# Effective Approach for Secure Outsourcing of Key Updates in Cloud

[1]Shabana.S,[2]G.Vijay Kumar,
[1]M.TECH Student,[2]Associate Processor,
[1]Computer science and Engineering Department,
[1]G.Pullareddy engineering college, Kurnool,India.

*Abstract:* One of the important service of cloud computing is cloud storage. The security of cloud storage faces many critical issues, among which key exposure resistance is one. To solve this issue, the best way is to use key redesign. Previously many existing solutions required client to update his secret key by himself that too for every time period which brings up a burden to the clients especially people from various organizations whose main motive is different from this issue. So, making the key updates transparent for client will be beneficial. Thus proposing a new paradigm called cloud storage auditing. Examining each procedure in the paradigm makes entire process secure and safe. The proposed protocol determines that key updates are safely outsourced to some authorized party known as TPA (Third party auditor). TPA who acts as interface between client and cloud performs all update operations on behalf of client but significantly TPA holds only encrypted version of key so that key is not exposed to anyone other than the owner. The client when needed to upload files to cloud can download the updated secret key from TPA and decrypt it. Apart from this, our design also provides client with a option of verifying the validity of encrypted secret key provided by TPA. These features help client to complete his cloud storage works in a secure method. A security model is designed to formulate this paradigm along with performance simulation.

***Index Terms***- Cloud storage, Cloud storage auditing, Key update, Outsourcing computation

## I. INTRODUCTION

Cloud computing is a huge promising and popular technology as it provides unlimited resources and services [1][18][19]. Cloud computing maintains and deploys time consuming workloads without extra capital; so that users need not to maintain hardware and software instead cloud provides services to maintain them. Heading computation to cloud is a recent trend now used widely worldwide in scientific applications, linear algebraic computations, linear programming computation and many more.[1][19] Among the unlimited services provided by the cloud computing, one of the most popular service is cloud storage services offered by many companies like Amazon web services (AWS) , salesforce.com, GoogleAppEngine, and many more with respect to users data that has to store in cloud with a full secured policy[3][15].

The major and basic advantage of cloud computing is that it has the benefits of centralized large computational power, space and efficiency. As we know cloud computing is used for non demand network access that can help users to outsource the complex problem to the cloud. It faces security based challenges like checkability and confidentiality for user's private data [10][5].

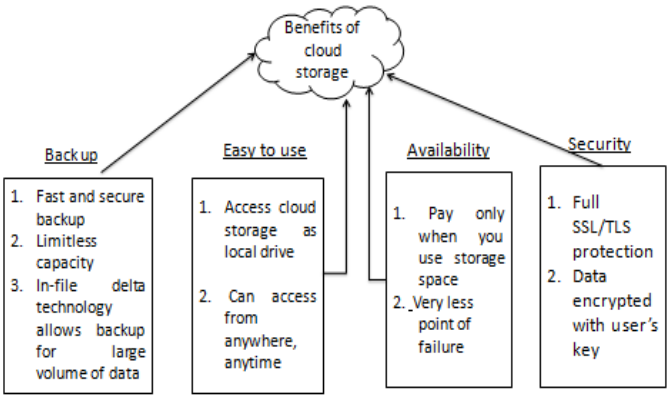


Figure.1 cloud storage benefits

The benefits of cloud storage on the bases of Backup, easy to use, Availability and Security are discussed in the figure 1.

Although there are tremendous benefits of cloud storage service, security remains a challenge [2][4][5][7][8][18]. Cloud security is an important aspect to be achieved since cloud computing cannot work without an internet.

It is quite common for users to expect complete security for their data which might be confidential so, cloud storage auditing is one of the most effective techniques proposed in this paper to make sure the integrity of the data is achieved.[1][17].

Data owners worry about many complex problems like data loss in infrastructure of cloud or trust issues with cloud management. Integrity of data play major role in cloud storage to assure owners/clients if their data is safely stored [17].

The security issues in cloud computing encompasses not only data but also many technologies like network, operating system, virtualization, resource scheduling, concurrency control, memory management and load balancing[1][2]. The network had to be securely carried out in cloud. Virtualization in cloud computing can leads to difficult problem while mapping virtual machines to physical machines. Similarly Memory management and resource allocation algorithms should be capable of security. Finally some techniques in data mining can leads to malware detection in cloud.[14][15]

Some aspects of secure cloud computing are Adopting effective ways of storing data in foreign machines, Encrypted data is always preferred to avoid 90% of the security problems and Secure query processing of data[5].

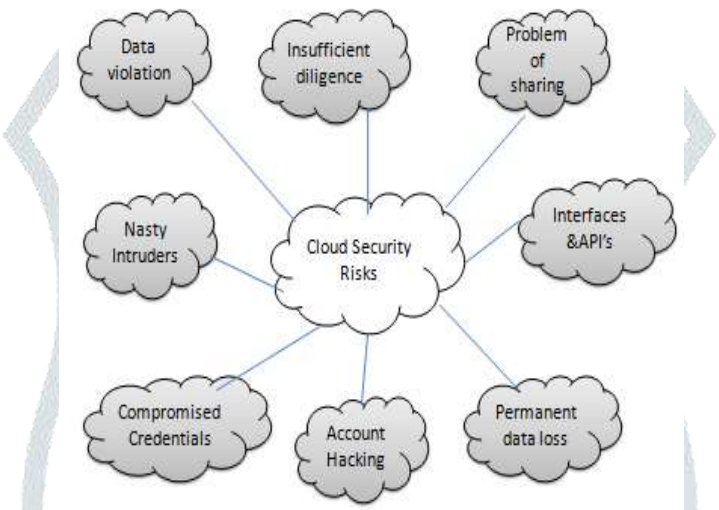


Figure.2 cloud security risks

The figure 2 shows the security risks occurs in the cloud computing such as Account hacking, permanent data loss, nasty intruders, compromised credentials, insufficient diligence, problem of sharing and data violation.

The cloud storage auditing is a term to be defined as an examination of the management controls on the basis of information technology infrastructure.[5][6] The evaluation of obtained result determines if the information system are safeguarding assets, managing data integrity and effective operation to achieve the respective goal. In general, auditing are of different types which includes IT audits popularly known as automated data processing audits and computer audits. Some types of audits are as follows:

System and applications: Audit to verify if the system and applications are effectively controlled and ensure validity and reliability. System and process assurance audits form focus on business IT systems.Information Processing Facilities: It is a type of audit to verify if the processing facility is controlled to ensure timely, accurate and efficient processing of applications under normal and potentially disruptive conditions.System Development: An audit to verify the system under development process.

Cloud is having the aggregated management of elastic resources user's data might contain business information, private and sensitive information. So to protect user's data, security key maintenance is essentially outsourced and performed under encrypted format. The internal operations are not transparent to customer. Security remains primary concern in the outsourcing computations [10].

## II. RELATED WORK

A few conventions like powerful examining, Outsider evaluating, Clump reviewing executes cloud security. Under powerful reviewing, dynamic activities are performed and it make utilization of bilinearity property of bilinear matching strategy with the goal that it tackles information protection issue and group inspecting underpins numerous proprietors and mists additionally works as a section in unique auditing[7]. These two inspecting conventions join and confirm the verification of accuracy and

lessen evaluators work stack by moving information to the server. To give security safeguarding reviewing convention cryptography strategy is in any case utilized. The verification amongst reviewer and server to comprehend or to answer a test is a key part. Thiswhole inspecting framework will enhance its execution if the significant methods, for example, information part and homomorphic unquestionable labels are connected in which information piecesystem lessens over-burden and by homomorphic certain labels; correspondence cost is decreased in the middle of inspector and server. The procedure of this framework begins from proprietor introduction, arrangement reviewing and test inspecting.

Jiayu and Kuiren [1] proposed a mechanism where third party auditor plays the crucial role of updating secret keys and checking the integrity of owner's data. The most advanced feature is that, TPA couldn't see the secret key; instead encrypted version of key is used by TPA to avoid trust issues.One more important topic to be discussed is Outsourcing computation since it is used in many application domains. In order to help users to perform difficult computations Chaum and Pedersen [28] proposed wallet databases with observers in which hardware is used. The outsourcing algorithm proposed by Hohenberger and Lysyanskaya [7] proposed the algorithms of outsourcing computations. This determines precomputation methods and server aided computations. Linear programming, homomorphic functions andOutsourcing algorithms for attribute based signature are introduced in this proposed system.Atallah and li [29] designed a algorithm for secure delegation of elliptic curve pairing which is declared as most effective algorithm.

Data sharing with multiuser modification can be done using a public auditing protocol proposed by Yuan and yu [30]. Another public protocol also proposed by Sookhak et al [26] it is based on algebraic signature for making data securely saved. Cloud storage auditing protocol also deals with provable data possession proposed by Ateniese et al [8] and proof of retrievability proposed by juels et al [13] to make sure that client data is safe with trusted servers.

Fair arbitration is one of the important elements to be included in between CSP and clients because in some cases both CSP and client can be dishonest due to which cloud data gets affected. So, to avoid this, the best idea is to usedigital signature exchange which is widely used in every field.

According to HaoJin and Hong Jiang fair arbitration is necessary in the form of Third Party Arbitrator who is trusted by both parties.Third Party Arbitrator who resolves disputes adopts index switches to maintain mapping between block indices and tag indices, usually tag indices and block indices are used in tag computation or logicalpositions of data blocks. This index switches and dynamic auditing scheme is much explained in [14].

On the other hand Kang Yang and Xiaohua [15] proposed privacy preserving protocol which helps to solve data privacy issues. A method to prove encryption by using some technique named bilinearity property which helps to verify correctness of proof. The major aim of this is to reduce communication cost between auditor and server. It performs security model so as to be secure from attacks like replace attack, forgery and replay attacks. Three different phases of privacy preserving auditing protocol is discussed each with an efficient operation, apart from this batch auditing also involves for only multiple clouds with many owners.

Linear programming [10] is most effective method to deal with. It maximizes or minimizes a linear function with variables and constraints. This linear function is also known as objective function, which we seek in feasible region. The optimal solution lies under feasible region. Linear programming is used in many domain of real world systems like flow control, power management and data packet routing.Some techniques like Homomorphic encryption, symmetric key encryption are also used efficiently to make sure that the key is well encrypted.All the mentioned auditing protocols [1][7][8][10][26][28][29][30] are determined in an assumption that client's secret key is not exposed to outside world.

The key exposure problem has been a serious issue in a system. The security of a system is totally in a risk once the key is exposed. This problem is rapidly increasing because of people using their portable devices for many transactions. When key exposure is this much problematic, the security measures had to be taken.To address this issue, many approaches are proposed such as minimizing exposure of the key by splitting the key into different parts and storing it in different places. Many methods like threshold signature, proactive secret sharing and many more helps to reduce this problem.

## III. ORGANIZATION

The paper is organized as follows: In following sections we introduce system model, definitions, and algorithms of our work. Then we discuss the proposed protocol in section 3. The section 4 describes security and performance analysis. We conclude the paper in section 5.

## IV. SYSTEM MODEL

System model shows the clear view of cloud storage auditing with an effective approach of outsourcing key updates. The three parties in this model are: client, cloud and the Third Party Auditor (TPA).

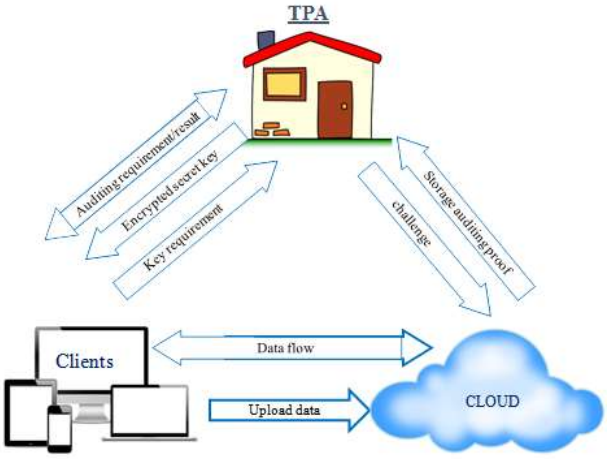


Figure.3 Process of cloud storage auditing

The client can upload any number of files to the cloud, size of the files is not fixed, and client can upload in different point of times based on his necessity. Where the cloud acts as host to store the data and provide download option with some security features. TPA has two roles to perform; one is to audit the data files that are stored in cloud and the other is to update the encrypted secret keys of client in each time period. TPA holds powerful computation capability and lifetime of flies in cloud is divided into T+1 time periods.

Each time period, the TPA updates the encrypted secret key for cloud storage according to the next time period but public key remains unchanged in the entire time period.

The client sends a key request to the TPA only when he wanted to upload a new file to his storage in cloud. And then TPA response back sending the encrypted secret key to client, to which client can decrypt and download it easily to get real secret key. Using this real key client can generate Authenticators for files, uploads files with authenticators. In addition to it, TPA will audit every time that if the clients files are safely stored or not.

The above system model formalizes the adversaries with different reasonable abilities who try to cheat the challenger that he owns a file but in real, he doesn't know entirely [1]. Our cloud storage auditing protocol with effective approach is said to be secure if it satisfies the following condition, whenever an adversary let the challenger to accept its proof with non-negligible probability, there exists extractors that can effectively extract challenged file blocks and then a valid proofs are taken as output.

The protocol may also find some corrupted blocks for which detection operation must be done and verification is important to check if valid encrypted keys provided by TPA or not.

Under cloud storage auditing protocol with secure outsourcing of key updates, there are seven different algorithms composed which are listed in this section with description.

Algorithm 1:
System Setup: This algorithm is run by the client who takes an input parameter for k, time periods can be considered as T and encrypted key is assumed as$ESK_0$. Consider decrypted key as DK, public key as PK.

Client = DK whereas $ESK_0$=TPA.

Algorithm 2
Ekey Update: Encrypted key update is run by the TPA who takes input as $ESK_J$ where j acts as current time period. When a new encrypted key is generated it becomes $ESK_J$+1 for time period j+1.

Algorithm 3
VerESK: This algorithm is to verify encrypted secret key by the client. It takes input $ESK_J$ to verify it.

If $ESK_J$ is well formed,
return 1;
Else return 0;

Algorithm 4
DecESK: This algorithm is also holds by client which performs decryption to the secret key. Its input is $ESK_J$ and DK (decryption key), j as current time period, which results in clients original secret key $SK_J$.

Algorithm 5

AuthGen: This is authentication generation algorithm which takes input as file F, secret key $SK_J$, public key PK and generates set of authenticators in each time period j.

Algorithm 6
ProofGen: This algorithm is run by the cloud with input file F, set of authenticators, a challenge C, public key PK, therefore generates a proof P which proves that F is stored safely.

Algorithm 7
ProofVerify: TPA runs this algorithm to verify the proof using proof P, challenge C, public key PK.
If P is valid return true;
Else false;

Our proposed protocol uses the binary tree structure [4] to evolve keys. A cryptographic scheme is used to provide security. The binary tree structure from [4] is useful for our proposed protocol to make key updates very fast and short in size. The major difference between existing protocols and proposed protocol is that, proposed protocol has binary trees structure to update encrypted secret key instead of real secret key (plain text). The major problem to be noted here and get solved is that TPA should agree the condition that it performs outsourcing computations only in an encrypted version.

Since the existing protocols were not able to update keys in encrypted version so blinding technique is proposed with homomorphic property to perform encryption. With this technique any kind of forgeries can be prevented and helps to make key updates transparent for the client. This particular property is used under Ekey Update algorithm which is mentioned above.

In case if client do not want to verify the encrypted secret key, this feature could be removed from the scheme. The VerESK algorithm included in our protocol has to be deleted.Bilinearity, non-degeneracy and Computability are the elements that are used in determining the above algorithms.

The malevolent cloud is seen as the enemy in our security display. We utilize three amusements (Game 1, Game 2 and Game 3) to depict the foes with various bargaining capacities that are against the security of the proposed convention. In particular, Game 1 depicts an foe, who completely bargains the TPA to get all encoded mystery keys E S K j (periods j = 0, . . . , T ), attempts to fashion a legitimate authenticator in whenever period. This amusement, truth be told, demonstrates the security ought to fulfil that the TPA can't assist the cloud with forging any authenticator in whenever period regardless of whether it knows the encoded mystery keys.

Amusement 2 portrays an enemy, who bargains the customer to get D K, endeavours to fashion a substantial authenticator in whenever period. This diversion, truth be told, demonstrates the security ought to fulfil that an enemy can't fashion any authenticator in whenever period regardless of whether it gets the unscrambling mystery key D K by assaulting the customer. Diversion 3 gives the enemy more capacities, which depicts an enemy, who bargains the customer and the TPA to get both E S K j and D K at one day and age j, attempts to produce a legitimate authenticator before day and age j . This diversion, indeed, demonstrates the security ought to fulfil that a foe can't produce any authenticator earlier to one certain day and age in the event that it assaults the TPA and the customer all the while to get their mystery enters in this era.

## V. PERFORMANCE ANALYSIS

Under security analysis, the theorem of correctness for each random challenge and one valid proof

$P = (j, U, \sigma, \mu, \Omega_j)$

The following equation holds the proof verification for the given challenge.

$$= e^{\wedge}(R.\ \pi^{t}_{m=1} Rwj|m\ hwj\ |m, H1(R)^{\sum i \in I\ vi})\ .\ \hat{}e\ (U, u^{\mu}\ \pi_{i\epsilon l} H3\ (name||i||\ j, U)^{vi})$$

$$= e^{\wedge}(g, \pi i_{\epsilon 1} \sigma_i^{vi})$$

Our auditing protocol is detected using the formula given below:

$$PX = P\{X \geq 1\}$$

$$= 1 - P\{X = 0\}$$

$$= (1 - n - t)/n\ (n - 1 - t)/n - 1 \cdots\ (n - c + 1 - t)/n - c + 1$$

Thus, we can get

$$PX \leq 1 - (n - t))^{c}$$

Where n is number of total blocks of a cloud file,
Let X be the discrete random variable defined as number of blocks by the challenger and c be the number of challenged blocks including “t” deleted blocks. If at least one block matches the block of modified one by adversary it denotes as PX.

The evaluation of proposed scheme performance is done using a method named Pairing-Based Cryptography [3]. To perform this we need a Linux server with 2.70 GHz and 4GB memory. The following figures show the outcomes of proposed scheme and existing scheme [4] and their descriptions.

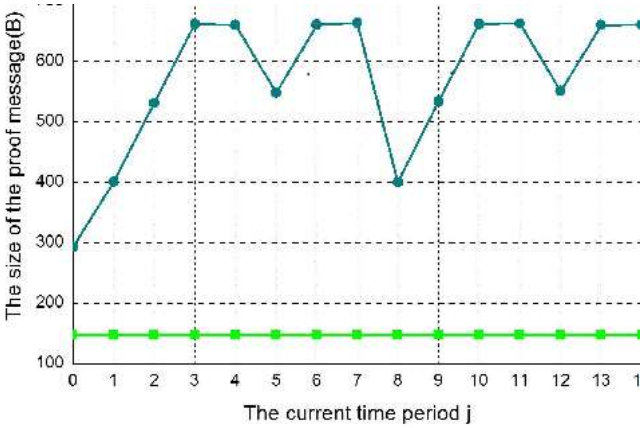


Figure.4 Key update time of existing and proposed scheme

The figure 4 analysis the key update time of both existing model [4] and proposed model, where in existing model, client himself has to update key in each time period if client is related to a binary tree, if depth of the node corresponding to current time period is 0 or 1 then key update time is 11.6ms. When it is 2, update time becomes 0. Hence time variations occur in existing model due to self updating process. Focusing on proposed model, key update time remains 0 always because TPA performs the update operations.

In figure 4, a graph is represented indicating proposed model in green colour showing a constant update time whereas existing scheme[4] varies time to time as shown clearly in the above graph.

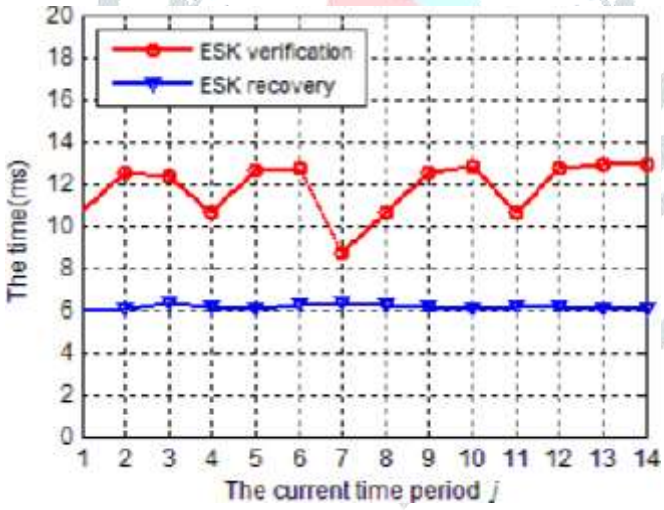


Figure.5 Encrypted secret key verification and recovery

Whenever the client needs to upload a file into the cloud, it has to verify the validity of encrypted secret key from TPA and secret key recovery has to be done. In the above figure 5, graph implements encrypted secret key verification in different time periods and at the same time recovery of secret key. A point to be noted here is this happens only when the user want to upload new file to the cloud.

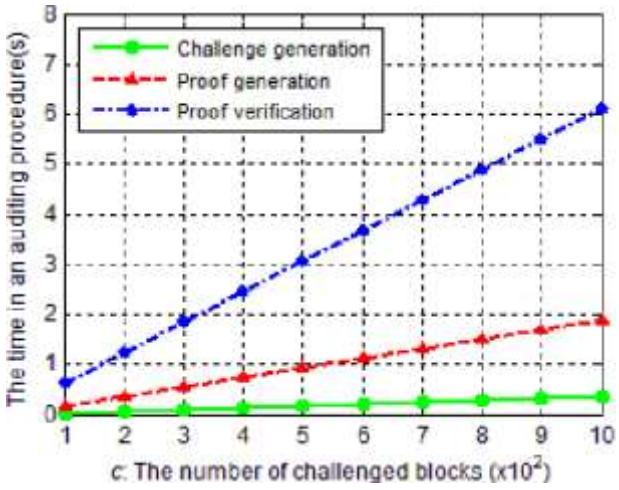


Figure.6 Time of auditing procedures

Demonstrate the time of the challenge generation process, proof generation process and proof verification process in the above graph with different number of checked blocks. These three are the auditing procedures to evaluate with checked blocks.

The figure 7 Considering our evaluation the number of checked data blocks varies from 100 to 1000, as the number of checked blocks increases the time of these processes also increases linearly. Among the three procedures, the challenge generation process spends the least time of all which is 0.35s, the proof generation occupies more time in between 0.19s to 1.89;the proof verification process spends time varying between 0.62s to 6.12s.

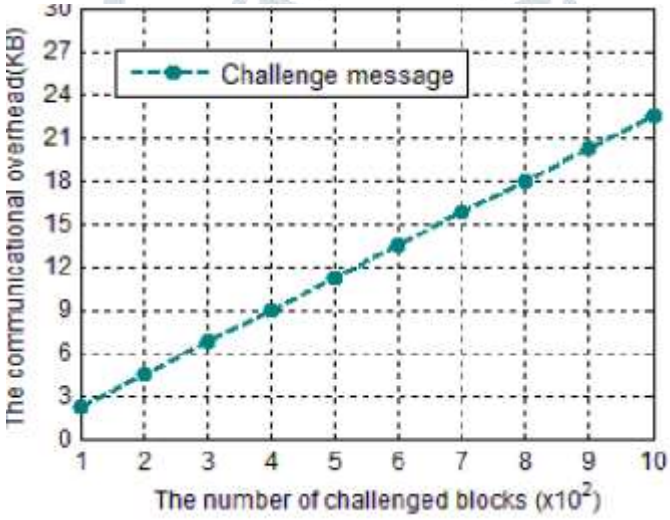


Figure.7 Size of challenge message with different number of checked blocks

The challenge and proof processes generates communication messages. The size of challenge message is 22.5kb when checked blocks are1000 and 2.25kb when there are only 100 checked blocks. In some cases, when checked blocks are 460, the TPA can detect data in problem with 99% probability, so immediately receives a challenge message with 10.35kb.

The size of proof message varies with depth of nodes corresponding to time periods. In period 0, the proof message will be the shortest one with 276.5 bytes whereas the longest proof message will be about 0.66KB. The variations are shown in the figure 8.

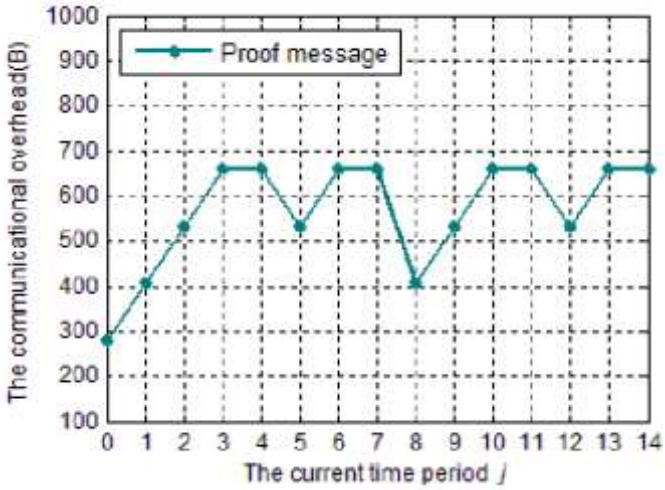


Figure.8 Size of the proof message in different time periods

The figure 9 shows the external structure of the proposed system that how a client's secret key is outsourced to the TPA and hence the operations of file uploading and file downloading is done using the update key provided by the TPA for every time period. The important point to notice is here that each time the key gets updated and same key for more than one operation is not allowed.

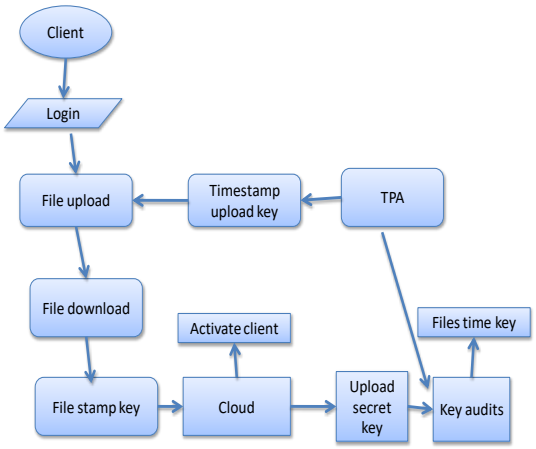


Figure.9 flowchart of the output of the proposed system

The figure 9 shows the modules of the output design the client, cloud and TPA with their respective operations and file stamp keys.

## VI. CONCLUSION

We first study how to outsource key updates for cloud storage auditing, proposing an effective auditing protocol with verification. Using this protocol, security key updates are outsourced to Third Party Auditor (TPA) so that client need not update his/her secret key each time. The TPA which plays major role adopts only the encrypted version of client's secret key and provides updated key each time when client wants to upload or download files from cloud storage, Client can further verify the validity of encrypted secret key when downloading from TPA. We also include formal security proof with performance simulation.

## REFERENCE

[1] Yu, Jia, Kui Ren, and Cong Wang. "Enabling cloud storage auditing with verifiable outsourcing of key updates." IEEE Transactions on Information Forensics and Security 11.6 (2016): 1362-1375J.

[2] Yu, Jia, and Huaqun Wang. "Strong key-exposure resilient auditing for secure cloud storage." IEEE Transactions on Information Forensics and Security 12.8 (2017): 1931-1940
[3] Lynn, Ben. "The pairing-based cryptography library." Internet: crypto. stanford. edu/pbc/[Mar. 27, 2013] (2006).
[4] Yu, Jia, et al. "Enabling cloud storage auditing with key-exposure resistance." IEEE Transactions on Information forensics and security 10.6 (2015): 1167-1179
[5] Brodkin, Jon. "Gartner: Seven cloud-computing security risks." Infoworld 2008 (2008): 1-3.
[6] Yu, Jia, et al. "One forward-secure signature scheme using bilinear maps and its applications." Information Sciences 279 (2014): 60-76.
[7] Hohenberger, Susan, and Anna Lysyanskaya. "How to securely outsource cryptographic computations." Theory of Cryptography Conference. Springer, Berlin, Heidelberg, 2005.
[8] Wang, Cong, et al. "Privacy-preserving public auditing for data storage security in cloud computing." Infocom, 2010 proceedings ieee. Ieee, 2010.
[9] D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing of algebraic computations," in Proc. 6th Annu. Conf. Privacy, Secur. Trust, 2008, pp. 240–245.
[10] C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in Proc. IEEE INFOCOM, Apr. 2011, pp. 820–828.
[11] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," in Proc. 17th Eur. Symp. Res. Comput. Secur., 2012, pp. 541–556.
[12] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientific computations," Adv. Comput., vol. 54,pp. 215–272, 2002.
[13] Juels, Ari, and Burton S. Kaliski Jr. "PORs: Proofs of retrievability for large files." Proceedings of the 14th ACM conference on Computer and communications security. Acm, 2007.
[14] Jin, Hao, Hong Jiang, and Ke Zhou. "Dynamic and Public Auditing with Fair Arbitration for Cloud Data." IEEE Transactions on Cloud Computing(2016).
[15] Yang, Kan, and XiaohuaJia. "An efficient and secure dynamic auditing protocol for data storage in cloud computing." IEEE transactions on parallel and distributed systems 24.9 (2013): 1717-1726.
[16] Li, Yannan, et al. "Privacy preserving cloud data auditing with efficient key update." Future Generation Computer Systems 78 (2018): 789-798.
[17] Angadi, Abhinay B., Akshata B. Angadi, and Karuna C. Gull. "Security Issues with Possible Solutions in Cloud Computing-A Survey." International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)2.2 (2013): pp-652.
[18] Srinivasamurthy, Shilpashree, and David Q. Liu. "Survey on cloud computing security." Proc. Conf. on Cloud Computing, CloudCom. Vol. 10. 2010.
[19] Gupta, Garima, P. R. Laxmi, and Shubhanjali Sharma. "A survey on cloud security issues and techniques." International Journal on Computational Sciences & Applications (IJCSA) 4 (2014): 125-132.
[20] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 598–609.
[21] H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2008,pp. 90–107.
[22] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., 2008, Art. ID 9.
[23] F. Sebe, J. Domingo-Ferrer, A. Martinez-balleste, Y. Deswarte, and J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034– 1038, Aug. 2008.
[24] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in Proc. 28th IEEE Int. Conf. Distrib. Comput. Syst., Jun. 2008, pp. 411– 420.
[25] M. Sookhak, A. Gania, M. K. Khanb, R. Buyyac, "Dynamic remote data auditing for securing big data storage in cloud computing", *Inf. Sci.*, Sep. 2105
[26] X. Chen, J. Li, X. Huang, J. Li, Y. Xiang, D. S. Wong, "Secure outsourced attribute-based signatures", *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 12, pp. 3285-3294, Dec. 2014.
[27] Chaum, David, and TorbenPryds Pedersen. "Wallet databases with observers." Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 1992.
[28] Atallah, Mikhail J., and Jiangtao Li. "Secure outsourcing of sequence comparisons." International Journal of Information Security 4.4 (2005): 277-287.
[29] Yuan, Jiawei, and Shucheng Yu. "Public integrity auditing for dynamic data sharing with multiuser modification." IEEE Transactions on Information Forensics and Security 10.8 (2015): 1717-1726.