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

Mobile large data storage security in cloud computing environment-a new approach

N. Priya*, J. Sridhar, M. Sriram
Department of computer Science engineering, Bharath University, Chennai, India.
***Corresponding author: E-Mail: msr1sriram@gmail.com**

ABSTRACT

Data security in cloud computing is considered as the difficult task. Above all else, the definitions, model, structure, application, research association and related learning of cloud computing is presented. At that point, the information security confirmation routines which utilized as a part of this proposal including symmetric and deviated encryption framework, characteristic based encryption calculation and Merkle Hash Tree are discussed. The security challenge, advantage, defensive measures and security structural engineering of information security situated in cloud computing environment are condensed with numerous distributed computing attributes, for example, monstrous, virtualization, motion and expansibility.

KEY WORDS: Cloud computing, data security, mobile large data, information flow control, trusted cloud computing.

1. INTRODUCTION

Cloud computing provides a large number of IT resources such as hardware and software as a service to users through the network. In cloud computing service model, users host data and application to the cloud, due to the cloud service transparency, they lose control of the data. Because it is difficult to assess cloud provider's credibility for users, data security has become the primary concern in cloud computing.

Since cloud computing does related operations of user demand, confirmation in the middle of clients and cloud suppliers can maintain a strategic distance from illegal access from accepted personality. Because of the expansive number of clients, how to acknowledge the verification to the sympathy toward and clients and administration suppliers. Having been verified, clients can utilize the information stockpiling commission computing administrations. Clients transfer a lot of information to the cloud and cloud administration suppliers to compute without the nearby duplicate put away. In spite of the fact that the cloud administration supplier is with solid specialized quality and upkeep, it is unrealistic to totally forestall information harm or spillage happens. For static stockpiling of information, because of the mass of information, it is no more appropriate to check uprightness subsequent to downloading information to neighborhood in conventional way. In the event that clients discover information uprightness is traded off, they can just supplicate the cloud administration supplier's fiasco recuperation component works. In light of the attributes of multi-occupant in the cloud, client's entrance information and register through the administration process for element information in computing benefit, the procedure transporter of shared access get to be point of convergence of power. But it is hard to accomplish powerful confinement and control of distinctive clients' information by shared consents on OS level, information segregation component of utilization exclusively is effortlessly skirted, so information secrecy and respectability in multi-occupant environment stay to be determined. On the off chance that the information exposure truly happens, it is a key issue to charge administration suppliers' obligation. Current responsibility components need points of interest of cloud administrations, which are identified with cloud administration suppliers' competitive advantages, therefore it is hard to accomplish. Moreover, because of the absence of trusted assurance component, security instrument may be assaulted, altered or circumvent, in like manner it falls flat. The essence of the cloud information security issue is the trust administration between information proprietor and service provider, certain information limitations ought to be framed between them. They accomplish certain information use understanding through notoriety and specialized method for limitation, the legitimate use of data and prevent from destroying.

Users can depend on service provider side by coming to a commonly tasteful security component to amplify wellbeing and security, service providers won't have a spot to live in once he lost validity. In this setting, cloud service providers are willing to participate with users to take information security insurance innovation, and never do deliberate annihilation of client information, however they might conceal information wellbeing mishap. Starting here of perspective, the postulation concentrates on the validation, static memory information insurance, dynamic calculation data security and trusted cloud computing, and so on are considered, to give far reaching information security assurance to cloud users.

Technology of data security: To clear data storage security issues of the cloud computing, we analyze data integrity and data privacy protection in this paper.

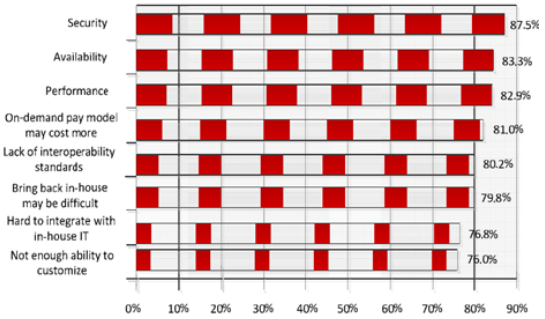

Figure.1. The key problem of user attention

According to the key problem of user attention (Fig.1), we can obtain that users are mostly focus on data security. In the side of data integrity protection, we proposed the algorithm of proofs of irretrievability: M-POR which based on the message authentication code(MAC) with the purpose of making the user learn the data state in the cloud, algorithm generates sentinels through MAC and verify the data integrity through the process of "challenge-respond-verify". Sentinels not only can verify the data integrity but also can position the error message. We also bring in RS code so that we can recovery data when the proportion of damaged data is not large and take into account of redundant replica of cloud computing. In the side of data privacy protection, aiming at the privacy of text data, we proposed the MC-R strategy. MC consists of three modules: data masking, data concealing and data marker. MC prevents data leakage when data is uploading or downing through masking and concealing data in the client, R enciphers data with the computing advantage of cloud computing in the cloud using the public key uploading from the client.

Key technology: Research on the key technology of secure cloud data storage auditing scheme, i.e data aggregate signature algorithm. After analysis of existing works, we come with a new identity-based aggregate signature scheme, where each user keeps less number of private keys and the computational complexity. Furthermore, we propose a new efficient identity-based aggregate signature scheme with both advantages of batch-verification signature and aggregate signature. It could offer large scale of data verification in the multi-user setting with high efficiency. In particular, this scheme is quite suitable for data verification in multi-user and multi-cloud settings of cloud computing.

On this basis, according to the data storage's dynamic operation characteristics and less of verification support in cloud computing environment, the thesis has put forward a scheme which is based on the Merkle Hash Tree structure. The main ideas and safe assumption of the scheme are introduced. Also the pretreatment and validation method of the file and data dynamic operation process including insertion, modification and deletion are described. The scheme is data file's proposed access control problem analyzed as well. In addition, due to solving the cloud computing environment, the thesis has a solution which is based on attribute-based encryption algorithm and introduced the main ideas and safe assumption of the scheme. The participants and related definitions are described. The thesis has designed initialization of scheme, file access and the change of access permission in details. Finally, the scheme is also analyzed.

Data storage strategy: Here, we put forward three kinds of mobile storage model. Mobile data management architecture based on mobile database (MDMA, Mobile Data Management Architecture) and storage management solution (SMS, Storage Management Solution) (Fig. 2) are proposed. Mobile database is the most efficient mode for mobile distributed environment data organization and storage, which will provide data foundation of mobile business operations, because mobile applications are implemented based on mobile databases. Aiming at the characteristics of mobile environment, mobile data management architecture and storage management solution are proposed, and the pre-fetch and replication, cache synchronization, transaction process, concurrence control, broadcast mechanism and other key technologies are discussed. These will provide available and conventional runtime methods for the data storage and management under mobile environment

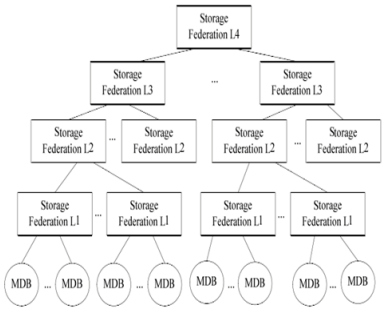

Figure.2.SMS A model of hieratical storage system based on wireless mesh network is proposed

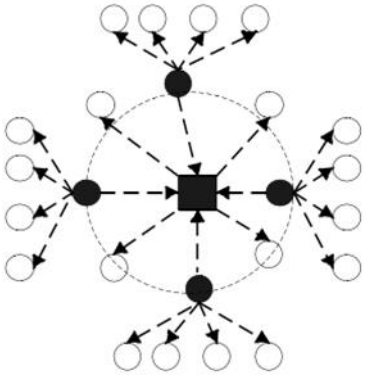

Figure.3.Wireless mesh network architecture unit

Firstly, the dissertation proposes the hierarchical storage system model based on wireless mesh network (HSSWMN), and the storage model, access algorithms and performance optimization methods are analyzed and researched. Secondly, name space and metadata service, search and looking for service, registration and logout, scalability, load balance, fault tolerant, data safety, replication and cache mechanism, topology reconstruction of HSSWMN are researched. At last, by the simulation analysis, simulation testing discloses that the delay, throughput, error code and etc., performance analysis is carried for the feasibility, availability and reliability of HSSWMN storage system.

A QoS cross layer model of storage service of mobile environment oriented (QCLMSS, QoS Cross Layer Model of Storage Services) (Fig. 4), and QoS guarantee algorithm of storage service (QASS, QoS Guarantee Algorithms of Storage Service) are proposed. The dissertation first does research on the QoS technologies of mobile environment storage service, analyzes the properties and relations between layers. Secondly, the QoS guarantee algorithms and performance model are proposed, and researches are done on QoS guarantee algorithms. At last, Global optimization, local optimization, mluti-state optimization, and self-adaptive optimization algorithms are proposed, and analysis and comparation of the mobile storage system QoS examples are analyzed, simulation test and analysis research is taken on disk I/O performance of wired network and wireless network access mode.

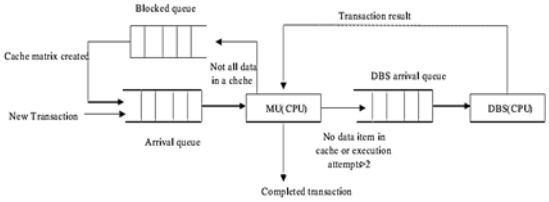

Fig.4. HSSWSN

2. CONCLUSION

Mainly, this paper focuses on the current research of cloud storage security. The technical aspects of the security concern are confidentiality, integrity, availability, monitoring and audit. In this paper, current research on cloud storage security is summarized and introduced according to the security properties above. Then, this paper introduces a file-share method to solve the data storage problem. The method focuses on the confidentiality, integrity and key distribution and sharing problem.

REFERENCES

Achudhan M, Prem Jayakumar M, Mathematical modeling and control of an electrically-heated catalyst, International Journal of Applied Engineering Research, 9 (23), 2014, 23013.

Almorsy M, Grun J and Ibrahim AS, Collaboration-Based Cloud Computing Security Management Framework, 2011 IEEE 4thInternational Conference on Cloud Computing, 2011, 364-371.

Delettre C, Boudaoud K. and Riveill M. Cloud Computing, Security and Data Concealment.International Conference on Information Science and Cloud Computing, 2011, 424-431.

Frank Gens, Rebert Mahowald, Richard Villars L, Cloud computing 2010 An IDC Update, IDC Executive Telebriefingp, 2009, 09.

Gopalakrishnan K, Sundeep Aanand J, Udayakumar R, Electrical properties of doped azopolyester, Middle - East Journal of Scientific Research, 20 (11), 2014, 1402-1412.

Gopinath S, Sundararaj M, Elangovan S, Rathakrishnan E, Mixing characteristics of elliptical and rectangular subsonic jets with swirling co-flow, International Journal of Turbo and Jet Engines, 32 (1), 2015, 73-83.

Ilayaraja K, Ambica A, Spatial distribution of groundwater quality between injambakkam-thiruvanmyiur areas, south east coast of India, Nature Environment and Pollution Technology, 14 (4), 2015, 771-776.

Kerana Hanirex D, Kaliyamurthie KP, Kumaravel A, Analysis of improved tdtr algorithm for mining frequent itemsets using dengue virus type 1 dataset: A combined approach, International Journal of Pharma and Bio Sciences, 6 (2), 2015, 288-295.

Lingeswaran K, Prasad Karamcheti SS, Gopikrishnan M, Ramu G, Preparation and characterization of chemical bath deposited cds thin film for solar cell, Middle - East Journal of Scientific Research, 20 (7), 2014, 812-814.

Premkumar, S., Ramu, G., Gunasekaran, S., Baskar, D., Solar industrial process heating associated with thermal energy storage for feed water heating, Middle - East Journal of Scientific Research, 20 (11), 2014, 1686-1688.

Shulman-Peleg A, Harnik D, Pinkas B, Side Channels in Cloud Services Deduplication in Cloud Storage. IEEE Security and Privacy Magazine, pedal issue of Cloud Security, 8 (6), 2010, 40-47.

Sundar Raj M, Saravanan T, Srinivasan V, Design of silicon-carbide based cascaded multilevel inverter, Middle - East Journal of Scientific Research, 20 (12), 2014, 1785-1791.

Thooyamani KP, Khanaa V, Udayakumar R, Partial encryption and partial inference control based disclosure in effective cost cloud, Middle - East Journal of Scientific Research, 20 (12), 2014, 2456-2459.

Thooyamani KP, Khanaa V, Udayakumar R, Application of pattern recognition for farsi license plate recognition, Middle - East Journal of Scientific Research, 18 (12), 2013, 1768-1774.

Thooyamani KP, Khanaa V, Udayakumar R, Efficiently measuring denial of service attacks using appropriate metrics, Middle - East Journal of Scientific Research, 20 (12), 2014, 2464-2470.

Thooyamani KP, Khanaa V, Udayakumar R, Using integrated circuits with low power multi bit flip-flops in different approch, Middle - East Journal of Scientific Research, 20 (12), 2014, 2586-2593.

Thooyamani KP, Khanaa V, Udayakumar R, Virtual instrumentation based process of agriculture by automation, Middle - East Journal of Scientific Research, 20 (12), 2014, 2604-2612.

Thooyamani KP, Khanaa V, Udayakumar R, Wide area wireless networks-IETF, Middle - East Journal of Scientific Research, 20 (12), 2014, 2042-2046.

Udayakumar R, Kaliyamurthie KP, Khanaa, Thooyamani KP, Data mining a boon: Predictive system for university topper women in academia, World Applied Sciences Journal, 29 (14), 2014, 86-90.

Yang J S and Choi H K, IP Based Security Architecture of Virtual Network in Cloud ComputingSystem. Wireless Communications and Mobile Computing Conference, 2012, 709-715.