International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 04 | Apr 2023 www.irjet.net p-ISSN: 2395-0072

A SECURED AUDITING PROTOCOL FOR TRANSFERRING DATA AND PROTECTED DISTRIBUTED STORAGE WITH SOCIAL MEDIA

M. Anitha[1] , P. Abirama Sundari[2] , Samuel Solomon[3] , S. Aswath Naraayanan[4]

[3&4] UG Scholar, Department of Computer Science and Engineering
[1&2] Assistant Professor, Department of Computer Science and Engineering
[1234] Prince Dr. K. Vasudevan College of Engineering and Technology, Chennai, TamilNadu, India

---

Abstract – There are numerous ways to handle a company's data. Everything of the company's data, including its transactions, history, and auditing procedures, must be handled correctly. To manage these things effectively, a different database needs to be built. To access the database information for that database, we require distinct connectivity and accessibility tools. Also, the database needs to keep each person's data separately.

***Key Words*: Cloud, Database, Data, Big data, Transactions, Managing and Auditing data, Social Media**

1.INTRODUCTION

A possible alternative is to encrypt your whole file prior sending it to the cloud. It creates the signatures needed to confirm this encrypted file's integrity. Lastly, submit the cloud with the encrypted file and accompanying signatures. With this technique, confidential information can be hidden such that only the file's owner can decode it. All users who share data with the data owner have read-only access to it, and the data owner holds the secret key that allows for data modification. Permission to read and write is granted. Auditing of public integrity is the algorithm employed. Hardware and software malfunctions, or the service provider receives information about an external hostile attack. The file owner just needs to keep a limited handful of the outsourced file's attributes and the secret key. PDP algorithm is employed (Provable Data Possession). File owner, proxy, auditor, register, and storage server are examples of used entities. The registration is in charge of setting up the client register and the system. Anti-malware technologies may be very effective in detecting malware. Just 20% to 30% of the 10,000 evolving malware variants were detected. Modularized attack features are loaded using approaches in dynamic code generation. Most malware from our generation may be detectable. The client may at any time update his private key. Make the client transparent to enable a key update. More storage is needed, and the key is secure.

Cloud provider and consumer typically sign a service level agreement (SLA).

A variety of security measures to verify the availability and integrity of data that has been outsourced. The client to a third party we'll refer to as the verifier. The majority of solutions only allow client read-only applications since they assume that only the original data owner has the right to modify shared data. For clients who are spread out, cloud storage systems offer convenient file storage and sharing options. According to testing results and security analyses, it offers robust security with desirable efficiency. The detection rates of the current AMTs for the 10,000 evolving malware variants are only 20%–30%. A significant problem for comprehensive cyber defence in security applications is key-exposure resistance. For the client, the key modifications are as visible as feasible. A brand-new paradigm termed cloud storage auditing is proposed. Key updates can be trustworthily delegated to a qualified party. This will minimise the client's key-update burden.

2. EXISTING SYSTEM

Hardware issues could result in the loss of cloud data. The delicate information shouldn't be made public. If a hacker has altered a file, it can only be recovered. More content, including images, is posted on OSN. phoney social network profiles are challenging to spot. There are no restrictions on sharing co-photos. Users are encouraged to post co-photos and tags on services like Facebook and more people sharing photos online.

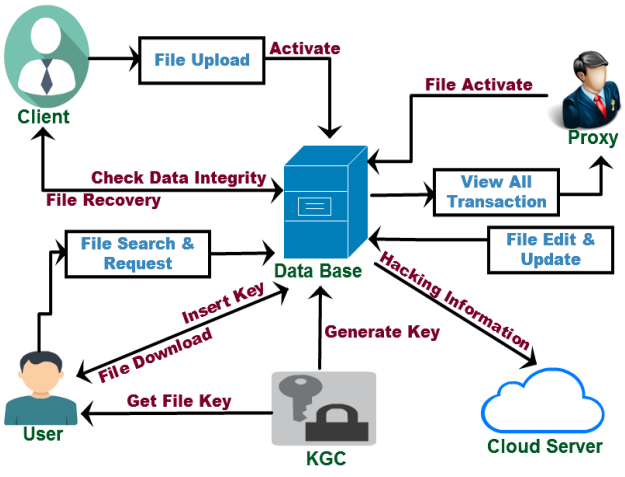

Fig -1: Existing System

3. DISADVANTAGES OF EXISTING SYSTEM

Posting a coworker's photo without consent is a privacy infringement. Co-owners need some degree of control over shared photos. Both the shared users and the cloud are unreliable. Users must shoulder a significant burden to keep the data locally due to the data's rapid increase. The sharing of data cannot be supported by remote data integrity auditing techniques. It is incompatible with multi-user modification. Process can only be read by users. It was still able to upload the corrupted file. Access is simple for hackers. When signals are hacked, the user cannot receive them. Because there is no security, a hacker can quickly access the data. It cannot be kept in the file and shared anonymously. It offers high computational expense. Using malware samples from the GENOME collection of Android malware, a malware meta-model for modularizing typical attack activities in brief strategies for evasion in reusable features. Minimal time complexity, stateless verification, unrestricted query use, and data retrievability are some further drawbacks. entrusted data to store financial information and storage space for backup procedures.

4. PROPOSED SYSTEM

In the future, remote data integrity auditing will be used to ensure data integrity. Some popular cloud storage solutions have cloud files with sensitive data in them. Find out how to share data while masking sensitive information. Every user record kept in the database is verified by the administrator. Users can match their profiles and learn about their matches' likes and dislikes before submitting requests. Before joining, users have the option to accept or reject the group before it is formed. Detects a false profile by looking at the activity of the postings. Before posting any pictures, get the user's approval. Our plan enables sharing and use of the cloud-based file as a result. It is necessary to use the commercial public cloud as a reliable backend datacenter in order to manage the exponential growth of images involved in social discovery.

We provide a safe and effective indexing structure to facilitate quick and scalable similarity search over hundreds of thousands of encrypted photos.

ConSecIdx –contains secret key and image profile set to secure the profile.

PrimaryInsert-contains profile identifier and user metadata.

RandomProbe-contains profile identifier,user metadata and random probe range.

The suggested model can correctly predict more than 80% of friends under the strongest social tie strength, according to the results.

The proposed approach is effective in terms of privacy preservation, communication cost, flexibility, and scalability, according to performance analysis and evaluation. This algorithm can more accurately identify influential users.

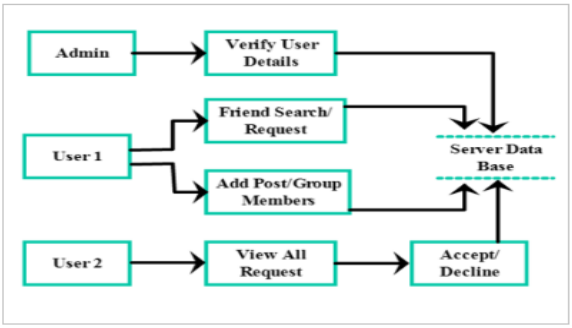

Fig -2: Proposed System DFA diagram

5. MODULE DESCRIPTION

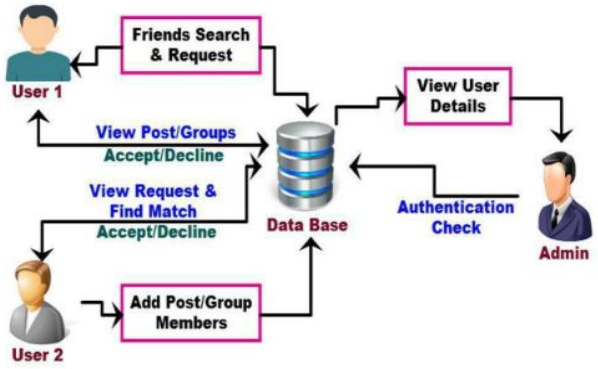

Fig -3: Proposed System

ENROLLMENT

After enrolling, the user has to enter a valid user name, email address, and password in order to access their account.

If credentials are valid, the system will allow access to the websites; otherwise, it will generate a user name or user account alert.

REFORM THE ACCOUNT

The user's profile must be updated after logging in because it serves as the foundation for all subsequent system functions.

Users can add more information throughout the updating process, including their interests, educational background, the name of their college, and so forth.

When you select your profile picture and then click Update, the server will be updated.

ITINEARY ADD

People publish content to express their emotions to others (i.e., share among friends).

You will be notified of any posts that contain your own profile's tagging if this happens.

Before the user accepts or rejects the post, no one will see it.

COMPANION APPEAL

The user types certain strings into the search bar and then requests the server using those strings.

When a user submits this kind of a request, the server automatically examines the likelihood of a response before responding to the user.

Responses only give the names of the individuals and no further details.

The user can submit a friend request to any individual on the list if they desire to be friends.

CONTOUR PAIRED

When a user submits a request, the server runs this module.

The server first retrieves the other user's name and profile information from the database before collecting the requested user's profile information.

Server uses a profile matching algorithm to match both profiles using the five parameters that are given.

Users that receive requests view the request information using a single value generated based on the matching of five parameters, and they may then choose whether to accept or reject the request.

PROTECTED CONTOUR

Users have the option of uploading images to serve as their profile pictures, which are visible to the public and allow for friend-to-friend communication.

When a profile image is updated by another user, the original user is notified.

Images can only be viewed with the user's consent; otherwise, the administrator may ban the user.

ASSOCIATION OPERATIONS

Users have the option of creating groups to share information with certain users.

You were added by the group administrator with the consent of each person.

Each person will receive informed of that group's participation.

If the user agrees to the request, they can join that group.

6. RESULTS AND DISCUSSIONS

Test	Requirements or Purpose	Test data	Expected result	Actual result	P/F
1	Data Owner Registration.	Username, password, email-id, captcha.	Getting registered into the server	Same as expected	Pass
2	Data user Login.	Username, password.	Getting logged into the server	Same as expected	Pass
3	File upload and file sending.	Select the File from cloud storage.	Upload the file & Send to destination	Same as expected	Pass
4	File uploading is complete.	Server sleep mode is activate.	Server goes to sleep mode	Same as expected	Pass
5	Server sleep mode activate.	Mail will be send in server admin.	Mail received server	Same as expected	Pass
6	Download the original file.	To click the download button.	Download the file from cloud server	Same as expected	Pass

Table -1: TEST RESULTS

7. CONCLUSIONS

The ability to effectively conduct the distant information honesty examination is still present.

The proposed plot's security evidence shows that security and productivity are achieved. The proposed system reduced the complications of implementing the older database design to access the data. Thus, the newer design provides flexibility of accessing social media in an effective manner.

8. FUTURE ENHANCEMENT

By adding a proxy component to verify for integrity, this can be accomplished.

The fact that the data owner does not need to remain for integrity verification is an extra benefit.

Face detection is based on the training of a classifier utilising a large number of negative photos that indicate features or items that should not be detected as well as a big number of positive images that represent the object to be recognised.

To assess the face feature, the region of the image with the highest likelihood of the feature is regionalized.

As it eliminates false positives, which decreases the area that needs to be checked, the speed of detection is boosted.

REFERENCES

[1] I. Altman. Privacy regulation: Culturally universal or culturally Specific Journal of Social Issues, 33(3):66–84, 1977.

[2] A. Besmer and H. Richter Lipford. Moving beyond untagging: photo privacy in a tagged world. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, pages 1563–1572, New York, NY, USA, 2010. ACM.

[3] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein. Distributed optimization and statistical learning via the alternating direction method of multipliers. Found. Trends Mach. Learn., 3(1):1–122, Jan. 2011.

[4] B. Carminati, E. Ferrari, and A. Perego. Rule-based access control for social networks. In R. Meersman, Z. Tari, and P. Herrero, editors, On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops, volume 4278 of Lecture Notes in Computer Science, pages 1734–1744. Springer Berlin Heidelberg, 2006.

[5] J. Y. Choi, W. De Neve, K. Plataniotis, and Y.-M. Ro. Collaborative face recognition for improved face annotation in personal photo collections shared on online social networks. Multimedia, IEEE Transactions on, 13(1):14–28, 2011.

[6] K. Choi, H. Byun, and K.-A. Toh. A collaborative face recognition framework on a social network platform. In Automatic Face Gesture Recognition, 2008. FG '08. 8th IEEE International Conference on, pages 1–6, 2008.

[7] Z. Stone, T. Zickler, and T. Darrell. Toward large-scale face recognition using social network context. Proceedings of the IEEE, 98(8):1408–1415.

[8] Z. Stone, T. Zickler, and T. Darrell. Autotagging facebook: Social network context improves photo annotation. In Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on, pages 1–8. IEEE, 2008

[9] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69–73, Jan 2012.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.

[11] A. Juels and B. S. Kaliski, "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 584–597.

[12] H. Shacham and B. Waters, "Compact proofs of retrievability," J. Cryptology, vol. 26, no. 3, pp. 442–483, Jul. 2013.

[13] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, 2013.

[14]S.G.Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," Comput. Electr. Eng., vol. 40, no. 5, pp. 1703–1713, Jul. 2014.

[15] C. Guan, K. Ren, F. Zhang, F. Kerschbaum, and J. Yu, "Symmetric-key based proofs of retrievability supporting public verification," in Computer Security – ESORICS 2015. Cham: Springer International Publishing, 2015, pp. 203–223.

[16] W. Shen, J. Yu, H. Xia, H. Zhang, X. Lu, and R. Hao, "Light-weight and privacy- preserving secure cloud auditing scheme for group users via the third party medium," Journal of Network and Computer Applications, vol. 82, pp. 56–64, 2017.

[17] J. Sun and Y. Fang, "Cross-domain data sharing in distributed electronic health record systems," IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 6, pp. 754–764, June 2010.

[18] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th international conference on Security and privacy in communication netowrks, 2008, pp. 1–10.