INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

ROBUST SECURITY TO DATA FOR ENDEMIC USERS

P.Baskar[1], M.Lakshmanan[2]

[1] M.E. CSE, Department of Computer Science Engineering, Mailam Engineering College, affiliated to Anna University (Chennai), Mailam, Villupuram, Tamilnadu- 604304, India
[2] Assistant Professor, Department of Computer Science Engineering, Mailam Engineering College, affiliated to Anna University (Chennai), Mailam, Villupuram, Tamilnadu- 604304, India.

Abstract

Data stored in cloud services, they shared along with multiple users more than storage. From the integration of cloud service data the existence of hardware and software failures subject to human errors. Shared data from existing mechanism reveals confidential information through public auditing. The public verifiers which efficiently identify the privacy for auditing data that computer verifies for data inside data that share data with correctness. Each block shared in private with public verifiers able to efficiently verify the shared data integration for entire file without retrieval of identity. Simultaneously by verifying each and every audit results we can propose new secured database services. In our new proposed prototype we imply algorithm for data encryption and make it stronger through splitting up of data into numerous parts depending on paradigm value. Redundant data will be eliminated and stored as unique copy of these split up of data. User attempts to decrypt database then that will be integrated into one file and can be viewed by the authenticated user. In our approach we take number of backup for split up data thus we ensure no loss of data.

Keywords*:* Public audit, data sharing, public signature, private signature, data integration, data split up.

1. Introduction

For efficient and scalable cloud data storage providers for low cost margin of traditional approaches shares standard feature. The cloud integration for scrutiny for data storage in cloud can easily lose and corrupted due to hardware inevitability. Data utilization of computational service over cloud verification for maintaining reputation of service avoids data error.

Data correctness for checking cloud conventional approach that checks appropriate data cloud services successfully. The efficient cloud data for traditional approach in which the cloud data will have doubt will be rectified with data integration. Large cloud data verifying the data integrity in general costs irrelevant user computational amount which uses their communication resources.

When data corruption in cloud uses many of the cloud data with data mining and machine learning which do not necessarily need users for downloading entire cloud data for local devices. Computation services offered for cloud providers which directly exist on large scale data. The proposed owner allows efficient mechanism for public verifier which performs integrity checking without downloading. Researcher or the data user who utilizes owner’s data through cloud service or auditor as a third party owner can check expert integrity services.

Advanced auditing mechanism for advance design during public auditing of cloud the private content of data belongs to personal user no disclosed to any of the public verifiers. Personal data in cloud auditing solutions made public focused. Sharing the data among multiple users motivates the engaging feature that ensures shared data is correct in cloud.

Verifying shared data integrity extended to public auditing mechanism. For privacy issues in significant case of shared data that uses existing mechanism to identify the privacy leakage mechanisms to public verifiers. When a group shared a file into number of small blocks then each independent block signed by one or two authenticated users with existing public auditing solutions will be authenticated. Different users signs different blocks due to modification of these two users.

Entire data for integrity in order to audit in correct way chooses appropriate public verifier for public key in each block. Learning the public verifier identity for signing each block for unique binding between identity and each block through public key for digital certificates will be under well constructed public key infrastructure.

From batch auditing for performing multiple auditing tasks simultaneously efficiency improvising of verification of multiple editing tasks. With random masking compatible with privacy data preserving utilization of public verifier for leveraging index for hash tables from public auditing solutions. Comparing for high level of random masking to support dynamic data leads to public auditing solutions.

The original users and the group of users are two types of users who initially create shared data in cloud that shares it with group users. As both of them are member of groups every member will be allowed to access and modify shared data. Verification of metadata for shared data with signatures stored in cloud server. Third party auditor which provides data auditing services for public verifier intends to outside user group of data utilizing shared data. Verification of integrity of stored shared data along with cloud server.

2. Encrypting data with ECC algorithm

Protection of information by transforming or encrypting it into an unreadable format termed to be cipher text. Only person who possess secret key can decrypt or decipher the content to plain and readable text message. Using code breaking scheme encrypted messages can be broken and sent. The other techniques like virtually unbreakable messages prevails strong electronic security.

For making data more secured the information to be shared with our proposed model will be encrypted with Elliptic Curve Cryptography known as ECC algorithm. For applying elliptic curve cryptography the important paradigm is key value which involves public key and private key in which the source message from the sender side will be encrypted with the public key and the receiver side will decrypt the key with private key. For key generation they make it randomly using random number generation equation which generates both public key and private key and make message a cipher text.

The message we sent will represent the generated message that is key of a curve which have in depth implementation that is there exists numerous levels of curve level cryptography which is impossible to break all the levels of curve random number generation. In need of public key cryptographic system for set of algorithms difficult for one direction is critical for functions. Public key and private key undergoes many mathematical procedures applied to message for cryptography. The private keys are not accessible to other users but the public key is accessible to everyone.

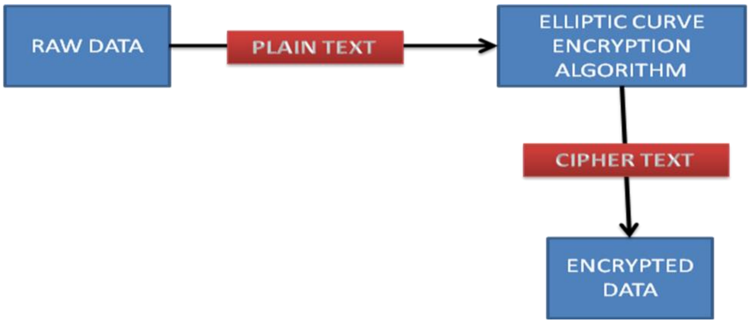

Figure 1: Implementing ECC algorithm for Encryption and Decryption.

Even when a public key is accessible to everyone they cannot able to view decrypted messages using that key as that is very protective and very hard to follow the mathematical procedures to break the key. Only the person who is having authenticated private key can decrypt the cipher text messages using its backtracking method. For stronger protection first the sender must create private signatures and send it before sending encrypted messages and they verify some other authentication for messages before sending the key.

The user in receiver side will open the cipher text which have encrypted message will be converted from cipher text to normal text as decrypt procedure with the help of the private digital key signatures. In existing methods they imply third party auditor who audits for the public key and private signatures which costs very high. There may be the chance for this third party auditor themselves turned to be a hacker of the integrity of data as they have clue about the private and public signatures. It takes much time to verify the data integration by third party auditor where the performance will be reduced for integrity of data.

3. Data Splitting of Cipher Text

The encrypted cipher text in our proposed approach will be split up into n number of parts and then stored in cloud storage area. The different parts of file will be stored in different cloud servers as cipher text. The n value for number of storage denotes the number of cloud server exists where each different part of file will be stored. Thus the split files needs accurate information or the legitimate private key for integration of files again into single file. The data split up information will be stored in the local client system for security reasons.

For securing information using data splitting and integration includes access control of data makes communication so secure which protects private data that process inappropriate observations or modification from their intervention. In cloud computing new security paradigm relates to static and dynamic data that increases protection to security threat usually accustomed in cloud computing services.

The data to be stored will be encrypted as a cipher text first and then that will be split up into number of parts equivalent to number of cloud servers existing in the network. Then each part of the file will be stored in each cloud server. The information about splitting and integrating all the files together into one will be saved separately in the local client system which makes sure the integration part will never let go out of the authenticated system.

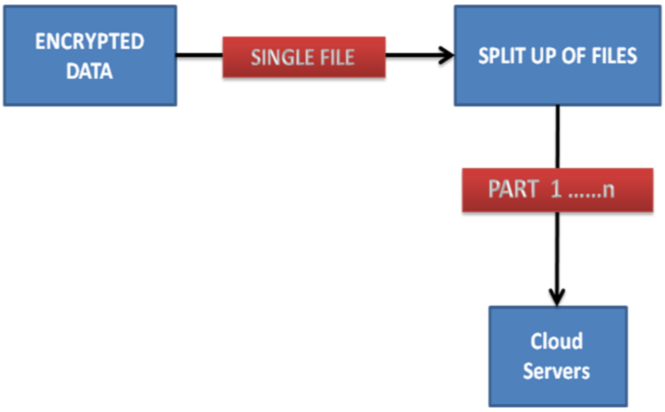

Figure 2: Representation of Split up of Data and Integration.

The security of the data for integration will be preserved in safe asylum which will be in the legitimate users system. When data need to be integrated this information will be reclaimed and all the data from each cloud server will be integrated in that particular order. Then by using the digital signatures the encrypted cipher text will be decrypted to readable text using private signature keys.

Number of file split ups according to number of servers will be taken a copy or back up into various database. This data backup does not affect the security of data as the two different parts of a single encrypted file which cannot be integrated with one another will be stored in a one particular server. If any one of the server gets crash down or any loss in related information of data under attack then those data will be recovered using this data backup. As there are number of data backups for a single file we ensure data will never lost due to any other reason.

The data to be stored in the server will be first parted into different number of files. The count for number of cloud servers will be directly proportional to the strength of security given to that data. The number of backup needed will also be determined for data recovery. After data retrieval they will be integrated according to the local information stored. Such integrated data will be decrypted then it will convert them into original plain text.

5. Conclusion

In this public auditing of privacy preserving of shared data in cloud service the signatures for authenticators will ensure and audit shared data integrity without fetching the complete data. The data to be sent securely using encryption and decryption techniques will be further split up and sent creating public and private signatures. The authorised user holding private key will be enabled to use the data integrity code and integrates all the ciphered text together and then decipher it using decryption private key. As advanced security provided to cloud service we can use this for our wide range of data transmission. From our approach data will be secured by the user itself and not by any other third party auditing. This kind of third party auditing may also be a intruder or attacker of our system or data even in the cloud service. Data can be recovered from the cloud service even if there is any loss in particular server or data set or even when a server is completely crashed as we have n number of back up data in different servers which cannot even be integrated one another without any digital signatures.

REFERENCES

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf. Cloud Computing, pp. 295-302, 2012.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Pub-lic Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[4] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[6] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf. Comm. and Network Security (CNS '13), pp. 90-99, 2013.

[7] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.

P.Baskar – has received his B.Tech.(IT) degree in the year 2012. At present he is pursuing M.E. (CSE) in Mailam Engineering College, Villupuram, Tamil Nadu, India. He attended 2 papers in National conferences. His research interests lies in the areas of Mobile Computing, Data Mining, Cloud Computing and Software Engineering.

M.Lakshmanan – Completed his B.E. (CSE) degree in the year 2008, M. Tech (CSE) degree in the year 2011.Currently he is working as Assistant professor in Computer Science and Engineering at Mailam Engineering College, Villupuram, Tamil Nadu, India. His research interests lies in the areas of Data mining, Software engineering and Cloud Computing. He has published 2 papers in National conferences. He attended many workshops & National seminars in various technologies and also attended Faculty Development Programme.