RESEARCH ARTICLE OPEN ACCESS

Cloud Computing Security Issues Problem and Strategy

Michael *, John Presto **
*(Chaudhari Technical Institute, MCA Department, Gujarat)

Abstract:

The fast developing computer technology has gone through the spectacular advances in computing Security processing and networking technology. Lot of users and research organizations are now using cloud-computing concepts for easy and efficient solutions to their computing and data sharing needs. In fact, the cloud computing Security problems/challenges with fundamental security issues such as data privacy. The implementation of cloud computing will help the universities by reducing the expenditure with decreasing their demand for software licensing and it has operational benefits. multi-layered security strategy can, however, help organizations address this security problem.

Keywords **—Cloud Computing Security , Public cloud, Data protection strategy**,

I. Introduction:

The universities all over the world are under increasing pressure to employ the Information Technology for the welfare of faculty members, students, operational staff and management. Developing a strategy for a problem like data privacy is to fully define and understand the problem itself. Cloud environment is comprised of software and hardware resources in the data centers that run different services over the internet or network to satisfy the user's needs and it depends on sharing resources instead of having local servers to handle application for a certain individual or organization. The numerous cloud enterprise system looks for these advantages to be used in various applications. The service of the cloud makes it possible to access the data at anytime from anywhere. Cloud computing utilize the networks of a huge group of servers naturally brings a low rate data processing with specialized connection.

It has a great impact on the development of IT by enhancing its existing capabilities and increasing flexibility. In the recent years, cloud computing has made significant

Changes in IT industry and has become a promising part of IT world. In fact, the cloud subscriber does not typically know the location of the data center and storage hardware, and/or what networks are transmitting the data. Perhaps most critically, cloud subscribers must recognize that moving into the cloud extends a great deal of trust and responsibility to the cloud provider.

II. Theoretical Concept of Cloud Computing:

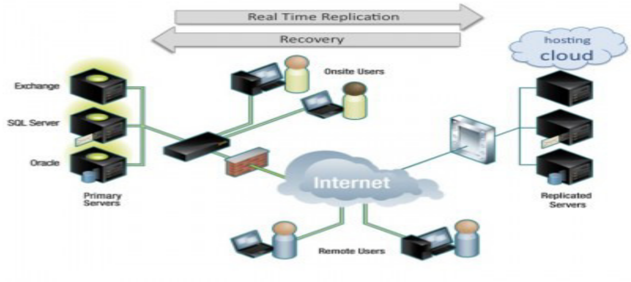
The cloud computing is considered as fifth generation of computing with reference to mainframe, personal computer, client server computing, and the web. In essence, cloud computing is a construct that allow you to access applications that actually reside at a location other than your computer or other Internet–connected device; most often, this will be a distant data centres.Cloud computing is a distributed computing environment that provides on demand services to the users for deploying their computational needs in a virtualized environment without the knowledge of technical infrastructure. Due to reliability, scalability, high performance and low band width most of the organizations are running their applications in cloud. The cloud service providers provide the services to the registered cloud users on payment basic across the glove.

III. Require user Permission for data Access control :

A role is a higher level representation of access control.In cases of Organization by means of user id fraud, a simple solution can be offered - user namely, requesting actual user permission for data access. As a cloud security check, the id must always detect when a user is attempting to access data. In every visit, the valid id should be verified of the access data request. A notification message can be sent to the data owner (valid user) via messaging system. The valid user can then either allow or invalid data access permission to the requesting party. Most importantly, researcher points out that this simple data security strategy is both cost effective and assures the data's data is always secure.

IV.Distributed Servers

The Client-server architecture is a way to provide a service from a central source. There is a single server that provides a service, and many clients that communicate with the server to consume its products. In this architecture, clients and servers have different jobs. The server's job is to respond to service requests from clients, while a client's job is to use the data provided in response in order to perform some tasks. Peer-to-Peer System: The term peer-to-peer is used to describe distributed systems in which labour is divided among all the components of the system. All the computers send and receive data, and they all contribute some processing power and memory to a distributed computation. As a distributed system increases in size, its capacity of computational resources increases.



1.The infrastructure models of clouds

V. Challenges of cloud computing:

The Hardware Layer

As more functionality moves to the internet cloud every provider and user is developing their own definition. Industry experts and researchers are struggling to formulate a standard set of terms to describe all the different functions. with three constituents to the cloud infrastructure layer. The figure represents the inter-dependency between the different layers in the cloud.

The Virtualization Layer

This layer is also known as the infrastructure layer. The virtualization layer is the result of various operating systems being installed as virtual machines. It is a very useful concept in context of cloud systems. It is the software implementation of a server to execute different programs like a real machine. The remote data center provides different services in a full or partial
virtualized manner.

Infrastructure as a service

The infrastructure layer builds on the virtualization layer by offering the virtual servers as a service to users. The clients are billed for these virtual servers but not for the actual hardware. This reduces the cost of unnecessary hardware procurement physical servers or data storage systems.

Platform as a service

This layer provides an operating system platform for hosting various applications. Platform as a service solutions are basically the development platforms for which the development tool itself is hosted in the Cloud through Infrastructure as a service and accessed through a browser. With Platform as a service**,** developers can build Web applications as per their native systems and to deploy those applications in the cloud virtualized server without any specialized systems administration skills.

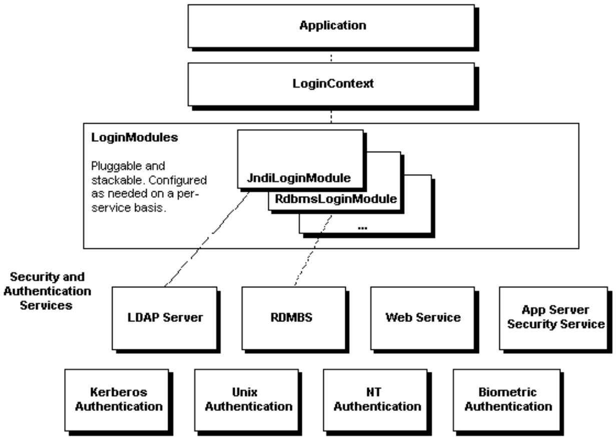
Software as a service

If the users do not want to develop the cloud application, the Software as a service layer is the solution. The users simply procure a service, such as email or CRM Billing can be based on utilization of these services. In this case, it is a simple way to get the application functionality that the users need without incurring the cost of developing that application.

VI.Authentication with identifier/password format :

In the single-server model, where a single server is involved and it keeps a database of user passwords. Most of the existing password systems follow this single-server model, but the single server results in a single point of vulnerability in terms of offline dictionary attacks against the user password database. The servers are equally exposed to users and a user has to communicate in parallel with several or all servers for authentication. The main problem with the plain multi-server model is the demand on communication bandwidth and the need for synchronization at the user side since a user has to engage in simultaneous communications with multiple servers. This may cause problems to resource-constrained mobile devices such as hand phones and PDAs.

A passive adversary follows honest but-curious behaviour, that is, it honestly executes the protocol according to the protocol specification and does not modify data, but it eavesdrops on communication channels, collects protocol transcripts and tries to derive user passwords from the transcripts, moreover, when an passive adversary controls a server, it knows all internal states of knowledge known to the server, including its private key (if any) and the shares of user passwords. In contrast, an active adversary can act arbitrarily in order to uncover user passwords. Besides, we assume a secret communication channel between SS and CS for this basic protocol.



VII. Security Visualization :

With two-server password system, single point of vulnerability, is totally eliminated. Without compromising both servers, no attacker can find user passwords through offline dictionary attacks. The control server being isolated from the public, the chance for it being attacked is substantially minimized, thereby increasing the security of the overall system. The system is also resilient to offline dictionary attacks by outside attackers. This allows users to use easy to remember passwords and still have strong authentication and key exchange. The system has no compatibility problem with the single-server model.

VIII. Conclusion :

Despite its many benefits, cloud computing presents significant problems with fundamental security issues like data privacy. proposed a password-based authentication that is built upon a novel two-server model. Compared with previous solutions, our system possesses many advantages, such as the elimination of key exchange system, avoidance of any sort of cryptographic techniques such as encryption, hashing and high efficiency with provable security. In contrast to existing multiserver password systems, our system has great potential for practical applications. It can be directly applied to fortify existing standard single server password applications, e.g., FTP and Web applications. By employing two servers, the system is able to offer considerably more protection of sensitive user data than any single-server approach could permit.

IX.Reference:

[1] Piyush Singh Katiyar "Cloud Computing Security Problem (Data Privacy) and Strategy" G International Journal of Computer Science and Engineering (SSRG-IJCSE) – volume1 issue9 Nov 2014.

[2] Ranjit Panigrahi,M.K. GhoseMoumita,Pramanik" Cloud Computing: A new Era of Computing in the Field of Information Management" International Journal of Computer Science Engineering (IJCSE)

[3] Prateek Bhanti, Sushma Lehri, Narendra Kumar "cloud computing: a new paradigm for data storage in indian universities" Indian Journal of Computer Science and Engineering.ISSN-0976-5166.

[4] W. Jansen, T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing", National Institute of Standards and Technology, 2011.

[5] Yanjiang Yang, "Enabling Use of Single Password over Multiple Servers in Two-Server Model ", Computer and Information Technology (CIT), 2010 IEEE 10th International Conference.

[6] G. Boss, P. Malladi, S. Quan, L. Legregni and H. Hall, "Cloud computing. Technical report", IBM high performance on demand solutions, 2007-10-08, Version 1.0, 2007.

[7] Vaquero, L.M.; Radero-Merino, L.; Linder, M. (2009): A break in clouds towards a cloud definition, SIGCOMM Comput. Communication Rev. 39, pp.50-55.

[8] S. Bellovin and M. Merritt, "Encrypted Key Exchange: Password Based Protocols Secure against Dictionary Attacks," Proc. IEEE Symp. Research in Security and Privacy, pp. 72-84, 1992

[9] D.P. Jablon, "Password Authentication Using Multiple Servers," RSA Security Conf., pp. 344-360, 2001.

[10] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, Page: 393– 422, Published by Elsevier, 2002.