Received: December 7, 2018

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Efficient and Secure Cloud Storage Auditing Based on the Diffie-Hellman Key Exchange

Rokesh Kumar Yarava[1]* **Rajendra Prasad Singh[1]**

[1]*Department of Computer Science Engineering,*
Sri Satya Sai University of Technology & Medical Sciences, Sehore, India
* Corresponding author's Email: rokeshy1@gmail.com

Abstract: Cloud storage auditing technique helps to verify the data integrity in the cloud on behalf of the user. Earlier researcher proposed many techniques on the cloud auditing, but it still lags in computational overhead for the resource constraint users. In this research, the Diffie-Hellman method is used to exchange the key in the Third Party Auditor (TPA) to improve the performance of the auditing method. The key is generated in the third party auditor and this is shared with the user as an encrypted key. The Diffie-Hellman creates the shared encryption key between the two parties and can be communicate in the insecure channel. The Diffie-Hellman generates ephemeral keys and this is extremely fast in generating new key pairs. This method is suitable for the big server and have more efficiency over the state-of-art method, which doesn't involve in ephemeral key generation. The proposed method is evaluated in the simulated environment and compared with the other state-of the art methods. The verification cost of the proposed auditing method has achieved 1.1 s, while the existing method has 1.19s.

Keywords: Cloud storage auditing, Diffie-hellman method, Encrypted key, Integrity of data, Third party auditor, Verification cost.

1. Introduction

Cloud computing is the fusion and development of the parallel computing, distributed computing and grid computing, that connects large scale of storage and computing resources together through the Internet [1]. In an economic recession, cloud computing technology can play a considerable role in public organizations and private sector companies since it reduces the cost of using Information Technological (IT) services [2]. The key features of the cloud computing are on-demand self-service, location-independent resource pooling, broad network access, rapid resource elasticity, and measured service [3]. The Cloud Service Provider (CSP) is responsible for supplying not only plenty of hardware or software resources to host the clients' databases, but also mechanisms for clients to create, access, and update their outsourced data [4]. To host critical infrastructure services in the cloud, a cloud provider needs to offer guarantees, which can be assured, in terms of security and resilience. In elastic cloud environments, services are often subjected to continuous refinements and unpredictable changes, which can change the security and resilience posture of a service, and invalidate the certificates [5]. Cloud data centers should have some mechanisms able to specify storage correctness and data integrity stored on a cloud. Cloud storage auditing helps to verify the integrity of cloud data [6]. The auditing schemes can be broadly categorized into following schemes such as private auditing scheme, which only allows the data owner to check the integrity of the cloud data.

The public auditing scheme allows any public verifier to check integrity of the cloud data [7]. A number of protocols designed to verify the data integrity in the cloud and various techniques used for auditing. In all these protocols, the data owner computes a signature on each block of the data and outsources the data together with the corresponding signatures to the cloud [8]. A typical third-party auditing scheme includes three parties such as the

data owner who outsources its data and signatures into the data center [9]. This technique is also useful for CSP to maintain its reputation by getting higher reliability, consistency, and data integrity ratings [10]. In the proposed method, the Diffie-Hellman method is proposed to improve the efficiency of the cloud auditing technique. The third party auditor generates the key based on the Diffie-Hellman method and the secret key is shared with the user. The proposed method evaluated in the simulated environment and compared with other existing methods. The performance of the proposed method is shown in the experimental result.

The organization of the paper is composed as follows, Literature survey in the section 2, the proposed method explanation is provided in section 3 and the evaluated result is presented in the section 4.

2. Literature survey

The latest research related to the third party auditing with different key generation methods reviewed in this section.

M. Suguna, and S. Mercy Shalinie [11] presented the simplified large scale distribution system with advanced computation power including storage capabilities. This method investigated the data intactness presented in the cloud and demanded data integrity from the service provider. This method introduced a third party verifier for checking the data and maintained dynamic metadata stored locally. The blockless process used in this method and checking was carried out using the bilinear mapping without retrieving the original data. This method reduced the computational overhead and achieved the verification of storage services. This method increased the communication overhead during the verification process.

D. Kim, H. Kwon, C. Hahn, and J. Hur [12] developed a public auditing protocol for an educational multimedia data stored in the cloud. The method ensured data privacy in the cloud by using random values and a holomorphic hash function. The method showed strong protection against lose attack and temper attack. This proposed protocol supports fully dynamic auditing. The result of performance analysis showed that the scheme is secure while guaranteeing minimum computational costs. The communication cost between the user and the TPA is high because the protocol need to ensure the security.

A. Li, S. Tan, and Y. Jia [13] proposed a verification method namely Provable Data Integrity (PDI) for the data, stored in the untrusted cloud. The method attempted to reduce the cost of the initialization phase for executing an auditing protocol by exploiting certain desirable attributes of bilinear groups. The method supports data dynamics and public verifiability. The performance of the method was evaluated by the experiments that showed high efficiency. The data fragment structure in the method affected the auditing time, which increased linearly with the value of the Server and TPA computation time.

J. Yu, K. Ren, and C. Wang [14] focused on making the key transparent as possible for the client and proposed the method for cloud storage auditing with verifiable outsourcing of key. This method outsourced the updated key to the cloud to reduce the burden of the client. TPA only holds the secret key of the client and all remaining key updates are taken care by the proposed method. The client only needs to download the secret key from the TPA while uploading the new files. The security proof and the performance simulation showed that the design is secure and efficient. This method is required to be tested on different attacks.

Y. Yu, L. Xue, M. H. Au, W. Susilo, J. Ni, Y. Zhang, and J. Shen [15] simplify the certificate management in the cloud data integrity by checking protocol using the Identity-Based Cloud Data Integrity Checking (ID-CDIC). This method was developed from the RSA signature supported variable-sized file blocks and public auditing. The scheme provided a security proof under the hardness of the RSA problem with a large public exponent in the random oracle model. The results showed the efficiency of the scheme. The method was unable to change the size of the block once the block size fixed to balance the computation cost of data owner and the verifier.

Wenting Shen, Jia Yu, Hui Xia, Hanlin Zhang, Xiuqing Lu and Rong Hao [16] blind the data before uploading and data auditing for improve the privacy in TPA. The masking technique is utilized by this method that prevent the audition to retrieve the real data from the cloud response. The cloud can retrieve the real data and store in the plaintext and this reduce the decryption time for the user. The challenge is replied to the user who possess the real authority and this method also set the expiry time for each authentication. The security investigation of this technique shows the privacy and soundness. The performance of the method is effective in terms of cost. The execution time need to be reduced in checking the integrity.

Guangyang Yang, Jia Yu, Wenting Shen, Qianqian Su, Zhangjie Fu and Rong Hao [17] developed a public auditing method to preserve the identity privacy and identity traceability. The framework created for the data sharing that can

support the public auditability on remote data. This method developed for the public auditing scheme for the shared cloud data in which identities of group members are anonymous to the TPA. The result showed that the proposed method has little overhead in traceability of the cloud data. More execution time and cost is high in the auditing method.

The Diffie-Hellman key exchange is proposed in the third party auditing to improve the efficiency of the cloud and to overcome the above limitations.

2.1 Key generation techniques of existing method

The key generation technique of W. Shen [16] and G. Yang [17] are shown in this section. As the proposed method uses the Diffie-Hellman method to generate the key pairs.

2.1.1. Algorithm setup (1^k) of Lightweight scheme [16]

In the research of W. Shen [16], the group manager generates the group's public-private key pair, the TPM's public-private key pair, the authorization and the secret seed.

1. The group manager choose a random value $x \in Z_p^*$ as the group private key, and computes $pk_g = g^x$ as the group public key. And then he picks a random element $r_0 \in Z_p^*$ to compute $Y_0 = g^{r_0}$ and $\beta_0 = r_0 + x.H_1(ID_{group}||time_1||time_2, Y_0) mod\ p$, where ID_{group} is the group manager's identity, $time_1$ is the start time and $time_2$ is the end time. Set β_0 as the TPM's private key used to generate data authenticator. Publish $pk_{TPM} = (g^{\beta_0}, u_1^{\beta_0}, u_2^{\beta_0}, \dots, u_s^{\beta_0})$ as the public key of the TPM.
2. The group manager creates the authorization $\{(ID_{group}, ID_{TPM}, time_1, time_2), Y_1, \beta_1\}$ by choosing a random element $r_1 \in Z_p^*$ to calculate $Y_1 = g^{r_1}$ and $\beta_1 = r_1 + x.H_1(ID_{group}, ID_{TPM}, time_1, time_2, Y_1) mod\ p$ as a part of authorization message, where ID_{TPM} is the TPM's identity. And then he chooses a random seed $k_1 \in Z_p^*$ as the input secret key of pseudo-random function. Finally, sends the authorization $\{(ID_{group}, ID_{TPM}, time_1, time_2, Y_1), Y_1, \beta_1\}$ and the private key β_0 to the TPM, and sends the secret seed k_1 to the cloud and users.

2.1.2. Key generation of efficient method [17]

The key generation technique of G. Yang [17] is as follows.

1. The AM runs $IG(1^k)$ to generate two multiplicative groups G_1, G_2 of some large prime order q and an admissible pairing $\hat{e}: G_1 \times G_1 \to G_2$.
2. The AM choose a cryptographic has function $H: Z_q^* \to G_1$, and selects two independent generators $g, u \in G_1$.
3. The AM randomly selects $x \in Z_p^*$ as the group secret key, and computes $PK = g^x$ as the group key
4. The AM randomly selects $x_j \in Z_q^* (j = 1, \dots, s)$ as the individual secret key of group member M_j. The AM sends the secret key x_j to each group member $M_j (j = 1, \dots, s)$, and sets the global parameters to be $(G_1, G_2, \hat{e}, g, u, H, PK)$.
5. The AM computes $x_j' = x - x_j (j = 1, \dots, s)$ as the partial secret keys for group members, and sends them to the GM. Then the GM initializes the IKL list as $IKL = \{(M_1, x_1'), \dots, (M_x, x_s')\}$.

3. Proposed method

Cloud computing is a new technology paradigm with promising growth, that becomes more and more popular nowadays. It can provide users with unlimited computing resource. In this research, the encryption has been made using the digital signature and Diffie-Hellman key exchange along with Integrated Encryption Scheme (IES) is used to provide security to the cloud user. The architecture of the proposed method is shown in the Fig. 1, which contains user and sharing of secret key. The IES technique is used to protect the data in the cloud with the help of ECDLP. If the key is hacked, the Diffie-Hellman makes the key as useless that has no use without the secret key. The secret key is provided to the user in the confidential manner and this will improve the security. The encrypted key is fed to the TPA in order to check the integrity of data without affecting the privacy. The proposed method protect the data based on the secret key which makes it tough for the hacker to access the cloud data. The data in the cloud is encrypted using the proposed method before send it to the TPA. The integrity has been

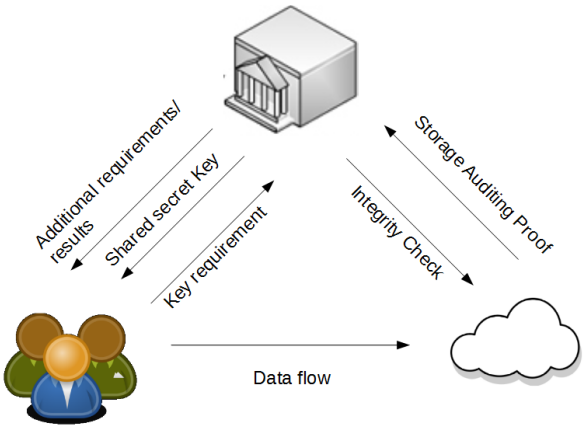

Figure.1 Architecture of cloud auditing

checked by the TPA and send the proof back to the cloud. The decryption key is provided to the user and the user can access the data with proof in the cloud using the key. This data identity is preserved even when it sends through the insecure channel, which increases the privacy of the cloud user.

3.1 Integrated encryption scheme

The elliptic curves are used for developing a cryptosystem, which is based on Elliptic Curve Discrete Logarithm Problem (ECDLP). This problem can be explained as follows: an elliptic curve E defined over a finite field Fq of q elements, a point G on the curve E(Fq) of order n, and a point P on the same curve, find the integer k ∈ [0, n - 1] such that P = k · G

So far, there is no algorithm to solve the ECDLP in an efficient way and this problem is more difficult to solve compared to other mathematical problems used in Cryptography, such as the Discrete Logarithm Problem or the Integer Factorization Problem. This characteristic of elliptic curve is well-suited for the devices with limited resources such as smart card and some mobile devices. In order to clarify the notation, some basic definitions and characteristics of elliptic curves has been presented. The general Weierstrass equation can be used to define an elliptic curve over a finite field from the Eq. (1).

$$E(\mathbb{F}_q): y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

Where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$ and$\Delta \neq 0$, Δ being the discriminant of the curve.

In practice, instead of the general Weierstrass equation, two short Weierstrass forms that depend on the properties of the finite field $\mathbb{F}_q$ are typically used:

If the finite field has p elements, where $p > 3$ is a prime number, then $\mathbb{F}_q = \mathbb{F}_p$, and the Eq. (1) is reduced to Eq.(2).

$$y^2 = x^3 + ax + b \quad (2)$$

If the finite field has 2^m elements, then$\mathbb{F}_q = F_{2^m}$, and the Eq. (1) can be written as follows in Eq. (3).

$$y^2 + xy = x^3 + ax^2 + b \quad (3)$$

The parameters in any elliptic curve implementation depend on the underlying finite field. When the field is$\mathbb{F}_q$, the parameters that define the curve is $\mathcal{P} = (p, a, b, G, n, h)$, whereas if the finite field is F_{2^m}, the parameter is $\mathcal{P} = (m, f(x), a, b, G, n, h)$. The meaning of each element in both sets is represented as follows:

- p is the prime number that characterizes the finite field $\mathbb{F}_p$.
- m is the integer number specifying the finite field $\mathbb{F}_{2^m}$.
- $f(x)$ is the irreducible polynomial of measure m defining $\mathbb{F}_{2^m}$.
- a and b are the elements in the finite field $\mathbb{F}_q$ taking part in the Eq. (2) and (3)
- G is the point of the curve that will be used as a generator of the points that belongs to a cyclic subgroup of the curve.
- n is the prime number whose value represents the order of the point G.
- h is the cofactor of the curve, computed as $h = \#E(\mathbb{F}_q)/n$, where $\#E(\mathbb{F}_q)$ is the number of points on the curve.

3.2 Diffie-Hellman

This method allows two principals A and B that communicate over a public network, which contains matching public/private keys to agree on a shared secret value. Diffie-Hellman generates the ephemeral keys and are extremely fast in the generating key pairs. This is convenient for the big server and provide much security. The encryption has been made on the cloud data before it process to the integrity check and the key has been provided to the user for decryption process.

$$\Pr[\Delta(g^{x_1}, g^{x_2}, g^{x_1,x_2} = "True"] - \Pr[\Delta(g^{x_1}, g^{x_2}, g^{r}) = "True"]| \geq \in \quad (4)$$

This difference of probabilities can be denoted as $Adv_G^{ddh}(\Delta)$, shown in Eq. (4). The problem of

DDH is $(T, \in)$ intractable if there is no $(T, \in)$-DDH-distinguisher for$\mathbb{G}$.

A $(T, \in)$-CDH-attacker for $\mathbb{G}$ is a probabilistic Turing machine Δ running in time T that given (g^{x_1}, g^{x_2}), outputs $g^{x_1 x_2}$ with probability at least$\in =$ $Succ_{\mathbb{G}}^{cdh}(\Delta)$. The CDH problem is $(T, \in)$-attacker for$\mathbb{G}$.

Let $\mathbb{G} =< g >$ be a cyclic group of prime order p and n be a polynomial-bounded integer. Let I_n be$\{1, \dots, n\}$, $\mathcal{P}(I_n)$ be the set of all subsets of I_n and Γ be a subset of $\mathcal{P}(I_n)$ such that$I_n \notin \Gamma$.

The group Diffie-Hellman distribution is defined in the Eq. (5)

$$GG - CDH_{\Gamma} = \{\cup_{J \in \Gamma}(J, g^{\Pi_{j \in J} x_j}) | (x_1, \dots, x_n) \in_R \mathbb{Z}_p^n\} \quad (5)$$

If$\Gamma = \mathcal{P}(I)/\{I_n\}$, we say that $G - CDH_{\Gamma}$ is the Full Generalized Diffie-Hellman distribution.

GivenΓ, a $(T, \in)$ $G - CDH_{\Gamma}$-attacker for $\mathbb{G}$ is a probabilistic Turning machine Δ running in time T that given $G - CDH_{\Gamma}$ outputs $g^{x_1, \dots, x_n}$ with probability at least ϵ .It denote this probability by$Succ_{\mathbb{G}}^{gcdh}(\Delta)$. The $G - CDH_{\Gamma}$ problem is (T, ϵ)-intractable if there is no $(T, \epsilon) - G - CDH_{\Gamma}$-attacker for$\mathbb{G}$.

In the same way, it can define a $G - DDH_{\Gamma}$ distinguisher as a probabilistic Turning machine that given $G - DDH_{\Gamma}$ and either $g^{x_1, \dots, x_n}$ or a random value, can distinguish the two situation with non-negligible probability.

Key exchange:

Public Information:

An odd integer$N > 6$. A prime$p > N$.

Distinct and invertible integers $\tau_1, \tau_2, \dots, \tau_N$ $(mod\ p)$.

The key extractor$E: B_{N+1} \to K_{N,p}$.

A publicly known element$u \in B_(N + 1)$.

Two subgroups ofB_N:

$$S_A =< x_1, x_2, \dots, \frac{x(N-1)}{2} >,$$
$$S_B =< \frac{x(N+3)}{2}, \frac{x(N+5)}{2}, \dots, x_N >.$$

Here $x_1, x_2, \dots, x_N$ denote the Artin generators ofB_{N+1}.

Secret keys:

Alice's secret key $X \in S_A$.

Bob's secret key $Y \in S_B$.

Public keys:

Alice's public key $X^{-1} u X$

Bob's public key $Y^{-1} u Y$

Shared Secret:

$E(X^{-1} Y^{-1} u X Y)$

3.3 Auditing

To check the integrity of the outsourced data, the TPA sends a request to the CSP, which containing a challenge key K_c , using a secure channel. After receiving the key, the CSP first computes F_c from the F and K_c using Diffie hellman, and then computes F_T using a double block transportation inverse key in Eq. (6) and (7):

$$F_c = H(F || K_c) \quad (6)$$

$$F_T = T(T(\sigma, K_{T2}), K_{T1}) \quad (7)$$

Finally, the CSP generates audit key K_a as Eq. (8).

$$K_a = F_T \ XOR \ F_c \quad (8)$$

Then, the CSP sends audit key K_a to the TPA. After receiving audit keyK_a, the TPA compares audit key K_a with verification key K_v. If the two keys match, then the TPA ensures that the file is stored correctly and is unmodified, denoted in Eq. (9).

$$K_v = K_a \quad (9)$$

This technique helps to verify the integrity of data in the cloud without affecting the privacy of the data. The proposed Diffie-Hellman in encryption method is processed and evaluated, then the result is compared with other state-of-art method.

4. Experimental result

The cloud computing incurs from some new security issues, for example, integrity checking for cloud data and the search of keyword carried on the encrypted cloud data. Cloud storage auditing is used to check the cloud data integrity. The new method has been proposed to increase the security and efficiency of the auditing technique. The Diffie-Hellman key exchanger technique used in the TPA helps to improve the performance. The proposed ADH technique is tested with the cloud environment and compared with other state-of-art encryption techniques. The section gives the efficiency about the performance of the proposed method. The experimental result has been tested with state-of-art methods to analysis the efficiency.

The research of [16] used the third party medium to perform the integrity check on the cloud on behalf

of the user. The blind data using simple operation used for the phase of data uploading and data auditing. The method used in the research [16] has considerable performance in cloud auditing. The public auditing method proposed in the research [17], preserved the privacy and identifying group member simultaneously. This method has a notable performance in the cloud auditing method for data privacy. These two methods are used to compare with the proposed ADH method of cloud auditing for analyzing the performance. The cost of challenge acquired by the proposed method compared with exiting method in the Table 1. The cost of proof generation compared with exiting algorithm is shown in the Table 2.

Table 1. Cost of challenge

Block Size	Challenge cost [16]	Challenge cost [17]	Challenge cost of ADH
0	0	0	0
200	0.13	0.08	0.15
400	0.21	0.19	0.16
600	0.24	0.25	0.19
800	0.32	0.37	0.28
1000	0.37	0.42	0.42

Table 2. Cost of proof generation

Block Size	Proof cost [16]	Proof cost [17]	Proof cost of ADH
0	0	0	0
200	0.39	0.21	0.16
400	0.72	0.42	0.31
600	1.17	0.65	0.45
800	1.52	0.91	0.53
1000	1.86	1.09	0.9

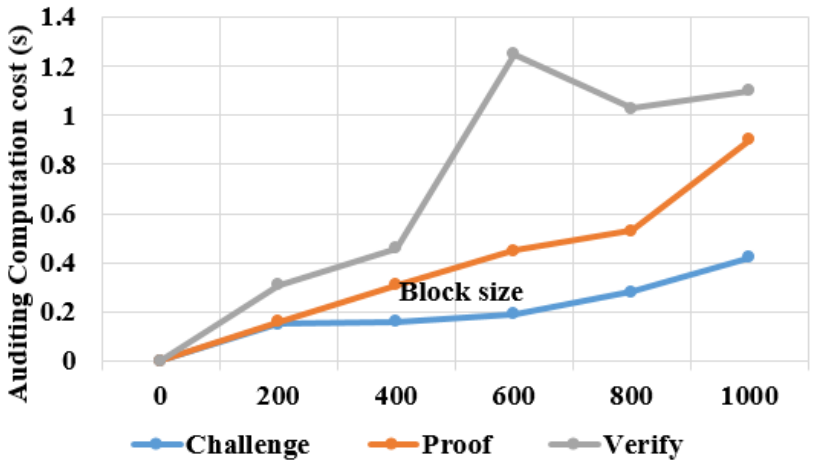

Figure.2 Auditing computation time of various process

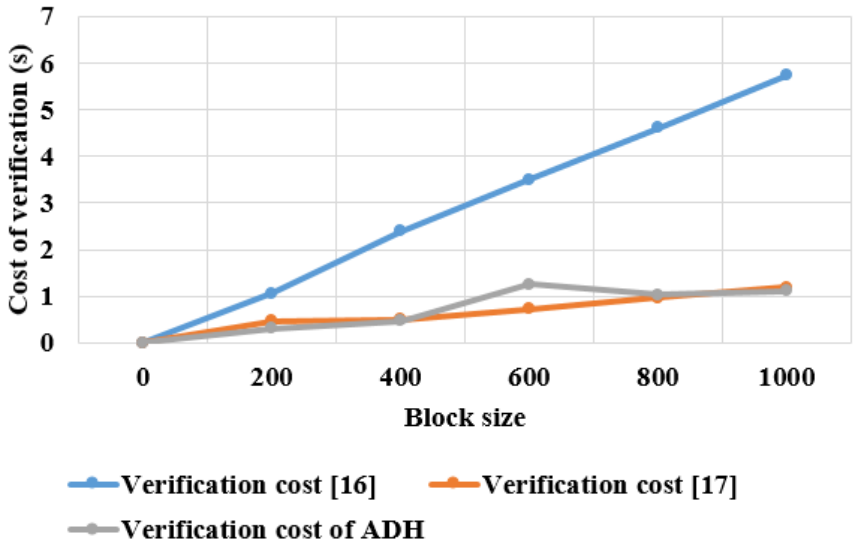

Figure.3 Verification cost

The computation cost is the time taken by the technique to complete the process that has been tested with a set of blocks. Set of blocks of data are processed through cloud and the integrity has been checked with the TPA using the proposed method. The computation cost of the auditing is measured for the various block sizes. The different process involves in computing auditing measured for different block size and plotted in graph, as shown in Fig. 2. The three processes in auditing are Challenge, proof and verifies, measured for the proposed method. The verification process has the higher computation cost compared to the other two processes.

The proposed method evaluated in the simulated environment. Along with this state-of-art method also evaluated in the same environment. The verification cost has been evaluated for the existing method and ADH, the values are compared in the graph, as shown in Fig. 3. The auditing method used in the research [16] has higher cost compared to the other two methods. The proposed method has higher performance in the most of block size. The verification cost of [17] has higher performance in the block size of 600. In the remaining scenario, the proposed method has better performance compared to other techniques.

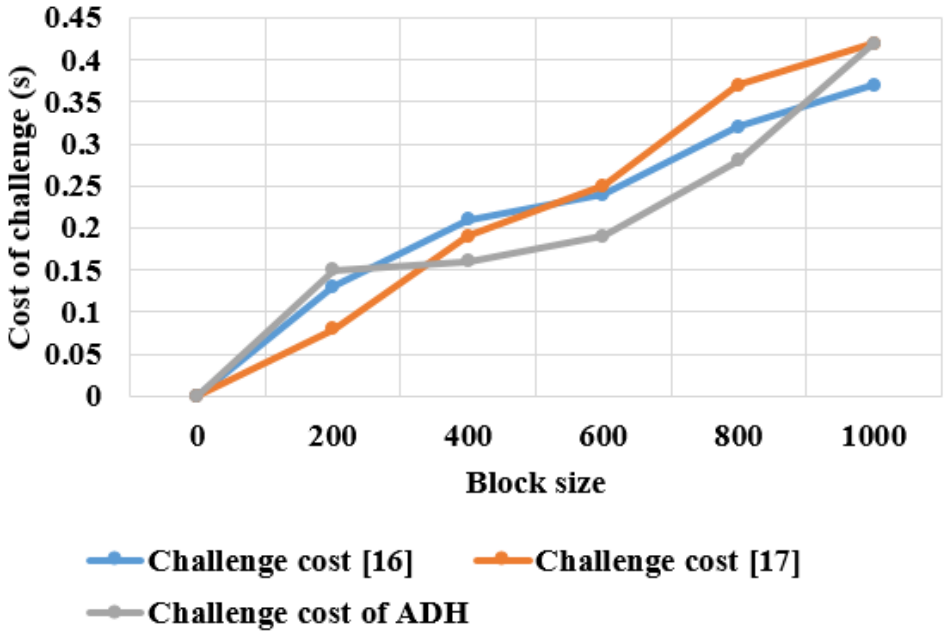

Figure.4 Challenge cost of different methods

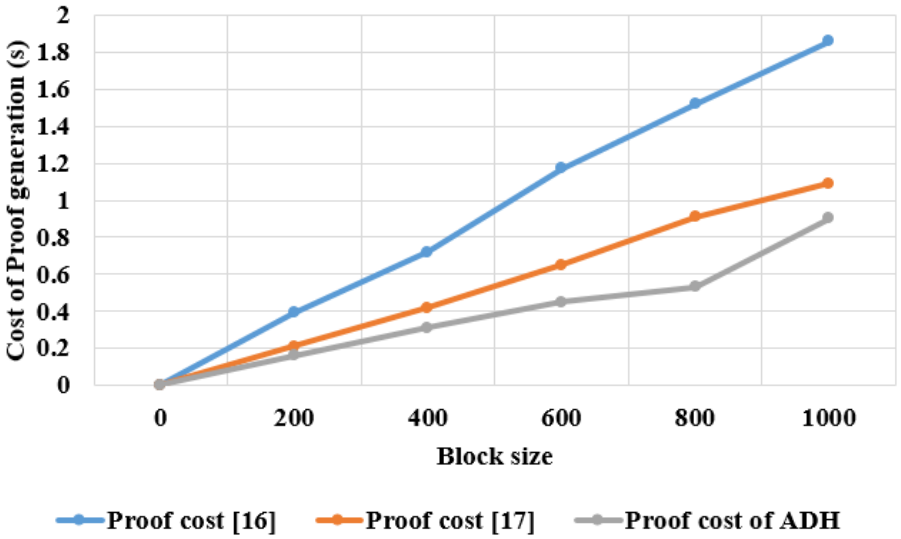

Figure.5 Cost of Proof generation

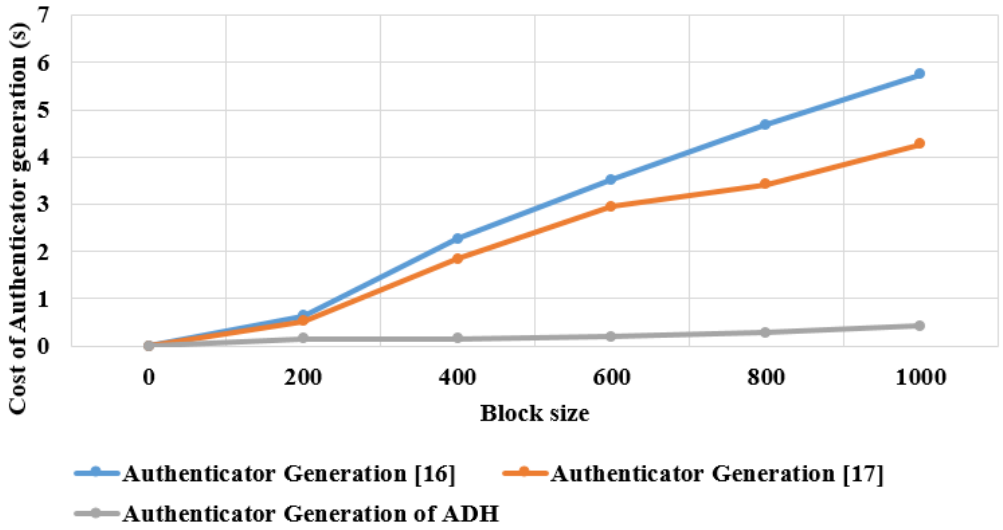

Figure.6 Cost of Authenticator generation

Table 3. Cost of authenticator generation

Block Size	Authenticator Generation [16]	Authenticator Generation [17]	Authenticator Generation of ADH
0	0	0	0
200	0.64	0.52	0.15
400	2.27	1.85	0.16
600	3.52	2.95	0.19
800	4.68	3.42	0.28
1000	5.75	4.27	0.42

The challenge cost is measured for three methods and comparative graph of those methods plotted in the Fig. 4. The challenge cost measured for the different block size and compared with three methods. In most scenarios, the proposed method showed higher performance compared to the other technique.

W. Shen [16] and G. Yang [17] methods are based on the generating the key for communication and key changes not occurs in the short period. The Diffie-Hellman generate ephemeral key and this helps to increases the security. As the Diffie-Hellman are extremely fast in generating the key pair and suitable for the big server. However, the existing methods are slow in creating key pairs compared to the proposed method. Due to this, cost function of the Diffie-Hellman is low compared to the existing method.

The cost of proof has been measured for the different method that has been compared in the graph, as shown in Fig. 5. The proof cost has been measured for the different block size and this value is compared with existing methods. This shows that the proposed method has higher performance compared to other two state-of-art method. The effectiveness of the proposed encryption method is shown in the Fig. 5 and the proof cost of method [17] has better performance than the method [16]. The cost of authentication is compared with exiting method in the Table 3.

The proposed method doesn't allow the third party to involve in the encrypted data and this can be communicated through insecure channel. The exiting method has the higher functions to encrypt the data compared to the proposed method. Hence, the proposed method has the lower cost compare to the other two existing methods. The complexity of the exiting method is also high compared to the proposed method.

The different auditing methods is evaluated in the same environment and compared with each other. The authenticator generation cost is measured for different blocks and shown in the Fig. 6. Therefore, the ADH method has higher performance in cloud auditing method compared to the other methods.

5. Conclusion

Several studies were made for checking the data integrity in the cloud using TPA. This research aims to improve the efficiency of the cloud auditing based on the Diffie-Hellman method for key exchange. The key is generated using the Diffie-Hellman and this key is shared with the user. The proposed encryption method is measured in the manner of various execution cost and this shows an effective performance. The proposed method is tested with state-of-art method to analyze the performance. The robustness of the proposed method discussed in the paper and this shows that Diffie-Hellman can be applied for commercial cloud auditing. The cost of proof generation of the proposed method is 0.9 s while the existing method is 1.09 s. The proposed

method has lower cost compared to the existing method due to the simpler key is used for encryption. The future work may involve in measuring the complexity of the key generation and increase the security.

References

[1] C. Yang, X. Chen, and Y. Xiang, "Blockchain-based publicly verifiable data deletion scheme for cloud storage", *Journal of Network and Computer Applications,* Vol.103, pp. 185-193, 2018.

[2] M. O. Alassafi, A. Alharthi, R.J. Walters, and G. B. Wills, "A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies", *Telematics and Informatics*, Vol.34, No.7, pp.996-1010, 2017.

[3] S.A. El-Booz, G. Attiya, and N. El-Fishawy, "A secure cloud storage system combining time-based one-time password and automatic blocker protocol", *EURASIP Journal on Information Security*, No.1, pp.13, 2016.

[4] 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.

[5] A. Hudic, P. Smith, and E.R. Weippl, "Security assurance assessment methodology for hybrid clouds", *Computers & Security,* Vol.70, pp.723-743, 2017.

[6] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage", *IEEE Transactions on Information Forensics and Security*, Vol.14, No.2, pp.331-346, 2019.

[7] Z. Xu, L. Wu, M.K. Khan, K.K.R. Choo, and D. He, "A secure and efficient public auditing scheme using RSA algorithm for cloud storage", *The Journal of Supercomputing*, Vol.73, No.2, pp.5285-5309, 2017.

[8] Y. Luo, M. Xu, K. Huang, D. Wang, and S. Fu, "Efficient auditing for shared data in the cloud with secure user revocation and computations outsourcing", *Computers & Security*, Vol.73, pp.492-506, 2018.

[9] C. Wan, J. Zhang, B. Pei, and C. Chen, "Efficient privacy-preserving third-party auditing for ambient intelligence systems", *Journal of Ambient Intelligence and Humanized Computing,* Vol.7, No.1, pp. 21-27, 2016.

[10] J.J. Zhang, H. Meng, and Y. Yu, "Achieving public verifiability and data dynamics for cloud data in the standard model", *Cluster Computing,* Vol.20, No.3, pp.2641-2653, 2017.

[11] M. Suguna and S.M. Shalinie, "Privacy preserving auditing protocol for remote data storage", *Cluster Computing*, pp.1-8, 2018.

[12] D. Kim, H. Kwon, C. Hahn, and J. Hur, "Privacy-preserving public auditing for educational multimedia data in cloud computing", *Multimedia Tools and Applications,* Vol.75, No.21, pp. 13077-13091, 2016.

[13] A. Li, S. Tan, and Y. Jia, "A method for achieving provable data integrity in cloud computing", *The Journal of Supercomputing,* pp.1-17, 2016.

[14] J. Yu, K. Ren, and C. Wang, "Enabling cloud storage auditing with verifiable outsourcing of key updates", *IEEE Transactions on Information Forensics and Security*, Vol.11, No.6, pp.1362-1375, 2016.

[15] Y. Yu, L. Xue, M.H. Au, W. Susilo, J. Ni, Y. Zhang, 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.

[16] 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.

[17] G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, "Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability", *Journal of Systems and Software*, pp. 113, pp.130-139, 2016.