Grenze Int. J. of Engineering and Technology, Vol. 1, No. 1, January 2015

SET for Cluster-based Cloud Computing: A Survey

Neelambike S[1] and Dr. B P Mallikarjunaswamy[2]
[1] Assistant professor, GM Institute of Technology,Davangere
Email: neelais@gmail.com
[2] Professor, Sri Siddhartha Institute of Technology, Tumkur
Email: drbpmswamy@rediffmail.com

***Abstract*— secure data transmission is a critical issue for Cloud computing networks. Clustering is an effective and practical way to enhance the system performance of cloud. Paper provides study about a secure data transmission for cluster-based cloud (CCNs), where the clusters are formed dynamically and periodically. The paper proposes two Secure and Efficient data Transmission (SET) protocols for CCNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for Cloud, while its security relies on the hardness of the discrete logarithm problem. The paper shows the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The expected results of using the proposed protocols is the increase in performance of the existing secure protocols for CCNs, in terms of security overhead and energy consumption.**

***Index Terms*— SET;SET-IBS;SET-Iboos;Cloud;CCN.**

I. INTRODUCTION

In existing System of Cloud computing networks, Secured socket layer (SSL) is being used to provide the security for efficient data transmission. A disadvantage of SSL Just because a site uses SSL to secure personal data does not mean it is completely safe. As research conducted by ethical hackers show, as many as 30 percent of SSL sites are unsafe [1].

In the Proposed System, Secure and efficient data transmission is thus especially necessary and is demanded in many such practical CCNs. So this paper proposes two Secure and Efficient data Transmission (SET) protocols for CCNs, called SET-IBS and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively. Advantages of proposed system This paper has been proposed in order to reduce the computation and storage costs of encrypting data, by applying digital signatures to message packets, which are efficient in communication and also applying the key management for security. So, the transactions are secured by using the digital signatures.

II. LITERATURE REVIEW

In Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks [2] paper the results

Grenze ID: 01.GIJET.1.1.509

show that SET-IBS and SET-IBOOS protocols provides better performance for efficient data transmission in Cluster based wireless sensor networks. For achieving the efficient data transmission in cloud network introduces the same two protocols [SET-IBS and SET-IBOOS].

Cluster-based data transmission in WSNs has been investigated by researchers in order to achieve the network scalability and management, which maximizes node lifetime and reduce Bandwidth consumption by using local collaboration among sensor nodes [3]. Using the clustering algorithms easily identified which cloud is free then allocates the task to that particular cloud to achieve the specific task.

Adding security to LEACH-like protocols is challenging, because they dynamically, randomly and periodically rearrange the network's clusters and data links [4]. These same concepts are used in proposed system for making the dynamic clusters for achieving the fast and efficient result.

The symmetric key management for security, which suffers from a so-called orphan node problem [5]. This problem occurs in CWSNs when a node does not share a pairwise key with others in its preloaded key ring. In order to mitigate the storage cost of symmetric keys, the key ring in a node is not sufficient for it to share pairwise symmetric keys with all of the nodes in a network. In proposed work uses the symmetric key management for achieving the key exchange.

The feasibility of the asymmetric key management has been shown in WSNs recently, which compensates the shortage from applying the symmetric key management for security [6]. Digital signature is one of the most critical security services offered by cryptography in asymmetric key management systems, where the binding between the public key and the identification of the signer is obtained via a digital certificate [7]. The Identity-Based digital Signature (IBS) scheme [8], based on the difficulty of factoring integers from Identity-Based Cryptography (IBC), is to derive an entity's public key from its identity information, e.g., from its name or ID number. Recently, the concept of IBS has been developed as a key management in WSNs for security. Carman [9] first combined the benefits of IBS and key pre-distribution set into WSNs, and some papers appeared in recent years [10–11]. The IBOOS scheme has been proposed in order to reduce the computation and storage costs of signature processing. A general method for constructing online/offline signature schemes was introduced by Even et al. [12]. The IBOOS scheme could be effective for the key management in WSNs. Specifically; the offline phase can be executed on a sensor node or at the BS prior to communication, while the online phase is to be executed during communication. Some IBOOS schemes are designed for WSNs afterwards, such as [13] and [14]. The offline signature in these schemes, however, is precompiled by a third party and lacks reusability, thus they are not suitable for CWSNs.

Proposes two **S**ecure and **E**fficient data **T**ransmission (SET) protocols for CCNs, called **SET-IBS** and **SET-IBOOS**, by using the **IBS** scheme and the **IBOOS** scheme, respectively. The key idea of both SET-IBS and SET-IBOOS is to authenticate the encrypted data, by applying digital signatures to message, which are efficient in communication and applying the key management for security. In the proposed protocols, secret keys and pairing parameters are distributed and preloaded in all cloud, which overcomes the key escrow problem described in ID-based crypto-systems [15].

Our objective is to build a fully secured data transmission for cluster-based cloud (CCNs), where the clusters are formed dynamically and periodically. The paper proposes two Secure and Efficient data Transmission (SET) protocols for CCNs, called SET-IBS[16] and SET-IBOOS, by using the Identity-Based digital Signature (IBS) scheme and the Identity-Based Online/Offline digital Signature (IBOOS) scheme, respectively[16,17].

SET Protocol: In this module, Secure and Efficient data Transmission (SET) protocol for CCNs. The SET-IBOOS protocol is designed with the same purpose and scenarios for CCNs with higher efficiency. The proposed SET-IBOOS operates similarly to the previous SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. First introduce the protocol initialization, and then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards.

Key management for security: In this module, security is based on the each services request from the client. The corresponding private pairing parameters are preloaded in the cloud during the protocol initialization. The IBOOS scheme in the proposed SET-IBOOS consists of following four operations, extraction, offline signing, online signing and verifications.

Key management: In this Module, the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security.

Storage cost: In this module, represents the requirement of the security keys stored in each service provider.

Network scalability: In this module, indicates whether a security protocol is able to scale without compromising the security requirements. Here, "comparative low" means that, compared with SET-IBS and

SET-IBOOS, in the secure data transmission with a symmetric key management, the larger network scale increases.
Communication overhead: In this module, the security overhead in the data packets during communication.
Computational overhead: In this module, the energy cost and computation efficiency on the generation and verifications of the certificates or signatures for security.
Attack resilience: In this module, the types of attacks that security protocol can protect against.

III. Conclusions

In this paper, first reviews the data transmission issues and the security issues in CCNs. The deficiency of the symmetric key management for secure data transmission has been discussed. We then presented two secure and efficient data transmission protocols respectively for CCNs, SET-IBS and SET-IBOOS. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based crypto-system, which achieves security requirements in CCNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management.

Acknowledgment

The authors wish to thank My Guide Dr. B.P. Mallikarjunaswmay for his valuable support and suggestion for preparing papers, my grateful thanks to my brother and mother and sisters for their valuable supports.

References

[1] David Wagner and Bruce Schneier, "Analysis of the SSL 3.0 protocol" in Revised April 15, 1997.
[2] Huang Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, Mohsen Guizani, Fellow, IEEE, "Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM YEAR 2013.
[3] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Comput. Commun.*, vol. 30, no. 14-15, pp.2007.
[4] 2826–2841, 2007. L. B. Oliveira, A. Ferreira, M. A. Vilac¸a *et al.*, "SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. 87, pp. 2882–2895, 2007.
[5] L. B. Oliveira, A. Ferreira, M. A. Vilac¸a *et al.*, "SecLEACH-On the security of clustered sensor networks," *Signal Process.*, vol. 87, pp. 2882–2895, 2007.
[6] S. Sharma and S. K. Jena, "A Survey on Secure Hierarchical Routing Protocols in Wireless Sensor Networks," in *Proc. ICCCS*, 2011, pp.146–151.
[7] G. Gaubatz, J. P. Kaps, E. Ozturk *et al.*, "State of the Art in Ultra-Low Power Public Key Cryptography for Wireless Sensor Networks," in *Proc. IEEE PerCom Workshops*, 2005, pp. 146–150.
[8] W. Diffie and M. Hellman, "New Directions in Cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.
[9] A Shamir, "Identity-Based Cryptosystems and Signature Schemes," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1985, vol. 196, pp. 47–53.
[10] D. W. Carman, "New Directions in Sensor Network Key Management," *Int. J. Distrib. Sens. Netw.*, vol. 1, pp. 3–15, 2005.
[11] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures," in *Proc. IEEE CIT*, 2010, pp. 882–889.
[12] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital Signature," in *Proc. IEEE GLOBECOM*, 2010, pp. 1–5.
[13] J. Sun, C. Zhang, Y. Zhang *et al.*, "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 9, pp. 1227–1239, 2010.
[14] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," in *Lect. Notes. Comput. Sc. - CRYPTO*, 1990, vol. 435, pp. 263–275.
[15] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multisignatures for AODV and DSR Routing Security," in *Lect. Notes. Comput. Sc. - Inf. Secur. Privacy*, 2006, vol. 4058, pp. 99–110.
[16] J. Liu, J. Baek, J. Zhou *et al.*, "Efficient online/offline identity-based signature for wireless sensor network," *Int. J. Inf. Secur.*, vol. 9, no. 4, pp. 287–296, 2010.
[17] Y. Jararweh, Z. Alshara, M. Jarrah, M. Kharbutli, M. Alsaleh, "Teachcloud: a cloud computing educational toolkit", Proceedings of the 1st International IBM Cloud Academy Conference (ICA CON 2012), IBM, Research Triangle Park, NC, USA, 2012.