International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

Efficient data access control for multi-authority cloud Storage

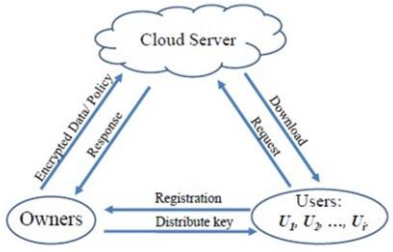
Priya.D[1], Sai kamala.S[2], A.N Sandya[3], Mrs.Devi Ramakrishnan[4]

[1,2,3] *Students, Computer Science and engineering, Panimalar Engineering College, Chennai ,India*
[4]*Assistant professor, Computer science and Engineering, Panimalar Engineering College, Chennai, India*

Abstract— *The customer and owner relationship breaks during a trade if any malpractice happens, in between the process of transporting the goods. Here we verify a security mechanism to ensure the accurate transport of goods to the customers in a large scale trade. Here, the trade information is passed in encrypted form, and the cipher text is outsourced to the cloud. Here the access policy update is used to secure information from third party authorities. The process of 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. . 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.*

Key words-Big data storage, access policy update, cloud computing, secret sharing

1. Introduction



BIG data is a high volume, and/or high velocity, high variety information asset, which requires new forms of processing to enable enhanced decision making, insight discovery, and process optimization [1].Due to its complexity and large volume, managing big data using on hand database management tools is difficult.

An effective solution is to outsource the data to a cloud server that has the capabilities of storing big data and processing users' access requests in an efficient manner.

For example in eHealth applications, the genome information should be securely stored in an e-health cloud as a single sequenced human genome is around 140 gigabytes in size [2], [3].

However, when a data owner outsources its data to a cloud, sensitive information may be disclosed because the cloud server is not trusted; therefore typically the cipher text of the data is stored in the cloud.

But how to update the cipher text stored in a cloud when a new access policy is designated by the data owner and how to verify the legitimacy of a user who intends to access the data are still of great concerns.

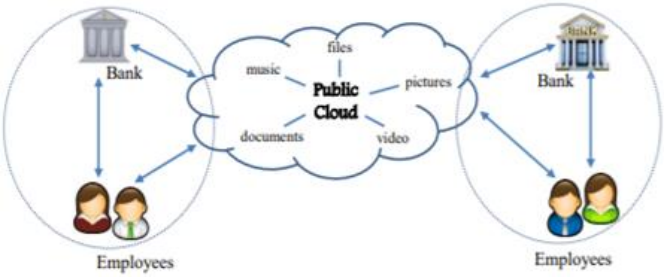


Figure: application of big data storage

2. OBJECTIVE

The main objective of this project is to encrypt user's sensitive data when users transaction process takes place. This will ensure that the third party vendors or merchants can't able to see user's personal data.

3. Problem statement

Nevertheless, verifying the access legitimacy of a user and securely updating a cipher text 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

4. Scope

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 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.

5. Overall concept

Before you begin to format your paper, first write and save the content as a separate text file. Keep your text and graphic files separate until after the text has been formatted and styled. Do not use hard tabs, and limit use of hard returns to only one return at the end of a paragraph.

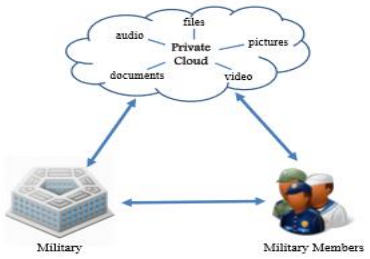


Fig. 2. An example application of big data storage in military.

Do not add any kind of pagination anywhere in the paper. Do not number text heads—the template will do that for you.

Finally, complete content and organizational editing before formatting. Please take note of the following items when proofreading spelling and grammar.

ALGORITHM

Algorithm 1 The Improved NTRU Decryption

1: Input: cipher text e, secret key {f, fp}.
2: Output: plaintext m;
3: The decryptor computes a = e ∗ f;
4: Γ = max{| max0≤i≤N−1{ai}|, | min0≤i≤N−1{ai}|};
5: τ = b Γ q/2 c;
6: If τ = 0
7: m = a ∗ fp (mod p).
8: Else
9: For 0 ≤ i ≤ N − 1,
10: Compute γ = b |ai| q/2 c;
11: If γ = 0
12: a 0 i = ai and c (1) i = c (2) i = · · · = c (τ) i = 0;
13: Else If ai ≥ 0
14: a 0 i = ai − q−1 2 γ;
15: c (1) i = c (2) i = · · · = c (γ) i = q−1 2 ;
16: c (γ+1) i = a 0 i ;
17: c (γ+2) i = · · · = c (τ) i = 0;
18: Else
19: a 0 i = ai + q−1 2 γ;
20: c (1) i = c (2) i = · · · = c (γ) i = − q−1 2 ;
21: c (γ+1) i = a 0 i ;
22: c (γ+2) i = · · · = c (τ) i = 0;
23: EndIf 24: EndFor
25: m0 = a 0 ∗ fp + c (1) ∗ fp + · · · + c (τ) ∗ fp (mod p);
26: EndIf
27: Output plaintext m0 .

6. FUTURE ENHACEMENT

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. Designing a secure, privacy preserving, and practical scheme for big data storage in a cloud.Furthermore, any keyless customer can freely check the legitimacy of the returned calculation result. Security examination shows that our arrangement is provable secure under the CDH supposition in the unpredictable proposed model. Results show that our tradition is in every practical sense gainful to the extent both communication and computation cost

7. EXISTING SYSTEM

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.

Moreover, it is also a challenging issue to dynamically and efficiently update the access policies according to the new requirements of the data owners in secret sharing approaches.

8. PROPOSED SYSTEM

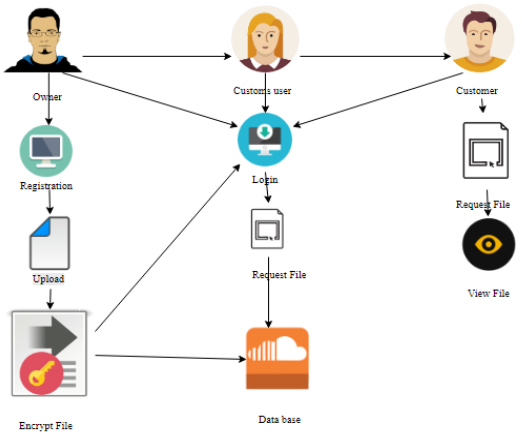
The verifying the shared secret information to prevent users from cheating and can counter various attacks such as the collusion attack.

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.Improved NTRU decryption algorithm is used.

NTRU is a patented and open source public-key cryptosystem that uses lattice based cryptography to encrypt and decrypt

data. It consists of two algorithms: NTRU Decrypt, which is used for Decryption, and NTRU Sign, which is used for digital signatures.

9. SYSTEM DESIGN



Owner choose the product and details example product id, product name, cost, piece, custom's name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom's side.

Custom's user one data receive so check the details, the details also encryption format so all information is print ***** only.

Custom's user view the original content and download the product. The custom's user sends to customer.

Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

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 verifying the shared secret information to prevent users from cheating and can counter various attacks such as the collusion attack.

USER INTERFACE DESIGN

To connect with server user must give their username and password then only they can able to connect the server.

If the user already exits directly can login into the server else user must register their details such as username, password and Email id, into the server. Server will create the account for the entire user to maintain upload and download rate. Name will be set as user id. .

Logging in is usually used to enter a specific page

OWNER UPLOAD DETAILS AND SEND TO CUSTOMS

Owner choose the product and details example product id, product name, cost, piece, custom's name, company name, net weight so all details and high level security of encryption and key also developed, owner send to custom's side.

CUSTOM'S USER CHECKS DETAILS

Custom's user one data receive so check the details, the details also encryption format so all information is print ***** only

REQUEST SEND TO OWNER

Custom's User view original data means send request to data owner. The data owner monitoring the file and accept.

CUSTOMS SEND TO CUSTOMER

Custom's user view the original content and download the product. The custom's user send to customer

CUSTOMER REQUEST SEND TO OWNER

Customer view the message only star format so customer send the request so the owner vie the inbox and accept the query, customer view the original data.

10. Advantages

- The data owner and eligible users to effectively verify the legitimacy of a user for accessing the data.
- To upload their endless data.
- Corresponding computations to a third party

11. Conclusion

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 cipher text 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 t1 other legitimate users and the correctness of the information provided by the t1 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 attribute based access control, which involves an access structure that can place various requirements for a user to decrypt an outsourced cipher text data in the cloud.

Meanwhile, we will investigate the security problems when a data owner outsources its data to multicloud servers and consider an attribute-based access structure that can be dynamically updated, which is more applicable for practical scenarios in big data storage.

Acknowledgment:

We would like to express our deep gratitude to our respected Secretary and Correspondent Dr.P.CHINNADURAI, M.A., Ph.D. for his kind words and enthusiastic motivation, which inspired us a lot in completing this project.

We express our sincere thanks to our Directors Tmt. C. VIJAYARAJESWARI Thiru. C .SAKTHI KUMAR,M.E., and TMT.SARANYA SREE SAKTHI KUMAR B.E., for providing us with the necessary facilities for completion of this project.

We also express our gratitude to our Principal Dr.K.Mani, M.E., Ph.D. for his timely concern and encouragement provided to us throughout the course.

We thank the Head of the CSE Department, Dr. S.MURUGAVALLI , M.E.,Ph.D., for the support extended throughout the project.

We would like to thank my Project Guide Mrs R.Devi and all the faculty members of the Department of CSE for their advice and suggestions for the successful completion of the project.

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.