes a large amount of energy. Data aggregation helps in reducing energy consumption and it is also knowns as 'Holy Grail'.

Data aggregation is the method of collecting the data, processing and summarizing it in a report format for future use. All the aggregated data is stored in the database, and relevant data is provided to end user based on their requests. Providing security to the aggregated data is known as secured data aggregation.

Data aggregation faces two main security issues that are confidentiality and integrity of data. Confidentiality is referred as rules that limit access to data or information where access to these-information can be restricted by authentication. Authentication means identification that is confirming sender and receiver's identity or confirming source and destination of the information. Usually username, passwords are used to authorize the user. These passwords have some protocols which make third-party hard to guess a password. Integrity of data is referred as maintaining accuracy, consistency, and trustworthiness of data. In this process information in the storage cannot be changed by third-party.

Confidentiality and Integrity of data can be achieved by cryptography. Cryptography is a method of transforming data into unreadable code formats and vice versa. Transforming data into the unreadable format is known as encryption and its reverse process is known as decryption. Normally symmetric and asymmetric methods are used for encryption. This paper focuses on the symmetric method where we use AES algorithm for both encryption and decryption.

In this paper we basically explain id based data aggregation system. based on user's identification we aggregate the data in data center. User's identification may be his password or username or it can be anything.

2. LITERATURE SURVEY

Each user can generate different signatures on different messages. So these signatures can be compressed to form an aggregated signature.

Boneh et al. [1] came up with the concept and in 2003 he introduced structure of aggregate signature scheme. After that many signature schemes had been proposed in [4][5][6][7]. But it was not an efficient method as these schemes had lot of problems involved. Later they came up with public key infrastructure(PKIs) where the public key is not associated or related with user's identification. It is an random string to be generated. This improves the storage cost, computations, and it also solves many problems related to id based cryptography. Since it generates random string, it needs

an trusted certificate authority for these keys. These id based cryptography schemes can be explained in [8][9][10][11]. In [12][13] they explained about public key infrastructure and in [14][15][16][17][18] they explained about certificateless public key cryptography. But in [17] and [19] they explained drawbacks of certificateless public key cryptography. In [16] it explains different kind of attacks. In [2] it involves lots of wastage of time and network bandwidth. In [3] it involves partial aggregation as well as complex calculations. In Cheng et al. [20] scheme achieves full aggregation and also seems efficient. But not based on signatures. In recent paper [21] scheme achieves aggregation using asymmetric methods in which it mainly focus on designing the aggregate signature scheme .

But in our paper we mainly focus on simplest and efficient way of achieving aggregation using symmetric methods which can resist coalition attacks.

3.PROPOSED SYSTEM

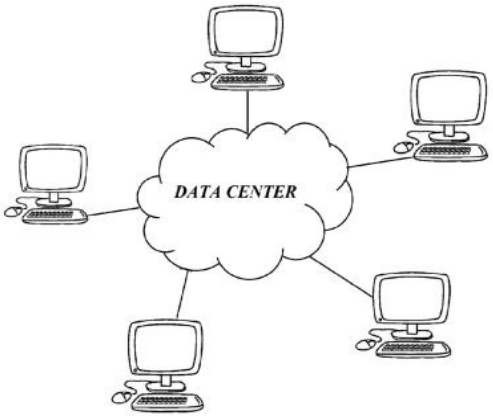

Fig -1: System Architecture

Fig. 1 gives a rough idea about our system. Here multiple nodes can exchange files with each other through data center. Data center stores all the files and aggregate files based on signature. Each node can access files from other nodes if it is present under their signature. At first each node must be registered. Each user must login with their corresponding user-id and password. This is to make sure that authentication is successful. Once the verification is complete each user can either upload a file to data-center or can download a file from data-center.

Fig-2 explains the process about uploading a file to data-center. It has a following steps:

1. Choose a file from system.

2. Generate a OTP for file.

3. Click on upload button.

4. When upload button is pressed, the file is encrypted then it is signed with the digital signature.

5. Then uploaded to the data-center.

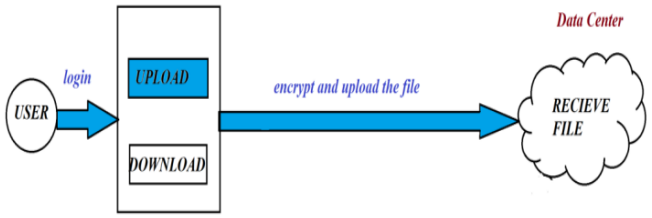

Fig -2: Block Diagram for Sender Site

Once the file is uploaded to data-center, based on the signature the files are aggregated. These aggregated files are stored in data-center. Each user can see only aggregated files stored under his signature. Files that are stored under other user's signature is not visible for him. Fig-3 explains the process about downloading a file from datacenter.

It has a following steps:

1. Choose a file from the list of files present under his signature.

2. Click on download button.

3. When download button is pressed, the file is verified with the digital signature and then it is decrypted.

4. Then downloaded to user's system

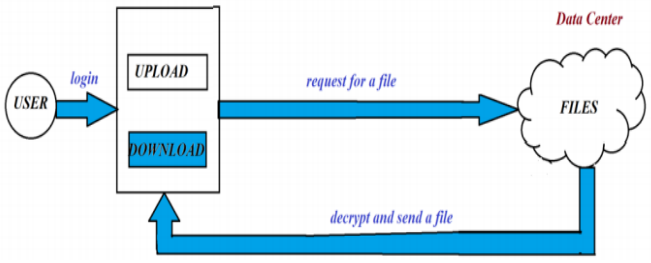

Fig -3: Block Diagram for Receiver Site

4.IMPLEMENTATIONS AND RESULTS

In this section we explain performance of id based aggregation scheme and also we evaluate these scheme based on aggregation and Un-aggregation scheme comparison:

Here we compare performance of these schemes. Performance of aggregated and un-aggregated schemes are shown below:

	Sensor node → Data center
Aggregation scheme	$\{2(n-1)\cdot\|G\|+\|M'\|+\|ID'\|\}+\{2n\cdot\|G\|+\|M\|+\|ID\|\}$
Un-aggregation scheme	$\{2(n-1)\cdot\|G\|+\|M'\|+\|ID'\|\}+\{(n+1)\cdot\|G\|+\|M\|+\|ID\|\}$

here, |M| indicates the overall length of {m1, m2, . . . , mn} . |M′ | indicates the overall length of {m1, m2, . . . , mn−1}. |ID| indicates the overall length of {ID1, ID2, . . . , IDn} . |ID′ | indicates the overall length of {ID1, ID2, . . . , IDn−1}. |G| indicates cyclic group

Performance can also be compared in terms of computation costs and communication costs.

Communication cost reduces (n-1) transfer of data aggregation in cyclic group. Hence it can also reduce (n-1) storage. Therefore cost of storage can also be reduced.

Since it can reduce transfer of data, computations can also be reduced . Hence it is feasible and performance can also be improved.

5.CONCLUSIONS

To reduce an amount of energy consumption in wireless sensor networks, we use data aggregation. In this paper, we propose data aggregation system for WSNs by providing a privacy for data, which can reduce storage cost. As we make use of digital signature and encryption-decryption techniques for files, it is more secure and efficient. In future, this system can be improved by deploying a private cloud for an organization that not only provides high-security for data but also can transfer files more quickly compared to other systems.

REFERENCES

[1] 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.

[2] X. Liu, H. Zhu, J. Ma, Q. Li and J. Xiong, “Efficient attribute based sequential aggregate signature for wireless sensor networks,” International Journal of Sensor Networks, vol. 16, no. 3, pp. 172-184, 2014.

[3] Y. Zhang, L. Sun, H. Song, et al., “Ubiquitous WSN for Healthcare: Recent Advances and Future Prospects,” Internet of Things Journal IEEE, 2014, vol. 1, no. 1, pp. 311-318, 2014.

[4] A. Lysyanskaya, S. Micali, L. Reyzin and H. Shacham, “Sequential aggregate signatures from trapdoor permutations”, in Proc. EUROCRYPT 2004, LNCS vol. 3027, pp. 74-90, 2004.

[5] A. Boldyreva, C. Gentry, A. O’Neill and D.H. Yum, “Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing”, in Proc. ACM Conference on Computer and Communications Security (CCS’2007), pp. 276-285, 2007.

[6] J.H. Ahn, M. Green and S. Hohenberger, “Synchronized aggregate signatures: new definitions, constructions and applications”, in Proc. ACM Computer and Communications Security (CCS’2010), pp. 473-484, 2010.

[7] Z. Shao, “Enhanced aggregate signatures from pairings,” in Proc. CISC 2005, LNCS 3822, Springer-Verlag, pp. 140-149, 2005.

[8] 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-Verlag, pp. 110-119, 2005

[9] G. Gentry and Z. Ramzan, “Identity-based aggregate signatures,” in Proc. Public Key Cryptography, LNCS vol. 3958, pp. 257-273, 2006.

[10] J. Herranz, “Deterministic identity-based signatures for partial aggregation,” The Computer Journal, vol. 49, no. 3, pp. 322-330, 2006.

[11] S.S.D. Selvi, S.S. Vivek, J. Shriram et al., “Identity based partial aggregate signature scheme without pairing,” in Proc. 35th IEEE. Sarnoff Symposium (SARNOFF), pp. 1-6, 2012.

[12] J. Li, K. Kim, F. Zhang and X. Chen, “Aggregate proxy signature and verifiably encrypted proxy signature,” in Proc. the International Conference on Provable Security, LNCS 4784, SpringerVeralg, pp. 208- 217, 2007.

[13] Y. Wen, J. Ma and H. Huang, “An Aggregate Signature Scheme with Specified Verifier,” Chinese Journal of Electronics, vol. 20, no. 2, pp. 333-336, 2011.

[14] Z. Gong, Y. Long, X. Hong and K. Chen, “Two certificateless aggregate signatures from bilinear maps,” in Proc. SNPD 2007, IEEE Press, Qingdao, China, pp. 188-193, 2007.

[15] L. Zhang, B. Qin, Q. Wu and F. Zhang, “Efficient many-to-one authentication with certificateless aggregate signatures,” Computer Networks, vol. 54, no. 14, pp. 2482-2491, 2010.

[16] H. Xiong, Z. Guan, Z. Chen and F. Li, "An efficient certificateless aggregate signature with constant pairing computations," Information Sciences, vol. 219, no. 10, pp. 225-235, 2013.

[17] F. Zhang, L. Shen and G. Wu, "Notes on the security of certificateless aggregate signature schemes," Information Sciences, vol. 287, pp. 32-37, 2014.

[18] S. Horng, S. Tzeng, P. Huang, X. Wang et al, "An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," Information Sciences, vol. 317, pp. 48-66, 2015.

[19] D. He, M. Tian and J. Chen, "Insecurity of an efficient certificateless aggregate signature with constant pairing computations," Information Sciences, vol. 268, pp. 458-462, 2014.

[20] Xiangguo Cheng, Jingmei Liu, and Xinmei Wang. Identity-based aggregate and verifiably encrypted signatures from bilinear pairing. In Computational Science and Its Applications - ICCSA 2005,, volume 3483 of Lecture Notes in Computer Science, pages 1046–1054. Springer, 2005.

[21] "A Secure and Efficient ID-Based Aggregate Signature Scheme for Wireless Sensor Networks" by Limin Shen, Jianfeng Ma, Member, IEEE, Ximeng Liu, Member, IEEE, Fushan Wei and Meixia Miao[2016-2017]