Science and Technology Publishing (SCI & TECH)
ISSN: 2632-1017
Vol. 3 Issue 7, July - 2019

Third Party Auditing System Of Cloud Computing

Mst. Jahanara Akhtar
Associate Professor
Department of Computer Science & Engineering,
Dhaka International University
Dhaka, Bangladesh
jahanara.cse@diu-bd.net

Md. Habibullah Belali
Assistant Professor
Department of Computer Science & Engineering,
Dhaka International University
Dhaka, Bangladesh
jahanara.cse@diu-bd.net

Md. Tahzib-Ul-Islam
Assistant Professor
Department of Computer Science & Engineering,
Dhaka International University
Dhaka, Bangladesh
tahzib.cse@diu-bd.net

Saiful Islam
Department of Computer Science & Engineering,
Dhaka University of Engineering and Technology
Gazipur, Bangladesh
saiful.buet@yahoo.com

***Abstract*— A huge number of data storage and computing facilities is proving in cloud computing system. Great volume number of peoples are involving to get better service in this system. Enterprises also offering various services with great facilities in cloud computing. But always a fair from security aspect both users and vendors as well as cloud providers. The data archives can be accessed by unauthorized users or hackers in the unsecured cloud network. This main in leaky of intimate data or data loss during the broadcast over the network. Hence securing the cloud plays a very important role in cloud environment. To ensure better security, a third party auditing system is proposed in this paper. Auditor will audit or inspect at runtime and offtime service. This effort, effective auditor will play a vital role in securing the cloud environment.**

Keywords*— *Cloud Computing, Auditing, online audit, offline audit

I. INTRODUCTION

About every people who are using the advanced technology in now in the world, they are making use of cloud systems from the inside or outwardly. This is valued as the development in storage technology against cloud systems. Most of the cryptographic techniques are suggested for performing security a great deal of stronger way. Therefore, people from various area of specialization particularly for business in companies are trusting on cloud. The data of client in cloud servers are unbroken hidden as well as secret which fence the secrecy of consumer and their data all over the cloud. Cloud computing has get more and more up to date in the recent years. As the resources are comely active, saved and virtualized, the data has to be more saved in cloud. Beside this, auditing is taking more attending for increased complexness of cloud resources for the researchers now. The auditing system makes potent and share with others of data easier in cloud [1].

Different cloud computing types involved Public, Private, Hybrid and Community based clouds used for different intention globally. The security and secrecy care happen due to transfer of data and uses on network resources and different security policies. Data stored, blowing and monitor of data external the handles of an organization affection an integral endanger and making it vulnerable to different attacks. Privacy preserving is an essential issue in business because the consumer who is accessing the cloud files may alteration the collection of the real file which may run to original effect in future. Therefore, security is the largest care when it comes to cloud computing environment. The chief contest here is to deal with the protection and secrecy part of business thinking of adopting it. Hacking the cloud systems and network infrastructure would impact many business customers so that their benefit which seriously need to be thought [2].

Data Auditability has been intentional for cloud storage and effective storage auditing rule has been suggested in this work. The suggested protocol uses active action with data unity and multiple group auditing procedure. This work adds new cryptologic technique for encrypting and decrypting the data files in multi cloud environment.

In section 2, we have talk about the existent work related to cloud protection. In section 3, system plan is discussed along with overall cloud scheme architecture. Section 4 gives the suggested solution for protecting the cloud. Section 5 focuses on results. Section 6 gives the conclusion to the work.

II. LITERATURE REVIEW

Various auditing model has been designed for cloud store house systems. Secrecy preserving storage auditing strategy has been granted for securing the cloud systems. The cloud computing security auditing scheme includes customers auditing

demand, current cloud facility supplier capacity for meeting auditing demand and technical attack for data security auditing. Two issues of particular auditing procedure add infrastructure security and data security auditing. The substructure auditing demand achieve IT security [3]. The public auditing scheme of data storage security in cloud supplier's secrecy saving auditing protocol. The scheme has outside auditor to audit outsourced data in cloud. The chief goal is to accomplished privacy preserving public auditing scheme for cloud data storage. The public audibleness permits TPA to check rightness of cloud data no doubt downloading data [4]. Privacy saving public auditability method is focused using TPA that in turn verify the unity of cloud data. The TPA insured cloud data without requesting copy of data and that as well the auditability content does not bring any exposure for customer's data files. TPA is used to check unity of user's information and privacy is secrecy saved as TPA does not have any knowledge all most user's data [5]. RSA based storage security (RSASS) strategy uses populace auditing of distant data for furnishing security. It is a public key cryptography strategy which usage data storage rightness and upkeep active operations on data and cut down server calculation. RSASS system bring forth signature using RSA algorithm that assist big and various size of files [6]. The public auditing strategy of data storage security suggested rule for fully active data action of block interpolation. It assists scalable and effective public auditing exploitation homomorphic authenticator's strategy in cloud computing. The scheme also attains group auditing for multiple works from various users by TPA. The rule is applied using Merkle Hash Tree (MHT) which is used for authentication of data files which assist both public auditability and data active operations [7]. Some other work assist remote unity checking strategy, effective and secure cloud storage scheme. The active privacy-preserving audit facility is used for conformation unity of outsourced storage. It attains considered together public auditability and active data action all over the cloud. The secrecy savings public auditing scheme is used to continuously public auditing on cloud information [8].

III. ROLE OF THIRD PARTY SERVICE PROVIDER IN AUDITING

In the surge of rapid utilization of internet all over the world, various security contents are implicated such as handling web attacks, data access control, enhancing dynamic allocation strategies, and controlling sensitive information flow. According to Information Systems Control and Audit, IT auditing can be outlined as a procedure of accumulation and evaluating reflect to judge whether a computation information system danger free resources, maintains data unity and secure sensible user data, attains organizational documentary effectively and consumes forcible and calcluting resources efficiently. Information authority controls in Governing documents such as DoDI 8500.2, NIST SP800-53 or Common Criteria have backing inspecting by dictating minimal requirements for audit regarding the case that assures right access control like authoriy, authentication and auditing to the forcible and practical resources used at public cloud supplier. It is also essential to assure the accessibility of the Internet-facing resources in a populace cloud being used by the organization. At the recipient grade of security, virtualization security menaces like system constellation change, imperfect access control of the hypervisor, faulty.

IV. PROPOSED PROTOCOL

Proposed framework mainly divided into three parts. 1) Cloud Users and Vendors 2) Auditor and 3) Cloud environment.

Cloud Users and Vendors: Cloud users are those persons or organizations or parties who want to get services or use services and applications or want to use cloud storages. Vendors are those parties who want to uses various applications or storages of cloud and using those applications or storages, they may deliver some services to other people or users.

Auditor: auditor means those party who will apply some rules and regulation to users or vendor and cloud environment to ensure secure communication among them. Commonly they apply various rules and regulation, such as strategy rules query access and query rules, audit trails, audit alerts and audit rules.

Cloud Environment: Cloud environment or site is the actual storage where all files and services resides. It contains various policies, database, access rules and regulation etc.

In this framework, tasks of auditor are divided into two parts i.e., runtime and off-time auditing. Runtime audit will be occurred when any users or vendors will initiate their services or uses of services. The framework is shown in Fig. 1. Let one user are entering in the cloud to get some services. Auditor will check his credential at runtime and apply some rules on the users. If the user passes through those rules and regulation, then he will enter into cloud. Moreover, auditor will observe all the step of the user and record of steps. Auditor will apply all access control rules to this user. Like this, auditor will apply all applicable rules and regulations to all users and vendors. For applying all rules and regulations, only valid users and vendors can enter into the cloud safely. Unauthorized users or vendors or intruders will not do any hamper of cloud. Off-time auditing will occur at idle time of users or vendors or cloud. Auditor will check users every steps from their logs. Auditor will check all history or log of users or vendors with applicable rules and regulations. If any doubt occurs, then auditor will inform immediately to the authority and set red alert to specific user or vendor. Auditor will also give suggestions to improve better services and security.

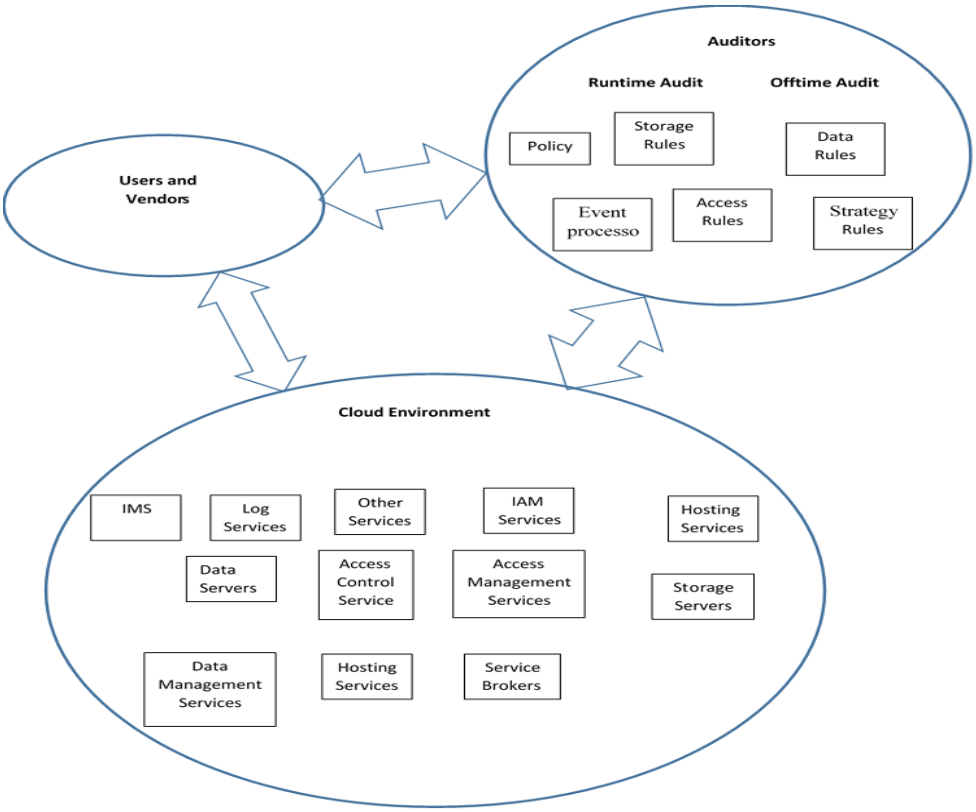

Figure-1. Third Party Auditing System

Auditor consists various modules such as various database, rules, managers, control modules etc. in database (DB) may contain policy DB. storage server, data server, log server contains storage and users or vendors log entry. Authentication and access management service contains all authentication and access rules and regulation. According to these service or rules and regulations, auditor control all authentication and accesses. Policy database stands the source of data security. Strategy rules describes the strategy idea for the execution of safety policy, asset management, communications and working management, data systems gaining & expansion & preservation, and business steadiness.

V. CONCLUSIONS

A third party public auditing system is displayed which delivers a privacy-preserving auditing procedure. The system supports a superior auditor to check the user's data with every steps logs in the clouds. So we have made an effort to validate the security of proposed system using the comparisons with the state-of-the art in cloud computing environment. The proposed system is also suitable for storage, processing, and retrieval of big data in a cloud environment.

REFERENCES

[1] M. Nazir, N. Bhardwaj, R.K. Chawda, R.G. Mishra, "Cloud computing: Reviews, Surveys, Tools, Techniques and Applications – An open-access ebook by HCTL open" ISBN-13(PDF): 978-1-62951-802-2.

[2] K. Ruth Ramya, T. Sasidhar, D. Naga Malleshwari & M.T.V.S. Rahul, "A review on security aspects of data storage in cloud computing", International Jounal of Applied Engineering Research, Vol 10, No 5, 2015. pp. 13383-13394.

[3] Hassan Rasheed, "Data and Infrastructure security auditing in cloud computing environments", International Journal of Information Management, 2014.pp. 364-368.

[4] C. Wang, Q. Wang, K. Ren and W. Lou, "Privacy preserving public auditing for data storage security in cloud computing", IEEE INFOCOM 2010, IEEE, 2010.

[5] Sonali. D. Thosar and Nalini.A. Mhetre, "Integrity checking privacy preserving approach to cloud using third party auditor", In proceedings of2015 International conference on pervasive computing (ICPC), IEEE 2015.

[6] M.Venkatesh, M.R. Sumalatha and C. Selvakumar, "Improving public Auditability, data

possession in data storage security for cloud computing", IEEE, 2012.pp. 463-467.

[7] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li, "Enabling public Auditability and data dynamics for storage security in cloud computing", IEEE TPDS, Vol.22, No.5, IEEE, 2011.pp. 847-859.

[8] A. R. Navajothi and S.J.A. Fenelon, "An efficient, dynamic, privacy preserving public auditing method on untrusted cloud storage", In proceedings of ICICES2014, IEEE, 2014.

[9] C.Wang, Q.Wang, K.Ren, N.Cao, W.Lou, "Towards secure and dependable storage services in cloud computing", IEEE, 2009. pp. 1-14.

[10] Sravan Kumar. R & Ashutosh Saxena, "Data Integrity proofs in cloud storage", IEEE, 2011.

[11] C.Wang & K.Ren, "Toward publicly auditable secure cloud data storage services", 2010, IEEE Network. pp. 19-24.

Authors

Mst. Jahanara Akhtar is now serving as an Associate Professor of the department of Computer Science and Engineering, Dhaka International University, Dhaka, Bangladesh. She is a Research Fellow (PhD) in the department of Computer Science and Engineering, Jahangirnagar University, Dhaka, Bangladesh. Jahanara completed B.Sc in Electronics & Computer Science and M.Sc. in Computer Science and Engineering from Jahangirnagar University. She has publications in national and international conference and journals. Her research interest includes Cryptography, Secure Wireless Sensor Network, Image Processing and Artificial Intelligence.

Md. Habibullah Belali is currently serving as an Asistant Professor of Computer Science and Engineering department, Dhaka International University, Dhaka, Bangladesh. Habibullah completed B.Sc. in Computer Science and Engineering from University of Dhaka. He has publications in national and international conference and journals. His research interest includes Image Processing, Data Mining and Advance Database.

Md. Tahzib-Ul-Islam is currently serving as an Assistant Professor of Computer Science and Engineering department, Dhaka International University, Dhaka, Bangladesh. He is a M.Sc. student in the Institute of Information and Technology, University of Dhaka, Dhaka, Bangladesh. Tahzib completed B.Sc in Computer Science and Engineering in Department of Computer Science and Engineering from University of Dhaka. He published research papers in national and international conference and journals. His research interest includes Cryptography, Network Security, Image Processing and Cloud Computing.

Saiful Islam is currently pursuing his Ph.D in Computer Science and Engineering degree in Dhaka University of Engineering and Technology (DUET), Gazipur, Bangladesh. Saiful completed B.Sc. in CSE and M.Sc. in EEE from Dhaka University of Engineering and Technology (DUET), Gazipur, Bangladesh. He also completed M.Sc. in ICT from Bangladesh University of Engineering and Technology (BUET), Bangladesh. He has publications in national and international conference and journals. His research interest includes Cryptography, Network Security, Wireless Sensor Networks, Cyber Physical System and Cloud Computing.