Elliptic Curve Digital Signature Algorithm for the Third Party Auditing

Srinivasulu Pathakamuri, B.V. Ramana Reddy, A.P. Siva Kumar

Abstract*: Cloud computing usage has been highly increased in past decades, and this has many features to effectively store, organize and process the data. The major concern in the cloud is that security is low and user requires verification process for the data integrity. Third Party Auditing (TPA) technique is applied to verify the integrity of data and various methods has been proposed in TPA for effective performance. The existing methods in TPA has the lower performance in communication overhead and execution time. In this research, Elliptic Curve Digital Signature (ECDS) is proposed to increase the efficiency of the TPA. Bilinear mapping technique is used for verification process without retrieving the data and this helps to reduce the communication overhead. The performance of ECDA is measured and compared with the existing method to analyze the performance.

Index Terms*: Bilinear mapping, Cloud computing, Communication overhead, Elliptic Curve Digital Signature and Third Party Auditing.

I. INTRODUCTION

Cloud computing has provided a way to store large data and due to its advantages like flexibility, scalability and reliability, cloud computing attracts many users. Cloud computing incur some security issues such as data integrity, data encryption etc. Cloud auditing is the technique to verify the integrity of data [1]. Cryptographic keys are generated for cloud data, which are required to be stored and protected. The key storage facility compromise may also lead to data loss. The cryptographic key is required to be stored with security and single point of failure should affect the data availability [2]. Despite the powerful machine and strong security mechanism provided by the Cloud Service Providers (CSP), remote data still faces security issues due to hardware and administration errors [3]. Cloud auditing is used to verify data integrity in the cloud. To reduce the burden for the client and make more convenient, Third-Party Auditing (TPA) was introduced [4]. The owner can modify, delete the existing block by using dynamic support and also owner can insert a new block. This is important step in the cloud storage and many applications were not limited to store the data in cloud [5].

Generally, cloud denotes a public cloud, users were not limited on access of the data in the cloud. Several users and devices can access the cloud and this should have access control mechanism [6]. Authenticators security is protected by using the Binary tree structure before the key exposure [7]. Traditional integrity verification method is very limited in the computation and communication abilities and doesn't satisfy the required applications [8]. To effectively process cloud auditing for the large amount of data with limited computation time, an efficient method is needed [9 - 10]. In this research, ECDSA method is used to increase the performance of the TPA for cloud auditing. The proposed ECDSA method has advantages of a lower key size and suitable for a constrained environment like TPA. The lower key size helps to minimize the computation overhead and computation time of the integrity check. Bilinear mapping technique is used to verify the data without need of the original data from the cloud.

The organization of the paper is given as, the literature works of existing TPA method is detailed in section 2, proposed ECDSA method is detailed in section 3, experimental result is discussed in section 4 and conclusion is provided in section 5.

II. LITERATURE WORKS

Cloud computing is highly used to run the application and store data due to its flexibility, scalability and reliability. One major concern in the cloud computing is that security and user require the proof for the integrity of data. Many research studies have been conducted in the TPA to check the data integrity. Recent research involved in the TPA in cloud storage is studied in this section.

Suguna and Shalinie, [11] proposed a technique for the generation of verification proof is called as a small signature that minimizes the client side auditing overhead. Bilinear mapping is applied to verify without retrieving the original data, is called as a blockless process. Merkel Hash Tree (MHT) is applied in the authentication process to increase security. The developed method has a higher performance for the verification process in the manner of storage and communication overhead. The de-duplication technique is used to increase the efficiency of the developed method.

Guo, *et al*. [12] proposed key generation authentication cryptosystem that creates a constant size key for the shared encrypted data in cloud computing. The authentication process is used to solve the key leakage problem. The cloud server uses the public key to identify the data owner to provide access.

Revised Manuscript Received on December 08, 2019
Corresponding Author*
Srinivasulu Pathakamuri*, Department of CSE, JNT University, Anantapur, India.
Dr. B.V. Ramana Reddy, Department of CSE, KSRM College of Engineering, Kadapa, India.
Dr. A.P. Siva Kumar, Department of CSE, JNT University, Anantapur, India.

The developed method is used to achieve the higher efficiency, secure data sharing and leakage-resistance. The key generation is stable and the security of the method is high. The generated key has the linear relationship with the classes in the data and key collusion is need to be reduced.

Li, *et al*. [13] developed a method of Provable Data Integrity (PDI) to verify the data integrity in the cloud. This technique is based on the bilinear group and provide simple and efficient audit service. The PDI supports the dynamic data and public verification in the cloud auditing. The developed method has the higher performance than the other existing methods. The developed method has the low client cost due the constant metadata generation and the cost of verification is reduced. The method security and efficiency is need to be increased.

Yu, *et al*. [14] developed a cloud data integrity auditing method using identity to increase the security. The method provides a model of the identity based on RSA technique. The identity based method with RSA technique supports the variable sized blocks. The identity based method reduces the complexity of the certificate in the cloud data integrity check. The communication overhead is reduced in the method and file retrieval is not conducted for verification rather spot checking technique is used. The security analysis of the developed method is shows that the performance of the method is considerable. The computation time of the auditing method is need to be reduced for efficient performance.

Xiang, *et al*. [15] proposed verifiable auditing method for the TPA to increase the security in the cloud. The method simultaneously process completeness and correctness of the query search and secure the data against the dishonest CSP. The method supports the flexible data dynamics and partial attribute retrieval. The security proof of the method shows that the developed method has the higher performance in the TPA. The partial attribute retrieval is used to minimize the communication overhead and the method analyze the data integrity at element level. The Dynamic adjustable capacity Cuckoo filter and paillier encryption is used to increase the performance of this method. The experimental analysis shows that the performance is high for the developed method. The communication overhead is further required to be reduced and de-duplication technique can be used.

III. PROPOSED ECDSA BASED THIRD PARTY AUDITING SCHEME FOR SECURE CLOUD STORAGE

Cloud computing usage is high due to its advantages of flexibility, scalability and reliability in storing the data. The major concern in cloud computing is security and the user requires a method to check the integrity of data. The TPA is used to check the user data integrity in the cloud and provide the proof of verification. Many existing methods were applied in the TPA process to check the integrity, and this has a higher overhead in the communication. In this method, ECDSA is used in the TPA to increase the efficiency of the data integrity method. The bilinear mapping is applied for data verification without affecting the integrity in the system. The proposed ECDSA method is evaluated in the TPA to evaluate the developed method efficiency. The basic process in the TPA is shown in the Fig. 1.

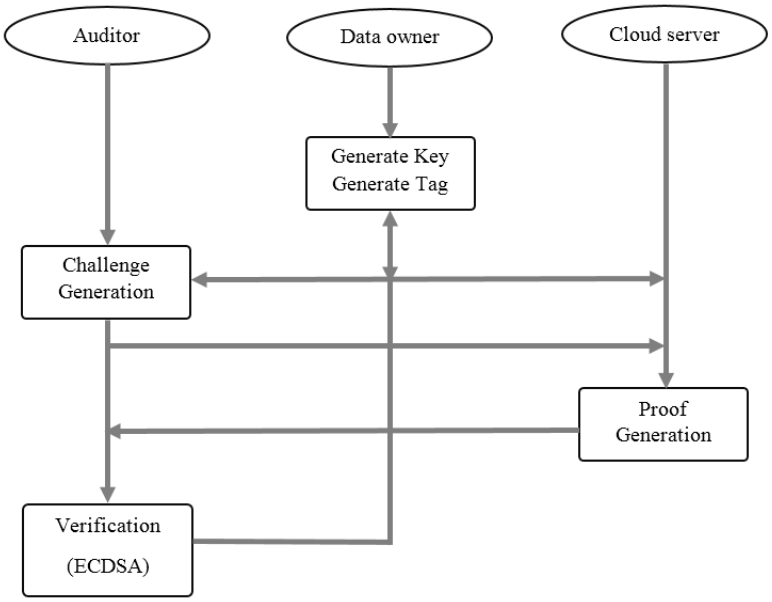

Figure 1. The basic operation in TPA based on ECDSA

System model: The proposed system for TPA has the three entities namely, Data owners, the cloud server and TPA. Each entity of the TPA is discussed as below:

Data Owner: The data owners are those who stored the data in the cloud and communicate with CSP to manage the cloud data. After the data is stored, data owner can verify the integrity of their data. In some cases, the data owner assigns the TPA to check the data integrity in the cloud.

Cloud Service Provider: CSP has the huge resources and expertise in building, managing and allow the user to store the data in the distributed manner to offer the storage and services to customer through Internet. The CSP is responsible for data maintenance and privacy.

Third Party Auditor: This will analyze the cloud data instead of Data owner without retrieving the original data. Data stored in the cloud are verified by the TPA and audition process is conducted to find data integrity. Once Data owner sends the request to the TPA, then TPA immediately sends the challenge request to the cloud server. The Cloud sends proper response to the TPA and provide the proof for the data integrity.

A. Bilinear Mapping

Bilinear map [15] is applied in the cloud data to generate the signature that is used to authenticate the signed messages. Consider three multiplicative G_1, G_2 and G_T is the cyclic group of prime order p, g_1. The g_1 and g_2 are the generator of G_1 and G_2 . A bilinear map e $G_1 \times G_2 \mapsto\to G_T$ consists of given properties:

1. Computability: The polynomial time algorithm is used for compute the map e effectively.
2. Bilinearity: For all $u \in G1$, $v \in G2$ and $a,b \in Zp, e(u\,a, vb) = e(u,v)ab$.
3. Non-degeneracy: $e(g1, g2) \neq 1$.

B. Ecliptic Curve Digital Signature

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a variant of Digital Signature Algorithm (DSA) based on the Elliptic Curve Cryptography. This method is most widely used in the FIPS 186-2, ANSI X9.62, ISO/IEC 15946-2 and IEEE 1363-2000 standards and several other draft standards. This method is compactable with Edwards Curves [16]. The first step in ECDSA is applying curve parameter for signal generation and verification. To create a similarity of message m, first an owner create a key pair (d,Q). The private key d is randomly chosen between $[1, n-1]$ and public key is processed as $Q = dG$, where G is the generation point of curve. The ECDSA algorithm signature generation for message m using signer's key pair is shown below.

Algorithm: ECDSA signature generation

Input: $D = (m, f(x), G, n, h)$, private key d, message m, hash function H.

Output: Signature (r, s).

1. Select $k \in_R [1, n-1]$.
2. Compute $KG = (x_1, y_1)$ and convert x_1 to an integer $\overline{x_1}$.
3. Compute $r = \overline{x_1} \bmod n$. If $r = 0$ got to step 1.
4. Compute $e = H(m)$.
5. Compute $s = k^{-1}(e + dr) \bmod n$. If $s = 0$ go to step 1.
6. Return (r, s).

Likewise, the public key signer's copy is required for a given message signature verification, as shown in algorithm below. Both algorithm uses the cryptographic hash function H , which must have output bit length, but not longer than n . If the condition is fulfilled, then the output of H can be truncated.

Algorithm: ECDSA Signature verification

Input: $D = (m, f(x), G, n, h)$, public key Q, message m, Signature s.

Output: Acceptance or rejection of the signature.

1. Verify that r and s are integers in the interval $[1, n-1]$. If verification fails return "**Invalid**".
2. Compute $e = H(m)$.
3. Compute $w = s^{-1} \bmod n$.
4. Compute $u_1 = ew \bmod n$ and $u_2 = rw \bmod n$.
5. Compute $X = u_1G + u_2Q$.
6. If $X = \infty$ return "**Invalid**".
7. Convert the x-coordinate x_1 of X to an integer $\overline{x_1}$; compute $v = \overline{x_1} \bmod n$.
8. If $v = r$ then return "**Valid**";
   Else return "**Invalid**".

The proposed ECDSA method is evaluated in the TPA and analyzed its performance for the method efficiency. The proposed ECDSA method is compared with the existing method to analyze the performance.

IV. EXPERIMENTAL RESULT

Cloud auditing method is applied to verify the cloud data integrity for users. Different methods were proposed in the TPA to effectively analyze the data integrity in the cloud. Existing methods of cloud auditing involves in the high computation overhead in integrity data check. In this research, the ECDSA is proposed for the TPA to increase the efficiency of the method. The ECDSA method is evaluated in the cloud auditing and analyzed its effectiveness.

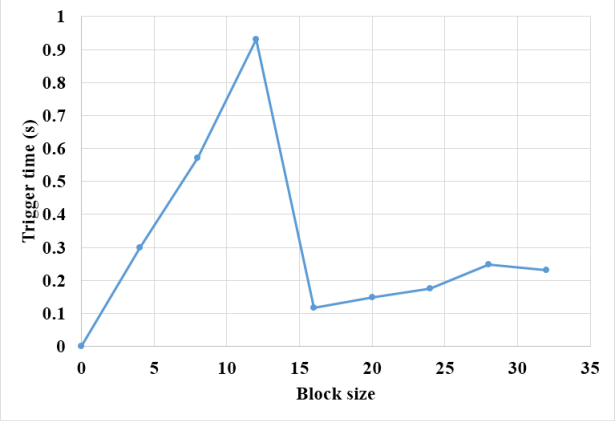

Figure 2. Trigger time of the proposed ECDSA method with various block size

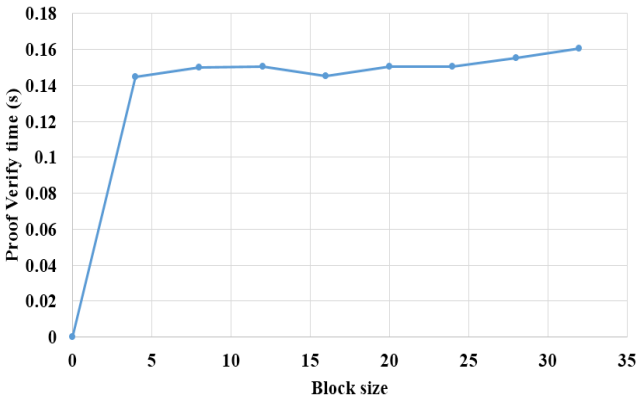

Figure 3. Proof verify time

The trigger time of the proposed ECDSA method is tested with various block size to analyze the performance, which is shown in Fig. 2. This shows that the ECDSA method has the lower trigger time for the various block size. For the blocks size with more than 20 has the lower trigger time and block size with 4 to 16 block size has the higher trigger time. The trigger time is higher for the block size of 16 and has 0.93 s. The trigger time of ECDSA method is low and can be applied to the cloud auditing process.

The proof verification time for the ECDSA method was evaluated with various block size and shown in the Fig. 3. The proof verify time of the proposed ECDSA is low and applied for the TPA process. The proof verification time is present in the range of 14 ms to 16 ms. The verification process has been carried out in the lower time consumption. For the block size of 32, the proof verification time is 0.1607 s.

The challenge time of the ECDSA method is calculated for various number of blocks, which is represented in Fig. 4. The challenge time of the ECDSA method is low and used for the TPA for the data check integrity. The challenge time for 1000 number of blocks is 15.14 s and challenge time for 500 number of blocks is 7.582 s. The challenge time is increases with increases of the number of blocks in the analysis.

Hence, the proposed ECDSA method has the lower computation time in the TPA for data integrity check in cloud. The challenge time of the ECDSA method is low and can be applied for the TPA.

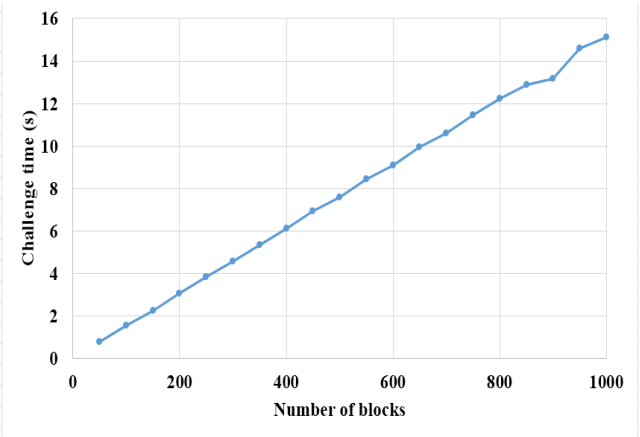

Figure 4. Challenge time

V. CONCLUSION

Cloud computing is highly used in the many organization as well as individuals, but one of the major thread is security. User requires the proof of integrity of data that are stored in the cloud and TPA technique is used to check the cloud data integrity. Many existing methods involves in the integrity check in the cloud. These methods have high communication overhead that affects the efficiency of the TPA. In this research, the ECDSA is proposed to increase the data integrity check efficiency. Bilinear mapping is used for the verification process without retrieving the actual data from cloud. ECDSA has the smaller encryption key and provides the faster computation with less storage space. The experimental analysis of ECDSA in TPA confirms that the ECDSA has the higher performance compared to other techniques. The future work of the method involves in develop ECDSA against key collusion.

REFERENCES

1. W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy-preserving secure cloud auditing scheme for group users via the third party medium," Journal of Network and Computer Applications, vol. 82, pp.56-64, 2017.
2. M. Ali, S.U. Malik, and S.U. Khan, "DaSCE: Data security for cloud environment with semi-trusted third party," IEEE Transactions on Cloud Computing, vol. 5, no. 4, pp.642-655, 2015.
3. H. Jin, H. Jiang, and K. Zhou, "Dynamic and public auditing with fair arbitration for cloud data," IEEE transactions on cloud computing, vol. 6, no. 3, pp. 680-693, 2016.
4. J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, "An efficient public auditing protocol with novel dynamic structure for cloud data," IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp.2402-2415, 2017.
5. Z. Ren, L. Wang, Q. Wang, and M. Xu, "Dynamic proofs of retrievability for coded cloud storage systemsm" IEEE Transactions on Services Computing, vol. 11, no. 4, pp.685-698, 2015.
6. J. Shen, D. Liu, D. He, X. Huang, and Y. Xiang, "Algebraic signatures-based data integrity auditing for efficient data dynamics in cloud computing," IEEE Transactions on Sustainable Computing, pp1-1, 2017.
7. J. Yu, and H. Wang, "Strong key-exposure resilient auditing for secure cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp.1931-1940, 2017.
8. D. He, N. Kumar, S. Zeadally, and H. Wang, "Certificateless provable data possession scheme for cloud-based smart grid data management systems," IEEE Transactions on Industrial Informatics, vol. 14, no. 3, pp.1232-1241, 2017.
9. G.S. Aujla, R. Chaudhary, N. Kumar, A.K. Das, and J.J. Rodrigues, "SecSVA: secure storage, verification, and auditing of big data in the cloud environment," IEEE Communications Magazine, vol. 56, no. 1, pp.78-85, 2018.
10. Y. Yu, M.H. Au, G. Ateniese, X. Huang, W. Susilo, Y. Dai, and G. Min, "Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage," IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp.767-778, 2016.
11. M. Suguna, and S.M. Shalinie, "Privacy preserving auditing protocol for remote data storage," Cluster Computing, pp.1-8, 2018.
12. C. Guo, N. Luo, M.Z.A. Bhuiyan, Y. Jie, Y. Chen, B. Feng, and M. Alam, "Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage," Future Generation Computer Systems, vol. 84, pp.190-199, 2018.
13. A. Li, S. Tan, and Y. Jia, "A method for achieving provable data integrity in cloud computing," The Journal of Supercomputing, vol. 75, no. 1, pp.92-108, 2019.
14. Y. Yu, L. Xue, M.H. Au, W. Susilo, J. Ni, Y. Zhang, A.V. Vasilakos, and J. Shen, "Cloud data integrity checking with an identity-based auditing mechanism from RSA," Future Generation Computer Systems, vol. 62, pp.85-91, 2016.

15. T. Xiang, X. Li, F. Chen, Y. Yang, and S. Zhang, "Achieving verifiable, dynamic and efficient auditing for outsourced database in cloud," Journal of Parallel and Distributed Computing, vol. 112, pp.97-107, 2018.
16. A.P. Fournaris, C. Dimopoulos, A. Moschos, and O. Koufopavlou, "Design and leakage assessment of side channel attack resistant binary edwards Elliptic Curve digital signature algorithm architectures," Microprocessors and Microsystems, vol. 64, pp.73-87, 2019.

AUTHORS PROFILE

P. Srinivasulu is a Research Scholar in CSE, JNT University, Anantapur, Andhra Pradesh, India. Pursuing Ph.D at JNTUA on Cloud Computing Security Area. He is dedicated to teaching field and having more than 10 years of Experience. His research areas included Network Security and Cloud Computing.

Dr. B. V. Ramana Reddy received B.Tech Degree from S.V. University, Tirupati, A.P., India in 1991. He completed M.Tech. in Computer Science from IPGSR, JNT University, Masab Tank, Hyderabad, India in 2002 and received PhD from JNTUA, Anantapur, A.P., India in 2011. He has more than 25 years of teaching and industrial experience. He worked as HOD, Dean, vice principal and principal in various reputed colleges. He is currently working as Professor in CSE & Coordinator/IQAC, KSRM College of Engineering, Kadapa, A.P., India. He is a life member of Indian Science Congress Association. He published nearly 40 papers in National and International Journals and conferences.

Dr. A. P. Siva Kumar received B.Tech Degree from JNT University, Hyderabad, A.P., India in 2002. He completed M.Tech. in Computer Science & Engineering from JNT University, Anantapur, A.P., India in 2004 and received PhD from JNTUA, Anantapur, A.P., India in 2011. He has more than 15 years of teaching and industrial experience. He worked as Additional Controller of Examinations in JNTUA, Anantapur. He is currently working as Asst. Professor in CSE & Nodal Officer of TEQIP, JNTUA College of Engineering, Anantapur , AP, India. He published nearly 40 papers in National and International Journals and conferences.