Implementation of Efficient Audit Service Outsourcing for Data Integrity by Interfacing the Mobile Device in Clouds

D.Kumuthavijay
Department of ECE
Ganadipathy Tulsi's Jain
Engineering College
Vellore, Tamilnadu, India

J.Nandhini
Department of ECE
Ganadipathy Tulsi's Jain
Engineering College
Vellore, Tamilnadu, India

V.Jayaprakasan
Department of ECE
Ganadipathy Tulsi's Jain
Engineering College
Vellore, Tamilnadu, India

ABSTRACT
Cloud computing provide much more effective computing by centralized memory processing, storage and bandwidth**.** The problem in cloud computing is that they are facing a potentially formidable risk for missing or corrupted data. Third party auditor should be able to efficiently audit the cloud data storage without demanding the local copy of data. DES algorithm can use for encryption in CSP. In this paper, we propose to implement the mobile devices that can be interfaces in between the Cloud Service Provider and Third party Agent to avoid the delay in sending the modification done in the data storage to the cloud and also client's owner. Also we implement a user authentication protocol named oPass which leverages a user's cell phone and short message service (SMS) to prevent password stealing and password reuse attacks in cloud computing we demonstrate to decrease the delay through mobile device. Our simulation results for the cost, computational and communication overhead can perform more effective in cloud computing.

Keywords
Cloud Storage, Audit Service, Email alert, Mobile device, Security, Delay, oPass, CSP.

1. INTRODUCTION
Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing data storage, processing and bandwidth. Cloud computing is broken down into three segments: "application", "storage" and "connectivity." Each segment serves a different purpose and offers different products for business individuals around the world. The cloud computing is a mixture of two models. Currently users of computers with operating systems and certain features built into them [20].

The Cloud computing wants to use the model based on client-server where applications (code or data) are centralized and located on a server or server farm and client can work with a simple client application type. The technology also allows for solving certain problems present the first model (centralized server) as the management of resources. Until now, companies engaged in a finite and limited number of resources for an application or service, but the computational load exceeded this forecast, obtained a denial of service due to overload. Cloud computing concept also includes the dynamic provisioning of resources such as CPU, RAM, hard drive, peripheral etc... [20].

The cloud storage services (CSS) relieves the burden of storage management and maintenance. However, if such an important service is vulnerable to attacks or failures, it would bring irretrievable losses to users since the data or archives are stored into an uncertain storage pool outside the enterprises. These security risks come from the following reasons: the cloud infrastructures are much more powerful and reliable than personal computing devices. However they are still susceptible to security threats both from outside and inside the cloud Armbrust et al [11] for the benefits of their possession, there exists various motivation for cloud service provider (CSP) to behave unfaithfully toward the cloud users Tchifilionova et al [12] furthermore, the dispute occasionally suffers from the lack of trust on CSP.

It is necessary for cloud service providers to offer an efficient audit service to check the integrity and availability of the stored data Yavuz et al [7]. Traditional cryptographic technologies for data integrity and availability based on hash functions and signature schemes Yumerefendi et al [4] cannot work on the outsourced data without a local copy of data. In addition, it is not a practical solution for data validation by downloading them due to the expensive transaction, especially for large-size files. Moreover, the solutions to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users Armbrust et al [11].

Therefore, it is crucial to realize public auditability for CSS, so that data owners may resort to a third party auditor (TPA), who has expertise and capabilities that a common user does not have for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and data assurance in clouds. Computing cloud provides computation, software, data access and storage resources without requiring cloud users to know the location and other details of the computing infrastructure [19]. There are 3 main types of cloud computing which are Software as a service (Saas), Platform as a service (Paas) and Infrastructure as a service (Iaas).

1.1 Benefits of Cloud Computing

1.1.1 Cost Effective

There are no need users to invest their time and money into using stand alone servers which would be a bit complication to use compared to the cloud method. It is a cheaper way to maintain the software and it will save time, as developers keep track of updates and maintain your programs while you use it. There is no need for replacing capital expenditures on a regular basis. The cost of using cloud resources is very economical for resources such as centralized, real estate, bandwidth and power. Users will also save money on software updates, management costs and data storage costs.

1.1.2 Speed & Scales

There is no need to purchase and setup hardware manually when using the cloud computing method. Depending upon their needs the user can quickly scale up or scale down.

1.1.3 Innovation

Users can now pay closer attention to the innovation process because they don't have to manually manage other resources. Cloud computing produces a faster development pace for prototype and testing phases. Projects at which users have to watch over for progress on a regular basis will benefit the most because of this advantage.

1.1.4 Convenient

Overheads are low when sharing the same infrastructure the services are available to use immediately. Payments are only billed for the times that the service is being utilized. They can easily check the cost of bill because the service provider will make them available online for you to view.

1.1.5 Location

Areas that have lower overheads are able o utilize this service and take advantage of the benefits as well. Many different websites are able to be set up in the case of a disaster recovery which helps the companies to cut costs in different ways.

1.1.6 Multiple Users at one time

Cloud computing is not only cost effective, but utilizing it also helps to cut back on global wastes. It is environmentally friendly since it is shared by multiple users. The down time is reduced and the resources are stretched.

1.1.7 Flexible

There is a high rate of flexibility when using cloud computing because people can use it whenever they want too. This is also one of the main reasons people loves to use this method. Service level agreements are what cover the costs in this case. If the correct quality is not provided then has to pay a penalty cost.

1.1.8 Device Diversity

The cloud computing method can be accessed through various different electronic devices that are able to have access to the internet. These devices would include iPod, smart phone, Laptop or desktop computer.

1.1.9 Maximum Storage Space

During the usage of the internet with cloud services, more number of files and data's can be stored.

1.2 Data Integrity

The assurance that data received are exactly as sent by an authorized entity (contains no modification, insertion, deletion or reply [21]. A variety of mechanisms used to assure the integrity of a data unit or stream of data units. In cloud computing integrity can apply to a stream of messages, a single message or selected fields within a message. A connection-oriented integrity service, one that deals with a stream of messages, assures that messages are receives as sent, with no duplication insertion, modification, reordering or replays. The destruction of data is also covered under this service. Thus, the connection-oriented integrity service addresses both message stream modification and denial of service.

On the other hand, a connectionless integrity service that deals with individual messages without regard to any larger context generally provides protection against message modification only. It can make a distinction between the service with and without recovery. Because the integrity service relates to active attacks, that are concerned with detection rather than prevention. If a violation of integrity is detected, then the service may simply report this violation and some other portion of software or human intervention required to recover from the violation. Alternatively, there are mechanisms available to recover from the loss of integrity of data and the incorporation of automated recovery mechanisms are the more attractive alternative.

1.3 DES Encryption

DES encryption can be explained with suitable flow chart and algorithms. Plaintext is broken into blocks of length 64 bits and the encryption is block wise.

1. A message block is first gone through an initial permutation IP, and then divided into two parts L0||R0, where L_0 is the left 32 bits.

2. Round i has input $L_{i-1} \| R_{i-1,}$ and output $L_i \| R_i$, where,

$$L_i = R_{i-1,} \quad R_i = L_{i-1} \Theta f(R_{i-1,} k_i)$$ and

k_i is the sub key for the ith round, where $1 \leq i \leq 16$.

3. After Round 16, L_{16} and R 16 are swapped, so that the decryption algorithm has the same structure as the encryption algorithm.

4. Finally, the block is gone through the inverse permutation IP^{-1} and then output.

5. The permutation and inverse permutation can be given in Table 1a and 1b.

Table 1 (a)

M1	M2	M3	M4	M5	M6	M7	M8
M9	M10	M11	M12	M13	M14	M15	M16
M17	M18	M19	M20	M21	M22	M23	M24
M25	M26	M27	M28	M29	M30	M31	M32
M33	M34	M35	M36	M37	M38	M39	M40
M41	M42	M43	M44	M45	M46	M47	M48
M49	M50	M51	M52	M53	M54	M55	M56
M57	M58	M59	M60	M61	M62	M63	M64

Where *Mi* is a binary digit, then the permutation *X* = IP (*M*).

Table 1 (b)

M58	M50	M42	M34	M26	M18	M10	M2
M60	M52	M44	M36	M28	M20	M12	M4
M62	M54	M46	M38	M30	M22	M14	M6
M64	M56	M48	M40	M32	M24	M16	M8
M57	M49	M41	M33	M25	M17	M9	M1
M59	M51	M43	M35	M27	M19	M11	M3
M61	M53	M45	M37	M29	M21	M13	M5
M63	M55	M47	M39	M31	M23	M15	M7

If the inverse permutation $Y = IP^{-1}(M)$ and decryption uses the same algorithm as encryption, except that the application of the sub keys is reversed.

2. AUDIT SYSTEM ARCHITECTURE

In this architecture, we consider a data storage service containing four entities [13].

Data owner (DO): Who has a large amount of data to be stored in the cloud.

Cloud service provider (CSP): Who provides data storage service and has enough storage spaces and computation resources.

Third party auditor (TPA): Who has capabilities to manage or monitor outsourced data under the delegation of data owner.

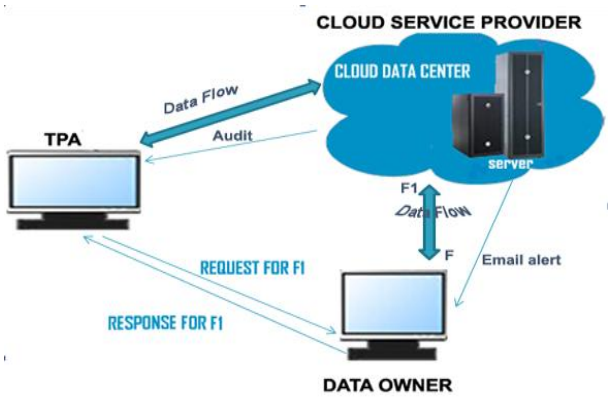
Granted applications (GA): Who have the right to access and manipulate stored data. These applications can be either inside clouds or outside clouds according to the specific requirements.

The above four entities plays an important role in the efficient audit service and the architecture in Yan Zhu et al [13] are known as the audit service outsourcing due to data integrity verification can be implemented by TPA without help of data owner. In that architecture, the data owner and granted clients need to dynamically interact with CSP to access or update their data for various application purposes. However, we neither assume that CSP is trust to guarantee the security of stored data nor assume that the data owner has the ability to collect the evidences of CSP's fault after errors occur. Hence, TPA as a trust third party (TTP) is used to ensure the storage security of their outsourced data. They assume the TPA is reliable and independent, and thus has no incentive to collude with either the CSP or the clients during the auditing process.

TPA should be able to make regular checks with the data owner, if any data can be lost or insert any extra information in the cloud service provider. TPA should be able to take the evidences for the disputes about the inconsistency of data in terms of authentic records for all data operations. This is because it is more easy and feasible to ensure the security of one TTP than to maintain the credibility of the whole cloud. Hence, the TPA could be considered as the root of trust in clouds. [6]

3. AUDIT SERVICE SYSTEM USING E-MAIL ALERT

The Figure 1 shows the efficient audit service in which the original data F can transfer to the CSP by using DES encryption algorithms. The encrypted data can be stored in the CSP due to the security risk in cloud computing. F1 is denoted as DES encrypted data which is to prevent from security risk or leakage of data. Client's owner supposed to store all the data (F) to the CSP by encrypted as F1 which is shown in Figure 1. To get a efficient audit service outsourced data from the CSP, the TPA is ready to audit outsourced data by requesting for F1 to the Data owner, then immediately the Data owner response for F1 (encrypted data) with efficient manner. The TPA can finished the auditing within its required time, then transmit to the CSP immediately



F →Original data: F1→ Encrypted data

Fig. 1 Using E-mail alert of audit service system in clouds

The CSP can transmit efficient auditing information to the Data owner through the E-mail alert which is observed in the Figure 1. This will causes a delay due to communication with many other users' application. So the Data owner cannot get the auditing information immediately with some unexpected situation.

4. PROPOSED WORK

We demonstrate to decrease the delay and also to reduce the cost, computational and communication overhead, then interfacing the Mobile Devices in between TPA and Data owner in the cloud computing. The proposed system allows TPA to perform auditing with minimum overheads in storage, communication and computation in figure 5 (a & b) and we motivate to avoid the security risks which occurs during the audit service outsourced for data integrity in clouds. We implement the Efficient Audit Service Outsourced for Data Integrity by interfacing the MOBILE DEVICE sending message as an alert. Mobile device can be interfaced between the THIRD PARTY AGENT and CLIENT'S OWNER to avoid delay process, because sometimes CLOUD SERVICE PROVIDER is busy with other application.

Once TPA finished it's auditing of the outsourced data storage, immediately information is transmitting to data owner with secret keys. Audit service will be monitored by using mobile device if any modification happen in data transmission between the third party auditor and audit service application, then instruction will intimate or alert the modification to the cloud owner. We implement a mobile device to minimize the delay through transmit the message i.e. (any modification or no modification) from TPA to data owner. The block diagram of Audit service in cloud computing for proposed system shown in Figure 2 and the abbreviation for MA is Mobile Alert.

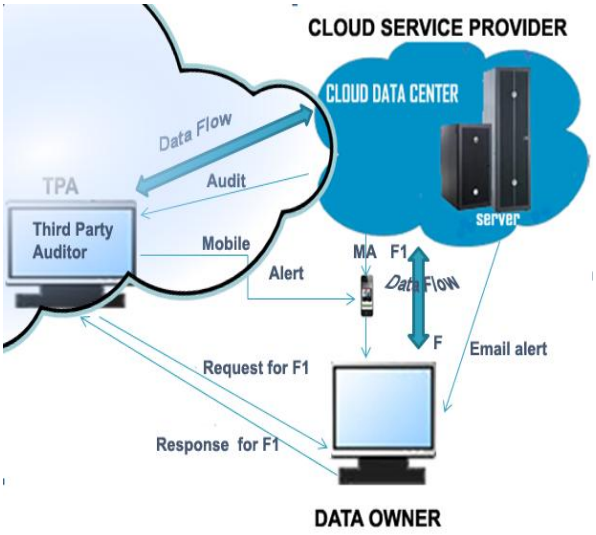


Fig. 2 Block Diagram of Audit Service system for Proposed System

Instead of using password in signs up page (B), OPass can send message directly to server which only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Figure 3 describes the overall module of the oPass system. For users to perform secure login on an untrusted computer (kiosk), and a web server that users wish to access. The user operates her cell phone and the untrusted computer directly to accomplish secure logins to the web server. The communication between the cell phone and web server is through the SMS channel in Eqn (2). The web browser interacts with the web server via internet. In our protocol design, we require the cell phone interact directly with the kiosk [18]. The general approach is to select available interfaces on the cell phone. In this protocol we use MAC algorithm and synchronous binary stream cipher for the confidentiality and integrity algorithms [17].

4.1 OPASS SYSTEM

We design a user authentication protocol named oPass which leverages a user's cell phone and short message service to thwart password stealing and password reuse attacks. OPass only requires each participating website possesses a unique phone Number, and involves a telecommunication service provider in registration and recovery phases [14]. Through oPass, users only need to remember a long-term password for login on all websites. The oPass consist of four module are

4.1.1 Enrolment Phase
The aim of this phase is to allow a user and a server to negotiate a shared secret to authenticate succeeding logins for the user. This user begins by opening the oPass program installed on her cell phone.

4.1.2 Server verification
Server can decrypt and verify the authenticity of the registration SMS and then obtain with the shared key. Server also compares the source of received SMS through a un trusted browser (on a kiosk). The user uses her cell phone to produce a one-time password and deliver necessary information encrypted with server via an SMS message. [5]

4.1.3 Client verification
They enter ID (account id she prefers) and ID (usually the website URL or domain name) to the program. The mobile program sends ID and ID to the telecommunication service provider (TSP). Once the TSP received the ID and the ID, it can trace the user's phone number based on user's SIM card. The login phase begins when the user sends a request to the server.

4.1.4 Accessing service
User enter the browser and Register to server, then server transmit through sms on long term password with encrypt to mobile. Immediately user receives the sms and send to server. Then server verify both password, if correct the password suddenly open the "view all detail", else if not match that password won't allow the site inside.

A password-based user authentication has a major problem that humans are not experts in memorizing text strings. [16] [5]. Florencio et al [15] indicated this attack is referred to as the password reuse attack. Despite the assistance of these two technologies—graphical password and password management tool—the user authentication system still suffers from some considerable drawbacks.

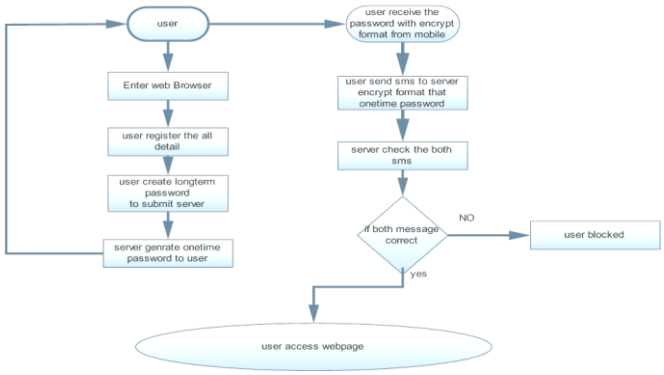


Fig.3 Overall Module of oPass System

We believe oPass is efficient and affordable compared with the conventional web authentication mechanisms [20]. The general formula is given in one-time password Eqn (1) can be generated by a secure hash is as

$$\delta_i = \mathrm{H}^{N-1}(c) \qquad (1)$$

And the cell phone sends an encrypted registration SMS to the server by phone number as follows

$$Cellphone \rightarrow S : ID_u, \{c \| \phi\} K_{sd} \qquad (2)$$

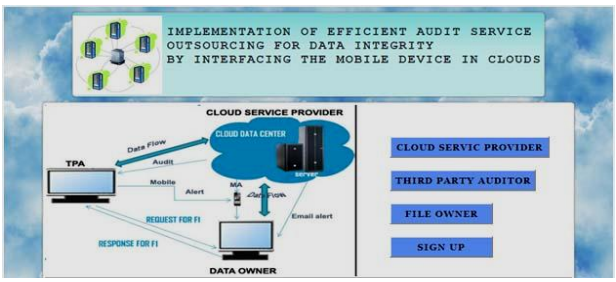
ID – Identity of entity, ϕ - Random seed, c – Secret shared credential between cell phone and the server and

K_{sd} - shared secret key between cell phone and the server. In oPass, they need a TSP (trusted proxy) to rectify the security [14]. Both the oPass system and mobile device can be combining to avoid the password which is to prevent from password stealing. Figure.2 shows by interfacing the mobile device in cloud computing to decreases the delay, communication overhead and computation overhead. The simulation graph can be shown in Figure.5 (a & b) which

various with the Meta file (MB) and data processing (MB) to decreases the overhead in communication and computation in cloud computing.

5. RESULTS AND DISCUSSION

In this paper, we have implemented the efficient audit service system with adding the E-mail alert based on the proposed solution in the Cloud computing. This system have been developed in an experimental cloud computing system environment which is constructed within the framework of the IaaS to provide powerful virtualization, distributed storage, and automated management. Next we proposed by interfacing the mobile devices to get an alert with immediate SMS to the Client's owner. This implementation used to avoid the delay in between CSP and Client's owner. Results can be given from various modules in Figure 4 (a - f) below. Finally we implement the OPass to prevent the password steeling or password reuse attacks in cloud computing. Instead of using the password box in Fig 4 (b), we implemented as in Fig 4 (f) i.e. without password in the login using oPass and then the simulation results of cost, computational and communication overheads can be shown in Figure 5 (a & b) and the comparison of existing and proposed scheme of communication and computation overhead can be given in Table.2 (a & b).

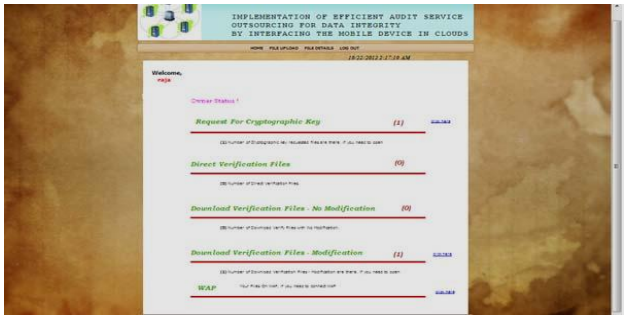


(a) Home page

(b) Data owner sign in page

(c) Key

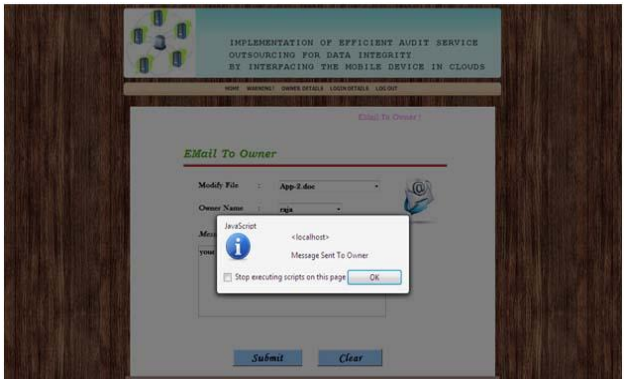
(d) Data owner



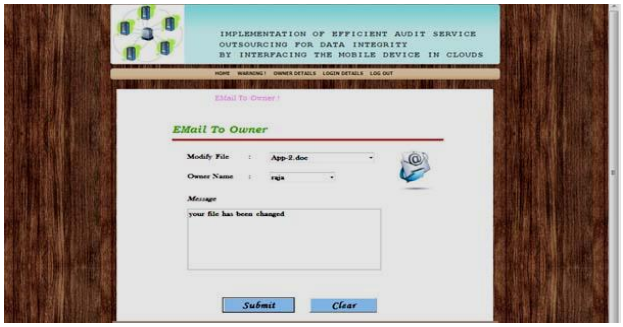
Data owner

(e) Csp login

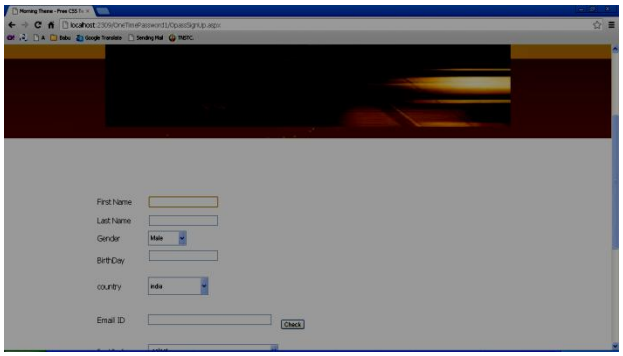
Csp



Csp

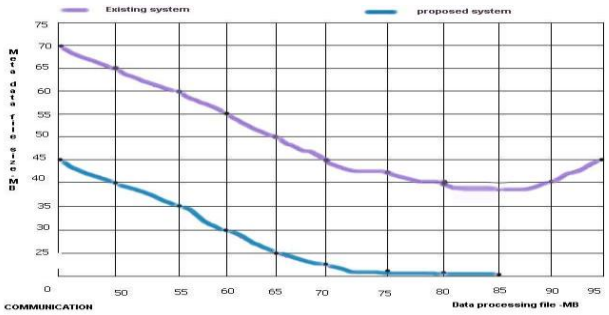


Csp

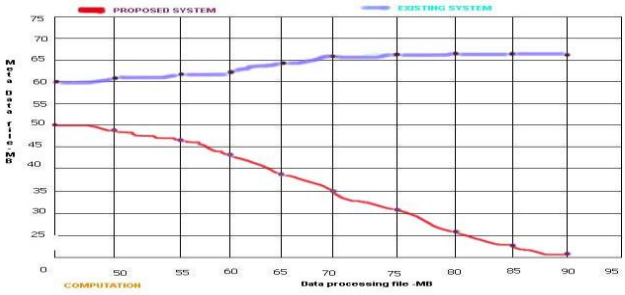


(f) Data owner sign up page using oPass

Fig. 4 various modules of Efficient audit results



(a) Communication overhead Vs Data processing



(b) **Computation(meta file) Vs Data processing**

Fig. 5 Simulation Results

Table.2 (a) Communication

Existing System (MB)	Data Processing (MB)	Proposed system (MB)
65	50	45
60	55	40
55	60	35
50	65	30
45	70	15
43	75	5

Table.2 (b) Communication

Existing System (MB)	Data Processing (MB)	Proposed system (MB)
60	50	49
62	55	46
64	60	43
65	65	39
66	70	35
68	75	31

The existing scheme and proposed system were transfer the data information through the meta file(MB) and the data processing in data file (MB). The table 2(a & b) defines the difference between the existing and proposed system in the cloud computing.

6. CONCLUSION

In this paper, we proposed the Efficient Audit service outsourcing for data integrity using an E-mail alert in cloud computing, where TPA can perform the storage auditing without demanding the local copy of data. TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process. Then implemented the mobile device by interfacing between the TPA and DO, which is to avoid delay by transferring the information of audit service through TPA from CSP to DO. Then, they combine to propose a user authentication protocol named oPass which leverages cell phones to avoid the password stealing. Both the process is done by mobile device through SMS. Our experiments clearly showed that our approach could minimize cost, computation and communication overheads. We believe all these advantages of the proposed schemes will shed light on economies of scale for Cloud Computing.

7. REFERENCES

[1] Cramer, R., Damgård, I., MacKenzie, P.D., 2000. Efficient zero-knowledge proofs of knowledge without intractability assumptions. In: Public Key Cryptography, pp.354–373.

[2] Boneh, D., Franklin, M., 2001. Identity-based encryption from the weil pairing. In: Advances in Cryptology (CRYPTO'2001). Vol. 2139 of LNCS, pp. 213–229.

[3] B. Ives, K. R. Walsh, and H. Schneider, "The domino effect of password reuse," Commun. ACM, vol. 47, no. 4, pp. 75–78, 2004.

[4] Yumerefendi, A.R., Chase, J.S., 2007. Strong accountability for network storage. ACM Trans. Storage (TOS) 3 (3).

[5] D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, 2007, pp. 657–666, ACM.

[6] Ateniese, G., Pietro, R.D., Mancini, L.V., Tsudik, G., 2008. Scalable and efficient provable data possession. In: Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, SecureComm, pp. 1–10.

[7] Yavuz, A.A., Ning, P., 2009. Baf: An efficient publicly verifiable secure audit logging scheme for distributed systems. In: ACSAC, pp. 219–228.

[8] Bowers, K.D., Juels, A., Oprea A.,2009. Hail: a high-availability and integrity layer for cloud storage. In: ACM Conference on Computer and Communications Security,pp. 187–198.

[9] Wang, C., Wang, Q., Ren, K., Lou, W., 2010. Privacy-preserving public auditing for Data storage security in cloud computing. In: INFOCOM, 2010 Proceedings IEEE, pp. 1–9, 14-19.

[10] Dodis, Y., Vadhan, S.P., Wichs, D., 2009. Proofs of retrievability via hardness amplification. In: Reingold, O. (Ed.), Theory of Cryptography, 6th Theory of Cryptography

[11] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M., 2010. A view of cloud computing. Commun. ACM 53 (4), 50–58.Conference, TCC 2009. Vol. 5444 of Lecture Notes in Computer Science. Springer, pp. 109–127.

[12] Tchifilionova, V., 2011. Security and privacy implications of cloud computing c lost in the cloud .In Camenisch, J., Kisimov, V Dubovitskaya.M.(Eds), Open Research Problems in Network Security. Vol.6555 of Lecture Notes in Computer Science Springer, Berlin/Heidelberg,pp 149-158.

[13] Yan Zhua.b, Hongxin Hu, Gail-Joon Ahn, Stephen S. Yau for data integrity in clouds: The Journal of Systems and Software85 (2012) 1083-1095.

[14] Hung-Min Sun, et.al 2012. "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks". Vol.7, No.7. TS 23.040: Technical Realization Short Message Service (SMS) 3 GPP [Online].

[15] S. Chiasson, A.Forget,E. Stobert,P.C.van Oorschot, and R.Biddle,"Multiple password interference in text passwords and click-based graphical passwords," in CCS'09: proc. 16th ACM Conf. Computer Communications Security, New York, 2009, pp. 500–511, ACM.

[16] S.Gaw and E.W. Felten, "Password Management Strategies for online accounts, in SOUPS '06: PROC. 2ND SYMP. Usable Privacy. Security, New York 2006, pp. 44-55, ACM.

[17] I. T. Report, ITU Internet Rep. 2006: Digital. Life [Online]. Available: http://www.itu.int/

[18] TS 35.201: Specification 3GPP Confidentiality Integrity Algorithms document 1: f8 and f9 Specification 3GPP [Online]. Et.al.

[19] By Earthnet: http/ earthnet.net/cloud.html, copyright from 1995-2012- Earthnet, Inc.

[20] By Eric Knorr, Galen Gruman "What Really Cloud Computing".

[21] By Williams Stallings Cryptography and Network Security principles and Practices, Fourth Edition, Publisher: Prentice hall, Pub Date: November 16, 2005, Pages: 592.

8. AUTHOR'S PROFILE

D.kumuthavijay received her Bachelor's Degree in Electronics and Communication Engineering from Anna University, Chennai, India in 2005. She has 6 years teaching experience in various Institutions. Currently she is pursuing Master Degree in Computer and Communication Engineering in Anna University, Chennai, India. She has published 1 research paper in International conference and 1 research paper in National conference. Her research interests include Wireless Network, Network Security and Wireless communication.

J.Nandhini received her Bachelor's Degree in Electronics and Communication Engineering from Madras University, India in 2000 and Master's Degree in Applied Electronics from Sathiya Bama University, Chennai, India in 2006. She has 6 and half years teaching Experience as Assistant professor in various Institutions. Her research interests include Communication Engineering and Networking. He is a life member of ISTE.

V.Jayaprakasan received his Bachelor's Degree in Electronics and Communication Engineering from Bharadhidasan University, Tiruchirappalli, India in the year 1999 and Master's Degree in Communication Systems from Anna University, Chennai, India in the year 2006. He has started his teaching profession in the year 2006 in Ganadipathy Tulsi's Jain Engineering College, Vellore. Earlier he has 11 years industrial experience in an electronics based industry. At present he is a Professor in Electronics and Communication Department. He has published 3 research paper in International Journals and 2 research papers in International Conferences. His areas of interest are Wireless communication, Networking and Signal Processing. He is a life member of ISTE.