Design and Implementation of Authentication as a Service (AaaS) in Windows Azure Cloud Platform

Dr. N. Veeraragavan

Christhu Raj College, Panjappur, Tiruchirappalli, Tamil Nadu, India

Abstract. Cloud computing is an internet based computing. It consists of various services and delivers on-demand basis from the user request. Data security is a necessary facet for any web applications. Authentication is an important security problem in cloud as well as internet facing applications. This paper proposes authentication algorithms for securing the cloud applications. Authentication is an essential factor among other security parameters such as authorization, auditing and availability. These proposed algorithms are used to protect the unauthorized access in cloud. User’s data are converted into different form using the different encryption techniques. These three algorithms are combined and provide as a single service to the cloud user. Proposed User authentication mechanisms are designed and developed in ASP.NET platform and deployed on Windows Azure platform of cloud System. This user authentication mechanism is simply matched with any kind of service within the cloud environment. The proposed user authentication algorithms have provided best security in cloud system. This mechanism can be used for agriculture, medical, education and IT based applications to firmly access the information in secured manner.

1. Introduction
Cloud computing is a complex infrastructure of hardware, software, storage that are available as an on-demand basis with pay-as-you-go method through internet. It is computing paradigm in which process are assigned to a combination of software, hardware, connections are accessed over the network. This network of servers and connections are combined together called as a “Cloud Computing”[1].The emerging of cloud computing allows IT companies to focus more on their core business and brings perceived economic and operational benefits. It provides three major services namely, Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). These services are delivered through four deployment models namely private, public, community and hybrid clouds[2]. NIST also provides a unifying view of five essential characteristics of the cloud services. They are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Cloud Service Provider (CSP) provide any services and computing resources through web, which can be accessed from anywhere, anytime using web browsers, smart phone and personal computers[3]. It provides so many advantages namely, reduce capital costs, increase storage, improve flexibility, streamline processes, improve accessibility, achieve economies of scale and minimize licensing new software[4].

2. Related Work
Cloud computing offers different benefits to the enterprises and users, but at the same time it has different security issues. Cloud security issues can be classified into four categories: authentication, data integrity, data confidentiality and access control. User authentication is the paramount requirement for cloud computing that restricts illegal access to cloud resources[5]. Patel Y et al. [6] proposed multilevel authentication scheme to protect cloud environment from unauthorized access and implement security measures to prevent users data stored in cloud. It provided service level security in cloud environment. It consist of two schemes namely, Site 1 and Site 2. Site 1 included application server and database server, which were provided web interface to user for uploading or downloading data from cloud environment. Ticket database generated valid ticket for the registered cloud user. This
Possession factor and Inherence factor. of the attacks. Multi-Factor Authentication (MFA) is a technique to authenticate user using various attributes. Traditional authentication system does not offer sufficient security for information in cloud to the most organizations, which establishes proof of identities to get access to resources in the system. Security is the utmost critical issues in a cloud computing. Authentication is a key technology for public cloud computing, where data or services are hosted and provided as a service to the user. There is a need of a proper user authentication service model and protocol for Cloud Computing. Randeep Soni P et al. [15] described a new multi-factor authentication framework for cloud environment. Data integration and access control are key requirements when dealing with multitenancy. Kerberos authentication protocol is used on the top of API designed for cloud computing environment that incorporates bio signals, ZKP and Rijndael’s encryption and decryption for user credentials. Electro dermal responses are used for initial authentication techniques. This framework is verified by Cloud Access Management (CAM) system which authenticates the cloud user based on multiple factors such as username, password, image captcha.

Chen N et al. [10] proposed an improved user authentication technique. This improved protocol ensure that the user legitimacy before enter the cloud computing. The mutual authentication protocols are formally proved by the strand space model theory and the authentication test method. This technique consists four phases namely, registration phase, login phase, authentication phase and password change phase. It leads more time taken for accessing the services in cloud environment. Jivanadham L B et al. [11] proposed a new authentication scheme called as CCA (Cloud Cognitive Authenticator). This scheme applies one round Zero Knowledge Protocol (ZKP) for authentication process. CCA is an API designed for cloud computing environment that incorporates bio signals, ZKP and Rijndael’s algorithm. CCA improves security in a public cloud by providing bio-level authentication. It also provides encryption and decryption for user credentials. Electro dermal responses are used for initial level authentication.

Pippal S et al. [12] described a new approach, shared database shared schema approach that offers larger number of tenants (institution) per database server as the single database serves the database requirements of multiple Institutions in different places. Authentication and authorization are key requirements when dealing with multitenancy. Kerberos authentication protocol is used on the top of multi-tenant database for participating educational institution in a heterogeneous environment, where a tenant can also freely participate with data centre. Dinesha H A et al. [13] denoted generation of new password by concatenating passwords at different stages. Authentication takes place at various levels- organization, group and user levels. At the user level, it authenticates the users’ privileges to access a specific resource in cloud system. It uses a multilevel approach. It is difficult to break multilevel security as compared to single level scheme. This mechanism is very hard to hack the password through social engineering and other non-technical attacks.

Chang H et al. [14] described various access control and user authentication that were used as security technologies in the cloud environment. In Cloud environment, misuse of access authority to resources and leak of personal information which were used to authenticate a user could affect the speed. For the effective user authentication in Cloud environment, the combined authentication technologies should be used or a secure user authentication method for Cloud Computing should be developed. So there was a need of a proper user authentication service model and protocol for Cloud Computing. Randeep Soni P et al. [15] described a new multi-factor authentication framework for cloud environment. Data Security is the utmost critical issues in a cloud computing. Authentication is a key technology for information security, which establishes proof of identities to get access to resources in the system. Traditional authentication system does not offer sufficient security for information in cloud to the most of the attacks. Multi-Factor Authentication (MFA) is a technique to authenticate which requires the production of two or more of the three following authentication factors namely Knowledge factor, Possession factor and Inherence factor.
3. Problem Definition and Motivation
Many security problems may occur in real time environment such as Yahoo, Gmail etc. Cloud atmosphere are often simply disclosed with different attacks from inside and outside the hackers. Several existing user authentication techniques are not fitted in cloud system. User authentication is compromised by different attacks Replay attack, Man-in-the-middle attack, Denial of Service, Masquerade attack, Password guessing attack. If hacker achieved success of authentication, it make huge loss for cloud users.

From the briefly survey on user authentication mechanism in cloud computing and found out that there is a need for authentication as a service in cloud environment.

4. Objective
The aim of this paper is to propose user authentication mechanism as an isolated service to the cloud system.
- To determine the user authentication by ensuring the authenticated user only
- To propose user authentication algorithms for security
- To implement user authentication algorithm in cloud environment.

5. Methodology
User authentication mechanism is focused to enhance security in cloud computing. Initially, cloud user request to access the cloud services. There are two stages in authentication. First stage is new user registration and the other is existing user registration. In new user registration, user submits their information to the CSP. Once the user registration is completed, proposed authentication password generation algorithm generates the password and send them to the registered users’ mail account. Then cloud server generates authentication key using authentication key generation algorithm and stores in cloud date center with encrypted format. The new user may come to know his user id and password when he / she opens his mail account. From login page, user entered the user id and password. On request to cloud services from CSP, it generated user Auth_key using Authentication Key Generation algorithm. Now, Cloud server checks the server Auth_key and User Auth_key. If match found then the user will be allowed to access the cloud services, otherwise user request for access control will be denied.

6. Algorithms for Proposed UIDAaaS
User IDentity based Authentication as a Service (UIDAaaS) includes algorithms, namely Authentication Password Generation (APG), Authentication Key Generation (AKG) and Authentication Verification (Auth_V).

APG and AKG are proposed authentication algorithm to provide Authentication as a Service (AaaS) from a CSP (Cloud Service Provider) in Cloud. APG generates password using user registration details and send to cloud users’ registered mail id with encrypted format as well as stores it in cloud server. Key generation is a separate service. It is used to generate the password and Auth_key in cloud server. AKG generates Auth_key using user credentials along with password and stores it in cloud server in encrypted format. With the help of user ID / owner ID and password, cloud user is able to access cloud services from CSP. After the verification, cloud user can change the password according to his wish. The proposed user authentication algorithm provides authentication as a separate service through the CSP. Procedures of proposed Authentication Password Generation (APG), Authentication Key Generation (AKG) and Auth_key verification Algorithms are as follows:

6.1 Procedure for Authentication Password Generation (APG)
Step 1. Digested values from the user input as plaintext.
Step 2. Plaintext is converted into ASCII code
Step 3. ASCII codes are converted into binary bit block 0s’ and 1s’
Step 4. Split the bit block into two by take alternate bits in the block.
Step 5. Reverse each block
Step 6. Find XOR operation for the two blocks
Step 7. Divide the block into 8 bits
Step 8. Convert the binary into decimal
Step 9. Convert the decimal into ASCII character code to produce the Password

6.2 Procedure for Proposed Authentication Key Generation (AKG)
Step 1: The given original text are converted into ASCII code
Step 2: ASCII codes are converted into binary values 0s’ and 1s’
Step 3: Split the bit block into two by take alternate bits in the original text.
Step 4: Perform OR operation on these two blocks
Step 5: Perform NOT operation after OR operation completed
Step 6: Get a Key K from KG and perform XOR operation
Step 7: Divide the block into 8bits
Step 8: Add each 8bits into others 8bits binary
Step 9: Get single 8bits binary
Step 10: Convert the 8bits binary into decimal
Step 11: Convert the decimal into ASCII character code to produce the Authentication key

6.3 Procedure for Proposed Authentication Verification (Auth_V)
Step 1. Users submit their credential for authentication
Step 2. Authentication key is generated from the user credential
Step 3. User authentication key is matched with authentication key registered in the UIDaaS
Step 4. If it is matched users are allowed to access the cloud services
Step 5. If it is not matched users are not allowed to enter into the cloud services

7. Experimental Results
This proposed UIDaaS mechanism is implemented using ASP.NET and deployed on Windows Azure Cloud Platform. The configuration setup of windows azure server is shown in Table 1.

| Applications          | Windows Azure Service Model |
|-----------------------|-----------------------------|
| Runtimes              | .NET 3.5/4, ASP.NET         |
| Operating System      | Windows Server 2008/R2-Compatible OS |
| Virtualization        | Windows Azure Hypervisor   |
| Server                | Microsoft Blades           |
| Database              | SQL Azure                   |
| Storage               | Windows Azure Storage (Blob, Queue, Table) |
| Networking            | Windows Azure-Configured Networking |

Windows azure platform provides separate domain name for each deployment of User applications. The proposed UIDaaS is requested in the domain name of http://uids.azurewebsites.net. Three procedures are separately configured in this cloud application. This application is provided as a cloud service for authentication service. The screenshots of the implemented authentication services is as follows; Figure 1 shows the registration of new user.

Figure 1. User Registration of UIDaaS
Figure 2 shows the successful registration of the user in the proposed cloud authentication service.
Once the registration completed successfully, username and password are generated and forwarded to the users' registered through mail. Figure 3 and Figure 4 show the confirmation message sent by the cloud service.

Figure 3. Message of Username and Password send your Email Screen

Figure 4. Login Received Information of User Mail Screen

Figure 5 shows the login screen for registered user. Users have to note the username and password received to their mail id. To login, users have to submit the username and password for accessing the cloud services.
Figure 5. Login Screen for Registered User Screen
Users login verification are valid then users are able access the cloud services otherwise their login is denied. Figure 6, shows the cloud services of authorized users.

Figure 6. Cloud Services Screen
The proposed UIDAaaS Authentication as a Service is compared with the existing authentication system like Multi-factor Cloud Authentication System and Cloud based Multitenant Database with Authentication and authorization Framework.

The comparison is based on the performance of existing and proposed authentication system with respect to different types of attacks such as DoS (Denial of service) and MITM (Man-in-the-Middle Attack). The Security level of proposed and existing authentication mechanism is measured by using Universal Hackman tool. This tool uses the attacks namely DoS and MITM to attack the existing and proposed authentication mechanism without knowing the username and password. The experiment is conducted for 30 times and finds the number of success and number of failure of existing and proposed authentication mechanism. Table 2 and Figure 7 show the comparison of existing and proposed authentication system.

Table 2. Comparison of Existing and Proposed Authentication System

|                      | Sanjeev Pippal et al. (Existing Authentication System) | Wenyi Liu et al. (Existing Authentication System) | Proposed UIDAaaS |
|----------------------|--------------------------------------------------------|--------------------------------------------------|------------------|
|                      | DOS | MMA | DOS   | MMA | DOS   | MMA   | DOS   | MMA   |
| NA                   | S   | F   | NA    | S   | F     | NA    | S     | F     |
| 30                   | 8   | 22  | 30    | 7   | 23    | 30    | 6     | 24    |
| 30                   | 2   | 28  | 30    | 1   | 29    |
Table 3 and Figure 8 show the percentage of the security level of existing and proposed authentication mechanism generated by the Universal Hackman tool. This tool calculates the security level from number of attacks, failures of existing and proposed authentication mechanism.

| S. No. | Name of the Authentication Mechanism | Security Level (%) |
|--------|--------------------------------------|--------------------|
|        |                                      | DOS    | MMA    |
| 1      | Sanjeev Pippal et al.                 | 63     | 67     |
| 2      | Wenyi Liu et al.                     | 80     | 83     |
| 3      | Proposed UIDAaaS                     | 93     | 97     |

From the results, it is clear that the proposed authentication mechanism produced maximum level security by protecting cloud service from different authentication attacks.

8. Advantages of proposed UIDAaaS Authentication Mechanism

User IDentity Authentication as a Service (UIDAaaS) is provided as a separate services to the cloud users. This authentication mechanism reduces the time taken for the user authentication process in cloud. User authentication mechanism prevents many attacks such as Man-in-the-middle attack, Denial of Service (DoS). The login credential of password includes characters and numeric values only. The authentication key generation algorithm generates the authentication key, which consists only single character. This key reduces the size of the memory in the cloud server and also, hackers could not find the original key without know the overall procedures.

9. Conclusion

Cloud computing is an emerging technology in present scenario. Authentication is an important issue of cloud security system. In this paper, we proposed UIDAaaS as a service, which to enhance the security to the owner of the data which is store in cloud server. User authentication algorithms are used to prevent the unauthorized access from outside and inside hackers in cloud. These three
algorithm provide as a separate authentication service to the user which is provided by any cloud Service Providers. Authentication password generation algorithm is to generate the user password and store in cloud server with encrypted format. Authentication key generation is used to generate the authentication key which is store in cloud server. Authentication key has single character, it reduce the memory size in the cloud server. This paper mainly focused on the design and development of user authentication algorithms using ASP.NET language. The developed user authentication mechanism provides as a separate service and deployed in windows azure cloud platform environment. From the results obtained, it is observed that the user authentication as a service could offer better security to user data on a cloud than the existing mechanisms.

10. References
[1] Liu F, Tong J, Mao J, Bohn R, Messina J, Badger L, Leaf D. 2011 NIST Cloud Computing Reference Architecture. Special Publication. NIST Special Publication 500-292. pp. 1-35.
[2] Arockiam L, Monikandan S, Parthasarathy G. Cloud computing: A survey. International Journal of Internet Computing, Volume 1(2), pp. 26-33.
[3] Irudayasamy A, Arockiam L, Veeraragavan N. 2013 Enhancing Data Security during Transit in Public Cloud, International Journal of Engineering and Innovative Technology (IJEIT). Volume 3(1), pp. 486-491.
[4] Mell P, Grance T. 2011 The NIST Definition of Cloud Computing.
[5] Veeraragavan N, Arockiam L, Monikandan S. 2015 Enhanced Framework for Authentication as a Service to Ensure Security in Public Cloud Environment. International Journal of Engineering Research & Technology (IJERT). Volume 4(7), pp. 442-445.
[6] Patel Y, Sethi N. 2014 Enhancing Security in Cloud Computing Using Multilevel Authentication. International Journal of Electrical Electronics & Computer Science Engineering, Volume 1(1), pp. 35-39.
[7] Ullah S, Xuefeng Z, Feng Z. 2013 TCLUD: A Multi – Factor Access Control Framework for Cloud Computing. International Journal of Security and Its Applications. Volume 7(2), pp. 15-26.
[8] Kataria S, Syal R. 2015 Secure Mutual Authentication for Cloud Environment. International Journal of Computer Science Engineering and Technology (IJCSET), Volume 5(7), pp. 214 – 218.
[9] Banyal R K, Jain P, Jain V K. 2013 Multi-factor Authentication Framework for Cloud Computing. Fifth International Conference on Computational Intelligence, Modelling and Simulation. IEEE, pp. 105-110.
[10] Chen N, Jiang R. 2014 Security Analysis and Improvement of User Authentication Framework for Cloud Computing, Journal of Networks. Volume 9(1), pp. 1-6.
[11] Jivanadham L B, YoshiakiKatayam A K M M. 2013 Cloud Cognitive Authenticator (CCA) A Public Cloud Computing Authentication Mechanism. IEEE, pp. 1-6.
[12] Pippal S, Sharma V, Mishra S, Kushwaha D S. 2011 An Efficient Schema Shared Approach for Cloud based Multitenant Database with Authentication & Authorization Framework. IEEE, pp. 213-218.
[13] Dinesha H A, Agrawal V K. 2012 Multi-level Authentication Technique for Accessing Cloud Services. International Conference on Computing, Communication and Applications (ICCCA). IEEE, Volume 22(24), pp. 1-4.
[14] Chang H, Choi E. 2011 User Authentication in Cloud Computing. Springer, pp. 338–342.
[15] Soni P, Sahoo M. 2015 Multi-factor Authentication Security Framework in Cloud Computing. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Volume 5(1), pp. 1065-1071.