Volume 4, Issue 11, November 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Sophisticated Protocol Service to Enhance Security at Cloud Server Using Combinational RBAC & MAC Algorithm

Sukhvinder Kaur[1], Mandeep Kumar Kashyap[2], Ms. Jagdeep Kaur[3]

Research Scholar, Department of CSE, PTU, India

Assistant Professor &HOD(CSE), HPTU Hamirpur, KCIET, Pandoga Una (H.P.), India

Assistant Professor & HOD, (CSE\IT), KCCEIT SBS Nagar, India

Abstract -The Cloud has become a new vehicle for delivering resources such as computing and storage to customers on demand. Cloud computing, a new internet-based technology, has been widely envisioned as the most promising technology of IT enterprise. But, security becomes the major concern for both cloud service provider and the clients who are using the cloud Resources. This paper is focused on detecting and analyzing the Distributed Denial of Service (DDoS) attacks in cloud computing environments using the integrated RBAC methodology which would reduce the number of requests to the server. This work also proposes to integrate the third party auditor using a MAC algorithm. The implementation run and analysis shows that the proposed approach is highly efficient and secure under existing security models.

Keywords— Cloud computing, DDoS, RBAC, MAC, Third Party Auditor.

I. INTRODUCTION

Cloud computing can be defined as a new style of computing in which dynamically scalable and often virtualized resources are provided as a service over the Internet. Advantages of the cloud computing technology include cost savings, high availability, and easy scalability.

Infrastructure as a Service**:-**Offering virtualized resources (computation, storage, and communication) on demand is known as Infrastructure as a Service (IaaS). A cloud infrastructure enables on-demand provisioning of servers running several choices of operating systems and a customized software stack. Infrastructure services are considered to be the bottom layer of cloud computing systems [7].

Platform as a Service:- In addition to infrastructure-oriented clouds that provide raw computing and storage services, another approach is to offer a higher level of abstraction to make a cloud easily programmable, known as Platform as a Service (PaaS). A cloud platform offers an environment on which developers create and deploy applications and do not necessarily need to know how many processors or how much memory that applications will be using. In addition, multiple programming models and specialized services (e.g., data access, authentication, and payments) are offered as building blocks to new applications [7].

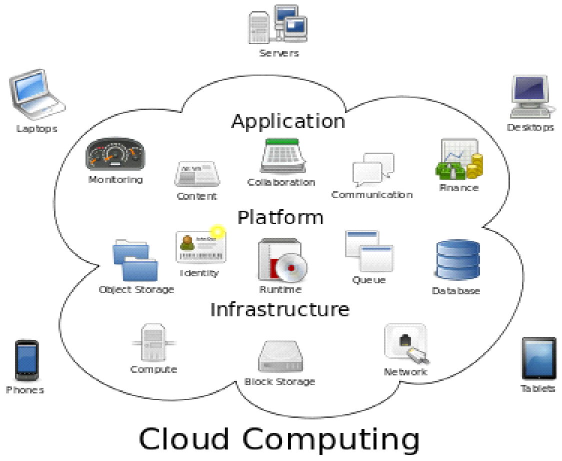

Fig. 1 Overview of Cloud Computing

Software as a Service: - Applications reside on the top of the cloud stack. Services provided by this layer can be accessed by end users through Web portals. Therefore, consumers are increasingly shifting from locally installed computer programs to on-line software services that offer the same functionally. Traditional desktop applications such as word processing and spreadsheet can now be accessed as a service in the Web. This model of delivering applications is known as Software as a Service [7].

II. MAC Algorithm

MAC (**message authentication code**) provides an efficient way to message authentication. It also separates the authentication function from confidentiality. This is an attractive feature for many applications (such as software package distribution) where confidentiality is not necessary. Encryption mechanism does not provide a good solution for message authentication is that it is difficult for the receiver to identify the legitimate plaintext. To address this problem, we can apply an error detection code to the message so that only legitimate plaintext can pass the error detection. Such error detection codes are used in the network communication to provide data integrity verification against bit errors introduced by communication channel noise. In light of error detection code, we can design a code that uses a secret key. Without the key, modifying the message in a way that it matches the code is impossible. This idea leads to the design of message authentication code (MAC) [6].

III. DDoS

DDoS attacks can be launched from either a single source or multiple sources. Multiple source DoS attacks are called distributed denial-of service (DDoS) attacks. DoS attacks do not wish to modify data or gain illegal access, but instead they target to crash the servers and whole networks, disrupting legitimate users' communication [16]. The most usual method of this attack is to transmit a mass saturation of incessant requests for external communication to the target. The target systems are flooded with requests from non-users, and often from non-visitors to the website. The goal of this attack is to create a heavy amount of false traffic such that legitimate web traffic intended for actual web users is delayed or slowed down. If the server becomes too slow, the live video (which carries time sensitive information) footage may be rendered entirely useless to legitimate end users.

IV. RBAC Mechanism

RBAC stands for role based access control. In this system there are roles and users are created according to the roles. Permission is applied to the role and they automatically get applied to every user related to the category.

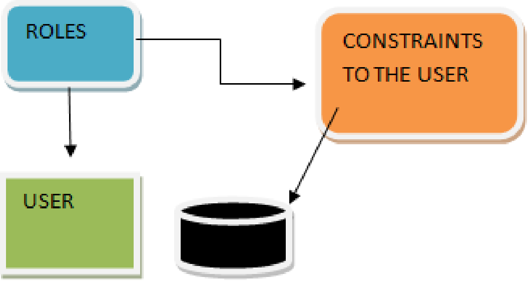

Fig. 2 Represents the flow diagram of the RBAC Mechanism

RBAC is a mechanism in which only those users can access the data that are authorized to it. This concept can relate to the server request sending mechanism. In such a mechanism only those users would be able to send a job or service request to the server who has the authority to send. [8]

V. Third Party Auditor

In this paper, we propose an effective and novel scheme about the third party auditor for cloud data storage. We succeed in moving the third party auditor function into the cloud service provider's architecture and make it trustful and security [13].

To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third-party auditor (TPA) to audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud.

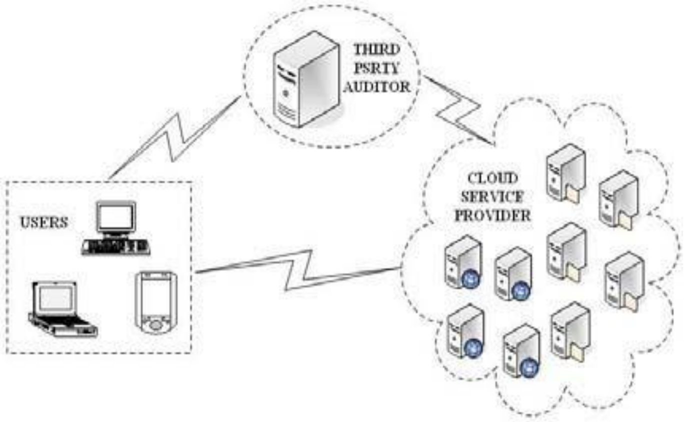

Fig. 3 The architecture of cloud data storage service

VI. OBJECTIVES

Objective of this research work is to enhance the security of the data using a third party integration algorithm in which the data to prevented using a MAC algorithm. MAC ALGORTIHM uses a special data set policy which takes the input as when so ever a data has been uploaded to the system and it changes to 1 if some un authenticated user tries to connect the data .The final data comparison would be done on the basis of the FRR and FAR rule base in which the FAR is the false acceptance rate and FRR is false rejection rate. The goal of this research work is to save the DDOS attack on the server using the above ontology

VII. METHODOLOGY

- To study and design a system with the integrated RBAC methodology which would reduce the number of requests to the server.
- To integrate the third party auditor to prevent the DATA Loss.
- To test the entire system over a cloud network (WINDOW'S AZURE – A Microsoft Cloud).
- The final data comparison would be done on the basis of the FRR and FAR rule base in which the FAR is the false acceptance rate and FRR is false rejection rate.

VIII. RELATED WORK

In our literature survey, we note that DDoS defense mechanisms are generally classified as preventive mechanisms and reactive Mechanisms. [7] This paper describes a generalized model of record sharing in cloud computing using attribute based encryption (ABE). This concept is implemented for financial organization. Therefore to adopt the hash based searching technique to retrieve the encrypted information in cloud. This work also proposes to integrate the third party application with financial organization. The implementation run and analysis shows that the proposed approach is highly efficient and secure under existing security models. The limitation of this paper is that it support only data integrity not data authorization.

[9]This paper works on conceptual cloud architecture by adopting an encryption algorithm with dynamic small size key to ensure the security and doesn't compromise any information with the cloud server. It involves a third party broker who encrypts the clients' information for ensuring the security, partitioned into multiple segments based on the remaining dynamic storage capacity presents in the VMs of cloud storage servers and store these encrypted segments of the clients' file on the corresponding VMs of the cloud storage providers. It then generate the hash value of the encrypted segments, store and manage these details for verification purpose. The performance measures like better encryption time and a quicker detection of compromise of the clients' files in cloud environment is possible with the proposed system.The major limitation is that it use RSA algorithm with small key size which is less secure.

[2]This paper describe,a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.It use Entropy based Anomaly Detection System in which number of routers are used which increased cost as well as traffic over the network.

[17]This paper present an approach for packet monitoring in Cloud Environment to prevent DDoS attacks. This new approach of Hop Count Filtering provides a network independent and readily available solution to prevent DoS attack in Cloud environment. Also, this method decreases the unavailability of cloud services to legitimate clients, reduces number of updates and saves computation time. The presented approach is simulated in CloudSim toolkit environment and corresponding results are then produced.It is limited to support the multiple users.

IX. CONCLUSIONS

In this paper we explained different existing techniques and their merits and demerits. We discussed their methods of data security and privacy etc. This work proposes to integrate the third party auditor using a MAC algorithm. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client. The third party is used to resolve any kind of conflicts between service provider and client. This paper also presents an analysis of the RBAC model and how it is helpful in preventing the DDOS mechanism.

REFERENCES

[1] A Corradi, R. Montanari, and D. Tibaldi " Context-based access control for ubiquitous service provisioning", *In Proc. of the 28th Annual International Computer Software and Applications Conference (COMPSAC'04), Hong Kong, China, IEEE,* pages 444–451 **September 2004**.

[2] Cong Wang, S.M. Chow, Qian Wang (2013) " Privacy-Preserving Public Auditing for Secure Cloud Storage", *IEEE TRANSACTIONS ON COMPUTERS, VOL. 62, NO. 2*,pp. 362-375, **February 2013**.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou "Towards Secure and Dependable Storage Services in Cloud Computing", *IEEE Trans. Service Computing, vol. 5, no. 2,* pp. 220-232 **June 2012.**

[4] E. E. Mon and T. T. Naing"The Privacy-aware Access Control System using Attributed-and Rolebased Access Control in Private Cloud", *Proceedings of the 4th IEEE International Conference on Broadband Network and Multimedia Technology*,pp. 447-451, **October 2011.**

[5] H. A. J. Narayanan and M. H. Gunes "Ensuring Access Control in Cloud Provisioned Health Care Systems",*Proceedings of the IEEE Consumer Communications and Networking Conference*,**2013**.

[6] Jueneman, R. R., Matyas, S. M., and Meyer, C. H.,"Message Authentication", *IEEE Communication, Vol 23, No. 9, pp 29-40.*

[7] K. Kanagasabapathi, S. Balaji " Secure Sharing Of Financial Records With Third Party Application Integration In Cloud Computing", *International Conference on Current Trends in Engineering and Technology, IEEE – 32107*,pp. 418-420, July 3, **2013**.

[8] Manpreet Kaur,Sahil Vashist" A Review Of The DOS-DDOS Attacks And Their Prevention Mechanisms In Cloud" *International Journal of Computer Application and Technology (IJCAT) Volume 1 Issue 1 (April 2014) ISSN: 2349-1841*

[9] P.Varalakshmi, Hamsavardhini Deventhiran "Integrity Checking for Cloud Environment Using Encryption Algorithm", *IEEE ISBN: 978-1-4673-1601, ICRTIT*, pp. 228-232, **2012**.

[10] Qian Wang, Cong Wang, Kui Ren" Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5*,pp. 847-859, **May 2011.**

[11] Santhosh K M and Elizabeth Isaac " Defending DDoS Attack using Stochastic Model based Puzzle Controller*", IJCSNS International Journal of Computer Science and Network Security*, VOL.13 No.4,pp. 100-105,**April 2013**.

[12] S. Sanka, C. Hota and M. Rajarajan"Secure Data Access in Cloud Computing", *Proceedings of the 4th IEEE International Conference on Internet Multimedia Services*, **December 2010.**

[13] Shuai Han, Jianchuan Xing " Ensuring Data Storage Security Through a Novel Third Party Auditor Scheme in Cloud Computing", *Proceedings of IEEE CCIS2011, 978-1-61284-204-2,* pp. 264-268, **2012**.

[14] S. Yu, C. Wang, K. Ren and W. Lou"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", *Proceedings of the 29th IEEE International Conference on Information Communication*, pp. 534-542,**2010**.

[15] Tamal Kanti Chakraborty, Anil Dhami, Prakhar Bansal and Tripti Singh"Enhanced Public Auditability & Secure Data Storage in Cloud Computing", *3rd IEEE International Advance Computing Conference (IACC), 978-1-4673-4529-3*,pp. 101-105,**2013**.

[16] Upma Goyal, Gayatri Bhatti and Sandeep Mehmi "A Dual Mechanism for defeating DDoS Attacks in Cloud Computing Model", *International Journal of Application or Innovation in Engineering & Management (IJAIEM),* Volume 2, Issue 3,pp. 34-39, **March 2013**.

[17] Vikas Chouhan & Sateesh Kumar Peddoju" Packet Monitoring Approach to Prevent DDoS Attack in Cloud Computing", *International Journal of Computer Science and Electrical Engineering (IJCSEE) ISSN No. 2315-4209, Vol-1 Iss-1*,pp.38-42,**2012**.