Identity Based Security Auditingfor Data Sharing with Sensitive Information Hiding using Cloud Storage

N.V.T.Bhuvaneswari, M.TrinathBasu, M.SriSathvik, Ravi Kumar Tenali

Abstract: A privacy-preserving public auditing mechanism is used in the cloud for data sharing in the cloud storage. To utilize this, we require digital signatures to construct homomorphism authenticators and also verifying the metadata which is needed for auditing thewanted data, so that a public verifier can able to reviewthe distributed data integrity without retrieving the entire data. In this paper, we have implemented sensitive information for sensitive data sharing mechanism in cloud system, where user can remotely store his/her data in cloud and can retrieve data whenever he/she wants.Data owner store the file in the database and he can send the key to the user with the SMTP(Simple Mail Transfer Protocol) and the user can download the file with encrypted format with the help of 16bit key user can access to the file. Here auditor can check the file that it is corrupted or not. If it is corrupted from the user then auditor can regenerate the file. In addition, this mechanism is able to perform multiple auditing tasks at the same time instead of validating them one by one. It cannot decide who the signer on each block. In addition, our mechanism is in a position to perform multiple auditing tasks at the same time rather than verifying them one by one. We advance extend our mechanism to support batch auditing.

***Index Terms*: Cloud computing, Privacy-preserving mechanism, Remote data integrity, Data Integrity.**

I. INTRODUCTION

A Cloud service providers recommend that clients efficient and scalable information storingin administrations with a much lower negligible expense than routine methodologies. The mutual information document is isolated into various small blocks, where each block is exclusively marked by one of the two clients with existing open reviewing arrangements. When an underwriter obstruct in this mutual record is upgraded by a client, this client needs to sign the new block utilizing his/her private key. At last, unique block are marked by various clients because of the adjustment presented by these two distinct clients. At that point, so as to effectively review the trustworthiness of the whole information, an open verifier needs to pick the right open key for each block. Thus, this open verifier will unavoidably gain proficiency with the personality of the endorser on each block because of the remarkable necessity between a character and an open key by means of advanced declarations under open key framework (PKI). It is an overwhelming weight forclients to store the aggregate sum of information locally.

Hence, an ever increasing number of organizations and people might want to store their information in the cloud. Be that as it may, the information put away in the cloud may be corrupted or lost because of the unavoidable programming bugs, equipment issues and human blunders in the cloud. So as to confirm whether the information is put away effectively in the cloud, numerous remote information uprightness evaluating procedures have been suggested. In remote information respectability evaluating plans, the information proprietor needs to create marks for information hinders before transferring them to the cloud. The information put away in the cloud is consistently shared over numerous clients in many distributed storage applications, for example, Google Drive, Dropbox and iCloud. Information sharing as a standout amongst the most widely recognized highlights in distributed storage affirms various clients to impart their information to other people.

However, these shared data stored in the cloud might containsome sensitive information of the user by considering the example of hospital's sensitive information where these EHRs are directly uploaded to the cloud which wants their sensitive information to be shared for research purposes. The sensitive information contains details of both patient and hospital will be inevitably exposed to the cloud. To overcome the following circumstances, it is important to finish data integrity on the preferences that are required for sensitive information of shared data in the cloud and also for storing the data to the user. In this paper I would like to propose six key important components which are related to data sharing in cloud.

These key components are listed below:

1). **Plain Text**: The main information to be transmitted to a specified receiver is the plain text.Like, if a sender wants to send a message as "good morning" to another person, thehere "good morning" is the plain text.

2). **Cipher Text:** The meaningless message that is obtained at the receiver side after the transmission is the cipher text. For example, the cipher text for the plain text "good morning" would be "25lh%%fg@t3".

3). **Encryption**: Conversion of the simple text into cipher text at the sender side is called as encryption. Here for the encryption process has two things are required

Revised Manuscript Received on April 06, 2019.

N.V.T. Bhuvaneswari, Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
M. TrinathBasu, Asst. Professor, Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram , AP, India.
M. SriSathvik, Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram ,AP,India.
Ravi Kumar Tenali, Asst. Professor, Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram , AP, India.

an algorithm and a key.

4). **Decryption:** Decryption is reverse process of encryption the cipher text is converted back into its original form. Even decryption method requires analgorithm and a key. Usually this algorithm will be similar for both encryption and decryption with minor modifications if necessary.

5). **Key:** A key is used during the encryption process for the translation of plain text into cipher text and during the decryption process for the translation of the cipher text into plain text.

6). **Hash Function:**Hash is a procedure, signature function that translates information into cryptic value.

II. LITERATURE REVIEW

S.M. Chow [1] the storage data in the cloud about the Third Party Auditor(TPA) who can effectively review the shared information in cloud, but can't recognize who is the underwriter on each blocks, but can provide security for clients who will store their information on the cloud. They will also use the ring signature to process the data verification about shared information. This verification will recognize the loop holes of the underwriter on each block of shared information in the cloud and will keep it private to an outsider examiner (TPA), who will also be ready to validate the honesty of shared information without recovering the total record.To keep the protection from the Third Party Auditor (TPA), in light of the fact that the personalities of underwriters on shared information may show that a specific client in the gathering or an extraordinary block in shared information is a more significant focus than others. The data is private to the gathering and ought not to be uncovered to any outsider.

B.Wang[2] has proposed the concept of data storage of data in the cloud and users can easily alter the data in the cloud and share the data in the cloud.At the point when a client in the gathering is exists, we permit the semi-confided in cloud to re-sign hinders that were marked by the dropped by the client with intermediary marks. The gathering can bar a lot of calculation and correspondence assets amid client denial. The usage of intermediary marks they enable the cloud to re-sign block for existing clients amid client denial; with the goal that current client can download the file. This procedure can bolster amass examining by confirming numerous reviewing undertakings simultaneously and can significantly improve the efficiency of client repudiation.

YueZhang[3]Distributed storage evaluating plans for shared information notice to checking the uprightness of cloud information shared by a gathering of customers. Notwithstanding, diminish the computational overhead effects on client repudiations become a key research challenge for accomplishing handy cloud information inspecting. We recommend a special stockpiling reviewing strategy that accomplishes profoundly proficient client renouncement autonomous of the complete number of document blocks impacted by the dropped client in the cloud.

Yan Zhu[4] A construction of dynamic audit services for untrusted and outsourced storage and verifying the integrity of untrusted data. Enhance the efficient of method for periodic sampling audit to enhance the performance of TPAs and storage service providers. This method is based on the inquiry and occasional check for improving the execution of review audit services. In this paper audit system verifies the integrity with less computation and requiring less extra storage for audit metadata.

C. Wang [5] The clients can remotely store there data in the cloud platform. The users never again have ownership of the potentially extensive size of re-appropriated information makes the information honesty to makes the data integrity security in Cloud Computing. Thus, enables public auditability for cloud data storage security that users can have a possibility to an external audit party to check the integrity of outsourced data when it required. To securely introduce an effective third party auditor, should be able to efficiently review the cloud data storage without demanding the local copy of data.

ANALYSIS

A. Problem Identification

The data from the cloud issues are increasing in the sharing of data to other. To support efficiently managed of multiple auditing tasks in the cloud .So, that digital signature to extend our main result into a multi-client tasks, where third party auditor can perform multiple auditing tasks at the same time. Wide security and performance investigation demonstrates that security in the cloud and retrieve the data whenever we want. The proposed scheme are additional secure and highly efficient.

B. Existing System

The existing technique for new significant privacy issue introduced in the case of shared data with the use of the leakage of identity privacy to public verifier. The conventional methodology for checking informationcorrectness is to recover the whole data from the cloud, and afterward confirm information respectability by checking the accuracy of marks. To solidly present a compelling outsider examiner (TPA), the accompanying two major necessities must be met: 1) TPA ought to have the capacity of effectively review to the cloud information stockpiling without requesting the nearby duplicate of information, and present no future on-line weight to the cloud client. 2) The outsider auditing process ought to usher in no new vulnerabilities towards user data privacy.

Limitations:

The clients no longer actually own the storage of their data; traditional cryptographic primitives for the purpose of data security protection cannot be directly approved.

- They do not perform the multiple auditing tasks simultaneously.
- Loss of data.
- Does not supply any privacy for private data.
- Authentication time takes too long.

C. Proposed System

The proposed framework, a security safeguarding open evaluating techniques for shared information in the cloud.We utilize computerized marks to build homomorphism authenticators, so an open verifier can check the common information respectability without recovering the entire information, yet it can't recognize who is the endorser on each block. To improve the power of checking various reviewing undertakings, we further stretch out our instrument to help bunch evaluating. There are two interesting issues we will keep on contemplating for our future work. The capacity for the gathering administrator to uncover the personality of the underwriter dependent on confirmation of metadata in some extraordinary circumstances.

SMTP Stands for "Simple Mail Transfer Protocol".This can be the protocol used for causation e-mail over the web. Your e-mail shopper uses SMTP to send a message to the mail server, and also the mail server uses SMTP to relay that message to the proper receiving mail server. Basically, SMTP could be a set of commands that certify and direct the transfer of electronic message. Once configuring the settings for your e-mail program, you always ought to set the SMTP server to your native net Service Provider's SMTP settings. However, the incoming mail server ought to be set to your mail account's server, which can differ than the SMTP Server.In the admin page Data owner, User and Auditor can register the details then process began. Data owner store the file in the database and he can send the key to the user with the SMTP and the user can download the file with encrypted format with the help of 16bit key user can access to the file. Here auditor can check the file that it is corrupted or not. If it is corrupted from the user then auditor can regenerate the file.

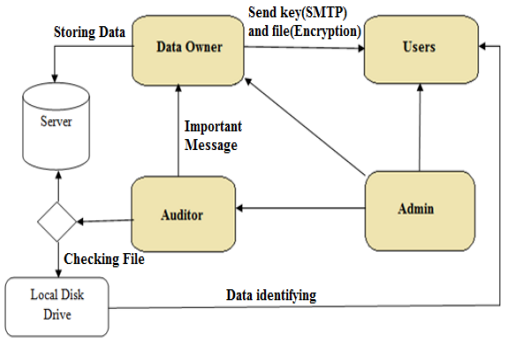

Fig.1The System Model

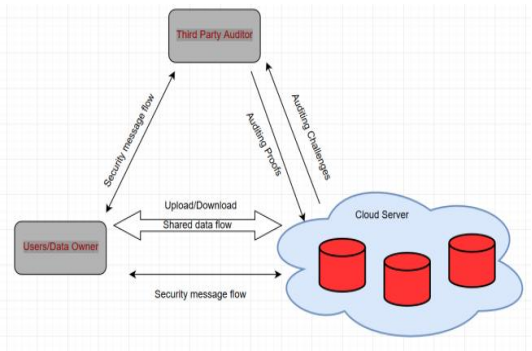

Fig.2 Storing of data in cloud and auditing the data

Table.1: It represents an overview of the proposed system; the components used as test case in detailed as follows:

Test Case	Check Field	Objective	Expected Result
TC-001	Admin	Login	Login Success or failure
	Admin	(If login is success) Creating registration forms	SMTP(Simple mail transfer protocol)
	Admin	User Revocation	Delete users from database
TC-002	Data owner	Login	Login Success or Failure
	Data owner	(If Login is success) Upload files	It will store in database (Encryption)
TC-003	Users	Login	Login Success or failure
	Users	(If login success) Download files	Decrypt that information
	Users	Send request to auditor for checking files	Get response from auditor
TC-004	Auditor	Login	Login Success or failure
	Auditor	(If login is success) Check files	Whether it is corrupted or not
	Auditor	If file is corrupted	Send mail to data owner

III. ADVANTAGES OF CLOUD OVER DATABASE

- **Usability:** Most cloud storage services provide their users the facility to drag and drop the concerned files between the local storages and cloud storages which improve the flexibility of usage.
- **Bandwidth:** Instead of sending files in a traditional way like emailing, one can send a web link to the involved recipients which greatly reduce the bandwidth usage.
- **Easy Accessibility:** Through Internet one can be able to access the stored files from anywhere.
- **Backup and Disaster Recovery:**Cloud offers easier backup and recovery facilities when compared to the physical device.Even at the time of extreme disasters, cloud is capable of providing sound technology that helps to retrieve or access any kind of information.
- **Low cost:** The annual operating costs of Businesses and organizations can be reduced by utilizing distributed storage; a cloud storage cost isabout 3 cents for each gigabyte (Gb) to store information internally.Clients can see additional cost investment funds since it doesn't require

interior capacity to store data remotely.

IV. RESULTS AND DISCUSSION

Fig.3. Home Page

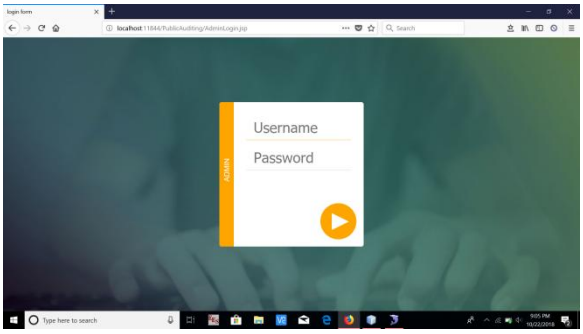

Fig.4. Admin Login Page

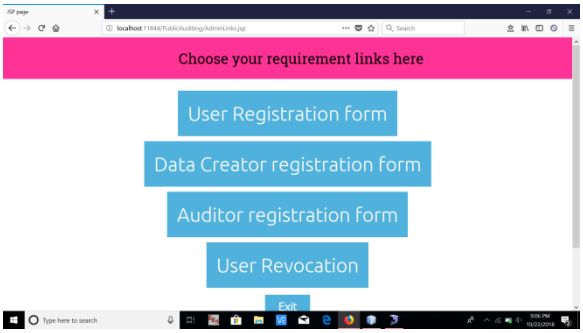

Fig.5. Registration Form

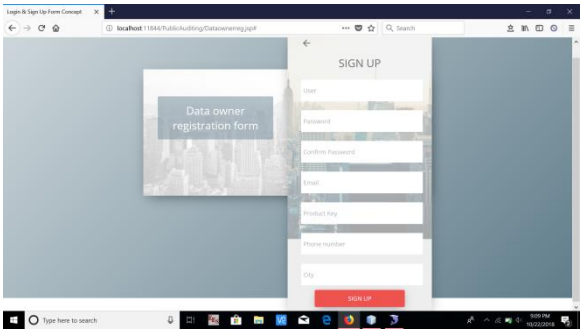

Fig.6. Data Owner Registration Form

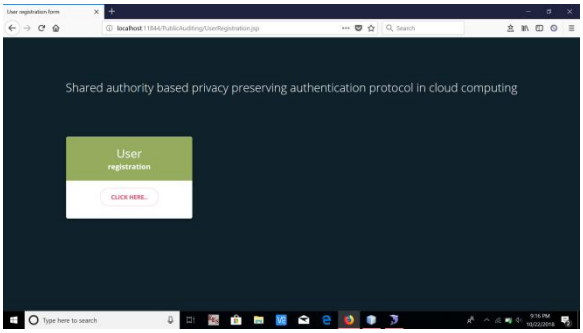

Fig.7. User Registration

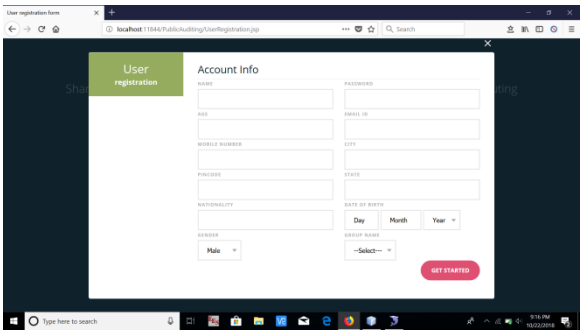

Fig.8. User Registration Form

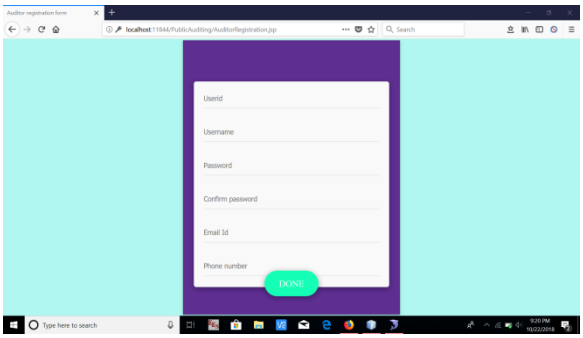

Fig.9. Auditor Registration Form

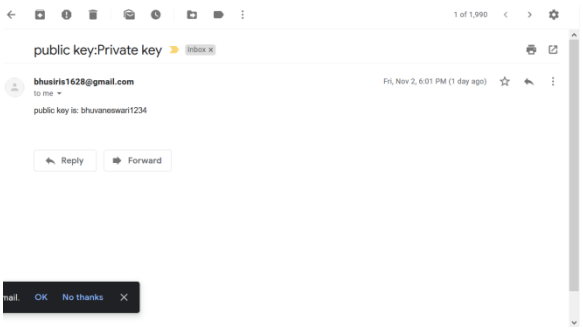

Fig.10. Public Key sent to the user mail

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

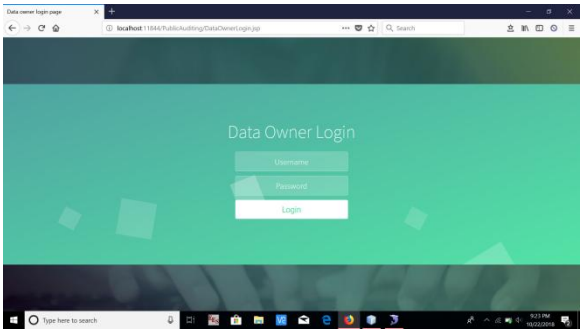

Fig.11. Data Owner Login Page

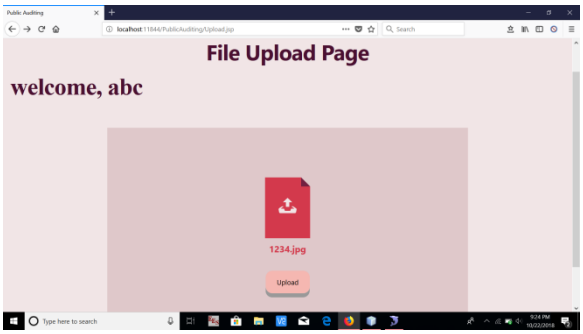

Fig.12. Data Owner File Upload Page

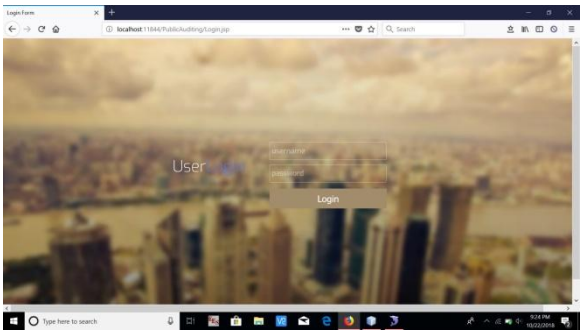

Fig.13. User login page download the file

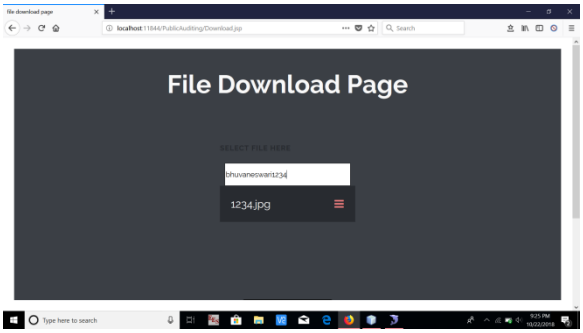

Fig.14. User File Download Page

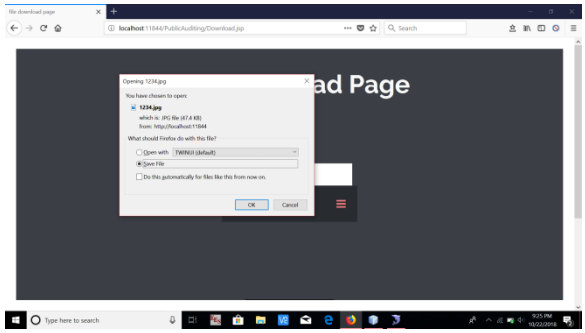

Fig.15. File Downloading Page

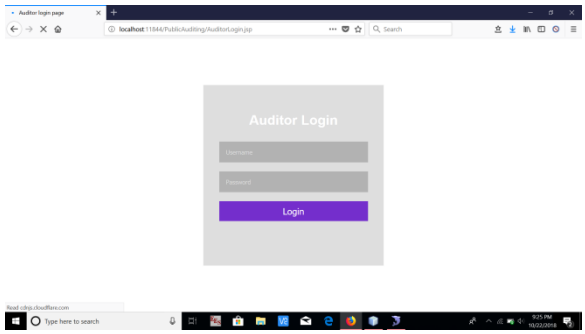

Fig.16. Auditor login page to check the file

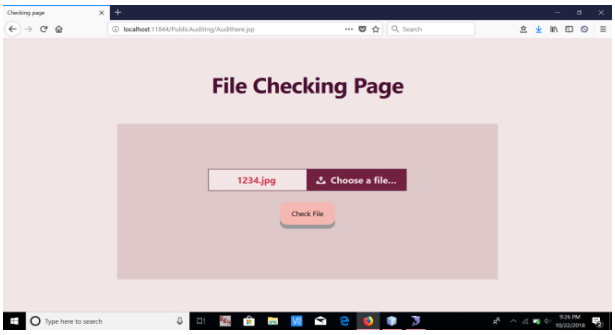

Fig.17. File checking page

Fig.18. File completely ok

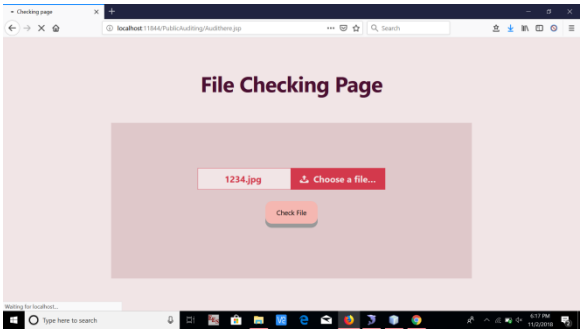

Fig.19. File checking page because it is corrupted are not checking

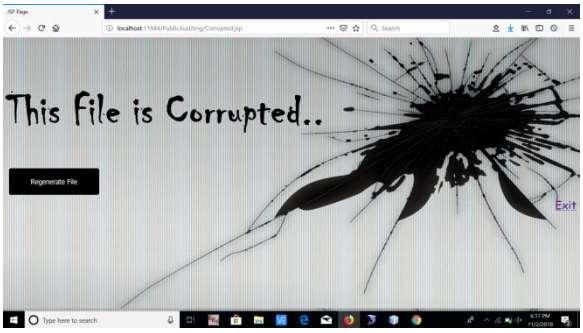

Fig.20. File is Corrupted

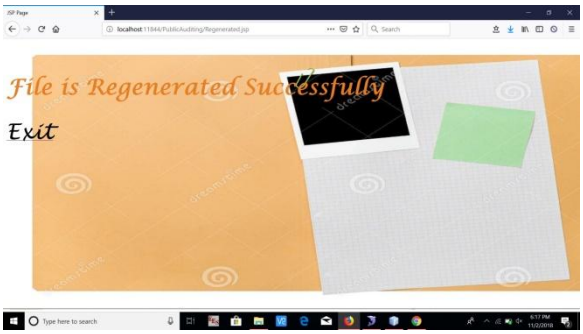

Fig.21. File is Regenerated Sucessfully

V. CONCLUSION

We propose a unique privacy-preserving mechanism, which supports anunrestricted reviewing on shared data stored in the cloud that is sensitive information that cannot retrieved by the others.The users can efficiently store their data in the cloud.The clients can effectively store their information in the cloud. The records which are put away in the cloud can be gotten to by other relying on the prerequisite that the delicate data of the document is ensured. By utilization of the homomorphism token with different verification of deletion coded information, our framework achieves the mix of capacity rightness of information detection in the localization. The storage of data in the cloud might be corrupted or lost due to the unavoidable software bugs, hardware errors and human errors in the cloud. So, as to confirm whether the information is put away effectively in the cloud, numerous remote information respectability examining procedures have been done to store the information in cloud. The proposed plan accomplishes the security and more efficiency.

VI. FUTURE SCOPE

The re-computation introduced by dynamic groups while still preserving identity privacy from the public verifier during the process of public auditing on shared data. To improve the efficiently of verifying multiple auditing tasks, we future extend this mechanism to support batch auditing.

REFERENCES

1. C.Wang “Privacy preserving public auditing for secure cloud storage,” IEEE Transactions on Computer, vol. 62,no. 2,pp. 362-375, 2013.
2. B.Wang “Panda: Public auditing for shared data with efficient user revocation in the cloud,” IEEE Transactions on Services Computing, Jan.-Feb, 2015.
3. Y.Zhang “Supporting efficient user revocation in identity-based cloud storage auditing for shared big data”, IEEE Transactions, 2018.
4. GailJoonAhn “Dynamic Audit Services for Outsourced Storages in Cloud, IEEE Transactions on Service Computing, April-June, 2013.
5. Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,IEEE infocom, C.Wang, 2010.
6. Certificate less Public Auditing for Data Integrity in the Cloud”, IEEE Conf. Comm. and Network Security, B.Wang, 2013.
7. Towards Secure and Dependable Storage Services in Cloud Computing,IEEE Transactions on Services Computing,W.Lou, 2011.
8. Proxy Provable Data Possession in Public Clouds, IEEE Transactions, Accepted, H.Wang, 2013.
9. Security challenges for the public cloud, IEEE Internet Computing, K.Ren, Jan 2012.
10. Identity-based remote data integrity checking with perfect data privacy preserving for cloud storage, IEEE Transactions on Information Forensics and Security,G.Ateniese April 2017.
11. Incentive and unconditionally anonymous Identity-Based Public Provable Data Possession, IEEE Transactions, H.Wang, 2016.
12. M.Ramesh Kumar, Ravi Kumar Tenali ,Dr.C Hari Kishan, BBVSVP, “Secured Data sharing in Cloud Using Single Key Based Decryption Method,” in Journal of Advanced Resear ch in Dynamical & Control Systems-JARDCS, 2018, vol. 10, pp. 1777-1782.
13. M Spandana, RK Tenali, KN Kumar, K Raju, “Coronary Illness Syndrome Identification System Using Data Mining Methods” in Journal of Advanced Research in Dynamical & Control Systems-JARDCS, 2018, vol. 10, pp. 1584-1590.
14. Ravi Kumar Tenali , M.Ramesh Kumar, M.Spandana, PSSR “Storage and Retrieval of Secure information in the Cloud Systems” in Journal of Advanced Research in Dynamical & Control Systems-JARDCS, 2018, vol. 10, pp. 773-778.
15. [15] A. Ajay Kumar, Tenali Ravi Kumar, TBAR “Human resource management leave and tour management data retrieval system” in International Journal of Engineering & Technology-IJET(UAE), 2018, vol. 07, pp. 186-188
16. [16]“Clinical Document architecture (CDA) Development and Assimilation for Health Information Exchange Based on Cloud Computing System”MM Aradhana, C Nagamani, RK Tenali ,International Journal of Computer Trends & Technology - IJCTT 4 (Special Issue)
17. [17]”Hash Method Elimination Of Data Duplication In Storage Clouds Using Contents Based”DKKK Tenali Ravi Kumar, M.Ramesh Kumar, T. SrinivasaRao International Journal of Pure and Applied Mathematics-IJPAM 117 (17), 109-11

AUTHOPROFILE

N.V.T.Bhuvaneswari, Department of ECM, IV/IV B.Tech, in Koneru Lakshmaiah Education Foundation,Vaddeswaram, AP, India.

M.TrinathBasu,working as Asst.Professor in the Department of Electronics and Computer Engineering and pursuing Ph.D fromKoneru Lakshmaiah Education Foundation, Vaddeswaram, AP in the area of Cloud computing .Completed M.TECH from Vardhaman College of Engineering and B.TECH from ST.Marys College of Engineering. Having a teaching experience of 6 years published 9 Scopus papers.

M.SriSathvik, Department of ECM, IV/IV B.Tech in Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.