ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Secured study Using Efficient Data Storage Techniques with Digital Forensics and Decoy Technology for Multi Owner, Dynamic Groups in the Cloud

J Sridhar*, M Sriram, KP Thooyamani,
Department of CSE, Bharath University, Chennai, Tamilnadu, India.
***Corresponding author: E-mail: sridhar.cse@bharathuniv.ac.in**

ABSTRACT

The expansion in plenitude of malevolent programming has turned out to be high need dangers to the PCs and system security. By and large the likelihood of maintaining a strategic distance from information hacking in the cloud environment by unapproved clients is an awesome test. Once imparted the login accreditations along to space to the part, the proprietor will screen the part's entrance to cloud environment. The programmers has the shot of accessing the cloud environment utilizing the part's login qualifications and can transfer/download the information put away in nature. Likewise while downloading/transferring, there is a probability of hacking the efforts to establish safety, for example, private and open keys. To conquer this, the part's IP Address can be checked by the gathering proprietor on the designated distributed storage. As a piece of efforts to establish safety, methods, for example, Digital Forensics and Decoy Technology can be utilized wherein Digital crime scene investigation will screen the client's conduct and if there is any infringement confronted amid this procedure, Decoy innovation will come into picture which will convey bogus data of documents. Likewise two extra strategies, for example, Digital Signature Algorithm and Advanced Encryption Standard for transferring and downloading the document in the cloud environment were utilize

KEY WORDS: Data Storage, Forensics, Cloud.

1. INTRODUCTION

Distributed computing is approved as a distinct option for conventional data innovation because of its characteristic asset sharing and low-upkeep highlights. In distributed storage registering, the cloud administration suppliers (CSPs) like Amazon can convey different administrations to cloud clients with the assistance of intense server farms. By movement of the neighborhood information administration frameworks into cloud servers, bunch individuals can appreciate the advantages of value administrations and save huge ventures on their nearby bases. A standout amongst the most essential administrations gave by cloud is information stockpiling. In an organization that permits its gathering individuals in the same gathering or division to store and share documents in the cloud. By using it, they can be totally discharged from the troublesome neighborhood information stockpiling and support. In addition there is a shot of noteworthy danger to the privacy of put away information records. Particularly, the cloud servers oversaw by cloud administration suppliers are not completely trusted by clients while the information records put away in the cloud environment may be delicate and classified like business and account arranges. To secure information protection against malignant malware, a fundamental arrangement is to scramble information records and transfer the encoded information into the distributed storage server. Additionally outlining a proficient and powerful secure information sharing for gathering individuals in the cloud environment is not a simple undertaking because of the accompanying high need testing issues.

To begin with, character security is one of the significant vital hindrances for the wide arrangement of distributed computing. Without this protection, clients may be unwilling to join in distributed computing frameworks environment in light of the fact that because of the reason that their genuine personalities could be effectively uncovered to cloud suppliers and programmers. For our better comprehension, a gathering part who acts up can bamboozle different individuals in the organization by sharing false records without being traceable. Traceability empowers the gathering proprietor to uncover the genuine character of a client, which is likewise very vital.

Second, it is profoundly prescribed that any part in a gathering ought to have the capacity to completely appreciate the information putting away and sharing administrations gave by the cloud otherwise called multi-proprietor. All the more correctly, every client in the gathering will have the capacity to peruse the information, as well as alter his/her a player in information in the whole information document shared by the organization.

Typically aggregate individuals are powerful by and by, for example, new gathering part support and current gathering part denial in an organization. The progressions of gathering participation make secure information sharing to a great degree monotonous. In such manner, the unknown framework gives opportunities to the new allowed bunch part to take in the substance of information records put away before their cooperation as it is troublesome for new conceded bunch part to keep contact with mysterious information proprietors and get the related decoding keys. On the other section, an effective gathering part renouncement system without overhauling the mystery keys of the remaining gathering individuals is additionally sought to diminish the unpredictability of key administration angles.

A few security plans for information sharing on untrusted servers have been presented. Amid this

proposition, bunch proprietors store the encoded information records in untrusted stockpiling and convey the relating decoding keys just to approved clients. Likewise strategies, for example, Digital Forensics and Decoy Technology can be utilized wherein Digital legal sciences will screen the client's conduct and if there is any infringement confronted amid this system, Decoy innovation will get empowered and will convey bogus data of records. In this way, unapproved clients and also stockpiling servers can't take in the substance of the information documents on the grounds that they have no learning on the decoding keys.

On the other hand, the complexities of client support and disavowal in these plans are straightly expanding with the quantity of information proprietors and the quantity of repudiated gathering individuals, separately. By setting a gathering with a solitary trait, proposed a protected provenance plan in light of the figure content approach characteristic based encryption method, which permits any part in a gathering to impart information documents to others. Besides, aggregate part disavowal issues are not tended to. Presented a versatile and fine-grained information access control plan in distributed computing in view of the key arrangement characteristic based encryption (KP-ABE) method. In any case, the single proprietor way frustrates the reception of their plan where any gathering part is allowed to store and share information.

To comprehend the difficulties introduced above, we propose Monitoring of IP location, Digital Forensics and Decoy Technology, a safe multi-proprietor information security plan for element bunches in the cloud. The real commitment in this paper incorporates:

We propose a plan, for example, Monitoring of IP location by the gathering proprietor to check whether the apportioned distributed storage is being utilized by the unapproved clients to guarantee security.

Our proposed plan can bolster dynamic gatherings productively by utilizing procedures, for example, Digital Forensics which includes procedure of planning, obtaining, safeguarding, looking at, examining and reporting of client conduct. In the event that there is any infringement in the client conduct, it will limit the client in getting to the cloud environment.

We give secured access control to clients through Decoy Technology which maintains a strategic distance from insider assaults by raising security examination and shares false data to unapproved clients recognized by utilizing Digital Forensics.

We apply the efforts to establish safety like Digital Signature Algorithm for Signature era and check, Advanced Encryption Standard for encoding and decoding of records to guarantee security

The rest of this paper is sorted out as takes after: Section 2 depicts the Related Work. Area 3 audits the Cryptographic Primitives. Segment 4 clarifies the Proposed System Model and Design Goals. Segment 5 clarifies the Proposed Scheme in point of interest. Segment 6 portray Conclusion of the paper and displayed the Future Enhancement in Section 7.

System Model: Give us a chance to consider a distributed computing building design with a case that an organization utilizes distributed storage to empower its staffs in the same gathering or division to share documents. The framework model comprises of five unique substances: the Cloud, a Group Owner, an expansive number of gathering individuals, Digital Forensics and Decoy Technology as showed in Fig. 1.

Cloud is worked by Cloud Service Providers and gives gigantic capacity administrations. Despite the fact that the cloud is not completely trusted by clients since the Cloud Service Providers are liable to be outside of the cloud clients trusted environment, the cloud server won't noxiously erase or change client information, however will attempt to take in the substance of the put away information and the physical access of the cloud environment clients.

Bunch proprietor assumes responsibility of client enrolment, client repudiation and client get to be specific login qualifications and so forth. The gathering proprietor goes about as the head who screens the client exercises and is trusted other than the cloud clients.

Bunch individuals are called as the approved clients who store their private information records into the cloud environment and offer them with other gathering individuals. It is to be brought up that the gathering enrolment access will get powerfully changed because of gathering part renunciation and new part enlistment.

Computerized legal sciences is an arrangement of exploratory methods used to group, perceive, gather, dissect and assess the information while keeping up the trustworthiness of the data all through the procedure which acts in enhancing the lawful proof found in distributed storage environment.

Bait Technology is utilized to identify the malevolent action by the programmers by initiating so as to observe client activities check capacity. This check capacity is all that much in charge of separating the bait records and ordinary reports. On the off chance that discovered any indistinguishable nature, caution will get activated.

Design Goals: In this area, we have clarified the primary outline objectives of the proposed plan which covers access control, information classification, namelessness and traceability, productivity.

Access control: The prerequisite of access control is bi-fold. To begin with gathering individuals can utilize the cloud asset for their operations of information documents. Most essential is that unapproved clients can't get to

the cloud asset whenever, and denied clients will have the capacity of utilizing the cloud again even they are as of now renounced.

Data confidentiality: It is highly essential that unauthorized users including the cloud are incapable of learning the content of the stored data. A challenging issue is to maintain its availability for dynamic groups. Also new users should decrypt the data stored in the cloud before their participation and revoked users were unable to decrypt the data moved into the cloud even after doing the revocation.

Anonymity and traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity. Even though it means an effective protection for user identity, it might create a potential risk to the system. Thus, to tackle the inside attack, the group owner should have the ability to reveal the real identities of data owners in order to have a clear traceability.

Efficiency: This can be defined as any group member can store and share data files with others in the group by the cloud. Group member revocation can be achieved without involving the remaining users as they need not update their private keys or perform re-encryption. New granted users can learn all the content data files stored before his participation without contacting with the group owner.

Cryptographic primitives:

Digital Signature Algorithm: The Digital Signature Algorithm (DSA) is one of the digital signatures which are a pair of large numbers represented in a program as strings of binary digits. The digital signature algorithm is computed using a set of rules and parameters such that the identity of the digital signatory and integrity of the user data can be verified. The Digital Signature Algorithm (DSA) also provides the capability to generate and verify digital signatures. Signature generation makes usage of a private key in generating a digital signature. Signature verification makes usage of a public key which is different as the private key. Each group member has a combination pair of private and public keys. Private keys are never shared to any members. Anybody can verify the signature of a member by employing the user's public key. Digital signature generation can only be performed by using the user's private key.

Advanced Encryption Standard: Advanced Encryption Standard (AES) is a block cipher with a block length of 128 bits. Advanced Encryption Standard (AES) also allows for three different key lengths: 128, 192, or 256 bits. Except for the last round, all other rounds are similar and identical. There are four steps used in each round of Advanced Encryption Standard (AES): (1) Substitution, (2) Shift rows, (3) Mix columns, and (4) Add round key. The order in which these four steps are executed will differ for encryption and decryption.

For Encryption, each round consists of the following four steps: 1) Substitute bytes 2) Shift rows 3) Mix columns 4) Add round key. The last step consists of XORing where the output of the previous three steps with four words from the key schedule.

For Decryption, each round consists of the following four steps: 1) Inverse shift rows 2) Inverse substitute bytes 3) Add round key 4) Inverse mix columns. The third step consists of XORing where the output of the previous two steps with four words from the key schedule. The order in which substitution and shifting operations are carried out in a decryption round the order while similar operations are being carried out in an encryption round.

Proposed work: The main aim of the project is to identify the unauthorized users in the cloud storage. In this we are using three approaches for secure analysis like monitor the IP address, Digital Forensics, Decoy Technology and two techniques for uploading and downloading the file such as Digital Signature Algorithm for signature generation and verification, Advanced Encryption Standard for encrypting and decrypting of files.

The proposed system is an effective one for securing the cloud storage and retrieval of data from unauthorized users and attackers. The techniques such as Digital Forensics involve process of preparing, acquisition, preserving, examining, analyzing and reporting of user behavior. Decoy Technology involves avoiding insider attacks by providing some security questions and provides false information to overcome hacking. Monitoring the IP address involves avoiding the other member access the cloud in unauthorized way by disclosing ID from the current member.

2. CONCLUSION

In this paper a simple yet effective scheme to identify misbehaving users who hack the data or cloud storage have been proposed. Especially, efficient user revocation can be achieved through revocation list and new users can directly decrypt files stored in the cloud before their participation. Malicious attackers or malware can be detected by Decoy Technology which involves avoiding insider attacks by providing some security questions and shares false information to overcome hacking. To preserve the integrity of digital evidence, static, live extract and deleted data from various source documents through user’s behavior through

Digital Forensics. By performing the high priority security analysis on project support new user joining and reduce the storage overhead through efficient user revocation by applying techniques such as Monitoring of IP address, Digital Forensics and Decoy Technology, satisfaction of the desired security requirements has been met and also guarantees cloud storage overheads in a better manner.

Future enhancement: As per the discussion done above which is basically on the security measures taken for identifying the unauthorized users using digital forensics and decoy technology by embedding them into cloud storage environment. In future, these security techniques will provide us a better solution in order to have a secured network with impossibility of hacking. There should be some better ways for security by migration of cloud computing services. Flat Corporate Network and social engineering path may be one of the future enhancements in the cloud security computing.

In this project we can identify unauthorized users using Digital Forensics and Decoy Technology. In future by using advanced techniques before entering into the cloud environment and also using advanced security algorithms after enter in to the cloud storage. And our project can be enhanced using monitoring the IP address and between with IP & without TP, before DF, DT & after DF, DT efficiency can also be done.

REFERENCES

Armbrust M, Fox A, Griffith R, Joseph AD, Katz RH, Konwinski A, Lee G, Patterson DA, A sight of Cloud Computing, Comm. ACM, 53 (4), 2010, 50-58.

Ateniese G, Fu K, Green M, Improved Proxy ReEncryption Schemes with Applications to Secure Distributed Storage, Proc. Network and Distributed Systems Security Symp. (NDSS), 2005, 29-43.

Boneh and Franklin M, Identity-Based Encryption from the Weil Pairing, Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), 2001, 213-229.

BrinthaRajakumari S, Nalini C, An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, 7, 44-46, 2014.

Goh E, Shacham H, Modadugu N, and Boneh D, Sirius: Securing Remote Untrusted Storage, Proc. ``Network and Distributed Systems Security Symp. (NDSS), 2003, 131-145.

Jayalakshmi V, Gunasekar NO, Implementation of discrete PWM control scheme on Dynamic Voltage Restorer for the mitigation of voltage sag /swell, 2013 International Conference on Energy Efficient Technologies for Sustainability, ICEETS 2013, 1036-1040.

Kaliyamurthie K.P, Udayakumar R, Parameswari D, Mugunthan S.N, Highly secured online voting system over network, Indian Journal of Science and Technology, 6 (6), 2013, 4831-4836.

Kaliyamurthie KP, Parameswari D, Udayakumar R, QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, 6 (5), 2013, 4648-4652.

Kallahalla M, Riedel E, Swaminathan R, Wang Q, and Fu K, Plutus: Scalable Secure File Sharing on Untrusted Storage, Proc. USENIX Conf. File and Storage Technologies, 2003, 29-42.

Kamara S and Lauter K, Cryptographic Cloud Storage, Proc. Int'l Conf. Financial Cryptography and Data Security (FC), 2000, 136-149.

Khanaa V, Thooyamani K.P, Saravanan T, Simulation of an all optical full adder using optical switch, Indian Journal of Science and Technology, 6 (6), 2013, 4733-4736.

Khanaa V, Thooyamani KP, Using triangular shaped stepped impedance resonators design of compact microstrip quad-band, Middle - East Journal of Scientific Research, 18 (12), 2013, 1842-1844.

Kumaravel A, Dutta P, Application of Pca for context selection for collaborative filtering, Middle - East Journal of Scientific Research, 20 (1), 2014, 88-93.

Lu R, Lin X, Liang X, and Shen X, Secure Provenance, The Essential of Bread and Butter of Data Forensics in Cloud Computing, Proc. ACM Symp. Information, Computer and Comm. Security, 2010, 282-292.

Naor M Naor, and Lotspiech JB, Revocation and Tracing Schemes for Stateless Receivers, Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), 2001, 41- 62.

Raj M.S, Saravanan T, Srinivasan V, A modified direct torque control of induction motor using space vector modulation technique, Middle - East Journal of Scientific Research, 20 (11), 2014, 1572-1574.

Saravanan T, Raj MS, Gopalakrishnan K, VLSI based 1-D ICT processor for image coding, Middle - East Journal of Scientific Research, 20 (11), 2014, 1511-1516.

Sengottuvel P, Satishkumar S, Dinakaran D, Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling, Procedia Engineering, 64, 2013, 1069-1078.

Sundararajan M, Optical instrument for correlative analysis of human ECG and breathing signal, International Journal of Biomedical Engineering and Technology, 6 (4), 2011, 350-362.

Thamotharan C, Prabhakar S, Vanangamudi S, Anbazhagan R, Anti-lock braking system in two wheelers, Middle - East Journal of Scientific Research, 20(12), 2014, 2274-2278.

Udayakumar R, Khanaa V, Saravanan T, Saritha G, Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, 16 (12), 2013, 1781-1785.

Vanangamudi S, Prabhakar S, Thamotharan C, Anbazhagan R, Design and fabrication of dual clutch, Middle - East Journal of Scientific Research, 20 (12), 2014, 1816-1818.

Vanangamudi S, Prabhakar S, Thamotharan C, Anbazhagan R, Design and calculation with fabrication of an aero hydraulwicclutch, Middle - East Journal of Scientific Research, 20 (12), 2014, 1796-1798.

Waters, Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization, Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, 2008.

Yu S, Wang C, Ren K, and Lou W, Achieving Secure, Scalable, and Fine-Grained Data Access power in Cloud Computing, Proc. IEEE INFOCOM, 2010, 534-542.