ADVANCE SECURITY FRAMEWORKS IN CLOUD COMPUTING USING BLOWFISH

Ashok B. Hajgude*

Abstract: -

Cloud computing is one of today's most exciting technologies due to its ability to reduce cost associated with computing. This technology worldwide used to improve the business infrastructure and performance. At present cloud user authentication can be done by several ways like password authentication, Graphical and 3D password etc. In this paper I proposed the Advance Security frameworks in Cloud Computing Using Blowfish Algorithm. This Security Framework will provide Two times user authentication which will execute in different modules like user registration, user authentication, and password change.

KEYWORDS

Cloud Computing, password change, session management, Registration of User, and Authentication of User, Dual Authentication.

* SMGOE, hyderabad

I. INTRODUCTION

The success of any technology always depends on the effectiveness of the norms and easy to use by user and its security. Cloud Computing is a model of Performance business and also infrastructure management methodology. [1]. Cloud computing model for enabling convenient on demand for network access to both users and IT managers. It Provides configurable computing resources like networks, servers, storage and release with minimum management efforts or service providers [2]. Cloud computing models are divided into private cloud, public cloud and hybrid cloud according to the different service objects. Public clouds are virtualized data centers outside of firewall and service provider makes resources available for customer or demand over internet [3]. The private cloud is deployed in the company and security can be made easily. Private clouds virtualized cloud data centered inside firewall and it is private space dedicated to system within cloud data center. Private cloud refers to internal data center of business or other organization [4]. Hybrid cloud is the combination of two or more clouds. Hybrid cloud combines both private as well as public clouds [5] [6].

The cloud service model includes [6]

- Software as a Service (SaaS):- In the SaaS model cloud provider installed and operates application software in the cloud and cloud users access software from cloud client [7]. Cloud users do not manage the cloud infrastructure and platform on which application is running. This eliminates need to installed and run the application on the cloud.

- Platform as a service (PaaS):- In PaaS model cloud provider deliver a computing platform typically including operating system, programming language execution environment, database and web server [8]. Application developer can develop and run their software solution on a cloud platform without the cost and complexity of buying and managing the hardware and software layers [9].

- Infrastructure as a Service (IaaS):- Primary objective of an organization is to reduce time and money required to produce, provision and install new hardware system [10]. IaaS fulfill the primary objectives i.e. equipment is outsourced to supports operation. The service

providers are responsible for housing, running and maintenance of equipment. Many companies and organization are placing their data into cloud. As cloud computing are involved reliability, ownership, data backup and many more things like security [11]. The application security and identity management, access control and Authentication [12]. Confidentiality does not guarantee of security. It has to Consider authentication and authorization features[13] .

2. LITURATURE SURVEY

Cloud server architecture is used in cloud computing in large scale. For Dual user authentication in cloud computing, I have survey some existing authentication scheme. Most of the popular remote authentication procedure was suggested by Lamport in 1981[14]. In this server stores both User_Id and password in hash table for verification. The password generation uses hash function, which generate service of password. Existing some password authentication schemes have been proposed [15]. Smartcard is used to prevent from the attack. In order to make a secure usage of services provided by the cloud. Cloud user authentication systems can be use different password techniques like 1) simple text password 2) Graphical password authentication 3) 3D password object. The weakness of password authentication system is, it can be break and very much vulnerable to attack. Graphical password requires memory space which is found less or equal space to textual password. Whereas graphical password require large space and time [16]. 3D password having its own limitations. Some systems have proposed authentication based on sending the SMS, but it doesn't guarantee to delivery of SMS on time.

So as review of above mentioned existing systems, in this paper I have proposed use of Blowfish Algorithm and Two times user authentication process along with password change facility and send password to registered Email_Id.

3. SYSTEM ARCHITECTURE

Cloud security structure is shown in the figure. Where I have proposed authentication scheme. In figure 1 authentication server (AS) is for authentication of user and cloud web server providing the services to the user.

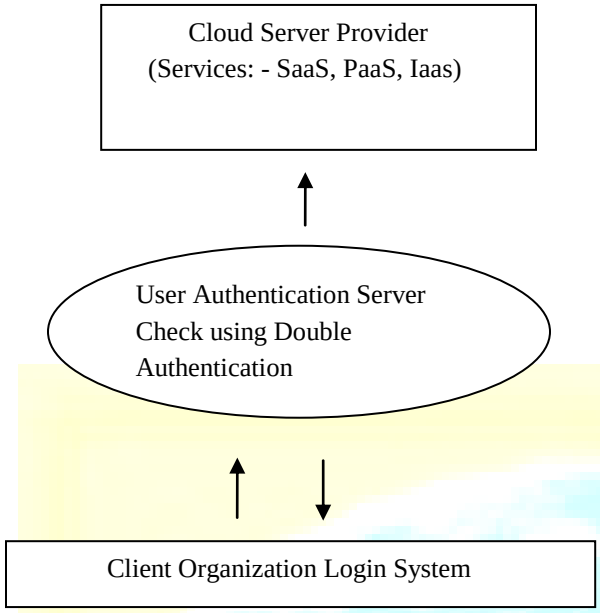

Figure 1:- System Architecture

1) User_id and password is entered by user in his system
2) System sends them as an input to the cloud server.
3) Authentication server generates a onetime password and sends to the registered Email_id.
4) User enter that password value as an input within the session time because after the expired of session user has to login again.
5) After the successful login, user is allowed to access the resources.

4. PROPOSED TWO TIMES VERIFICATION FOR USER AUTHENTICAION

4.1 Registration Phase

Whenever user wants to access cloud resources, user has to register first on to the cloud. Following are the steps to register on the cloud.

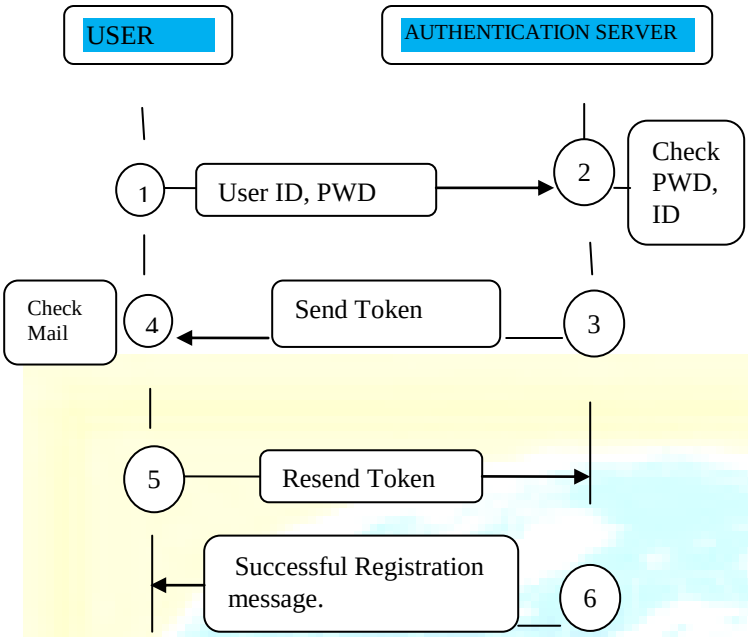

Figure 2:- Registration Phase

1) User has to provide valid Email_Id and password to the authentication server.
2) Authentication server checks the Email_Id against the availability of that Email_Id. Email_Id should not repeat or match with existing user's Email_Id.
3) After checking the availability of Email_Id, The authentication server sends a token to the user's Email_Id.
4) User checks the Email and token send by the authentication server.
5) User enters the token value for further authentication and confirm for the registration.
6) After getting the valid token value, Authentication server send message of successful registration to the user.

4.2 User Login and TWO TIMES Authentication

When user wants to access resources on the cloud, then user should login on to the cloud. Following are the steps to login on to the cloud.

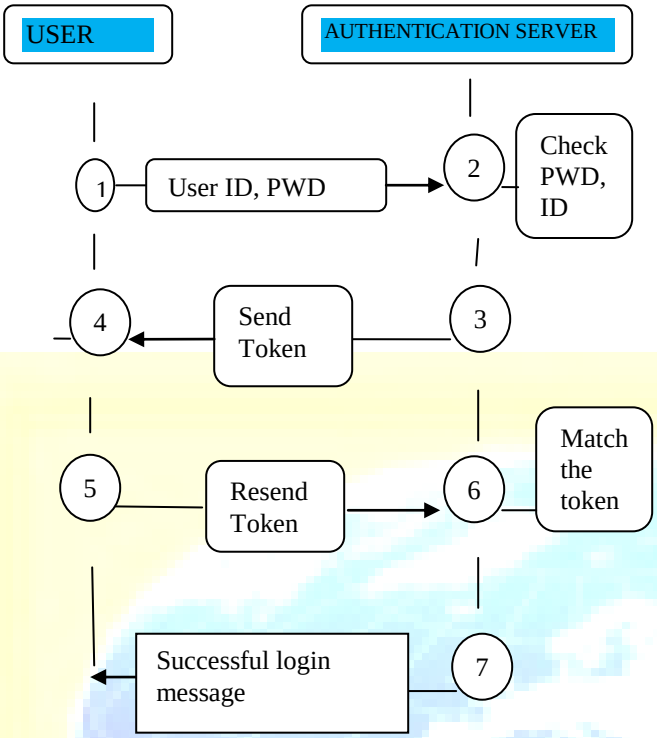

Figure 3:- User Login and Two Times Authentication.

1) Valid Email_Id and password should be entered by user in his login interface. User's system computes the secrete key using stored values, which was already provided by the user at the time of registration.
2) The authentication server checks the user_id and password provided by the user with the user_id and password which was provided by the user at the time of registration.
3) After matching the user_Id and password authentication server generates the dynamic token from hash table and send it to the user's Email_Id for DUAL authentication.
4) User checks his Email for getting the dynamic token for further authentication.
5) User has to enter the token value for DUAL authentication
6) Authentication server matches the token with the dynamic token which was send by itself.
7) After matching the token authentication, user will Authenticate and server provides access of resources to the user.

4.3 Password Change phase

This phase is used to provide facility of changing the password. User has to provide his old password and new password to change his old password. Following are the steps,

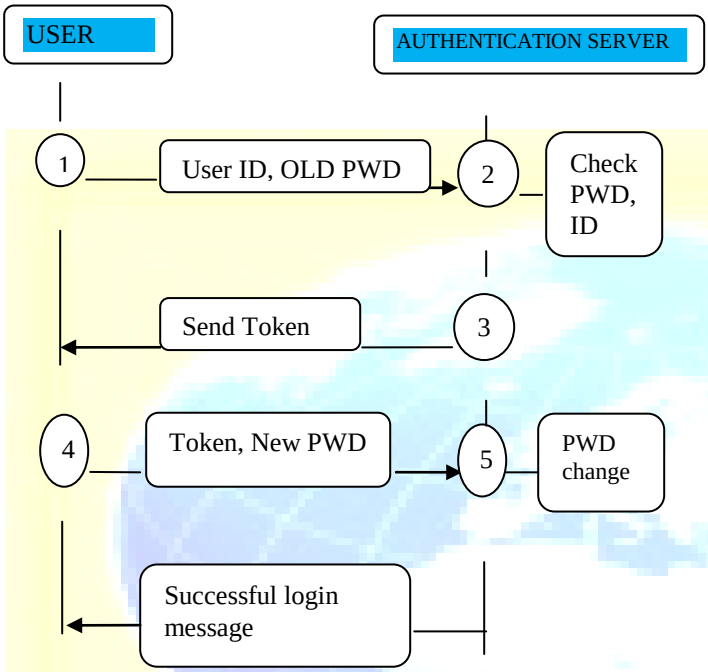

Figure 4:- Password Change Phase

1) User has to provide his user_id and old password to change The password
2) Authentication server checks the password with registered User_Id and password.
3) After the matching of User_Id and password it send the Dynamic token to the user's Email_Id.
4) User has to provide token as well as new password to the Authentication server.
5) Authentication changes his old password to the new Password and sends the message to the user for change of Password.

4.4 Blowfish Algorithm

The data transformation process for Pocket brief uses the Blowfish Algorithm for Encryption and Decryption, respectively. The details and working of the algorithm are given below

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneider as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses.

Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors.

Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encrypted. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

5. SECURITY ANALYSIS

In this system security is provided by TWO TIMES authentication and dynamic token send to user's Email_Id. There are some security features which satisfy this proposed system.

5.1 Dual Authentications

By providing dynamic token on to the user's Email_Id no attacker can receive the dynamic token which will be useful for DOUBLE authentication.

5.2 Session Managemen

Session key i.e. dynamic token is generated from hash table. This token will remain valid up to the particular session only. After the logout or some period of time it will get expired.

5.3 Use of Blowfish Algorithm

Use of this Algorithm provides system with additional security as compared to others.

6. CONCLUSION AND FUTURE ENHANCEMENT

Cloud computing provides the variety of internet based on demand services like software, hardware, server, infrastructure and data storage. To provide secure services to the customer, I have used DOUBLE authentication technique with many security features such as DOUBLE authentication, session management. I have also introduced extra feature of changing of password to the user and provide a high security to the server to resist the attacks like password stolen attacks,

replay attacks.

7. REFERENCES

[1] Center Bo Wang, HongYu Xing "The Application of Cloud Computing in Education Informatization, Modern Educational Tech..." Computer Science and Service System (CSSS), 2011 International Conference on IEEE, 27-29 June 2011, 978-1-4244-9762-1, pp 2673 – 2676

[2] Mell P. and Grance T., "The NIST Definition of Cloud Computing", vol 53, issue 6, 2009.

[3] A Platform Computing Whitepaper, enterprise cloud computing: Transforming IT. Viewed 13 March 2010

[4] Dooley B 2010, 'Architecture requirement of The Hybrid Cloud'. Information Management Online, Viewed 10 February 2010

[5] Global Netoptex Incorporated, 2009, Demystifying the Cloud. Important opportunities, choices, Viewed 13 December 2009.

[6] Lofstrand M, 'The VeriScale Architecture: Elasticity and Efficiency for Private Clouds", *Sun Microsystems*, Sun Blueprint, Online, Part No 821-0248-11, Revision 1.1, 09/22/09

[7] S. Roschke, et aI., "Intrusion Detection in the Cloud," presented at the Eighth IEEE international Conference on Dependable, Chengdu, China, 2009.

[8] Leavitt N, 2009, 'Is Cloud Computing Really Ready for Prime Time?' *Computer*, Vol. 42, pp. 15-20, 2009.

[9] Brodkin J, 2008, 'Gartner: Seven cloud-computing security risks', 13 march 2009 from http://www.infoworld.com/d/security-central/gartner-seven-cloudcomputing

[10] Reddy B. ET. Al., "Cloud computing security issues and challenges", 2009.

[11] Almulla S. A., Yeun C. Y., "Cloud Computing Security Management", Engineering Systems Management and Its Applications (ICESMA), Second International Conference, 2010.

[12] Lamport L., "Password authentication with insecure communication," Communications of the ACM, vol. 24, issue 11, Nov 1981.

[13] Hwang M.S., and Li L H., "A New Remote User Authentication Scheme using Smart Cards", IEEE Transactions on Consumer Electronics, vol. 46, issue 1, 2000.

[14] X. Suo, Y. Zhu, G. S. Owen, "Graphical passwords: A survey," in Proc. 21st Annual Computer Security Application. Conf. Dec. 5–9, 2005, pp. 463–472.