Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

A modified Boneh-Lynn-Shacham signing dynamic auditing in cloud computing

Adnan Alrabea

Prince Abdullah Bin Ghazi Faculty of Information and Communication Technology, Al-Balqa Applied University, Al-Salt, Jordan

ARTICLE INFO

Article history:
Received 28 March 2020
Revised 22 May 2020
Accepted 1 June 2020
Available online xxxx

Keywords:
Cloud computing
Auditing
Security
Multiple batch
Cloud security

ABSTRACT

Cloud Computing is an alternative to conventional IT Outsourcing. As a result, cloud computing migration between organizations is rapidly growing. The adoption of this technology brings many positive aspects but prescribes various risks and concerns. An organization that officially provides its cloud computing services to external providers and implies that its IT functions and process are outsourced to third-party providers of BPO services. For privacy-making public audit processes in dynamic cloud data storage, a modified Boneh-Lynn-Shachame Dynamic Auditing (MBLSDA) algorithm is suggested in this paper. The proposed algorithm executes an audit process for multiple users based on a batch audit simultaneously and effectively to enable Third Party Auditing (TPA). This paper integrates the homomorphic authenticator in an algorithm of dynamic signing audit by random marking in terms of the privacy conserving public auditing process. When the user of cloud service, store or update the data, it encrypts using Rijndal algorithm, and Boneh-Lynn-Shacham signature generation is used for key generation. Finally, a hybrid of these a proposed Modified Boneh-Lynn-Shacham Signing Dynamic audit the data to provide the security.

1. Introduction

Cloud storage systems can give a flexible on-demand data storage service to the cloud user at any time and anywhere (Qiu et al., 2016). However, the Cloud Service Provider (CSP) owned the user data physically as well as virtually. In this cloud environment, the cloud data are not controlled by the cloud user. Instead, cloud auditors manage cloud data. But this process does not ensure data integrity, which means unauthorized cloud users can alter the data without the owner's knowledge. The individual belongs to a group that can modify the data of other members in the same group (Fig. 1).

Thus to avoid these kinds of issues, this work proposed a Modified Boneh-Lynn-Shacham Signing Dynamic Auditing (MBLSSDA) algorithm for privacy-preserving public auditing process in dynamic storage in the cloud. To enable the Third Party Auditing (TPA) simultaneously and efficiently, the auditing process for single users as well as batch auditing for multiple users is efficiently done in this proposed work. Additionally, this work implements the Rijndael algorithm for generating an encryption key by data owner when the group user is requesting the data owner to access the data. This process is done based on the algorithm SHA-512 for creating the hash key, which is used by TPA for checking the integrity of cloud data, and one of the added advantages of this proposed work is a one-time password verification scheme.

The main objective is to build a cloud storage platform to optimize privacy and protection to increase users' trust in moving to the cloud. A secure cloud-computing system to improve the protection and privacy of cloud services users is the specific aims. A new audit framework that allows users to create their own rules to enhance auditing. A system of auditing in which administrators and users have their independent audit protocols and third parties may amend these protocols. The paper is structured to explain the attempt to protect knowledge in cloud computing in the following sections.

1.1. Existing auditing schemes

The confidentiality of the data has not been retained while the current research has effectively preserved confidentiality and pub-

Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

E-mail address: dr.alrabea@bau.edu.jo

https://doi.org/10.1016/j.jksuci.2020.06.001

Please cite this article as: A. Alrabea, A modified Boneh-Lynn-Shacham signing dynamic auditing in cloud computing, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2020.06.001

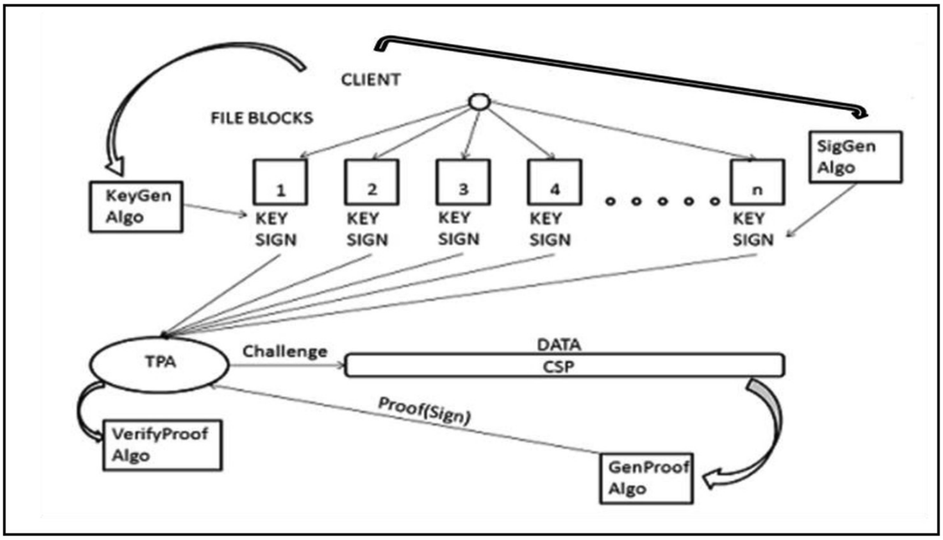

Fig. 1. Basic privacy preserving in public auditing.

lic auditing. The TPA allows public audits of data on user data stored. Preserving the integrity of TPA ensures that the data used for data auditing is nil in the information. It is one of the key factors to be achieved. TPA itself may be malicious, and the information from the user may leak. This is also important that the user data is not identified. The original form on the cloud server is not safe to store and can be targeted by external assailants. Encryption methods must be used to provide improved data protection.

In the existing methods, a cloud manager is responsible for measuring evidence of the quality of the data, which often maintains vast amounts of user data. Therefore, the storage problem and the verification duty to produce evidence on the cloud server are increased. In the auditing process, a system must be introduced to overcome the load of the cloud. For a trustworthy system, all of the above factors are critical and must be accomplished. An efficient and secure auditing scheme is, therefore, necessary to effectively perform public audits by ensuring that the stored data is maintained both fully and confidently.

Mutual Verifiable Protection in Public Cloud Storage Provable Data Auditing reveals that the device is unsafe from falsify, replay attacks, and erase attacks. The protection claimed in the scheme is not met. After the study, the reasons for these attacks, the proposed research resolve these attacks. Finally, the safety of the proposed research is evaluated and shown to be safe.

It is necessary to develop an effective public auditing protocol to overcome the limitation of the existing auditing schemes. The proposed system is developed to verify the correctness of cloud data using TPA. It performs the task of auditing either periodically or on-demand. It assures that no data content is leaked to TPA during the auditing process. It maintains the integrity and confidentiality of the stored data.

To overcome the limitation of existing audit schemes, an effective public audit protocol needs to be developed. To verify cloud data accuracy with TPA, the system has been established. This performs a regular or on-demand auditing function. It ensures that during the audit process no data material is leaked to TPA. It means the data stored are kept important and confidential.

2. Privacy-preserving public auditing scheme

This work integrates an authenticator with a random marking approach in terms of privacy-preserving public auditing process using Modified Boneh-Lynn-Shacham Signing Dynamic Auditing (MBLSSDA) algorithm. A linear combination of sampled blocks in cloud service answer is masked with randomly generated Pseudo-Random Function (PRF). In the random making, the Third Party Auditor (TPA) no longer needs the user data to build a correct group and therefore, cannot originate the data content of the user (Zhang et al., 2012; Wu et al., 2015). A public auditing scheme basically contains four different algorithms such as VerifyProof, GenProof, SigGen, KeyGen which runs according to the user implantation setup.

The data owner uses SigGen to produce authentication metadata, which may contain MAC signatures or related auditing material (Vijayalakshmi et al., 2014; Kiraz et al., 2016; Jachak et al., 2012). GenProof is run by the cloud service to assert data storage accuracy, while the TPA applies VerifyProof to verify cloud service code proof. This proposed work adapts a batch auditing scheme using Rijndael algorithm.

2.1. Public auditing

It permits the TPA to verify the cloud data correctness on demand and without take care of actual cloud data. In addition, by presenting any added online burden to the cloud authenticated users (Ezhilarasi and Krishnaveni, 2019). This process has two different phases such as built the public auditing system and auditing process.

2.2. Batch auditing

Users may concurrently request the auditing service from the TPA and each auditing task for individual group or cloud user (McNevin et al., 2004). But this process directs very inefficient and creates the added burden on the Utilization of batch auditing is one of the solutions of these kinds of issues. Here the TPA can concurrently perform the multiple auditing tasks for the different cloud users. During this process, multiple users' forwards aggregate authenticator to the TPA, after this process the TPA batches together all the incoming requests and forwards it as a single request to the CSP. Then the CSP compute the aggregate authenticator and again forward it to the TPA (Patidar and Bhardwaj, 2011).

Please cite this article as: A. Alrabea, A modified Boneh-Lynn-Shacham signing dynamic auditing in cloud computing, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2020.06.001

2.3. Data dynamics

The cloud External auditor has to manage the data integrity where the cloud user may wish to do some of the data block level processes, for example, modify, delete and update the files. Hence, this proposed system offers the dynamic support.

Block Insertion: In the block insertion operation, server can insert anything on the existing client's file or introduce new client file.

Block Deletion: In data block deletion operation, a server or user can delete anything on the user's data file at any time.

Block Modification: In data block modification operation, a user or server can modify anything on the user's data file at any time.

Block Verification: In block verification operation the TPA offers acknowledgment regarding whether the block is altered or not altered.

Log History:log details about the user activity is maintained in log file.

3. Multiple batch auditing

Another important process in public auditing process is multiple batch auditing. In this multiple batch auditing process the TPA may simultaneously handle the multiple auditing processes upon various requests of the user. In the separate auditing tasks, the TPA can be tedious and also this process leads to inefficiently. For example, given K auditing process on K different data form k distinct cloud users, it is more beneficial for TPA to process the batch auditing process and these multiple tasks are collected and audit at one-time process (Jose et al., 2011; Kumari).

Thus, keeping this necessary demand in mind this work proposed a new Modified Boneh-Lynn-Shacham Signing Dynamic Auditing (MBLSSDA) algorithm which is used to support the multiple signatures' aggregation is done by different signers on different messages into a single signature (Mahalle and Pawade, 2014; Hemlatha and Ganesh, 2013). Hence, this process gives the efficient verification during the authentication for each data blocks. Utilizing this MBLSSDA process can achieve the simultaneous auditing process of multiple tasks at a time.

4. Modified Boneh-Lynn-Shacham signing dynamic auditing

In this proposed work the data sharing between users in a group is done with the great secure way in the cloud. The authorized group members only can access the shared data and it is done by using Rijndael algorithm based on the SHA-512 algorithm and Random key generation procedure. It also consider the user revocation process and data integrity during the public verification process without downloading the whole data. It identifies signer on each and every data blocks in shared data and preserved the private information from the public verifier. This approach also offers a novel public preserving auditing mechanism for the shared data integrity with efficient group member revocation. Additionally, this work uses, one-time password generation scheme for attaining the high data integrity which is depicted in the following Fig. 2.

4.1. Multiple batches auditing design construction

This section involves module of multiple batches auditing design to form an efficient user revocation and public auditing as shown in Fig. 3.

4.1.1. User registration

The user registration is a typical procedure which is done by the cloud admin; during this registration process, the group user must register their details using their personal information. After the registration process, the user gets a personal ID for processing the cloud dynamic data sharing operation. For example, add or delete. In case any user needs to edit their personal information they have to submit the appropriately altered details to the cloud admin, then the cloud admin can update and edit that appropriate user information and this whole process is controlled by cloud admin as shown in Fig. 4.

4.1.2. File uploading

The file uploading process the information is shared by the group user and in this work, encrypted operation is done by using Rijndael algorithm based on a SHA-512 algorithm.

Rijndael is well-known block cipher and standard symmetric key encryption algorithm which is to be utilized to encrypt sensitive data (Khan and Malluhi, 2013). Therefore, the decryption or encryption of the data block is accomplished by multiple iterations with particular transformation (round function see Fig. 5). This algorithm has also defined an approach by creating a series of sub keys from the users' original key. The created sub key are utilized as input with round function.

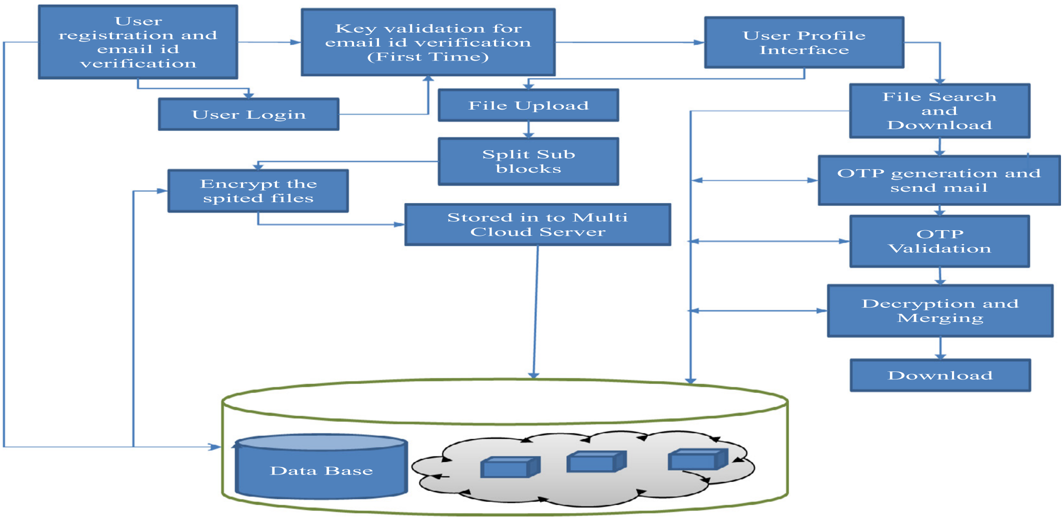

Fig. 2. User validations using one time password.

Please cite this article as: A. Alrabea, A modified Boneh-Lynn-Shacham signing dynamic auditing in cloud computing, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2020.06.001

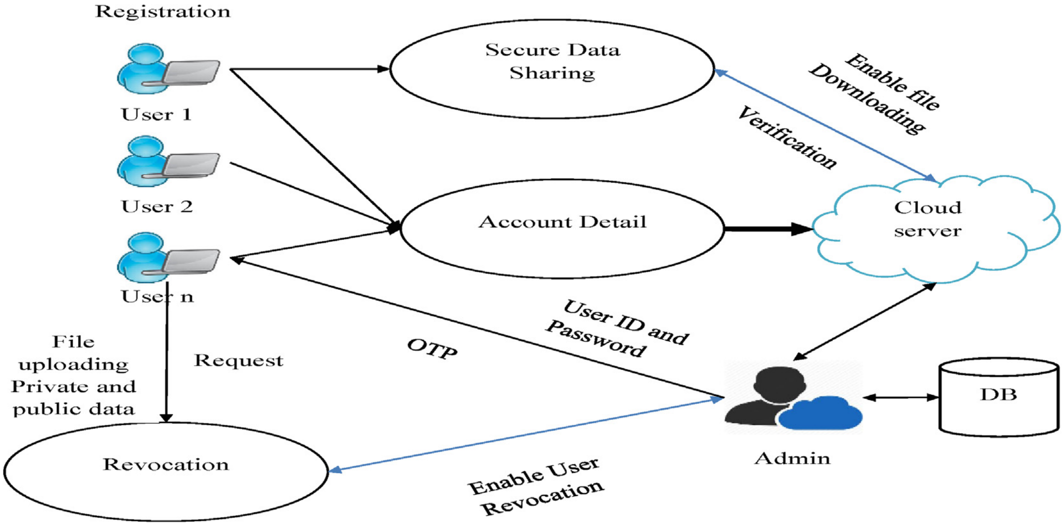

Fig. 3. User revocations and public auditing.

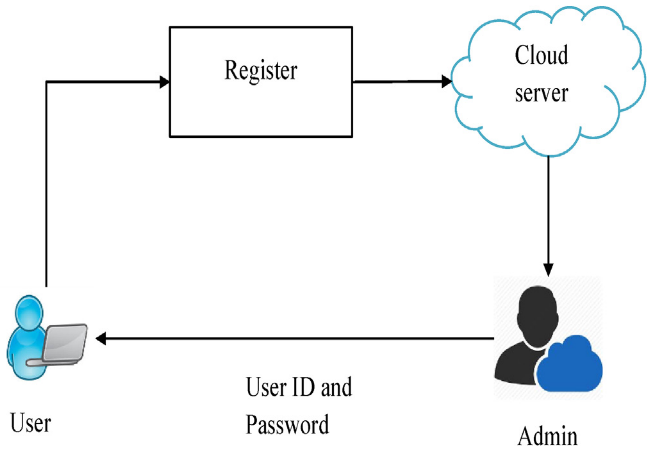

Fig. 4. Registration.

The basic pseudo code is as follows:

```
Pseudo code-Rijndael algorithm
//Consider the Number of rounds performed is Nr //data block
   (Nb)
//length of the key (Nk)
//cipher results = state
Rijndael(State,CipherKey) {
KeyExpansion(CipherKey,ExpandedKey);AddRoundKey(State,
   ExpandedKey);
For(i = 1 ; iFinalRound(State,ExpandedKey + Nb*Nr);
}
//The Round function is
Round(State,RoundKey) {
ByteSub(State);
ShiftRow(State);
MixColumn(State);
AddRoundKey(State,RoundKey);
}
```

5. Modified Boneh-Lynn-Shacham using cloud data auditing

In this proposed work the cloud data auditing process is done by using Modified Boneh-Lynn-Shacham Signing System in every Gap Diffie-Hellman (GDP) category G. It also includes a hash function from message space to group G and is aligned with the proven signature scheme of the Pedersen and Chaum (Cimato et al., 2013; Nagarajan and Karthikeyan, 2012; Vasarhelyi and Halper, 1991).

Exactly, Consider $G = \langle g \rangle$is a Gap Diffie-Hellman group of prime order p, with a hash function $H : \{0, 1\}^{*} \rightarrow G$, considered a random oracle, any string may be signed and a signature identified as a single element of group G. The scheme contains following algorithms.

```
Key Gen Algorithm
//generates an asymmetric key pair (x,v) ∈ Zn * Gn with public
   key v and private key x
Data:generator g2 for G2,prime number p
Result:private key × ∈ Zn,public key v ∈ G2
Choose random × ∈ Zn
V → g2x
Return (x,v)
SigGen Algorithm
//SigGen used when signing a message M with the private key
   x.
// This algorithm needs a hash function H that can hash the
   message to an elementh ∈ G1.
//Assume that H is a random hash function.
Data: private key × ∈ Zn,message M ∈ {0,1}*
Result: signature σ ∈ G1
h ← H(M) ∈ G1
σ ← h^x
Return σ
Verify Algorithm
//Verify the signature with public key
Data: public key v ∈ G2,signature σ ∈ G1,message M ∈ {0,1}*
Result: boolean value
h ← H(M) ∈ G1
Return Test ((g^2,v,h,σ)
```

Please cite this article as: A. Alrabea, A modified Boneh-Lynn-Shacham signing dynamic auditing in cloud computing, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2020.06.001

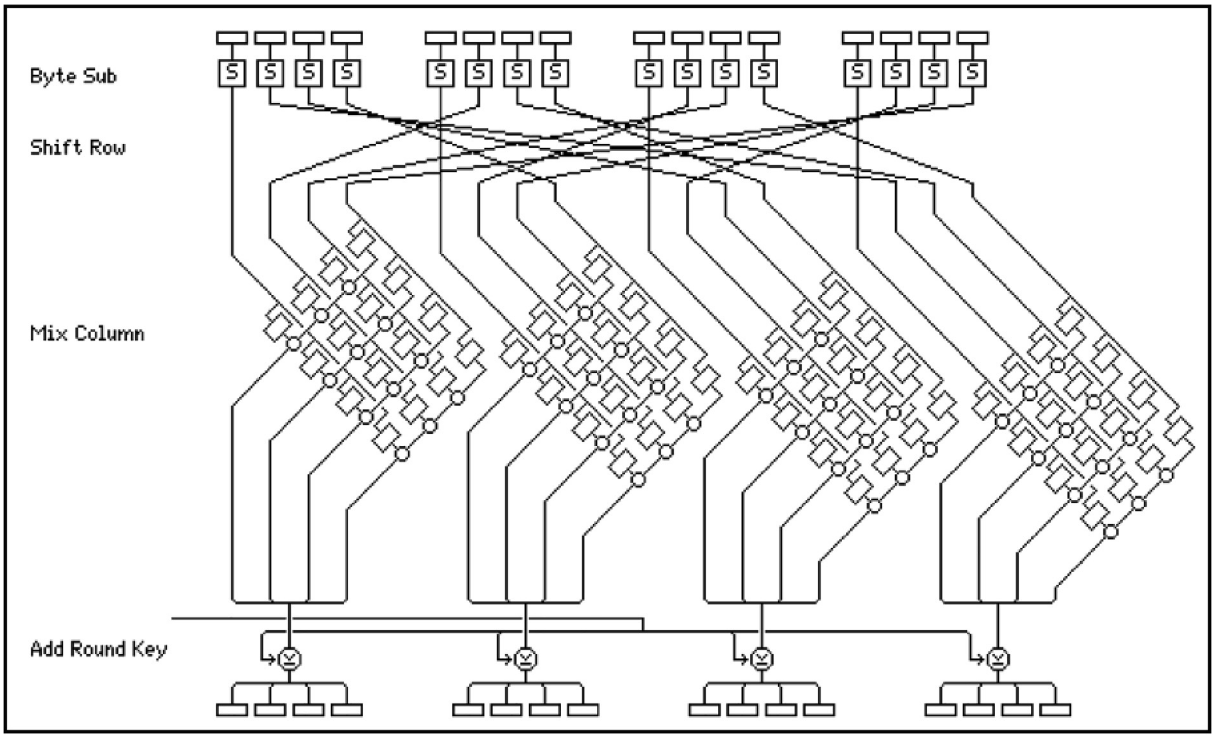

Fig. 5. Rijndael's round functions.

During this auditing processas shown in Fig. 5, each and every group user are authenticated by using one-time password approach and this password generated by using a SHA-512 algorithm.

The Secure Hash Algorithm (SHA) was developed by according to Federal Information Processing Standard (FIPS 180) and National Institute of Standards and Technology (NIST) in 1993 (Massonet et al., 2011; Ezhilarasi and Krishnaveni, 2018). SHA is worked based on the hash function MD4. SHA-1 is also stated in RFC 3174.

5.1. Forwarding OTP to cloud user

After generating the OTP it should be sent to the cloud user by using a gateway operation to the user mail or mobile. Here, the URL is used for this process as a library and command line tool for transferring data across it.

1.curl_init() :It is utilized to initialize a session.

2.curl_setopt() :Set a possibility for the URL transfer.

3.curl_exec() :Perform a cURL session.

4.curl_close() :Close a cURL session and set free all the cloud resources.

Following procedure shows the overall process of proposed Modified Boneh-Lynn-Shacham Based cloud auditing with Rijndael algorithm based data integrity checking process (Tsai et al., 2009).

A Modified Boneh-Lynn-Shacham Signing Dynamic Auditing

Step 1: Cloud service controller or community customer first do server registration. After authentication, OTP is created to transfer user phone or mail. Entering OTP number user can login and view their cloud info. Using Rijandael algorithm is generated when user operations are complete performance.

(*continued*)

A Modified Boneh-Lynn-Shacham Signing Dynamic Auditing

Step 2: Cloud user register and after enter the OTP to login. If the user want to access a file, initially user send the request to server for authorization of file.

Step 3: Cloud server block the user or accepts request or itdepends on user validation. After accept the request, server sends the encryption key to the users mobile or mail. Rijandael algorithm is used for generating the Encryption key which is used for security purpose.

Step 4: Entering the encryption key user can modify or update the file and upload the file to the cloud server again. A new hash value is generated after the file is uploaded.

Step 5: Now, the Third Party Administrator login and batch auditby comparing changed file hash value and original file, if the hash valuesobtained is same, then file is not altered otherwise it is altered by User.

Step 6: After this process cloud admin do login and will send the list of files that have been altered over the SMS or mail to the cloud user.

Step 7: The cloud user will review the tempered files and will discard the change made by user or overwrite the original file.

5.2. Download verification

The final process is verification of integrity which is shown in Fig. 6, here the TPA request to the user for the secret key to check the file integrity. The data owner in the group grantswq2 permission to TPA for downloading the file and after this process,

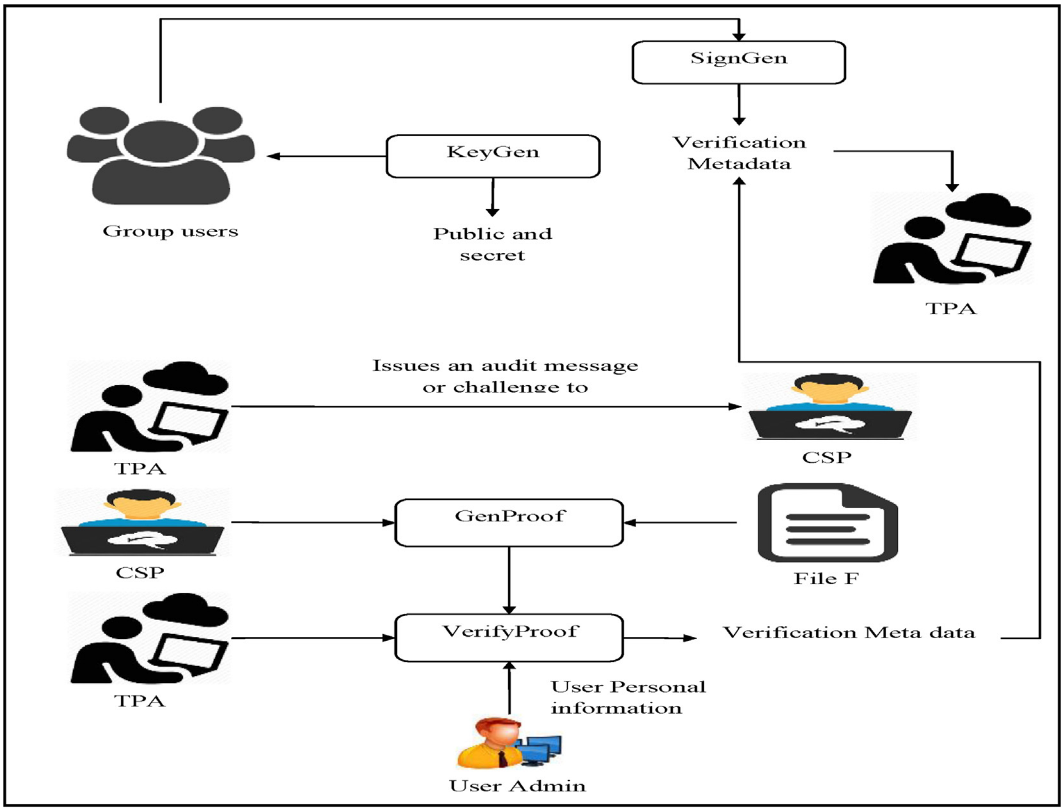

Fig. 6. Proposed modified Boneh-Lynn-Shacham based cloud auditing.

TPA can check the integrity. In case any altered or modification is performed on the file it will be reflected on cloud admin sideand the data owner side. At this time the cloud admin sends warning to data owner in case the proposed files have any alteration or modification by TPA. Without any secret key verification or metadata verification, the data owner can understand the data is altered.

6. Results & discussion

This proposed work implemented using Java and Cloud Sim. From the result in Fig. 7 shows that the public key generation time is comparative to the group size of proposed Modified Boneh-Lynn-Shacham Signing Dynamic Auditing (MBLSSDA) with Rijndael algorithm.

Fig. 8 shows that the signature generation time is comparative to the block size. Since the master user required to create secret

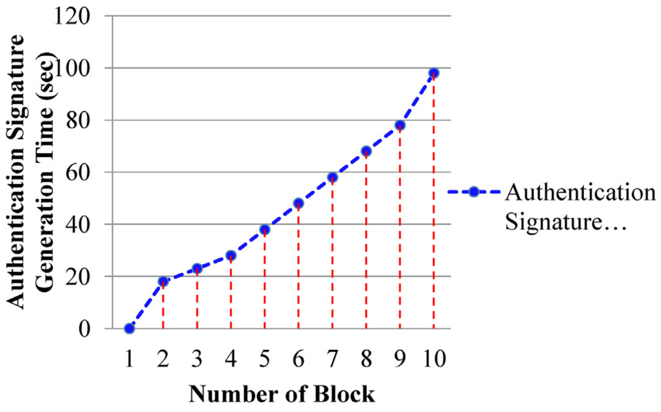

Fig. 8. Authentication signature generation Time of MBLSSDA-RIJNDAEL algorithm.

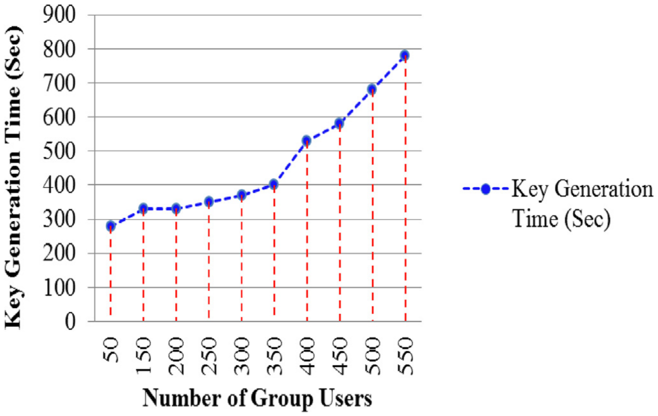

Fig. 7. Key generation time of MBLSSDA- RIJNDAEL algorithm.

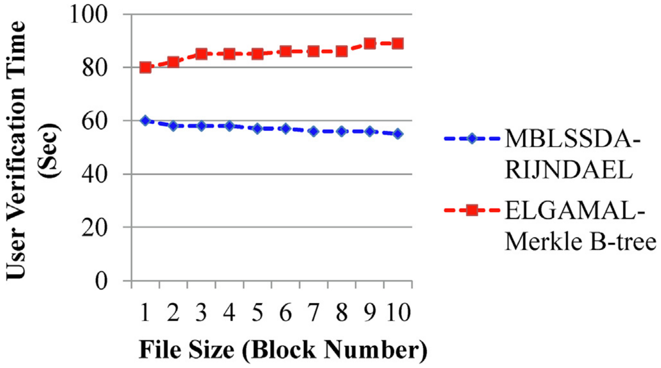

Fig. 9. User verification time of MBLSSDA-RIJNDAEL.

keys for each and every group user during the catch auditing process individually. Fig. 9 shows the comparison results of proposed Modified Boneh-Lynn-Shacham Signing Dynamic Auditing (MBLSSDA) with Rijndael algorithm and ELGAMAL digital signature scheme with Merkle B-tree (Nayana et al., 2013) in terms of user verification time.

From the results it indicates that, although ELGAMAL-Merkle B-tree scheme has very high User verification time when compared with the proposed work. This is because ELGAMAL-Merkle B-tree scheme needs a number of multiplication operations and exponentiation operations on Group number during the batch auditing process for challenging blocks.

7. Conclusion

This paper presents MBLSSDA algorithm for privacy-preserving public auditing process in term of dynamic cloud data storage. It enables the TPA to perform efficient auditing process for multiple users as well as doing in the batch auditing for multiple users. Additionally, this work implements the Rijndael algorithm to generate encryption key by data owner and at the time of other group user requesting the data owner to access the data.

This process is done based on the SHA-512 algorithm for creating the hash key which is used for TPA to check the integrity of cloud data and one of the added advantages of this proposed work is one-time password verification scheme. At last, the TPA verifies the data integrity. The result proves that by comparing single auditing with batch auditing process, the later one performs better and it enhances the whole system performance.

The data are divided into parts and are then stored for storage in the encrypted cloud format, thereby retaining data privacy. On request of the data owner, data integrity is verified by TPA, both by checking signatures, one created by the data owner and the other provided by the data owner. This simply checks whether or not the stored data is abused and notifies the data owner of it. Only the encrypted type of data is stored on a cloud server. Cloud server does not involve proof computing verification, which reduces the cloud server online burden. All auditing specifications have been met and the proposed approach reduces the burden on the cloud server. Data intensive operations will be carried out in the future, such as reviewing, removing and adding data.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Cimato, S., Damiani, E., Zavatarelli, F., Menicocci, R., 2013, June. Towards the certification of cloud services. In: 2013 IEEE Ninth World Congress on Services, IEEE, pp. 92–97.

Ezhilarasi, M., Krishnaveni, V., 2018. A survey on wireless sensor network: energy and lifetime perspective. Taga J. Graph. Technol. 14.

Ezhilarasi, M., Krishnaveni, V., 2019. An evolutionary multipath energy-efficient routing protocol (EMEER) for network lifetime enhancement in wireless sensor networks. Soft. Comput. https://doi.org/10.1007/s00500-019-03928-1.

Hemlatha, S.M., Ganesh, S., 2013. A brief survey on encryption schemes on cloud environments. Int. J. Comput. Org. Trends 3 (9).

Jachak B, K et al., 2012. Homomorphic authentication with random masking technique ensuring privacy & security in cloud computing. Bio. Secur. Informat. 2 (2), 49–52.

Jose, G.J.A., Sajeev, C., Suyambulingom, D.C., 2011. Implementation of data security in cloud computing. Int. J. P2P Network Trends Technol. 1 (1), 18–22.

Khan, K.M., Malluhi, Q., 2013. Trust in cloud services: providing more controls to clients. Computer 7, 94–96.

Kumari, Garima, madhuri, Lakshmi. Key aggregate cryptosystem & intrusion detection for data sharing in cloud. Multidisc. J. Res. Eng. Technol. 1(3): 308–317.

Kiraz, Mehmet Sabır, 2016. A comprehensive meta-analysis of cryptographic security mechanisms for cloud computing. J. Amb. Intel. Hum. Comp. 7 (5), 731–760.

Mahalle, R.V., Pawade, P.P., 2014. A review of secure data sharing in cloud using key aggregate cryptosystem and decoy technology. Int. J. Sci. Res. 3 (12), 2694–2697.

Massonet, P., Naqvi, S., Ponsard, C., Latanicki, J., Rochwerger, B., Villari, M., 2011, May. A monitoring and audit logging architecture for data location compliance in federated cloud infrastructures. In: 2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum, IEEE, pp. 1510–1517.

McNevin, T.J., Park, J.M., Marchany, R., 2004. pTCP: a client puzzle protocol for defending against resource exhaustion denial of service attacks. Virginia Tech Univ., Dept. Elect. Comput. Eng., Blacksburg, VA, USA, Tech. Rep. TR-ECE-04-10.

Nagarajan, M., Karthikeyan, S., 2012, March. A new approach to increase the life time and efficiency of wireless sensor network. In: International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME-2012), IEEE, pp. 231–235.

Patidar, P., Bhardwaj, A., 2011. Network security through SSL in cloud computing environment. Int. J. Comp. Sci. Inform. Technol. 2 (6), 2800–2803.

Qiu, M., Dai, W., Vasilakos, A.V., 2016. Loop parallelism maximization for multimedia data processing in mobile vehicular clouds. IEEE Trans. Cloud Comput. 7 (1), 250–258.

Tsai, H.Y., Huang, Y.L., Wagner, D., 2009. A graph approach to quantitative analysis of control-flow obfuscating transformations. IEEE Trans. Inf. Forensics Secur. 4 (2), 257–267.

Vasarhelyi, M.A., Halper, F.B., 1991. The continuous audit of online systems. Audit. J. Pract. Theor. 10 (1), 110–125.

Vijayalakshmi, T et al., 2014. An Efficient Security Based Multi Owner Data Sharing for un-trusted Groups using Broadcast Encryption Techniques in Cloud. Int. J. Appl. or Innov. Eng. Manag. 3 (3), 15–21.

Wu, Y., Zhao, Z., Bao, F., Deng, R.H., 2015. Software puzzle: a countermeasure to resource-inflated denial-of-service attacks. IEEE Trans. Inf. Forensics Secur. 10 (1), 168–177.

Zhang, C., Cai, Z., Chen, W., Luo, X., Yin, J., 2012. Flow level detection and filtering of low-rate DDoS. Comput. Netw. 56 (15), 3417–3431.

Please cite this article as: A. Alrabea, A modified Boneh-Lynn-Shacham signing dynamic auditing in cloud computing, Journal of King Saud University – Computer and Information Sciences, https://doi.org/10.1016/j.jksuci.2020.06.001