A Secure Privacy Preserving Auditing Protocol with Hybrid Model

B.JesseKiranmai[1],N.V.AshokKumar[2],Dr.C.P.V.N.MohanRao[3]
[1]Final MTech Scholar,[2]Associate Professor,[3]Professor,
[1,2,3]DeptofCSE,AvanthiInstituteofEngineeringandTechnology,Visakhapatnam,A.P

Abstract : In this paper we propose an efficient auditing service with authentication, probity of data and security as primary factors in the architecture. The proposed work determines that user can access the data in cloud as without bothering about the exactness of the data. We improved the previous approach with efficient cryptographic method and secure authentication method. We also proposed dynamic block updating of corrupted block while intimated by the third party auditor with proxy and authentication request can be forwarded to proxy server by the cloud service provider, it minimizes the additional over head of user authentication verification and data confidentiality of cloud service provider and performance of the service can be improved. Our regenerated code based auditing improves the performance than traditional approaches.

I. INTRODUCTION

In present days' cloud storage had more popularity because it offers user friendly data outsourcing on-demand. It is data access with location, independence and personal maintenances etc. It is reminded that data owners lose control on the data uploaded or outsourced data. On the other side the integrity of the data became risk to maintain the data in cloud services. In cloud service providers, some providers may act as dishonestly and attempting to hide data loss or distraction of the data. It is clearly making the users must use more efficient protocols and maintain data correctly.

In many methods dealing with the outsourced data without any backup of the original data. It is very risk that without any data it is very hard to make data exchange under different security models. In among all data security methods, provable data possession model is more efficient method in data exchange protocol. In case of large data, distributed storage systems play vital role. To safe guard the data it will store the data in the data in redundant manner. This method is more effective more because it segments the large data and maintain it as segments in different memory locations. So, it will be easier that maintain the data more secure. When it comes to data retrieving all segments collected from the various locations and integrated as one.

There is another concept we must know in this paper, that is regenerating codes. These are the classes of codes proposed for providing reliability of the data and efficient repair of failed nodes in various distributed storage systems. When coming to cloud storage it is very useful when low band widths. Cloud storage is a model of the data storage in which the digital data and it is stored in logical parts. In some organizations people buy the storage capacity from the providers to store the data in cloud.

Distributed storage depends on very virtualized foundation and resembles more extensive distributed computing as far as available interfaces, close moment flexibility and adaptability, multi-tenure, and metered assets. Distributed storage administrations can be used from an off-premises benefit or conveyed on-premises. Distributed storage regularly alludes to a facilitated question storage benefit;however, the term has expanded to incorporate different sorts of information storage that are presently accessible as an administration, likesegment storage.

II. RELATED WORK

Provable data possession that allows a client that has stored data at a cloud storage to verify the that the cloud possesses the original data without retrieving the data. The model generates optimal proofs of possession by giving the random sets of segments from the cloud and it reduces input output costs. The user maintains a sufficient data to verify the proof. The response protocol transmits a small and constant data which minimizes network communication. So, PDP model for remote data verifying supports enormous amounts of data in distributed storage systems.

Verification of the authentication is more hard issue in storage system. Because of untrusted cloud servers, user protocol prevents the servers from modifying the data by providing the authentication credentials when accessing the data. It is insufficient to detect the data have been modified or deleted. When data access because it may be too late recover the data. If the data of the given file is large, then the I/O cost increases. Previous solutions do not meet these requirements for proving data possession. Some schemes provide a weaker guarantee by enforcing storage complexity: The server should store an amount of data at least as large as the client's data, but not necessarily the same exact data. Moreover, all previous techniques require the server to access the entire file, which is not feasible when dealing with substantial amounts of data.

We characterize a model for provable information ownership (PDP) that gives probabilistic evidence that an outsider stores a document. The model is novel in that it permits the server to get to little parts of the record in creating the verification; all different methods must get to the whole record. Inside this show, we give the principal provably-secure plan for remote information checking. The customer stores a little O(1) measure of metadata to check the server's verification.

Both schemes utilize homomorphic certain labels. Since of the homomorphic property, labels processed for different record squares can be consolidated into a solitary esteem. The customer pre-figures labels for each piece of a record and after that stores the record and its labels with a server. Later, the customer can confirm that the server has the record by creating an arbitrary test against an arbitrarily those set of document squares. Utilizing the questioned pieces and their relating labels, the server produces a proof of ownership.

III. PROPOSED WORK

We are proposing an efficient multi owner privacy preserving auditing technique over cloud. Secure authentication and key generation can be handled between data owners and proxy and verification also done at same phase. Data owners forward the data components meta data so it prevents the misusage of data component from the auditor end. Data components can be segmented and encoded with cryptographic approach and applies a novel signature algorithm and uploads to the cloud service.

Advantages:

- Auditing can be performed in efficient way without direct transmission
- Over head of CSP can be reduced with external proxy server for data confidentiality
- Exact corrupted blocks can be identified

Data Owner(DO): He or she has the data files to be stored in the cloud database and depend on the cloud for data maintenance and it can be a customer or an organization. Data owner uploads the data components in the cloud.

CloudStorage Service Provider(CSP): It provides data storage service and has enough storage space to maintain clients data and updates blocks if any corrupted over database. Cloud service provider allows an authorized auditor to monitor the data components and instant mails can be forwarded to Data owner.

Third Party Auditor(TPA): A trusted person who control or monitor data deployed by the data owner. Auditor receives initiation and authentication parameters and then monitors data components.

Signature and Tag generation:

In our method data owner apply signature generation method on each blocks of the data and creates the hash code and encrypts the content with AES algorithm and uploads in to the server. Data Components sre divided into $m_1,m_2….m_n$& generates random tag key set$(t_1,t_2…..t_n)$. Every individual block can be encrypted with tag keys and then it forward the file meta data details and key to the third party auditor (verifier). There the auditor process same signature generation method and generates signature on the blocks and then verifies the both signatures if any block code is not matched that sends alert message to the data owner, then the administrator can forward only the revised information instead of total content then the user can browse the information which is given by the cloud service provider.

Signature Authentication with ECDSA :

The generation of the public key in ECDSA involves computing the point, Q, where Q = dP. In order to crack the elliptic curve key, adversary Eve would have to discover the secret key d. Given that the order of the curve E is a prime number n, then computing d given dP and P would take roughly $2^{n/2}$ operations [1]. For example, if the key length n is 192 bits (the smallest key size that NIST recommends for curves defined over GF(p)), then Eve will be required to compute about 2^{96} operations. If Eve had a super computer and could perform one billion operations per second, it would take her around two and a half trillion years to find the secret key. This is the elliptic curve discrete logarithm problem behind ECDSA.

1. Select an elliptic curve E defined over a finite field F_p such that the number of points in $E(F_p)$ is divisible by a large prime n.
2. Select a base point, P, of order n such that $P \in E(F_p)$
3. Select a unique and unpredictable integer, d, in the interval [1, n-1]
4. Compute Q = dP
5. Sender A’s private key is d
6. Sender A’s public key is the combination (E, P, n, Q)

Proxy Implementation :

Basically proxy server plays an intermediary between the client computer and the server computer. The clients usually take the help of proxy server for requesting any files, any web pages or any other resources. The proxy server acts as an identification shield between the server and the client machine. Authentication and data confidentiality can be taken care of proxy server, authentication request can be forwarded to proxy server by the cloud service provider,it minimizes the additional over head on CSP and performance of the service can be improved.

AES algorithm :

The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows:

- 10 cycles of repetition for 128-bit keys.
- 12 cycles of repetition for 192-bit keys.
- 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

1. KeyExpansions—round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more.

2. InitialRound

1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.

3. Rounds

1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.

2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.

3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

4. AddRoundKey

4. Final Round (no MixColumns)

1. SubBytes

2. ShiftRows

3. AddRoundKey.

IV. CONCLUSION

We have been concluding our current research work with efficient auditing protocol and proxy implementation. Our efficient signature algorithm efficiently authenticates the blocks of the data component and verifies successfully. Multiple owners can upload the data component and audit with various auditors with out direct transmission of data component. Our experimental results shows efficient results than traditional approaches.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," National Institute of Standards and Technology, Tech. Rep., 2009.
[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," Commun. ACM, vol. 53, no. 4, pp. 50–58, 2010.
[3] T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach, 1st ed. New York, NY, USA: McGraw-Hill, Inc., 2010, ch. 7.
[4] J. Li, M. N. Krohn, D. Mazi`eres, and D. Shasha, "Secure untrusted data repository (sundr)," in Proceedings of the 6th conference on Symposium on Operating Systems Design & Implementation, Berkeley, CA, USA, 2004, pp. 121–136.
[5] G. R. Goodson, J. J. Wylie, G. R. Ganger, and M. K. Reiter, "Efficient byzantine-tolerant erasure-coded storage," in DSN. IEEE Computer Society, 2004, pp. 135–144.
[6] V. Kher and Y. Kim, "Securing distributed storage: challenges, techniques, and systems," in StorageSS, V. Atluri, P. Samarati, W. Yurcik, L. Brumbaugh, and Y. Zhou, Eds. ACM, 2005, pp. 9–25.
[7] L. N. Bairavasundaram, G. R. Goodson, S. Pasupathy, and J. Schindler, "An analysis of latent sector errors in disk drives," in SIGMETRICS, L. Golubchik, M. H. Ammar, and M. Harchol-Balter, Eds. ACM, 2007, pp. 289–300.
[8] B. Schroeder and G. A. Gibson, "Disk failures in the real world: What does an mttf of 1, 000, 000 hours mean to you?" in FAST. USENIX, 2007, pp. 1–16.
[9] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A cooperative internet backup scheme," in USENIX Annual Technical Conference, General Track. USENIX, 2003, pp. 29–41.
[10] Y. Deswarte, J. Quisquater, and A. Saidane, "Remote integrity checking," in The Sixth Working Conference on Integrity and Internal Control in Information Systems (IICIS). Springer Netherlands, November 2004.

BIOGRAPHIES

B.Jesse Kiranmai completed B.Tech IT (Information technology) from Vishnu institute of technology under the jntuk.M.Tech Dept.of Computer Science and Engineering from Avanthi Institute of Engineering and Technology Visakhapatnam, Andhra Pradesh. Under jntuk.

N.V.Ashok Kumar. M.Tech(CSE) He received theB.Tech degree in Computer Science and Engineering from JNT University Kukatpalli, Hyderabad and received the M.Tech degree in Computer Science and Engineering from JNT University, Kakinada Presently he is working as Associate Professor in Computer Science and Engineering in Avanth iInstitute of Engineering and Technology, Vizag, A.P. His research interests include Network Security, Data Warehousing and Data Mining and RDBMS .He has Published more than 10 papers in various national and international journals.

Dr.C.P.V.N.J Mohan Rao is Professor in the Department of Computer Scienceand Engineering, Avanthi Institute of Engineering &Technology - Narsipatnam. He did his PhD from Andhra University and his research interests include Image Processing, Networks, Information security, Data Mining and Software Engineering. He has guided more than 50 M.Tech Projects and currently guiding four research scholars for Ph.D. He received many honors and he has been the member for many expert committees, member of many professional bodies and Resource person for various organizations.