International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 30th June 2020. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-06

Title: **A SECURE AND VERIFIABLE ACCESS CONTROL WITH VERIFICATION SCHEME IN BIG DATA STORAGE**

Volume 09, Issue 06, Pages: 164-169

Paper Authors

MEDARAMETLA RASMI, C.RAMI REDDY

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A SECURE AND VERIFIABLE ACCESS CONTROL WITH VERIFICATION SCHEME IN BIG DATA STORAGE

MEDARAMETLA RASMI, C.RAMI REDDY
PG SCHOLAR.DEPT OF CSE, SIR C.V. RAMAN INSTITUTE OF TECHNOLOGY & SCIENCE, AP, INDIA
ASSOCIATE PROFESSOR, DEPT OF CSE, SIR C.V. RAMAN INSTITUTE OF TECHNOLOGY & SCIENCE,, AP, INDIA

ABSTRACT: Due to the complexity and volume, outsourcing cipher texts to a cloud is deemed to be one of the most effective approaches for big data storage and access. Nevertheless, verifying the access legitimacy of a user and securely updating a ciphertext in the cloud based on a new access policy designated by the data owner are two critical challenges to make cloud-based big data storage practical and effective. Traditional approaches either completely ignore the issue of access policy update or delegate the update to a third party authority; but in practice, access policy update is important for enhancing security and dealing with the dynamism caused by user join and leave activities. In this paper, we propose a secure and verifiable access control scheme based on the NTRU cryptosystem for big data storage in clouds. We first propose a new NTRU decryption algorithm to overcome the decryption failures of the original NTRU, and then detail our scheme and analyze its correctness, security strengths, and computational efficiency. Our scheme allows the cloud server to efficiently update the cipher text when a new access policy is specified by the data owner, who is also able to validate the update to counter against cheating behaviors of the cloud. It also enables (i) the data owner and eligible users to effectively verify the legitimacy of a user for accessing the data, and (ii) a user to validate the information provided by other users for correct plaintext recovery. Rigorous analysis indicates that our scheme can prevent eligible users from cheating and resist various attacks such as the collusion attack.

1. INTRODUCTION

Most existing approaches for securing the outsourced big data in clouds are based on either attributed-based encryption (ABE)or secret sharing. ABE based approaches provide the flexibility for a data owner to predefine the set of users who are eligible for accessing the data but they suffer from the high complexity of efficiently updating the access policy and ciphertext. Secret sharing mechanisms allow a secret to be shared and reconstructed by certain number of cooperative users but they typically employ asymmetric public key cryptograph such as RSA for users' legitimacy verification, which incur high computational overhead. As a data owner typically does not backup its data locally after outsourcing the data to a cloud, it cannot easily manage the data stored in the cloud. Besides, as more and more companies and organizations are using clouds to store their data, it becomes more challenging and critical to deal with the issue of access policy update for enhancing security and dealing with the dynamism caused by the users' join and leave activities. To the best of our knowledge, policy update for outsourced big data storage in clouds has never been considered by the existing research. Another

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

challenging issue is how to verify the legitimacy of the users accessing the outsourced data in clouds. Existing schemes do not support user eligibility verification. On the other hand, verifiable secret sharing based schemes rely on RSA for access legitimacy verification. As multiple users need to mutually verify each other using multiple RSA operations, such a procedure has a high computational overhead. Furthermore, the classic asymmetric crypto solutions such as RSA could be broken by quantum computing in the near future. The NTRU cryptosystem is a type of lattice-based cryptography, and its security is based on the shortest vector problem (SVP) in a lattice. The major advantages of NTRU are quantum computing attack resistance and lighting fast computation capability. However, NTRU suffers from the problem of decryption failures. In this paper, we first propose an improved NTRU cryptosystem to overcome the decryption failures of the original NTRU. Then we design a secure and verifiable scheme based on the improved NTRU and secret sharing for big data storage. The cloud server can directly update the stored ciphertext without decryption based on the new access policy specified by the data owner, who is able to validate the update at the cloud. The proposed scheme can verify the shared secret information to prevent users from cheating and can counter various attacks such as the collusion attack. It is also deemed to be secure with respect to quantum computing attacks due to NTRU. The multi-fold contributions of the paper can be summarized as follows: • We propose a new NTRU decryption procedure to overcome the decryption failures of the original NTRU without reducing the security strength of NTRU. • We propose a secure and verifiable access control scheme to protect the big data stored in a cloud. The scheme can verify a user's access legitimacy and validate the information provided by other users for correct plaintext recovery. • We devise an efficient and verifiable method to update the ciphertext stored in clouds without increasing any risk when the access policy is dynamically changed by the data owner for various reasons.

2. LITERATURE SURVEY

Remote Body Area Networks (BANs) are required to assume a cru-cial job in patient-wellbeing observing sooner rather than later. Estab-lishing secure correspondences between BAN sensors and exter-nal clients is vital to tending to the predominant security and privacyconcerns. In this paper, we propose the crude capacities to im-plement a mystery sharing based Ciphertext-Policy Attribute-BasedEncryption (CP_ABE) plot, which encodes the information based onan access structure determined by the information source. We additionally designtwo conventions to safely recover the touchy patient information from aBAN and train the sensors in a BAN. Our investigation demonstrates thatthe proposed plan is achievable, can give message authentici-ty, and can counter conceivable real assaults, for example, plot attacksand battery-depleting assaults.

Remote Body Area Networks (WBANs) are relied upon to assume a noteworthy job in the field of patient-wellbeing observing sooner rather than later, which increases enormous consideration among analysts as of late. One of the difficulties is to set up a protected correspondence engineering among sensors and clients, while tending to the predominant

security and protection concerns. In this paper, we propose a correspondence engineering for BANs, and plan a plan to verify the information interchanges between embedded/wearable sensors and the information sink/information customers (specialists or medical attendant) by utilizing Ciphertext-Policy Attribute Based Encryption (CP_ABE) [1] and mark to store the information in ciphertext group at the information sink, henceforth guaranteeing information security. Our plan accomplishes a job based access control by utilizing an entrance control tree characterized by the characteristics of the information. We likewise plan two conventions to safely recover the touchy information from a BAN and educate the sensors in a BAN. We examine the proposed plan, and contend that it gives message validness and intrigue opposition, and is proficient and achievable. We additionally assess its presentation regarding vitality utilization and correspondence/calculation overhead.

As progressively touchy information is shared and put away by outsider destinations on the Internet, therewill be a need to encode information put away at these locales. One disadvantage of scrambling data,is that it tends to be specifically shared uniquely at a coarse-grained level (i.e., giving anotherparty your private key). We build up another cryptosystem for fine-grained sharing ofencrypted information that we call Key-Policy Attribute-Based Encryption (KP-ABE). Inour cryptosystem, ciphertexts are named with sets of qualities and private keys areassociated with access structures that control which ciphertexts a client can decrypt.We show the relevance of our development to sharing of review log informationand communicate encryption. Our development bolsters designation of private keys whichsubsumes Hierarchical Identity-Based Encryption (HIBE).

3. EXISTING SYSTEM

Outsourcing to clouds is one of the most popular approaches to securing the big data storage , in which the data owners encrypt their data based on cryptographic primitives and store the encrypted data to the clouds. In outsourcing, a secure mechanism should be established between a data owner and a cloud. In order for the cloud to perform operations over the encrypted data, “Fully Homomorphic Encryption” (FHE) was usually adopted, which allows direct addition and multiplication operations over the cipher texts while preserving decryptability. Homomorphic encryption was also applied to guarantee the security of data storage. Nevertheless, it is an immature cryptosystem, and is extremely inefficient in practice, which renders it hardly applicable in real world applications. Securely outsourcing big data computations to the clouds was also extensively studied but this topic is out of the scope of the paper. Adequate access control is key to protect the stored data. Access control has traditionally been provided by operating systems or applications restricting access to the information, which typically exposes all the information if the system or application is hacked.

There is no Verifiable Access Control Scheme to secure data more effectively. There is no Data integrity on owner data

4. PROPOSED SYSTEM

In this paper, we first propose an improved NTRU cryptosystem to overcome the decryption failures of the original NTRU. Then we design a secure and verifiable scheme based on the improved NTRU and

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

secret sharing for big data storage. The cloud server can directly update the stored cipher text without decryption based on the new access policy specified by the data owner, who is able to validate the update at the cloud. The proposed scheme can verify the shared secret information to prevent users from cheating and can counter various attacks such as the collusion attack. It is also deemed to be secure with respect to quantum computing attacks due to NTRU. The system proposes a new NTRU decryption procedure to overcome the decryption failures of the original NTRU without reducing the security strength of NTRU. The system proposes a secure and verifiable access control scheme to protect the big data stored in a cloud. The scheme can verify a user's access legitimacy and validate the information provided by other users for correct plaintext recovery.

The system devises an efficient and verifiable method to update the cipher text stored in clouds without increasing any risk when the access policy is dynamically changed by the data owner for various reasons. The system proves the correctness of the proposed scheme and investigates its efficiency and security strength. Particularly, we demonstrate that our scheme can resist various attacks such as the collusion attack via a rigorous analysis.

The system has efficient and verifiable method to update the cipher text if it is integrated by malicious users. The data security is more in the cloud server due to data integrity by data owner also.

5. SYSTEM ARCHITECTURE:

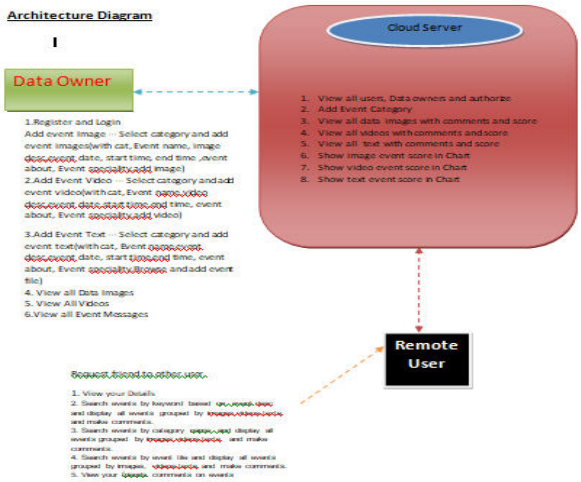

Fig 1 System Architecture

6. IMPLEMENTATION

Data Owner

In this module, the data owner uploads their data in the cloud server and performs the following operations Add event Image, Add Event Video, Add Event Text and View all Data Images, View All Videos, View all Event Messages

Cloud Servers

The Data Owner sends a request to Cloud Scheduler to provide services by assigning the task for any one cloud like View all users, Data owners and authorize,Add Event Category ,View all data images with comments and score,View all videos with comments and score,View all text with comments and scoreand Show image event score in Chart ,Show video event score in Chart, Show text event score in Chart.

End User

In this module, the user has to get Registered to Cloud server to access the Cloud services and need to Authenticate the user by Logging in by providing the User Name and operations the following operations such as View your Details and Search events by keyword based on event desc and display all

events grouped by images, videos, texts and make comments, Search events by category name and display all events grouped by images, videos, texts and make comments., Search events by event tile and display all events grouped by images, videos, texts and make comments.

Security

The proposed scheme should be able to defend against various attacks such as the collusion attack. Meanwhile, access policy update should not break the security of the data storage, disclose sensitive information about the data owner, and cause any new security problem.

Verification

When a user needs to decrypt a stored cipher text, its access legitimacy should be verified by other participating users and the secret shares obtained from other users must be validated for correct recovery.

Authorization

To reduce the risk of information leakage, a user should obtain authorization from the data owner for accessing the encrypted data.

7. CONCLUSION AND FUTURE WORKS

In this paper, we first propose an improved NTRU cryptosystem to overcome the decryption failures of the original NTRU and then present a secure and verifiable access control scheme based on the improved NTRU to protect the outsourced big data stored in a cloud. Our scheme allows the data owner to dynamically update the data access policy and the cloud server to successfully update the corresponding outsourced ciphertext to enable efficient access control over the big data in the cloud. It also provides a verification process for a user to validate its legitimacy of accessing the data to both the data owner and t□1 other legitimate users and the correctness of the information provided by the t□1 other users for plaintext recovery. The security of our proposed scheme is guaranteed by those of the NTRU cryptosystem and the (t; n)-threshold secret sharing. We have rigorously analyzed the correctness, security strength, and computational complexity of our proposed scheme.

Designing a secure, privacy preserving, and practical scheme for big data storage in a cloud is an extremely challenging problem. In our future research, we will further improve our scheme by combining the (t; n)-threshold secret sharing with attributebased access control, which involves an access structure that can place various requirements for a user to decrypt an outsourced ciphertext data in the cloud. Meanwhile, we will investigate the security problems when a data owner outsources its data to multi cloud servers and consider an attribute-based access structure that can be dynamically updated, which is more applicable for practical scenarios in big data storage.

REFERENCES

[1] M. A. Beyer and D. Laney, "The importance of big data: a definition," Stamford, CT: Gartner, 2012.

[2] V. Marx, "Biology: The big challenges of big data," Nature, vol. 498, no. 7453, pp. 255–260, 2013.

[3] G. P. Consortium et al., "A map of human genome variation from population-scale sequencing," Nature, vol. 467, no. 7319, pp. 1061–1073, 2010.

[4] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT 2005, pp. 457–473, 2005.

[5] C. Hu, F. Zhang, X. Cheng, X. Liao, and D. Chen, "Securing communications between

external users and wireless body area networks," in Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy. ACM, 2013, pp. 31–36.

[6] C. Hu, H. Li, Y. Huo, T. Xiang, and X. Liao, "Secure and efficient data communication protocol for wireless body area networks," IEEE Transactions on Multi-Scale Computing Systems, vol. 2, no. 2, pp. 94– 107, 2016.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 89–98.

[8] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," Public Key Cryptography– PKC 2011, pp. 53–70, 2011.

[9] C. Hu, N. Zhang, H. Li, X. Cheng, and X. Liao, "Body area network security: a fuzzy attribute-based signcryption scheme," IEEE journal on selected areas in communications, vol. 31, no. 9, pp. 37–46, 2013.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," Advances in Cryptology–EUROCRYPT 2011, pp. 568–588, 2011.

[11] C. Hu, X. Cheng, Z. Tian, J. Yu, K. Akkaya, and L. Sun, "An attributebased signcryption scheme to secure attribute-defined multicast communications," in SecureComm 2015. Springer, 2015, pp. 418–435.

[12] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.

[13] M. Dehkordi and S. Mashhadi, "An efficient threshold verifiable multisecret sharing," Computer Standards & Interfaces, vol. 30, no. 3, pp. 187–190, 2008.

[14] Z. Eslami and J. Z. Ahmadabadi, "A verifiable multi-secret sharing scheme based on cellular automata," Information Sciences, vol. 180, no. 15, pp. 2889–2894, 2010.

[15] M. H. Dehkordi and S. Mashhadi, "New efficient and practical verifiable multi-secret sharing schemes," Information Sciences, vol. 178, no. 9, pp. 2262–2274, 2008.

[16] J. Zhao, J. Zhang, and R. Zhao, "A practical verifiable multi-secret sharing scheme," Computer Standards & Interfaces, vol. 29, no. 1, pp. 138–141, 2007.

[17] C. Hu, X. Liao, and X. Cheng, "Verifiable multi-secret sharing based on LFSR sequences," Theoretical Computer Science, vol. 445, 2012.

[18] C. Hu, X. Liao, and D. Xiao, "Secret image sharing based on chaotic map and chinese remainder theorem," International Journal of Wavelets, Multiresolution and Information Processing, vol. 10, no. 03, 2012.

[19] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "Dac-macs: Effective data access control for multiauthority cloud storage systems," Information Forensics and Security, IEEE Transactions on, vol. 8, no. 11, pp. 1790– 1801, 2013.

[20] K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 7, pp. 1735–1744, 2014.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org