International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
www.ioirp.com ISSN: 2394-6364, Volume – 1, Issue – 8. July 2015

SECURE DATA SHARING IN WSN INTEGRATED MULTI CLOUD ENVIRONMENT

P.Madhubala[1],M.Savitha Devi[2]
[12]Research scholar, Mother Theresa Women's University, India

***Abstract*— Wireless networks in small or large coverage are increasingly popular as they promise the expected convergence of data services to users. Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. When the WSN is integrated with CLOUD the extensive amount of data can be stored in the scalable cloud storage. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. Therefore for en effective third party auditor (TPA), the following fundamental requirements have to be met should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user. In this article we proposed a public auditing system of data storage security and a privacy-preserving auditing protocol for the data outsourced in the WSN-Cloud integrated environment.**

Keywords*— *WSN, CLOUD, Privacy Preserving, Security

I. INTRODUCTION

Cloud Computing has been envisioned as the next-generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced into the Cloud. From users' perspective, including both individuals and enterprises, storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc . While these advantages of using clouds are unarguable, due to the opaqueness of the Cloud as separate administrative entities, the internal operation details of cloud service providers (CSP) may not be known by cloud users—data outsourcing is also relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time. Secondly, for the benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully. Towards the cloud users regarding the status of their outsourced data. Examples include cloud service providers, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed, or even hiding data loss incidents so as to maintain a reputation. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture.

II. CLOUD COMPUTING

As users no longer physically possess the storage of their data, traditional cryptographic prim- itives for the purpose of data security protection cannot be directly adopted. Thus, how to effi- ciently verify the correctness of outsourced cloud data without the local copy of data files becomes a big challenge for data storage security in Cloud Computing. Note that simply downloading the data for its integrity verification is not a practical solution due to the expensiveness in I/O cost and transmitting the file across the network. Besides, it is often insufficient to detect the data corruption when accessing the data, as it might be too late for recover the data loss or damage.

Considering the large size of the outsourced data and the user's constrained resource capability, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. Therefore, to fully ensure the

data security and save the cloud users' computation resources, it is of critical importance to enable public auditability for cloud data storage so that the users may resort to a third party auditor (TPA), who has expertise and capabilities that the users do not, to audit the outsourced data when needed. Based on the audit result, TPA could release an audit report, which would not only help users to evaluate the risk of their subscribed cloud data services, but also be beneficial for the cloud service provider to improve their cloud based service platform . In a word, enabling public risk auditing protocols will play an important role for this nascent cloud.

III. WIRELESS SENSOR NETWORKS

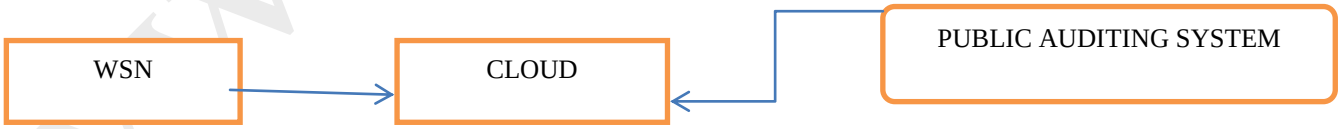
WSN is a network formed by large number of sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure etc…WSN devices have severe resource constraints in terms of energy, computation and memory.Key Management include the processes of key setup, the initial distribution of keys and key revocation (removal of the compromised key).Many Security-critical application that depend on key management processes demand a high level of fault tolerance when a node is compromised. WSNs are widely deployed in diverse arenas the most important ones are Health care, environment, and weather, military, forecasting, Internetof things (IoT), smart homes and offices. Fast adopting of wireless sensor networks, mandate to link sensors with one another to build situation-aware applications and make accessiblesensor-derived data via various Web-based social networks or virtual communities.Further, with the scale of WSN enlarging, the data volume is very huge, data source type is heterogeneous and process ability of WSN platform is very Limited, which are barriers forWSN's data to be efficiently managed, stored and analyzed.Cloud computing make a better use of distributed resources, put them together in order to achieve higher throughput, and be able to tackle large-scale computational problems.

IV. CLOUD INTEGRATED WIRELESS SENSOR NETWORKS

With the faster adoption of wireless sensor networks (WSNs),on the one hand sensor-derived data need to be accessed via various Web-based social networks or virtual communities and on the other hand, limited processing ability of WSNs is a hurdle. To address this issue WSNs can be integrated with cloud. Cloud enjoys ample processing ability and it is a capable infrastructure to deliver people-centric and context-aware services to users, thus expedites adoption of WSNs. In this article we utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for integrated WSN-CLOUD data storage security while keeping all above requirements in mind. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users.

V. PROPOSED SYSTEM

We introduced the following modules for batch auditing in our system to maintain the data storage security in WSN-CLOUD environment.



- PRIVACY-PRESERVING PUBLIC AUDITING MODULE
- BATCH AUDITING MODULE
- DATA DYNAMICSMODULE

A. PRIVACY-PRESERVING PUBLIC AUDITING MODULE

Homomorphic authenticators are unforgettable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, we propose to uniquely

integrate the homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF).

The proposed scheme is as follows:

- Setup Phase
- Audit Phase

BATCH AUDITING MODULE

With the establishment of privacy-preserving public auditing in Cloud Computing, TPA may concurrently handle multiple auditing delegations upon different users' requests. The individual auditing of these tasks for TPA can be tedious and very inefficient. Batch auditing not only allows TPA to perform the multiple auditing tasks simultaneously, but also greatly reduces the computation cost on the TPA side.

DATA DYNAMICS MODULE

Hence, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now we show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. We can adopt this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics.

VI. ALGORITHM FOR PUBLIC AUDITING SYSTEM

- A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, and VerifyProof).
- KeyGen: key generation algorithm that is run by the user to setup the scheme
- SigGen: used by the user to generate verification metadata, which may consist of MAC, signatures or other information used for auditing
- GenProof: run by the cloud server to generate a proof of data storage correctness
- VerifyProof: run by the TPA to audit the proof from the cloud server

We utilized the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously.

VII. CONCLUSION

In this article, we proposed a privacy-preserving public auditing system for data storage security in WSN integrated with Cloud Computing, where TPA can perform the storage auditing without demanding the local copy of data. We utilize the homomorphic authenticator and random mask technique to guarantee that TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner, i.e., simultaneously. Extensive security and performance analysis shows that the proposed schemes are provably secure and highly efficient.

Acknowledgment

I would like to express my sense of gratitude to DON BOSCO COLLEGE, Dharmapuri for their support and encouragement. And also I like to thank MOTHER THERESA WOMEN'S UNIVERSITY, Kodaikanal for providing me the opportunity to carry out the research work in Cloud Computing. Finally I like to thank my Research Supervisor Dr.P.Thangaraj for his guidance and valuable suggestions.

www.ioirp.com

References

[1] A. Agarwal and A. Agarwal, "The Security Risks Associated with Cloud Computing," *International Journal of Computer Applications in Engineering Sciences*, vol. 1,pp. 257-259, 2011.

[2] N. Tirthani and R. Ganesan, "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography," *IACR Cryptology ePrint Archive*, vol. 2014,p. 49, 2014.

[3] P. Rewagad and Y. Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing," in *Communication Systems and Network Technologies (CSNT), 2013 International Conference on*, 2013, pp. 437-439.

[4] Ravi Gharshi and Suresha, "Enhancing Security in Cloud Storage using ECC Algorithm," *International Journal of Science and Research*, vol. 2,no. 7, pp. 59-64, 2013.

[5] Arijit Ukil, *et al.*, "A Security Framework in Cloud Computing Infrastructure," *International Journal of Network Security & Its Applications*, vol. 5,no. 5, pp. 11-24, 2013.

[6] P. Ayers, "Securing and controlling data in the cloud," *Computer Fraud & Security*, vol. 2012,no. 11, pp. 16-20, 2012.

[7] S. K. Sood, "A combined approach to ensure data security in cloud computing," *Journal of Network and Computer Applications*, vol. 35,no. 6, pp. 1831-1838, 2012.

[8] M. A. AlZain, *et al.*, "A new model to ensure security in cloud computing services," *Journal of Service Science Research*, vol. 4,no. 1, pp. 49-70, 2012.

[9] D. A. Fernandes, *et al.*, "Security issues in cloud environments: a survey," *International Journal of Information Security*, vol. 13,no. 2, pp. 113-170, 2014.

[10] N. Gonzalez, *et al.*, "A quantitative analysis of current security concerns and solutions for cloud computing," *Journal of Cloud Computing*, vol. 1,no. 1, pp. 1-18, 2012.

[11] C. Yao, *et al.*, "A secure remote data integrity checking cloud storage system from threshold encryption," *Journal of Ambient Intelligence and Humanized Computing*, vol. 5,pp. 857–865, 2014.

[12] S. Rizvi, *et al.*, "A Trusted Third-party (TTP) based Encryption Scheme for Ensuring Data Confidentiality in Cloud Environment," *Procedia Computer Science*, vol. 36,pp. 381-386, 2014.

[13] L. Zhou, *et al.*, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," *IEEE Transactions on Information Forensics and Security*, vol. 8,no. 12, pp. 1947-1960, 2013.

[14] S. TAN, *et al.*, "An Efficient Method for Checking the Integrity of Data in the Cloud," *China Communications*, vol. 11,no. 9, pp. 68-81, 2014.

[15] J. Lai, *et al.*, "Attribute-based encryption with verifiable outsourced decryption," *Information Forensics and Security, IEEE Transactions on*, vol. 8,no. 8, pp. 1343-1354, 2013.

[16] K. Goodarzi and A. Karimi, "Cloud Computing Security by Integrating Classical Encryption," *Procedia Computer Science*, vol. 42,pp. 320-326, 2014.

[17] R. Mukundan, *et al.*, "Efficient integrity verification of replicated data in cloud using homomorphic encryption," *Distributed and Parallel Databases*, vol. 32,no. 4, pp. 507-534, 2014.

[18] Q. Wang, *et al.*, "Enabling public auditability and data dynamics for storage security in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 22,no. 5, pp. 847-859, 2011.

[19] R. M. Jogdand, *et al.*, "Enabling public verifiability and availability for secure data storage in cloud computing," *Evolving Systems*, vol. 5,no. 20, pp. 1-11, 2013.

[20] Y. Yu, *et al.*, "Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage," *International Journal of Information Security*, vol. 13,no. 63, pp. 1-12, 2014.

[21] X. Liu, *et al.*, "Mona: secure multi-owner data sharing for dynamic groups in the cloud," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24,no. 6, pp. 1182-1191, 2013.

[22] [22] Y. PENG, *et al.*, "Secure cloud storage based on cryptographic techniques," *The Journal of China Universities of Posts and Telecommunications*, vol. 19,no. 2, pp. 182-189, 2012.

[23] W. Itani, *et al.*, "SNUAGE: an efficient platform-as-a-service security framework for the cloud," *Cluster computing*, vol. 16,no. 4, pp. 707-724, 2013.

[24] P. Singhal, "Data Security Models in Cloud Computing," *International Journal of Scientific & Engineering Research*, vol. 4,no. 6, pp. 789-793, 2013.

[25] D. Chen and H. Zhao, "Data security and privacy protection issues in cloud computing," in *Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on*, 2012, pp. 647-651.

[26] M. Sudha, "Enhanced security framework to ensure data security in cloud computing using cryptography," *Advances in Computer Science and its Applications*, vol. 1,no. 1, pp. 32-37, 2012.

[27] M. Nabeel, *et al.*, "Privacy Preserving Policy-Based Content Sharing in Public Clouds," *Knowledge and Data Engineering, IEEE Transactions on*, vol. 25,no. 11, pp. 2602-2614, 2013.

[28] S. Singh, *et al.*, "A Performance Analysis of DES and RSA Cryptography," vol. 3, ed: Citeseer, 2013.

[29] P. Scholl and N. P. Smart, "Improved key generation for gentry's fully homomorphic encryption scheme," in *Cryptography and Coding*, ed: Springer, 2011, pp. 10-22.

[30] S. Zhu, et al., "Secure Cloud File System with Attribute Based Encryption," in Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on, 2013, pp. 99-102.

www.ioirp.com