OTP CRYPTOGRAPHY INTEGRATION WITH CLOUD

VARUN MITTAL[1], SHIVAM ADITYA[2]

[1]VIT UNIVERSITY,
VELLORE, TAMIL NADU
varun.mittal2011@vit.ac.in

[2]VIT UNIVERSITY,
VELLORE, TAMIL NADU
sa.shivam.aditya@gmail.com

Abstract: Cloud computing has proven to be one of the rapidly-growing technologies of and completely revolutionized the IT industry completely. The cloud has the participation of many parties and resources communicating with each other which makes security quite a major issue. oPass can be treated as a cloud because it involves a no. of online participating websites which all should possesses a unique phone number. and as we know all the websites accessible via the internet are acting like an open source cloud which raises the importance of feature essential for any online facility i.e. Security which includes user authentication requirements. We have use one time password in the oPass architecture system as a means of user authentication. In this paper the method for providing means to use OTP in an oPass cloud computing environment via identity management security protocol.

Keywords: oPass, OTP, Cloud, RSA Authentication, Diffie-Hellman, Identity.

1 Introduction

Cloud computing is defined as the delivery of computing power as service rather than treating it as a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet) (Wikipedia 2002).National Institute of Standards and Technology (NIST) propose that cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing has the following five essential features (1) On demand self-service , (2) Broad network access , (3) Rapid Elasticity , (4) Resource Pooling, (5) Measured Service . It has also several advantages like (1)

Data Fragmentation and Dispersal ,(2) Dedicated Security Team , (3) Greater Investment in Security Infrastructure ,(4) Fault Tolerance and Reliability, (5) Greater Resiliency, (6) Hypervisor Protection Against Network Attacks, (7) Possible Reduction of C&A Activities (Access to Pre-Accredited Clouds), (8) Simplification of Compliance Analysis,(9) Data Held by Unbiased Party (cloud vendor assertion), (10) Low-Cost Disaster Recovery and Data Storage Solution, (11) On-Demand Security Controls, (12) Real-Time Detection of System Tampering, (13) Rapid Re-Constitution of Services (Saqib 2009)

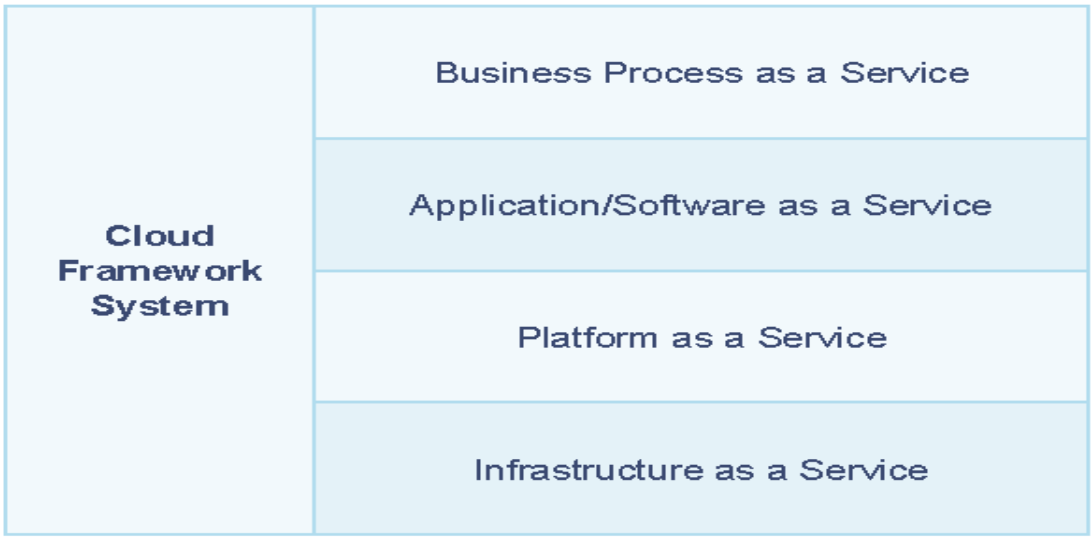


Figure 1. Cloud Computing Framework

Cloud uses three service models namely, (Software as a Service), PaaS (Platform as a service), IaaS (Infrastructure as a service as shown in fig 1.

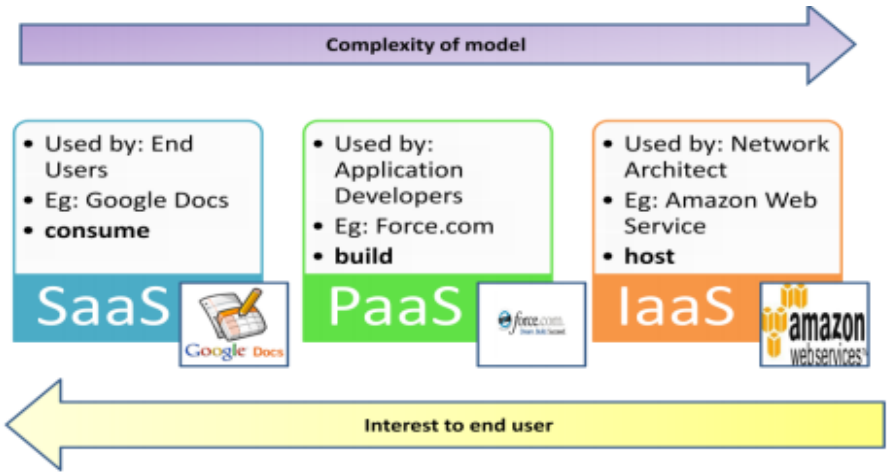
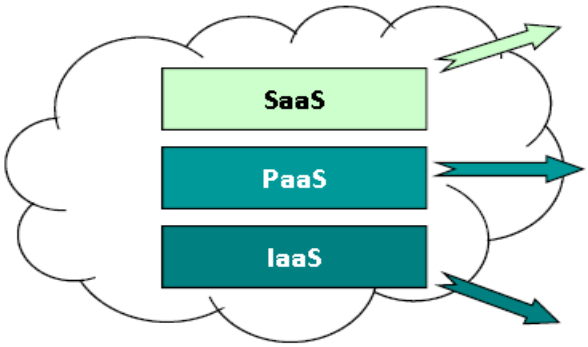


Figure 2. Cloud Service Layers

Saas contains applications (word processor, CRM, etc.) or application services (schedule, calendar, etc.) execute in the "cloud" using the interconnectivity of the internet to propagate data(Govinda 2005). PaaS model of cloud computing is used mostly by application developers, who use the platform from cloud as a service to develop, test, debug and deploy their applications. It is basically a middleware for developers. IaaS includes providing computing resources (processors, memory, storage, bandwidth, etc.) as in an as-needed, pay-as-you-go model. IaaS model is used by network analysts who create new opportunities such as cloud bursting: shifting usage spike traffic to alternate resources. (Govinda 2005)



Who Uses It	What Services are available	Why use it?
Business Users	EMail, Office Automation, CRM, Website Testing, Wiki, Blog, Virtual Desktop ...	To complete business tasks
Developers and Deployers	Service and application test, development, integration and deployment	Create or deploy applications and services for users
System Managers	Virtual machines, operating systems, message queues, networks, storage, CPU, memory, backup services	Create platforms for service and application test, development, integration and deployment

Figure 3. Different Types of Cloud Users

In general pay per use payment model is followed here. The end user is generally interested only in SaaS. The data is consumed as well as produced by the cloud. This data is used by cloud computing systems and client computing systems as well(Lintchicum 2009) .

Passwords are used by almost all business applications for authentication. However static passwords have lots of limitations e.g. passwords can get hacked; careless employee may write down passwords somewhere; system with saved passwords may be used by various users or a malicious user may reset all passwords just to create havoc. Hence it is advisable to move to a more dynamic password scheme like one time passwords or OTP. OTP are way more secure than static passwords as there are no chances to forget or reuse passwords. Each time a new password is generated for each login session. Authentication by one time passwords are more reliable and user friendly as well. OTP generation can be done by various OTP generation algorithms for generating strings of passwords. (Mittal 2014)

A onetime password (OTP) is just what the names implies, a password that is only valid for one login. The benefit of OTPs is that it offers much higher security than static passwords, in expense of user friendliness and configuration issues. OTPs is immune against password sniffing attacks, i.e. if an attacker use software to collect your data traffic, video records you when you type on your keyboard, or use social engineering, it doesn't matter since the password that the attacker gets hold on will not be valid to use. The advantages (Verma 2012) of OTP are

(i) **Dynamism**- The dynamic passwords are generated with the dynamic factor so that the generated dynamic .Password varies according to that factor.

(ii) **Randomization**-Dynamic passwords are generated randomly.

(iii) **One-time Usability**- A dynamic password can be used only once after that it will not be valid.

(iv) **Anti-theft Capability**-Dynamic passwords are anti-theft because of its one-time usability and randomization feature

Time-Based OTPs In the time-based method, a device with an internal clock generates passwords that are depending on the current time. For example, every minute a new password is generated in the device, and the same password is generated at the authentication server. When the user wants to login to a service or system, the current OTP that is displayed on the device is used.

oPass (Sun 2012) is a user authentication protocol that leverages a user's cell phone and short message service (SMS) to prevent password stealing and password reuse attacks. The main objective of oPass is to free users from having to remember or type any passwords into conventional computers for authentication. Unlike generic user authentication, oPass involves a new component, the cell phone, which is used to generate one-time passwords and a new communication channel, SMS, which is used to transmit authentication messages. oPass works on the principle of generating time based OTP for client and generating 'trial' for server side.

OTP should be used in cloud computing (Das 2013) because of the following reasons:-

- Provides better password solution for login procedures than the insecure method of static passwords.
- Provides better two-factor OTP authentication solution than those discussed above.
- Has an easy-to-understand registration system, which at the same time doesn't compromise the security.

- Uses an encryption algorithm that is secure but also fast, to be able to serve the vast amount of cloud users.
- Offers a solution that is free of charge in order to attract more customers to the cloud services.
- The security solution for cloud services must be easy to use, but also be very secure in order to protect the customer's data and gain the trust of the customers.

Cryptography (Acharya 2013) is a process which is associated with scrambling plaintext (ordinary text, or clear text) into cipher text (a process called encryption), then back again to plain text (known as decryption). The key feature of asymmetric cryptography system is encryption and decryption procedure are done with two different keys - public key and private key. Private Key cannot be derived with help of public key that provides much strength to security of cryptography.

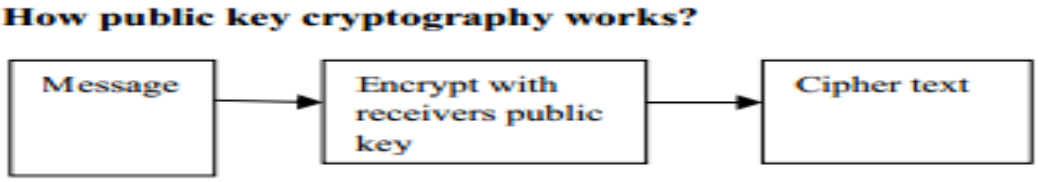


Figure 4. At sender's end

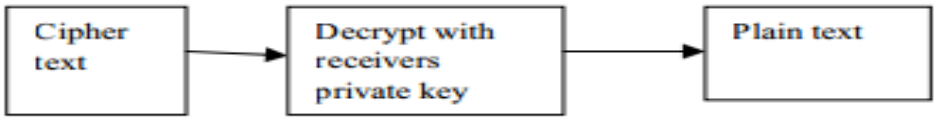


Figure 5. At receiver's end

To utilize the services of service providers (SPs), entities (e.g., users, services) have to authenticate themselves to SP's in order to utilise their services. The Personally identifiable information (PII) uniquely identifies the entities to an SP. In the traditionally used, application-centric Identity Management (IDM) model, each and every application keeps track of all the identities of the entities that utilise it. In cloud computing model, entities might have multiple accounts linked with different SPs, or one SP. Sharing of PIIs of the same entity across services along with their associated attributes can result in mapping of PIIs to the entity.

Privacy of a person means that the person is free from all the interferences. Privacy control permits the individual to preserve a degree of familiarity. Privacy is the safety measure for the truthful usage of private information of the cloud user. Privacy holes might create lots of troubles to the cloud users.

The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Charted Accountants (CICA) define that, *"Privacy is the right and obligation of individuals and organizations with respect to the collection, use, retention, and disclosure of personal information"*.

3rd party cloud service providers are private and hold their own virtualization infrastructure. In this several virtual machines are hosted in order to provide services to the clients. On the other hand, the InterCloud is a new perspective of cloud computing technology where clouds can cooperate with other associated ones with the goal to enlarge their computing and storage capabilities (Chowdhary 2013). Such a perspective opens various new scientific challenges, which may include federation, security and privacy. Identity Management (IdM) represents the first matter to be resolved in order to achieve the verification among heterogeneous clouds which establish the federation. Such task is not at all considered trivial, because it requires a high level of interoperability between diverse security technologies. As a matter of fact, each cloud service could hold a different authentication and IdM mechanisms making it to be different from each other. Furthermore, in order to achieve IdM in cloud computing, a crucial prerequisite is setting up of a trusted third party who is responsible for both storing and securing the access credentials.

1.1 RSA Algorithm

In 1978, Ron Rivest, Adi Shamir, and Leonard Adleman introduced a cryptographic algorithm, which was essentially to replace the less secure National Bureau of Standards (NBS) algorithm. Most importantly, RSA implements a public-key cryptosystem, as well as digital signatures. RSA is motivated by the published

works of Diffie and Hellman from several years before, who described the idea of such an algorithm, but never truly developed it. RSA uses a variable size encryption block and a variable size key . The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes may be 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors.

RSA (Kahate (2003),Stallings (2005)) algorithm:

1. Select two different prime numbers p and q
For security aim, the integer's p and q must be large.
2. Calculate

$$n=p*q. \quad (1)$$

n will be used as the module for public key and private key.
3. Calculate

$$f(n) = (q-1)(p-1). \quad (2)$$

Where f is a function of Euler's
4. Select an integer e such that 1<e<f (n) and e and f (n) are co-prime. Calculate

$$GCD(e, f(n)) = 1. \quad (3)$$

5. Determine d: d is multiplicative inverse of

$$e \bmod (f(n))\ (e * d) \bmod f(n) = 1 \quad (4)$$

Where d is the private key.

.Encryption:
M is plain text data.

$$C=M^e \bmod n. \quad (5)$$

Decryption:

C is received cipher text.

$$M=C^d \bmod n. \quad (6)$$

1.2 Diffie–Hellman key exchange (D–H)

This is a specific way of exchanging cryptographic keys. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. (Wikipedia, 2002)

Table 1: Notations

Name	Description
C	A random no. used to calculate OTP
$h(.)$	Hash function
N	Hash Length Chain
δ_i	One time Password
ID_s	4-digit pin code
P_u	Master Password
ϕ	Init secret entered by the user

2 Literature Survey

H.M.Sun (Sun 2012) offers oPass based on two main components: the cloud environment and the Time-Based OTPs. Cloud platforms are offered by the Cloud service providers (CSP's) for their customers to use and create their web services, much like internet service providers offer costumers high speed broadband to access the internet .Time-Based OTPs In the time-based method, a device with an internal clock generates passwords that are depending on the current time. Cryptanalysis of oPass (Mittal, 2014) helps in identifying the major issues in oPass mechanism use of SMS service, use of Communication Links etc.

Security issues in cloud environment like user identity (Kavitha 2011), physical security (Pranjape 2013), availability (Alazin 2012), compliance(Reddy 2011), governance etc. Mobile Security (Das 2013) also uses a similar system to the one presented in this paper but it is based on the system of image processing and generating optical images as a server based trial for user authentication and suffers from intrinsic attacks. Gemalto Security Systems Pvt. Ltd also suggested the need for providing authentication (Gemalto 2014) in cloud computing. Vishal Paranjape (Pranjape 2013)proposed an experimental setup which I have incorporated into my proposed system. Sagar Acharaya (Acharya 2013) also proposed a system for providing authentication by using smartphones based on Android Operating System that generates one time password offline and later on connects to the cloud server. Geetanjali Choudhury(Choudhry 2014) presented a method based on authenticating OTP by further providing it security by encryption of OTP into public key cryptography by using RSA algorithm. Veri-Sign (Choudhry 2014) , an IT company has presented a method to incorporate cloud based OTP service in their security solutions by using RSA Secure ID in their VIP(VeriSign 2010) (VeriSign Identity Protection (VIP) Authentication Service).William Stallings (Stallings 2005) provide the information about RSA cryptography which is being used in my proposed methodology.

3 Proposed Method

Many identity based privacy preservation issues can be identified that everybody should focus their attention on in the cloud computing environment: The first and foremost issue is the revelation of thin-skinned private information when exchanging data occurs between the cloud service inside the cloud environment and these thin-skinned personal information include: Personally identifiable information, Usage data, Unique device identities and so on. The next visible issue is that people getting unsuitable or unofficial access to personal data in the cloud by taking benefit of certain vulnerabilities, such as lack of access control enforcement, security holes and so on .The third problem is because the attribute of cloud computing is that it is a highly dynamic upbringing, In that service communications can be created in a more self-motivated way than traditional e-commerce scenarios. Services can potentially be aggregated and changed dynamically by service providers can revolutionize the provisioning of services. In such scenarios, private sensitive data may move around within an association or across governmental restrictions, so tolerable fortification of this information must be maintained even though there are changes(Bleikertz 2010). So design the method to protect the privacy in cloud computing must meet the dynamical exchange of data.

As it is already known the authentication method used is two-factor authentication with a one-time password in Opass .The same technique has been modified a bit slightly and is to be used in the login phase of oPass. The experimental setup of implementation (Kavitha 2011) of two factor authentication is done using the concept of Mobile OTP to access the private cloud. The proposed method has been implemented and tested by using the components given below.

3.1 Cloud Server Installation

(i) Server
(a) **Hardware Configuration**-Intel® Core™2 Duo processor
4 GBHard Disk , 4 GB RAM
(b) **Operating System**-Ubuntu 11.04
(c) **Software Recommended**-
1. Lamp Server (Linux, Apache, PHP, MySQL server)
2. CURL
3. Kaazing Gateway
4. ActiveMQ Daemon

(ii) **LAMP Server**-is a collection of open source software used to create a web server. The collection consists of Linux – the operating system, Apache server – the server, MySQL – the database system, PHP – the programming language.
(iii) **Mobile Specification**-Text Field-input for compatibility with modern touch screen and QWERTY smart phones (down to the simplest J2ME capable phones like the Nokia 6210) usage

3.2 Methodology

The user's mobile phone will work as the authentication device, in which a 4-digit PIN code has to be entered by the user for generating an OTP that can be used for login. This process is executed by launching a Java-application on the phone. The OTP generated by the Java-application on the mobile phone is based on three components which will be hashed together with SHA-256:

• The 4-digit PIN code that the user enter.
• A secret random number that was created during device-initialization (In-secret) using a pseudo-random number generator that only exists on the user's mobile device.
• The current time

After hashing, the mobile phone will display the first six numbers of the hash that will be used as the OTP for login. Since time is part of the hash, the OTP is only valid for two minutes and the user will have to redo the entire process again. The OTP will then be sent to the server during login. The server knows the In-secret and the pin-code that is stored in a database, and also the current time. Therefore the password can be verified by the server. The customer before entering the generated OTP login will get a trial (a text string, image random number etc.) from the authentication server that must be entered into the authentication device.

In our method the two factor authentication process is done via a 3rd party cloud service provider who preserves our privacy and maintains data security and integrity.

Figure 6. Proposed System Architecture

Whenever the communication is established between the user and the 3rd party cloud service provider or the 3rd party cloud service provider to the server, the system follows a simple protocol explained below.

1. The first phase of the protocol is the key generation and distribution phase. This phase starts with the sharing of user details with the 3rd party cloud service provider and then the user and the 3rd party cloud service provider share a unique key among themselves using the Diffie-Hellman Algorithm. This key will help the 3rd party cloud service provider to identify the user. In the same method the 3rd party cloud service provider and the server share a secret id of authentication between them using the same DH Algorithm (Khiva 2013).

The current phase further continues by key set generation with respect to RSA encryption. The user and the server will generate their own public key as well as the private key set. Now the User and the 3rd party cloud service provider share the public key and the same occurs at the other end for 3rd party cloud service provider and the server.

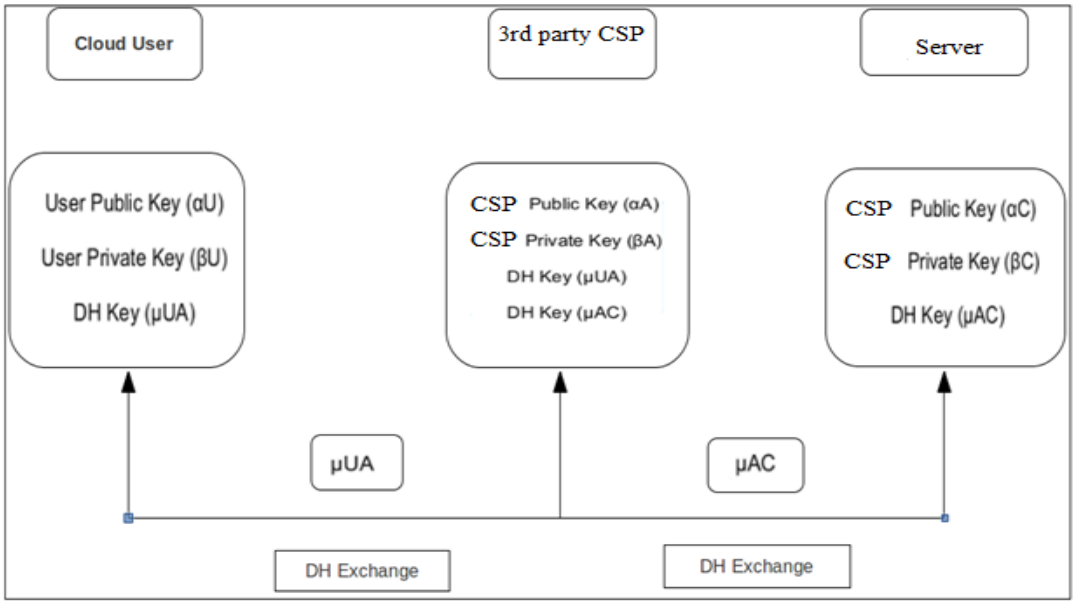


Figure 7: Keys exchanged in the Proposed System

The scenario shows how the method is used in the login phase of the Opass (Mittal,2014).

1. A client wishes to log in to a personal account through a web browser on an untrusted kiosk and surfs to the login page.

2. At the login page, a trial is presented to the client. This can be a text string, image, a random number etc. This will ensure that the user is not a machine.
3. The client enters the trial into an authentication device, and then the personal code into the same device.

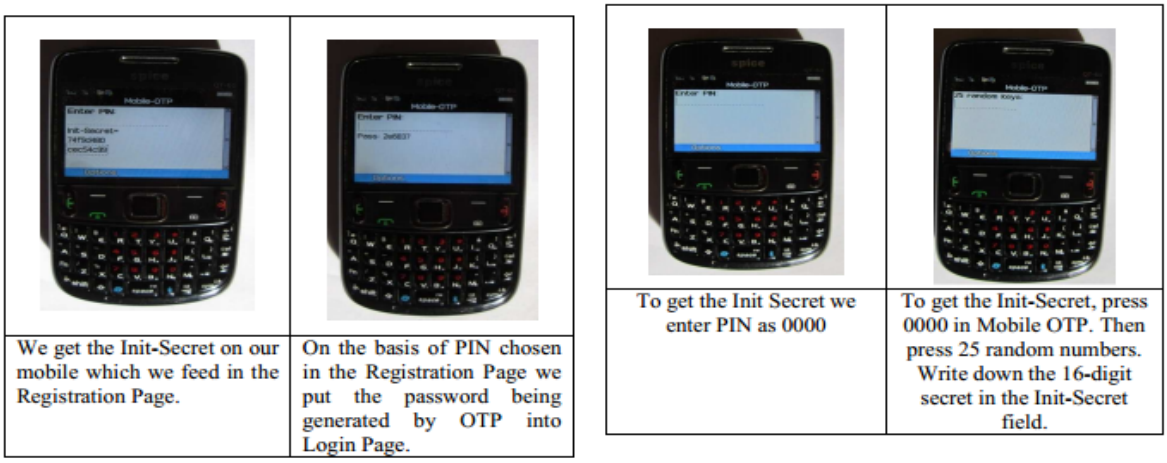


Figure 8. Init-secret generation

4. From these two values, an OTP is generated, based on an algorithm as shown below

$$c=h(P_u||ID_s||\phi) \tag{7}$$

$$\delta_i=h^{N-i}(c) \tag{8}$$

Where P_u is the master password for unlocking the phone, ID_s is the 4-digit PIN code and ϕ is the secret random number created during device initialisation and then the hashing takes place to generate the OTP presented to the client. Often time or a counter is also added to the algorithm to count the time between the OTP comes into existence and then terminates.

5. The client enters the OTP and sends it over the Internet to the server for authentication and verification via 3rd party cloud service provider. The user then has to encrypt his OTP with server's public key using RSA algorithm .He also computes the message digest for the ID using the MD5 algorithm and encrypts the signed ID using 3rd party cloud service provider's public key. This package is now sent to the 3rd cloud service provider.

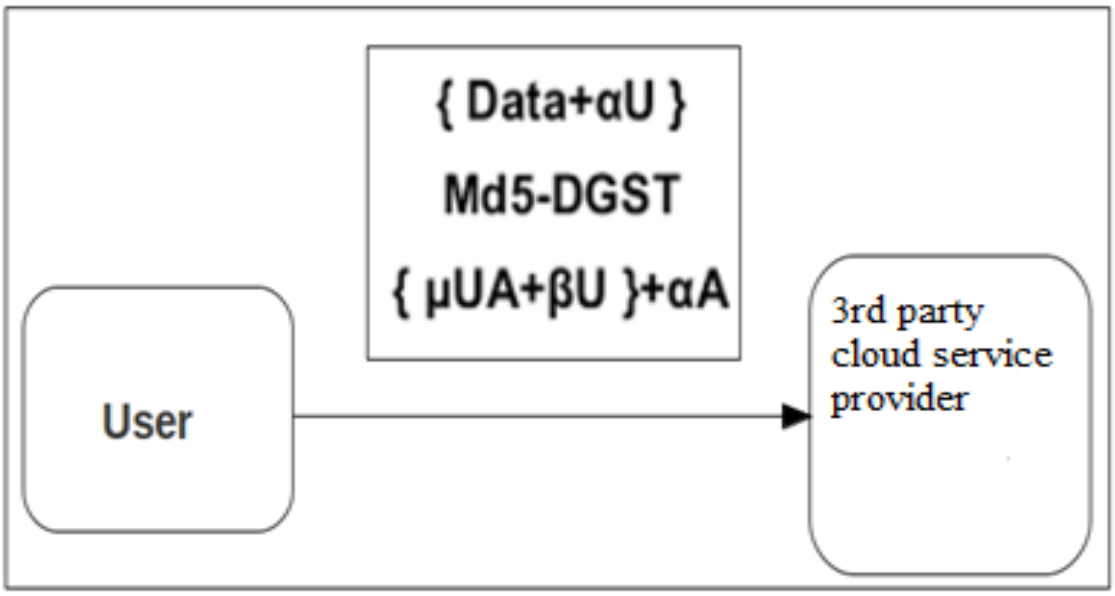


Figure 9. User sends OTP to 3rd party cloud service provider

6. The 3rd party cloud service provider now receives the package. He removes the attachment and decrypts the attachment and then un-signs with the user's public key in order to recognize the user with the ID and sends it to the server. Then the server gets the encrypted OTP from the user via the 3rd party cloud service provider and decrypts it with their own private key and store it in their database and match it to authenticate the user. Then server generate a random password (OTP) and encrypt it with users public key using RSA algorithm which is stored in database and send the OTP to user via 3rd party cloud service provider and the above same process repeats again. User will decrypt the encrypted one time password (EOTP) with their private key and match it to original generated OTP and if it matches, server is authenticated.

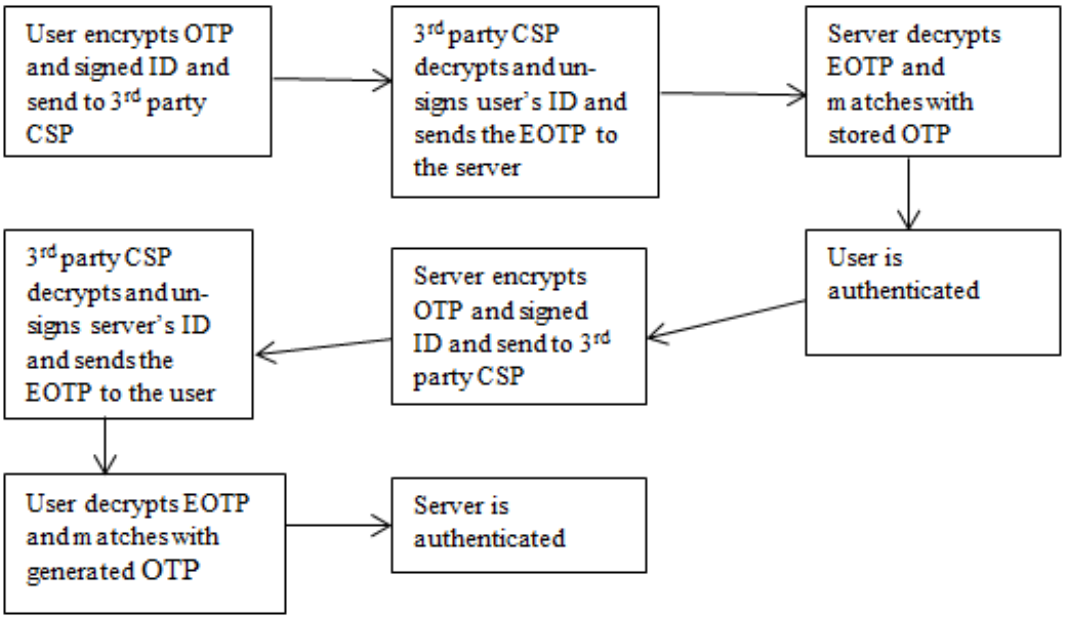


Figure 10. Process Flow

Advantages of the proposed system over conventional systems are:-

- Proposed system is highly secure based on key size.
- Proposed system is more efficient.as the only crucial information sent over the network will be the username and the OTP. Since the OTP is only valid for one time during a period of three minutes it will be of no value for an attacker.
- The OTP needs a private PIN code to be generated on the mobile phone, a PIN code that only the user knows.
- Since the user only has to use his mobile phone for the entire process, there is no need for additional authentication devices.

4 Conclusion

The above method has been employed by various types of companies. Facebook has recently launched a service where you can get an OTP sent to your mobile device Google Apps started with two factor authentication for some of its users and Amazon Web Services offers a time-based OTP solution in order to increase the security for its users. E-commerce and E-banking sectors have also found the proposed system to be useful. The implementation aspect of this prototype shows that the proposal is reasonable. There are plenty of freely available technologies and components based on open standards that support this implementation.

5 Future Work

Future developments include a user friendly GUI and extending the encrypted OTP algorithm so that system become more secure. Moreover the communication process can be improved by using Secure Sockets Layer Tunnel and 3G connection to improve the transfer rates of OTP between client and server and to improve privacy, confidentiality and integrity of the OTP.

6 References

K Govinda (2005), VIT UNIVERSITY Retrieved May 31, 2014 from VIT University website: http://academics.vit.ac.in/cloudcomputing.pdf

RSAandVeriSign(2010),http://webcache.googleusercontent.com/search?q=cache:http://www.channelinsider.com/c/a/Cloud-Computing/RSA-and-VeriSign-Partner-on-CloudBased-OTP-Service-146773

Saqib Ali(September6,2009*) IBM Developer Works*,
(https://www.ibm.com/developerworks/community/blogs/CloudComputing/entry/nist_s_definition_of_cloud_computing_what_is_cloud_computing?) Retrieved June 19,2009 from http://www.nist.gov/itl/cloud/

Security Gemalto (2010),http://www.gemalto.com/techno/downloads/otp_cloud_computing.pdf

Wikipedia(2002), http://en.wikipedia.org/wiki/Cloud_computing

Wikipedia(2002), http://en.wikipedia.org/wiki/DiffieHellman_key_exchange

Acharya Sagar, Polawar Apoorva, Pawar P.Y. (2013) : Two Factor Authentication Using Smartphone Generated One Time Password *IOSR Journal of Computer Engineering* (IOSR-JCE) Volume 11, Issue 2, pp. 85-90 e-ISSN: 2278-0661, p- ISSN: 2278-8727

Alzain M.A, Pardede E., Soh B., Thom J.A(2012).: "Cloud Computing Security: From Single To Multi Clouds", *45th Hawaii International Conference on System Sciences*.

Bleikertz Soren(2010) et al, "Security Audits of Multi-tier Virtual Infrastructures in Public Infrastructure Clouds", Chicago, USA. *ACM workshop on Cloud computing security workshop,* CCSW

Choudhury Geetanjali (2014).: Modified Secure Two Way Authentication System in Cloud Computing Using Encrypted One Time Password, . *International Journal of Computer Science and Information Technologies*, Vol. 5 Issue-3, pp. 4077-4080

Chowdhary Richa , Rawat Satyakshma (2013) One Time Password for Multi-Cloud Environment *International Journal of Advanced Research in Computer Science and Software Engineering* Volume 3, Issue 3,

Chhabra Randeep Kaur ,Verma Ashok(2012): Strong authentication system along with virtual private network: A secure cloud solution for cloud computing, *International Journal of Electronics and Computer Science Engineering* Volume1 Number3 pp.1566-1573 ISSN- 2277-1956

Das Indrajit , Das Ria(2013): Mobile Security (OTP) by Cloud Computing *International Journal of Information and Education Technology* (IJIET) Volume 2 Issue no. 4 pp.284-290 ISSN 2319-1058

Khiva Navdeep Kaur , Sharma Sandeep (2013): Secure Cloud Architecture for Preserving Privacy in Cloud Computing using OTP/WTP, *International Journal of Computer Applications* (0975 – 8887) Volume 13, Issue-.3, Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Mittal Varun , Aditya Shivam: Cryptanalysis of oPass *IEEE International Conference on Advanced Communication, Control and Computing Technologies* pp. 1945-1950. ISBN No. 978-1-4799-3914-5 (2014)

Paranjape Vishal , Pandey Vimmi(2013) An Improved Authentication Technique with OTP in Cloud Computing ,*International Scientific Research Organization for Science, Engineering and Technology* (ISROSET) Vol-1, Issue-3 pp.22-26 E-ISSN: 2320-7639

Reddy V.Krishna , B. Thirumal Rao, Dr. L.S.S. Reddy, P.Sai Kiran (2011)"Research Issues in Cloud Computing " *Global Journal of Computer Science and Technology*, Volume 11, Issue 11,

Sun Hun-Ming, Chen Yao-Hsin and Lin Yue-Hsun oPass (2012) :A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks, *IEEE Transactions on Information Forensics and Security* 7(2) 651 – 663

Subashini S., Kavitha V.(2011), "A survey on security issues in service delivery models of cloud computing"; *Journal of Network and Computer Applications*, Vol. 34(1), pp 1–11, Academic Press Ltd., UK, ISSN: 1084-8045.

Kahate Atul(2003): Cryptography and Network Security ,Tata McGraw –Hill Publishing Company Limited

Linthicum D.(2009), "Selecting the right cloud," book excerpt, InfoWorld Cloud Computing Deep Dive, InfoWorld,

Stallings William,(2005)" Cryptography and Network Security Principles and Practices", Prentice Hall, New Delhi.