ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(32), DOI: 10.17485/ijst/2016/v9i32/96525, August 2016* ISSN (Online) : 0974-5645

User Identity based Authentication as a Service (UIDAaaS) for Public Cloud Environment

N. Veeraragavan* and L. Arockiam

Department of Computer Science, St. Joseph's College (Autonomous), Tiruchirappalli – 620002, Tamil Nadu, India; veeraragavan1182@gmail.com, larockiam@yahoo.co.in

Abstract

Objectives: In today's Technological World, Information Security is an essential aspect for the internet applications. Cloud computing is an increasing current class of services for any type of users of the internet. Authentication is a major security problem in the cloud system and internet. This paper proposes an Authentication Password Generation (APG) algorithm, Authentication Key Generation (AKG) and Authentication Verification Algorithm (Auth_V) for security in the cloud system. **Methods/Statistical Analysis:** Authentication is more important among other security parameters such as integrity, confidentiality and privacy. Authentication mechanism includes different cryptography techniques that can be used for securing the data in cloud systems. These proposed three algorithms are used in the authentication process of cloud environment. It executes the ASCII code of each value in the original data. **Findings:** Proposed APG, AKG and Auth_V authentication algorithms are implemented in .NET and deployed on the windows azures platform of cloud environment. These proposed authentication algorithms easily fit into any type of service in the cloud system. APG is used to create a password which generates the alphabets along the special characters. **Application/Improvements:** Security is more important in the cloud computing. The proposed APG, AKG and Auth_V algorithms have provided better authentication mechanism to the cloud user. These techniques are suitable for education, healthcare and agriculture based applications to securely access the data in a cloud computing environment.

Keywords: Authentication, Authentication Key Generation, Authentication Password Generation, Authentication Verification, Cloud Security, Cryptography

1. Introduction

Cloud computing is internet based computing. With the rapid development of the Internet, global information tide expends the application of information in cloud computing environment. It also brings many economic and social benefits along with the widespread use of cloud computing systems. Cloud computing is an open system which faces in public; it must confront many safety requirements[1]. According to the NIST definition, Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). It is quickly and freely provisioned with least controlling effort or service provider's communication. Cloud system provides three service models, four deployment models and five essential characteristics[2]. In cloud computing, the users and Cloud Service Providers (CSPs) use the different resource at low cost without owning the resource needed[3]. It provides different computational resources like server, software, storage, network, etc., as on-demand services[4]. Cloud computing provides everything (X) as a service, where X denotes the application software, hardware, operating system, storage, etc. Though cloud computing provides numerous advantages to the enterprises, it has many security issues too. Here, data and resources are stored in the cloud, which is open to all[5]. CSP should make sure the security of their user's information and must be responsible for any security threat that may affect the user's service infrastructure. CSP deals with several services that may help his user such as quick access to their information from anywhere, scalability, pay-per-use, data storage, data recovery, prevention against intruders, instant safety controls and the use of web and infrastructure services[6]. Security plays a vital role

* *Author for correspondence*

in protecting resources against illegal access by hackers. Anyone who tries to access information from the cloud should be authorized by the cloud service provider. There are several ways to authenticate a person. Usually username and password were used in various authentication system, but an unauthorized user can easily crack it[7].

Recent web applications are built on username and password type of security schemes. Unfortunately, password replacement offers more security, but it is very difficult to use and expensive to deploy in real time situations. Authentication is a major issue to build security for web applications. This paper describes a new mutual authentication scheme called StrongAuth which preserves most of the password authentication advantages and concurrently improves security using cryptographic techniques. It includes three stages namely Registration phase, Authentication and Login phase, and Key renewal phase[8].

Secure mutual authentication is mandatory model for cloud computing. The Modified Diffie Hellman agent (MDHA) is used to provide mutual authentication which interacts with Authentication as a Service (ASaaS) instead of cloud server. Cryptographic techniques are used in this mechanism. The proposed mechanism includes four phases: connection establishment, registration phase, login phase and authentication phase. Two different agents namely cryptography agent and MDHA agent are placed in this scheme. Cryptography agent is used to provide encryption of user's data before transferring to the cloud server. MDHA agent decrypts the request from user side and sends responses based on the receiving message[9].

In cloud computing, the password authentication is a first level of security, which is aimed to guarantee only the legitimate users to access the cloud data. Multi-factor authentication schemes provide more than one factor that is used to verify the user information and then allows accessing the data. The proposed scheme has Two-Factor Authentication (2FA) that overcomes various cloud security barriers and reduces the cost. It used Zero-Knowledge and One-Time Password (OTP) to implement a Cloud-based two-factor authentication[10].

Sabout Nagaraju et al. described the uses of cloud computing technology to the investors to avoid the preliminary investment of expensive infrastructure setup, licensing original software, training for new employees and so on. The authors proposed a privacy preserved Multi-Factor Authentication (MFA) scheme. The MFA consists of effective access key distribution technique. This scheme incorporated with several factors namely biometric fingerprint along with user-id, password and One-Time Password (OTP), improved the existing Single Sign-On (SSO) and two-factor authentications switch over to multi-factor authentication. The main shortcoming of this approach was that remote users, cloud users and cloud service providers must trust the third party trustee[11].

Krishna Reddy et al. proposed a new approach for federated cloud system. This approach showed the security for every user independently in multi-cloud data center. A key aggregate searchable encryption was used to secure the data outsourcing in cloud system. They extended KASE for multi-cloud data center with reliable reasoning power to protect the federated cloud system[12]. The authors applied two methods in cloud setup with two factors namely, aggregate key based data distribution in cloud with effective and reliable user data storage and security for single cloud user in federated cloud system.

D. Ganesh Kumar et al. proposed a new approach to provide password authentication for cloud computing. During the registration phase, user provided all the information and stored it in the cloud server. Password could be generated by the user or server. After the registration process, the cloud user could access the cloud services through login process. Protocol based authentication and verification consisted of two modes. User credentials were send to the user's mobile devices. This procedure was used to avoid hacking of password and backtrack attack using the generated password. With help of unique identification number, duos system possessed website. Mobile service provider involved during the password recovery phase. It involved two-factors namely password phase and cloud space. Cloud consumer was able to modify their password easily in the password changing stage and update the user credentials on cloud environment[13].

2. Problem Definition and Motivation

Real time unauthorized access happens in Gmail, Yahoo and etc. Public cloud environment can be easily disclosed with various attacks from the unauthorised person from in and outside the cloud environment. There are several existing authentication mechanisms that are not suitable in different models in cloud environment. Authentication is compromised by various attacks such as DoS, men-

in-the-middle, brute force, etc. It makes huge loss to the users when authentication is broken.

Authentication protects the entry of malicious attacks in cloud. Brief study on the existing authentication mechanism was conducted and found out that there is a need for separate Authentication as a Service (AaaS) in cloud computing. It is evident that an efficient authentication system does not compromise the other security parameters, like confidentiality, integrity and etc.

3. Objective

The aim of this paper is to propose an Authentication as a Service (AaaS) for cloud to ensure the security. Following objectives are derived to achieve this aim.

- To determine the Authentication by ensuring the valid cloud user to access the cloud service.
- To propose authentication password generation algorithm for cloud security.
- To propose authentication key generation algorithm for cloud security.
- To propose authentication verification algorithm for cloud security.

4. Methodology

UIDAaaS mechanism is provided as a separate service to cloud users. This mechanism includes three algorithms, namely APG, AKG and Auth_V. Initially, User request to the new user page and submits their credentials. Once the user submits their credentials, APG generates the user password and send to the user registered mail account as well as stored in cloud server. AKG generates the server Auth_key and store to cloud server in encrypted format. Users could able to access the cloud services through user id and password. During the login process AKG generates the user Auth_key. If both user Auth_key and server Auth_key is matched, then user authorized to access the cloud services otherwise, the user request is denied. The methodological diagram of the proposed authentication mechanism is presented in Figure 1.

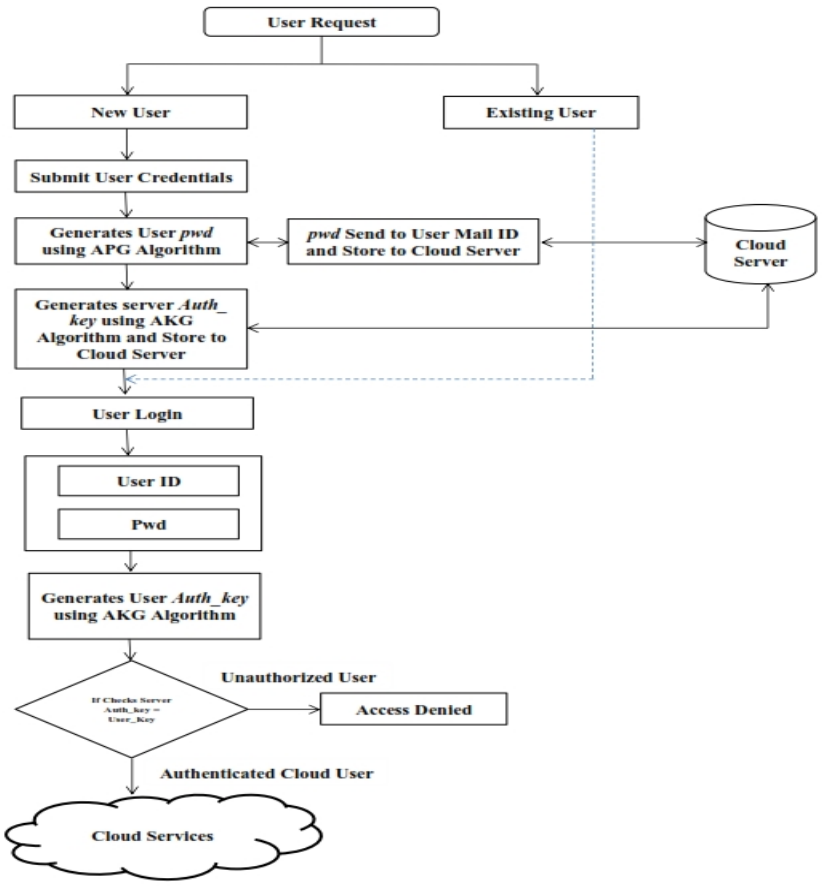


Figure 1. User Identity based Authentication as a Service (UIDAaaS).

5. Authentication Algorithms

User Identity based Authentication as a Service (UIDAaaS) includes three algorithms, such as:

- Authentication Password Generation (APG)
- Authentication Key Generation (AKG)
- Authentication Verification (Auth_V)

APG and AKG algorithms are proposed for the use of authentication process for cloud computing respectively. AKG is a key generation algorithm, is also provisioned from cloud service. APG sends the password to the CU's (Cloud User) registered mail account. With help of username and password, CU is able to access any services from CSP. After the verification, CU may change the password according to his favour. The proposed authentication algorithm is provided like a separate Authentication as a Service (AaaS) from a CSP.

5.1 Authentication Password Generation (APG) Algorithm

APG algorithm is used to generate authentication password. This password includes only the numeric values and special characters. The digested values consider as an input of APG algorithm, which is taken from user credentials. This digested value is converted into password using the various processes. Pseudo code of APG algorithm is presented below.

Declaration

PT← Plaintext
N← Size of PT
AS← ASCII codes of PT
BNY← Binary code for AC
BIT_BUF← Buffer Variable to append the binaries
XOR_PT← XOR value of PT_1 and PT_2
L← Number of 8bits binary
DIV← 8bits Binary
DECI←Decimal value of 8bits binary
PWD_BUFF← Buffer Variable to append the decimal values
AUTH_PWD ←Password
start
PT← Digested value from User_Inputs
N←sizeof(PT) // method to find the size of the PT
for i← 1 to N
AS[i]← ASCII(PT[i]) //method to convert into ASCII
BNY[i]←BINARY(AS[i]) //method to convert into 8 bits binary
BITS_BUF←APPEND(BNY[i]) // Buffer variable for combine all the binaries
next i
//Split the BITS_BUF into two blocks PT_1 and PT_2 by taken alternate bits in BITS_BUF
PT_1← Bits from Odd Positions
PT_2←Bits from Even Positions
Find the reverse of PT_1 and PT_2
XOR_PT← $PT_1 \oplus PT_2$
L← sizeof(XOR_PT)/8 // to find the no. of 8bits blocks
Spt=0
While(Spt<=L)
DIV[i]←SPLIT(XOR_PT, 8) //split the binaries into 8bits block
Spt++
loop
for i← 1 to L
DECI[i]←DECIMAL(DIV[i]) //convert the 8bits into decimal
PWD_BUFF← APPEND(ASCII(DECI[i]))
next i
AUTH_PWD← PWD_BUFF
End

5.2 Authentication Key Generation (AKG) Algorithm

AKG algorithm is used to generate the server Auth_key and user Auth_key. Both keys are store in the cloud server in encrypted format. These keys are used to verify the user identity during the login process. If the both keys are matched, then user is authenticated. Pseudo code of AKG algorithm is presented below.

Declaration

PT← Plaintext
AS← ASCII codes of PT
BNY← Binary code for AC
BIT_BUF← Buffer Variable to append the binaries
OR_PT← OR value of PT_1 and PT_2
NOT_PT← NOT value of OR_PT
L← Number of 8bits binary
DIV← 8bits Binary
BIT_ADD← Addition of 8bits each
DECI←Decimal value of 8bits binary
AUTH_KEY ← Authentication Key

```
start
PT← User_Name + AUTH_PWD
for i← 1 to N
  AS[i]← ASCII(PT[i]) //method to convert into ASCII
  BNY[i]←BINARY(AS[i]) //method to convert into 8bits binary
  BITS_BUF←APPEND(BNY[i]) // Buffer variable for combine all the binaries
next i
//Split the BITS_BUF into two blocks PT1 and PT2 by taken alternate bits in BITS_BUF
PT1← Bits from Odd Positions
PT2←Bits from Even Positions
OR_PT← PT1 | PT2
NOT_PT←!OR_PT
L← sizeof(NOT_PT)/8 // to find the no.of 8bits blocks
Spt=0
While(Spt<=L)
  DIV[i]←SPLIT(NOT_PT, 8) //split the binaries into 8bits block
  Spt++
    loop
for i← 1 to L
    BIT_ADD=BIT_ADD +DIV[i]
    next i
DECI←DECIMAL(BIT_ADD) // convert the 8bits into decimal
AUTH_KEY← DECI
End
```

5.3 Authentication Verification (Auth_V) Algorithm

Auth_V algorithm is used to verify the server Auth_key and user Auth_key. If these keys are matched, CSP allowed to access the services otherwise, user unable to access the services. Pseudo code of Auth_V algorithm is presented below.

1. *start*
2. *USR_AUTH_KEY ← call auth_key(User_Name, PWD)*
   //AUTH_KEY registered in UIDaaS
3. *If (USR_AUTH_KEY ==AUTH_KEY)*
   Users are Granted Permission to access cloud services
   else
   Users are not Granted Permission to access cloud services
4. *end if*
5. *End*

6. Experimental Results

6.1 Authentication Password Generation (APG) Algorithm

The proposed Authentication Password Generation (APG) is developed in .NET and deployed in windows azure platform. The APG efficiently produces the cipher for given digest values.

Step 1 → Get specified characters (maximum of 16characters - using message digest) from the user input as plaintext

Plaintext is "an11829894915046"

Therefore PT = an11829894915046

Step 2 → Converts PT into corresponding ASCII code

ASCII code values PT of ASCII code =

97	110	49	49	56	50	57
56	57	52	57	49	53	48
52	54					

Step 3 → ASCII codes are converted into binary bit block 0s' and 1s'

01100001011011100011000100110001001110000011001 00011100100111000001110010011010 00111001 00110 00100110101001100000011010000110110

Step 4 → Split the binaries bit block into two by take alternate bits in the block (odd and even position)

P1 denoted odd position of binaries bit

P2 denoted even position of binaries bit

P1 → 0100011101000100011001010110011001100100011 00100010001000100101

P2 → 1001101001010101010001000101010001010110010 10101011101000110011 0

Step 5 → Find the reverse of each block (such P1 and P2)

After reversing the P1 and P2 blocks are

P1 → 1010001000100010001001100010011001100110101 00110001000101110001 0

P2 → 0110011000101110101010100110101000101010001 00010101010100101100 1

Step 6 → Find the XOR of those two blocks such as P1 and P2

P1 ⊕ P2 →1100010000001100100011000100110001001100 01000010010001000101110 11

Step 7 → Now, divide the blocks into 8 bits order

11000100000011001000110001001100010011001000010 01000100010111011

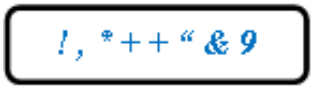
Step 8 → These each binary block are converted into decimal values

DEC = 196 12 140 76 76 132 136 187

→ Find which values are above 96 and below 32 and do the process of conversion After completion of the operations the final decimal values are,

33 44 42 43 43 34 38 57

Step 9 → Now, decimal values are converted into ASCII characters



The above ASCII characters are called Cipher Text of the PGA. This will be send to the Cloud User's (CU) registered mail account and using this password, the CU can login into the Cloud Service.

6.2 Authentication Key Generation (AKG) Algorithm

The proposed Authentication Key Generation (AKG) is developed and deployed in windows azure platform. The AKG efficiently produces the cipher for given digest values.

Step 1 → Given sample text as, and the given original text are converted into ASCII code

Sample text: veeraLL$

ASCII Code: 118 101 101 114 097 076 076 036

Step 2 → ASCII codes are converted into binary values 0s' and 1s'

01110110 01100101 01100101 01110010
0110000101001100 01001100 00100100

Step 3 → Split the bit block into two by take alternate bits in the original text

PT1→01010100010001010100001000100100
PT2→11101011101111001001101010100010

Step 4 → Find OR operation for this two blocks of bits

OR_PT→ 11111111111111011101101010100110

Step 5 → Find the NOT operation after OR operation

NOT_PT→ 00000000000000100010010101011001

Step 6 → Get a Key K from KG and perform XOR operation

Step 7→ Divide the block into 8bits

00000000000000100010010101011001

Step 8 → Add each 8bits into others 8bits binary

Step 9 → Now, Get single 8bits binary

Step 10 → Convert the 8bits binary into decimal 10000000 Decimal Value (DECI) → 128

Step 11 → Convert the decimal into ASCII character code to produce the Authentication key

The above authentication key is used to verify the legitimation of the cloud user (CU). If CU is an authorized person, he is allowed to access the Cloud service. Otherwise, his access to the cloud server is denied.

7. Advantages of Proposed UIDAaaS Authentication Mechanism

- UIDAaaS provides Authentication as a Service (AaaS) to cloud users.
- It reduces the time taken for Authentication process in cloud environment.
- It protects different attacks on authentication like Man-in-the-Middle and DoS (Denial of Service)
- The password consists of only numeric values and special characters.
- Authentication key size is a single character, so, it reduces the memory size of the data and stores it. Any unauthorized person could not find the original key which is generated by the AKG algorithm.

8. Conclusion

Cloud computing is a technology with rapid development. However, the security problem has become an obstacle for the popularity of cloud computing. Authentication is the most essential factor in cloud security. In this paper, a UIDAaaS (User Identity based Authentication as a Service) is proposed to ensure high security in the cloud for secure authentication. APG is used to generate the password and sent to the cloud users' registered mail account. This password includes only the numeric values and special characters. AKG is used to generate the authentication key which can be used to verify the user during the login process. The final key value has single character and has generated and stored in the cloud server. And also it reduces the size of the cloud storage. Auth_V is used to verify whether the user is a legitimate user. If the authentication key value is matched, then the legitimate users can access the data in cloud environment.

9. References

1. Kumar S, Ganapati A. Multi-authentication for cloud security: A Framework. International Journal of Computer Science and Engineering Technology. 2014 Apr; 5(4):295–303.
2. Lee S, Kim TY, Lee HJ. Mutual authentication scheme for cloud computing. Future Information Communication Technology and Applications. 2013; 235:149–57.
3. Jiang R. Advanced secure user authentication framework for cloud computing. International Journal of Smart Sensing and Intelligent Systems. 2013 Sep; 6(4):1700–24.
4. Banyal RK, Jain P, Jain VK. Multi-factor authentication framework for cloud computing. Fifth International Conference on Computational Intelligence, Modelling and Simulation, Seoul; 2013. p. 105–10.
5. Yu J, Wang G, Mu Y, Gao W. An efficient generic framework for three-factor authentication with provably secure instantiation. IEEE Transactions on Information Forensics and Security. 2014; 9(12):1–12.
6. Chen N, Jiang R. Security analysis and improvement of user authentication framework for cloud computing. Journal of Networks. 2014 Jan; 9(1):198–203.
7. Soni P, Sahoo M. Multi-factor authentication security framework in cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering. 2015 Jan; 5(1):1065–71.
8. Sadqi Y, Asimi A, Asimi Y. A cryptographic mutual authentication scheme for web applications. International Journal of Network Security and its Applications. 2014 Nov; 6(6):1–15.
9. Kataria S, Syal R. Secure mutual authentication for cloud environment. International Journal of Computer Science Engineering and Technology. 2015 Jul; 5(7):214–18.
10. Yassin A, Neima HZ, Abduljabbar ZA, Hashim HS. Efficient and secure mutual authentication scheme in cloud computing. International Journal of Engineering and Advanced Technology. 2013 Oct: 3(1):133–9.
11. Nagaraju S, Parthiban L. SecAuthn: Provably secure multi-factor authentication for the cloud computing system. Indian Journal of Science and Technology. 2016 Mar; 9(9):1–18. DOI: 10.17485/ijst/2016/v9i9/81070.
12. Reddy VK, Sushmitha Y, Rao KT. Distributed authentication for federated clouds in secure cloud data storage. Indian Journal of Science and Technology. 2016 May; 9(19):1–7. DOI: 10.17485/ijst/2016/v9i19/90646.
13. Kumar DG, Rajasekaran S, Prabu R. PB verification and authentication for server using multi communication. Indian Journal of Science and Technology. 2016 Feb; 9(5):1–6. DOI: 10.17485/ijst/2016/v9i5/87154.