Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 5, Issue. 11, November 2016, pg.52 – 56

SECURABLE IDENTITY BASED ENCRYPTION TECHNIQUE FOR WIRELESS NETWORK

S.SUSHMITHA, V.DEVI
M.E-CSE, Head of the Department
NPR College Engineering and Technology
sushmi633@gmail.com, devivenkataswamy@gmail.com

Abstract- Affirmative secure and efficient big data amalgamate methods is very attractive in the field of wireless sensor networks research. In real settings, the wireless sensor networks have been broadly applied, such as target tracking and environment remote oversight. However, data can be easily compromised by a vast of attacks, such as data interception and data tampering, etc. In this paper, we mainly focus on data integrity shelter; give an identity-based entirety signature scheme with a designated verifier for wireless sensor networks. According to the advantage of entirety signatures, our scheme not only can keep data integrity, but also can reduce bandwidth and storage cost for wireless sensor networks. Furthermore, the security of our identity-based entirety signature scheme is rigidly presented based on the Triple DES assumption in random oracle model.

Keywords: big data, wireless sensor network, identity- based, data aggregation, unforetold, aggregate signature, coalition attack, designated verifier.

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. RELATED WORK

A. Efficient many-to-one authentication with certificate less aggregate signatures

Aggregate signatures allow an efficient algorithm to aggregate n signatures of n distinct messages from n different users into one single signature. The resulting aggregate signature can convince a verifier that the n users did indeed sign the n messages. This feature is very attractive for authentications in bandwidth-limited applications such as reverse multicasts and senor networks. Certificateless public key cryptography enables a similar functionality of public key infrastructure (PKI) and identity (ID) based cryptography without suffering from complicated certificate management in PKI or secret key escrow problem in ID-based cryptography. In this paper, we present a new efficient certificate less aggregate signature scheme which has the advantages of both aggregate signatures and certificate less cryptography. The scheme is proven existentially unforgeable against adaptive chosen-message attacks under the standard

computational Diffie–Hellman assumption. Our scheme is also very efficient in both communication and computation and the proposal is practical for many-to-one authentication.

B. On security of a Certificate less Aggregate Signature Scheme

Aggregate signatures are useful in special areas where the signatures on many different messages generated by many different users need to be compressed. Very recently, Xiong et al. proposed a certificate less aggregate signature scheme provably secure in the random oracle model under the Computational Diffie-Hellman assumption. Unfortunately, by giving two kinds of concrete attacks, we indicate that the certificate less aggregate signature scheme of Xiong et al. does not meet the basic requirement of unforgeability.

C. A note on 'An efficient certificateless aggregate signature with constant pairing computations'

Recently, Xiong et al. [H. Xiong, Z. Guan, Z. Chen, F. Li, An efficient certificate less aggregate signature with constant pairing computations, Information Science, 219, pp. 225–235, 2013] proposed an efficient certificate less signature (CLS) scheme and used it to construct a certificate less aggregate signature (CLAS) scheme with constant pairing computations. They also demonstrated that both of the two schemes are provably secure in the random oracle model under the computational Diffie-Hellman assumption. Unfortunately, by giving concrete attacks, we point out that Xiong et al.'s schemes are not secure in their security model.

D. Achieving Effective Cloud Search Services: Multi-keyword Ranked Search over Encrypted Cloud Data Supporting Synonym Query

In recent years, consumer-centric cloud computing paradigm has emerged as the development of smart electronic devices combined with the emerging cloud computing technologies. A variety of cloud services are delivered to the consumers with the premise that an effective and efficient cloud search service is achieved. For consumers, they want to find the most relevant products or data, which is highly desirable in the "pay-as-you use" cloud computing paradigm. As sensitive data (such as photo albums, emails, personal health records, financial records, etc.) are encrypted before outsourcing to cloud, traditional keyword search techniques are useless. Meanwhile, existing search approaches over encrypted cloud data support only exact or fuzzy keyword search, but not semantics-based multi-keyword ranked search. Therefore, how to enable an effective searchable system with support of ranked search remains a very challenging problem. This paper proposes an effective approach to solve the problem of multi-keyword ranked search

over encrypted cloud data supporting synonym queries. The main contribution of this paper is summarized in two aspects: multi-keyword ranked search to achieve more accurate search results and synonym-based search to support synonym queries. Extensive experiments on real-world dataset were performed to validate the approach, showing that the proposed solution is very effective and efficient for multi- keyword ranked searching in a cloud environment 1.

E. Big Data Infrastructure for Active Situation Awareness on Social Network Services

Awareness computing aims at our final goal in computer science to simulate human's awareness and cognition. Awareness of social network knowledge in everyday life is actively enabled by big data society. In this paper, we investigate infrastructure for big data analytics for social network services, and propose TF-IDF calculation on big data infrastructure to be aware of social relations on social networks.

III. 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, i.e., it can reduce the communication and storage cost. Moreover, we have proved that our IBAS scheme is secure in random oracle model based on the Triple DES 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.

REFERENCES

- I. Paik, T. Tanaka, H.Ohashi and W. Chen, "Big Data Infrastructure for Active Situation Awareness on Social Network Services", 2013.
- E. Hargittai, "Is Bigger Always Better? Potential Biases of Big Data Derived from Social Network Sites," 2015.
- 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.

- I. Hashem, I. Yaqoob, N. Anuar, et al., "The rise of "big data" on cloud computing: Review and open research issues," 2015
- 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.
- H. Li, D. Liu, Y. Dai and T. Luan, "Engineering Searchable Encryption of Mobile Cloud Networks: When QoE Meets QoP,",2015.
- X. Liu, B. Qin, R. Deng, Y. Li, "An Efficient Privacy-Preserving Out-sourced Computation over Public Data," 2015.
- X. Liu, R. Choo, R. Deng, R. Lu, "Efficient and privacy-preserving out-sourced calculation of rational numbers" , 2016
- 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

