International Journal of Trendy Research in Engineering and Technology (IJTRET)
Volume 1 Issue 1 Aug- 2017

DATABASES USING MULTI-FACTOR AUTHENTICATION

Rajyashree. R
M.E student, Department of computer science, SVCE, Sriperumbudur, Chennai.-602 117, Tamil Nadu, India
ammukrishnan.r@gmail.com

Vaishnavi Moorthy
Assistant professor, Department of computer science engineering, Faculty of E&T, SRM University, Kattankulathur. 603203.. INDIA

Nedunchelian R
Professor , Department of computer science, SVCE, Sriperumbudur, Chennai.-602 117, Tamil Nadu, India
nedun@svce.ac.in

Abstract: **Cloud Computing is a model of service delivery and access where dynamically scalable and virtualized resources are provided as a service over the Internet. Secure environment is to be maintained to provide privacy and security of confidential information in a cloud environment. Authentication is a key technology for information security, which is a mechanism to establish proof of identities to get access of information in the system. Traditional password authentication does not provide enough security for information in cloud computing environment to the most modern means of attacks. A novel architecture that integrates cloud database services with data confidentiality and the possibility of executing concurrent operations on encrypted data is necessitated. In this paper, we propose a new multi-factor authentication framework for cloud computing. The proposed framework provides a feasible and a most efficient mechanism which can closely integrate with the traditional authentication system to ensure data confidentiality by encrypting the files before they are uploaded into the cloud drive. Random functions generated unique key that does not contain any data corresponding to the actual file data attributes used for decrypt the metadata and acquire information**

Keywords: cloud computing, security, multilevel authentication, unique client owned key.

I. INTRODUCTION

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. It is generating a lot of interest worldwide because of its lower total cost of ownership, scalability, competitive differentiation, reduced complexity for customers, and faster and easier acquisition of services[1-4].Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. In a cloud context, security and privacy are two major concern. In a cloud storage data is placed in a third party and controlled by service provider.

The security issues which include networks, databases, operating systems, virtualization, resource scheduling and allocation, transaction management, load balancing and memory management. The security issues and challenges associated in the cloud environment can be categorically referred in the different level namely (i) Network level include network protocols, security in distributed nodes, data (ii) Authentication level : encryption/decryption techniques, methods include authentication of distributed applications, access rights for nodes, logging (iii) Data level associated in the integrity of data, protection and distribution of data and finally (iv) generic level issues in the usage of different security tools and technologiesCloud provider ensure a security and allowing authorized user to assess the data, sometimes they may be lost/modified due to security breach.

Various cloud service providers adopt different technologies to safeguard the data stored in their cloud like usage of different encryption techniques such as: public key encryption and private key encryption as well encryption – decryption algorithm for secure data transfer, data can be broken into packets and then transferred through disjoint paths to the receiver etc.. The main issue with data-at-rest in the cloud is loss of control, even a non-authorized user/party may have access to the data (it is not supposed to access) in a shared environment . However, now-a-days, storage devices with in-built encryption techniques are available which are resilient to unauthorized access to certain extent. Even in such a case, nothing can be done in case the encryption and decryption keys are accessible to the malicious user. There are many existing technology such Cryptographic file systems, multi layer security, url security, account setting etc. [5-8].

Some of the existing architecture that are defines to preserve the confidentiality of data in the cloud include: Proxy based architecture (PSB) proxy server less architecture with distributed meta data (PSL-SM), proxy server less architecture with meta data in cloud database (PSL-CD) having their advantages and bottlenecks. The restricted access and single point of failure avoided in some extent while architecture of the type proxy-less database storing metadata in distributed cloud database. [9-12]

II. SECURE DBAAS

Secure DBaaS architectural design that allows the cloud tenants to take full advantage of DBaaS qualities exposing unencrypted data to the cloud provider. A

SecureDBaaS allow multiple and independent clients to connect directly to untrusted cloud, by managing encrypted database and metadata that prevents the violation of confidentiality by untrusted cloud provider. It is having advantages such as execution of concurrent and independent operations to the remote encrypted database from many geographically distributed clients including SQL statements so that database structure can be modified. It does not require any intermediate server but at the same time provides similar operation provided by DBaaS. Other proposals based on intermediate server(s) were considered impracticable for a cloud-based solution because any proxy represents a single point of failure and a system bottleneck that limits the main benefits (e.g., scalability, availability, and elasticity) of a database service deployed on a cloud platform. The limitation of this system is efficiency of data access and confidentiality. In other words, functions cannot be taking advantage of secret sharing outsourced to an untrusted cloud provider and it cannot store them in encrypted format. When considering scenarios like multiple clients that enabling concurrent access of the same database. Hence generic security framework is necessitated to work with any type of cloud environment that could block the threats originating from the internet and filter the data before they reach into the network.[13-15]. Original plain data must be accessible only by trusted parties that do not include cloud providers, intermediaries, and Internet.

III.PROPOSED SYSTEM ARCHITECTURE

The proposed architecture ensures data confidentiality by encrypting the files before they are uploaded into the cloud drive. The project implement code is using JAVA server page and Servlets and Java script by developing codes. [JSP, SERVLET), back end MY SQL 5.5 , Windows 07, IDE: Eclipse] It is helpful in estimating cost, planning team activities, performing tasks and tracking the teams and tracking the team's progress throughout the development activity. To accurately translate customer requirements into finished product we use case diagram, using system functions that are performed by actor and its roles are also depicted. In our used case diagram as shown in Fig 1., first user login into user window then if it is a valid user means then it can communicate with the cloud server.

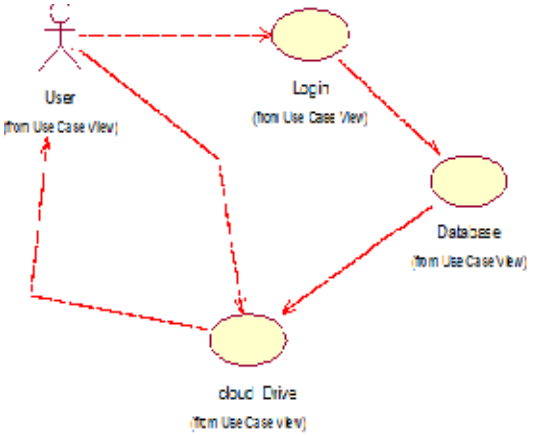

Fig 1. Case diagram

Recovery of available client data from the server is possible and in the case of unavailability, searching in the related clients that will be shared to the requester. Entity-relationship model is used to produce conceptual schema or semantic data in the server for effective processing and retrieving data to the requested client. Interface design focused here is login design with Partial knowledge information , so that login through user interface GUI, to connect user and media data base as well login screen in which user can input the details like name, password to check data base to access the data base and view the applications. User interface including data base structure, resource management with a software as service (SaaS) and information storage , metadata used in the study, schematically shown as system architecture in the Fig 2.

Authentication by user validation has been provided by a unique client owned key. A unique key which we refer as the master key is generated during the file encryption by a random method does not contain any data corresponding to the actual file data attributes. This method is more secure as it does not contain any data corresponding to the actual file data attributes. So no particular algorithm can be used to retrieve the key and the data corresponding with it as it is generated randomly. Here for security reason, client has to fill up the details through client login, entering id and password, with key code generated. Hence in this method only trusted clients that already know the master key can decrypt the metadata and acquire information that is necessary to encrypt and decrypt tenant data. The project can be enhanced to address more number of attacks through mobile phone to get hackers information and other real world requirements. The performance evaluation of the project can include some more metrics like speed of data flow from server to client, memory usage, network throughput etc also overhead of each node to access the data from server.[16-17]

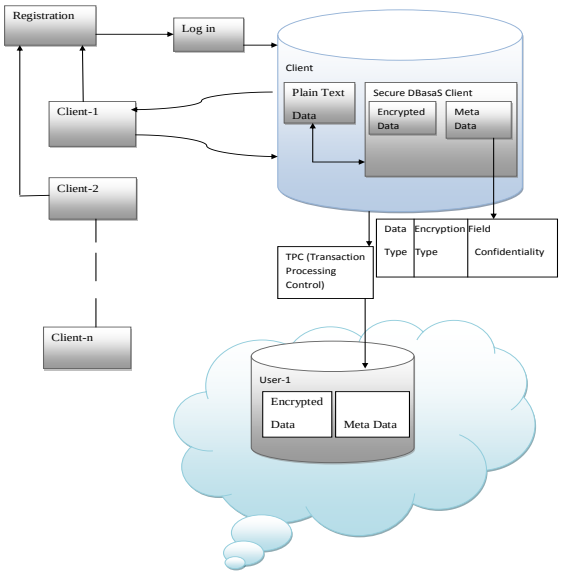

Fig 2. Safety key incorporated system architecture

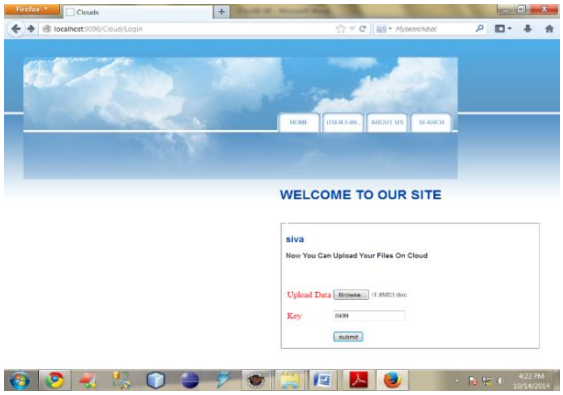

Fig 3. Screen shot showing the validation of the model .

Fig 4. Screen shot showing the validation of the model .

IV CONCLUSIONS

Cloud computing provides variety of Internet based on demand services like software, hardware, server, infrastructure and data storage. multifactor authentication with client owned master key provide privacy services to intended customer. Key generated does not include any file attributes without any algorithm for reconstruction of the key and hence it is more secure.

REFERENCES

[1]. L. Wang, Gregor Laszewski, Marcel Kunze, Jie Tao, "Cloud Computing: A Perspective Study", New Generation Computing- Advances of Distributed Information Processing, pp. 137-146, vol. 28, no. 2, 2008.

[2]. Michael Miller, "Cloud Computing, Web-Based Applications that change the way you work and collaborate online", Pearson, Eight Impression, 2013.

[3]. Qi Zhang, Lu Cheng, Raouf Boutaba, "Cloud Computing: State of the art and research challenges", Journal of Internet Services and Applications, , vol. 1, issue. 1,. pp. 7- 18 Feb, 2010.

[4] John W. Rittinghouse, James F. Ransome, "Cloud Computing Implementation, Management, and Security", CRC Press, August 17, 2009, ISBN 9781439806807, pp. 147-158, 183-212.

[5]. Atif Alamri, Wasai Shadab Ansari, Mohammad Mehedi Hassan, M.Shamim Hossain, Abdulhameed Alelaiwi, M.Anwar Hossain, "A Survey on SensorCloud: architecture, Applications, and Approaches, International Journal of Distributed Sensor Networks, pp 1-18 , 2013.

[6] H. Hacigm, B. Iyer, S. Mehrotra, "Providing Database as a Service", *Proc. 18th IEEE Int'l Conf. Data Eng.*, 2002.

[7] T. Mather, S. Kumaraswamy, and S. Latif, "Cloud security and privacy: an enterprise perspective on risks and compliance". O'Reilly Media Incorporated, 2009.

[8] "Amazon Web Services: Overview of Security Processes", Whitepaper, May, 2011. http://d36cz9buwru1tt.cloudfront.net/pdf/AWS_Security_Whitepaper.

[9] Muhammad Aamir, Xiang Hong,Muhammad Tahir,Atif Ali Wagan Cloud Computing and Associated Mitigation Techniques:A Security Perspective, journal of emerging trends and computing and information sciences , vol 5, pp 165-171, March 2014.

[10] A. Boldyreva, N. Chenette, and A. O'Neill, "Order-preserving encryption revisited: Improved security analysisand alternative solutions," in Proc. of the Advances in Cryptology – CRYPTO 2011, pp. 578–595. August 2011

[11]. W. Jansen, T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", 2011.

[12] A.J. Feldman, W.P. Zeller, M.J. Freedman, E.W. Felten, "SPORC: Group Collaboration Using Untrusted Cloud Resources", *Proc. Ninth USENIX Conf. Operating Systems Design and Implementation*, 2010-Oct.

[13]M. Hadavi, E. Damiani, R. Jalili, S. Cimato, Z. Ganjei, "AS5: A Secure Searchable Secret Sharing Scheme for Privacy Preserving Database Outsourcing", *Proc. Fifth Int'l Workshop Autonomous and Spontaneous Security*, 2013-Sept.

[14] V. Ganapathy, D. Thomas, T. Feder, H. Garcia-Molina, R. Motwani, "Distributing Data for Secure Database Services", *Proc. Fourth ACM Int'l Workshop Privacy and Anonymity in the Information Soc.*, 2011-, Mar.

[15]. J.Sasi Kiran , L.Sunitha , A. Venkata Mani Kumar , M.Naveen kumar, IJRETS, ICICSIT 2015 review on secured database as a service architecture to access encrypted cloud databases .

[16] Sumathi M , Sharvani G.S , Dinesha H A, " Implementation of Multifactor Authentication System for Accessing Cloud Service", International Journal of Scientific and Research Publications,pp. 1-8, Volume 3, Issue 6, June 2013.

[17]. Hyosik Ahn, Hyokyung Chang, Changbok Jang, and Euiin Choi, Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway ACN 2011, CCIS 199, pp. 132–138.