International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 6, October 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Secure One Time Password (OTP) Generation for user Authentication in Cloud Environment

Kyaw Swar Hlaing[1], Nay Aung Aung[2]

[1]Assistant Lecturer, Faculty of Computer System and Technology,
[1]Myanmar Institute of Information Technology, Mandalay, Myanmar
[2]Lecturer, Information Technology Support and Maintenance Department,
[2]University of Computer Studies, Mandalay, Myanmar

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. The major threat that the cloud is facing now is security. So, the user authentication is very important step in cloud environment. The traditional authentication (user name and static password or PIN code) can be easily broken by the skillful attacker. An Unauthorized user can easily enter into the system if he knows the user credentials. Encryption algorithms play a main role in information security systems. Efficient password generation for user authentication is an important problem in secure Cloud communications. In the paper, the One Time Password (OTP) approach is used to authenticate the cloud users. The generated OPT is encrypted by RSA public key encryption to be more secure for the cloud user authentication. So the third party is not required to generate OPT in the proposed paper. This paper can help to solve the user authentication problem in Cloud environment.

KEYWORDS: *Cloud computing, user authentication, password generation, OTP, RSA*

How to cite this paper: Kyaw Swar Hlaing | Nay Aung Aung "Secure One Time Password (OTP) Generation for user Authentication in Cloud Environment" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-6, October 2019, pp.89-92, URL: https://www.ijtsrd.com/papers/ijtsrd28037.pdf

IJTSRD28037

1. INTRODUCTION

Cloud computing is the communal term for a group of IT technologies which in teamwork are changing the landscape of how IT services are provided, accessed and paid for. Some of the supporting technologies have already been available for quite some time, but it is the combination of several technologies which enables a whole new way of using IT. 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, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The concept of Cloud Computing revolves around distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. 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. CSPs and ISPs (Internet Service Providers) both offer services. Cloud providers offer three types of services i.e.

1. Software as a Service (SaaS),
2. Platform as a Service (PaaS)
3. Infrastructure as a Service (IaaS)

In addition, organizations can easily meet the needs of rapidly changing markets to ensure that they are always on the leading edge for their consumers. The clients of commercial clouds rent computing power (virtual machines) or storage space (virtual space) dynamically, according to the needs of their business. With the exploit of this technology, users can access heavy applications via lightweight portable devices such as mobile phones, PCs and PDAs. There are also four different cloud deployment models namely.

1. Private cloud. The cloud infrastructure is operated for a private organization. It may be managed by the organization or a third party, and may exist on premise or off premise.
2. Community cloud. The cloud infrastructure is shared by several organizations and supports a specific community that has communal concerns. It may be managed by the organizations or a third party, and may exist on premise or off premise.
3. Public cloud. The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
4. Hybrid cloud. The cloud infrastructure is a composition of two or more clouds (private, community, or public).

2. CLOUD COMPUTING

Cloud computing is the on-demand delivery of compute power, database, storage, applications, and other IT resources via the internet with pay-as-you-go pricing. Whether you are using it to run applications that share photos to millions of mobile users or to support business critical operations, a cloud services platform provides rapid access to flexible and low cost IT resources. With cloud computing, you don't need to make large upfront investments in hardware and spend a lot of time on the heavy lifting of managing that hardware. Instead, you can provision exactly the right type and size of computing resources you need to power your newest idea or operate your IT department. You can access as many resources as you need, almost instantly, and only pay for what you use. Cloud computing gives you access to servers, storage, databases, and a broad set of application services over the Internet. A cloud services provider such as Amazon Web Services owns and maintains the network-connected hardware required for these application services, while you provision and use what you need via a web application.

3. CLOUD SOLUTION

These services are categorized into five prominent sections as follows:

1. Infrastructure as a Service (IaaS): This provides a platform virtualization environment as a service rather than purchasing servers, software, data centers etc.
2. Software as a Service (SaaS): This service deploys software over the Internet which is deployed to run behind firewall in your LAN or PC.
3. Platform as a Service (PaaS): This kind of cloud computing provide development environment as a service. You can use the middleman's (broker) equipment to develop your own program and deliver it to the user through the Internet and Servers.
4. Storage as a Service (StaaS): This is database like services billed on utility computing services basis; e.g gigabyte per month
5. Desktop as a Service (DaaS): This is the provisioning of the desktop environment either within a browser or as a terminal server

4. CRYPTOGRAPHY

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The pre-fix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing."

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy, web browsing on the internet and confidential communications such as credit card transactions and email.

4.1. Cryptographic Techniques

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption) as shown Figure 1. Individuals who practice this field are known as cryptographers.

Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

Modern cryptography concerns itself with the following four objectives:

1. Confidentiality: the information cannot be understood by anyone for whom it was unintended
2. Integrity: the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected
3. Non-repudiation: the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information
4. Authentication: the sender and receiver can confirm each other's identity and the origin/destination of the information

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

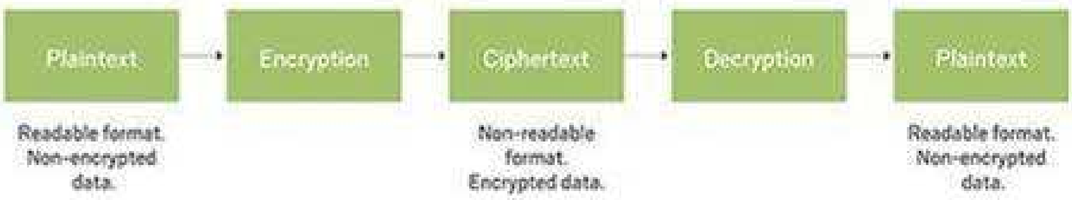
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Readable format. Non-encrypted data.
Non-readable format. Encrypted data.
Readable format. Non-encrypted data.

Figure1. Cryptography

4.2. Public Key Cryptography

Public key encryption, or public key cryptography, Figure 2, is a method of encrypting data with two different keys and making one of the keys, the public key, available for anyone to use. The other key is known as the private key. Data encrypted with the public key can only be decrypted with the private key, and data encrypted with the private key can only be decrypted with the public key. Public key encryption is also known as asymmetric encryption. It is widely used, especially for TLS/SSL, which makes HTTPS possible.

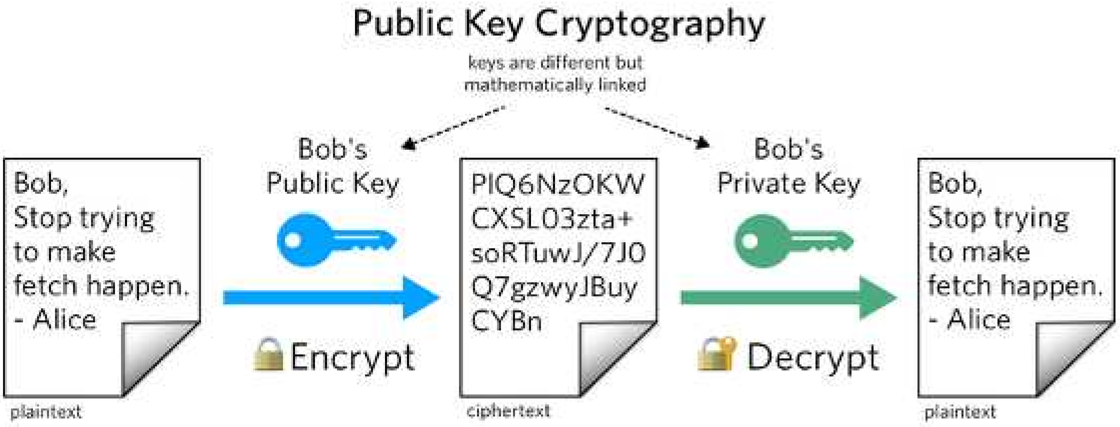
Public Key Cryptography
keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen. - Alice
plaintext
Encrypt
PIQ6NzOKW CXSL03zta+ soRTuwJ/7J0 Q7gzwyJBuy CYBn
ciphertext
Decrypt
Bob, Stop trying to make fetch happen. - Alice
plaintext

Figure2. Public Key Cryptography

5. RSA PUBLIC KEY CRYPTOGRAPHY

RSA (Rivest–Shamir–Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem". The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician working for the British intelligence agency Government Communications Headquarters (GCHQ), had developed an equivalent system in 1973, but this was not declassified until 1997.

A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but only someone with knowledge of the prime numbers can decode the message. Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem remains an open question. There are currently no published methods to defeat the system if a large enough key is used.

RSA is a relatively slow algorithm, and because of this, it is less commonly used to directly encrypt user data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

RSA Key Generation Algorithm

- Select two different prime numbers p and q for security aim, the integer's p and q must be large.
- Calculate n=p*q n will be used as the module for public key and private key.
- Calculate f(n)=(q-1)(p-1), Where f is a function of Euler's
- Select an integer e such that 1<e<f(n) and GCD (e, f(n))=1; e and f(n) are co-prime.
- Determine d: d is multiplicative inverse of e mod (f(n)) (e * d) mod f(n) = 1 d is the private key.

Encryption:

- M is plain text data.
- C=m^{e} mod n

Decryption:

- C is received cipher text.
- M= C^{d} mod n

6. EXISTING SYSTEMS

There are several systems for dealing with two way mobile authentication. They may differ in delivering the password to the authorized user or a different entity based on the security constraints. Some of them are as follows:

1. Token: A token is a device used to authorize the user with the services. A token may be software or hardware. Software tokens are used to identify the person electronically, i.e. it may be used as a password to access something. Hardware tokens are small hand held devices which carry the information which stores cryptographic keys, digital signatures or even bio-metric data by which we can send generated key number to a client system. Mostly all the hardware tokens have a display capability. The hardware tokens include a USB, digital pass etc. Drawbacks A token shall be carried all the time. Special software is required to read the token. Anyone can access the information that has the token i.e. in case of theft.
2. Biometric: A biometric authentication is the advanced form of authentication. A biometric authentication is nothing but it scans the user's characteristics such as finger print and eye retina and stores in the form of a string. When the user tries to authenticate it matches with the stored data and then gives access when a commonality is achieved and when the user has gained access he can enter the password to view the required information. Drawbacks Biometric authentication is convenient only for limited applications, since the system becomes very slow for a large number of users. Finger prints can be taken on a small tape and can be provided for the hardware Additional hardware is required to detect the fingerprints and eye retinas.
3. One Time Password: Dynamic password (namely, One-Time-Password) technology is a sequence password system and is the only password system proved non-decrypted in theory. Its basic idea is to add uncertain factor in authentication so that users need to provide different messages for authentication each time. By this way, the applications themselves can obtain higher security guarantee than those use static password technology. When login request from user is received, server system generates a one-time password and sends it through a SMS to a GSM cell phone registered for that specified user. The one-time password has a default timeout. In the second phase of the authentication, a request is sent with the user id and a hash of the one-time password. If both the onetime and user specified password is valid then the user will be authenticated.

7. PROPOSED SYSTEM

The Proposed system is based on the OPT existing system. In the proposed, first user need to generate a key pairs, using any public key cryptography algorithm (e.g. RSA algorithm). In the proposed system user will request for login with ID and PIN (static password). If it matches with data stored in data based then server generate a random password (OTP) and encrypt it with the stored user's public key and send it to user. User will decrypt the encrypted one time password (EOTP) and send it to sever and if it match with original one time password (OTP) user is authenticated. RSA algorithm is used in the proposed system as public key cryptography algorithm. In the proposed system third party such as GSM mobile number or email id is not required. User will generate a key pairs using RSA algorithm and stores public key into the database during registration of users account. Proposed system Figure 3 works as follows:

1. User will request for login with ID and PIN.
2. Server will verify ID and PIN and generate a OPT and encrypt it with users public key which is stored in database and send the encrypted OTP to user.
3. User will decrypt the encrypted OTP with private key and send the result to server.
4. Server will match it with generated OTP; if it matches then user is authenticated.

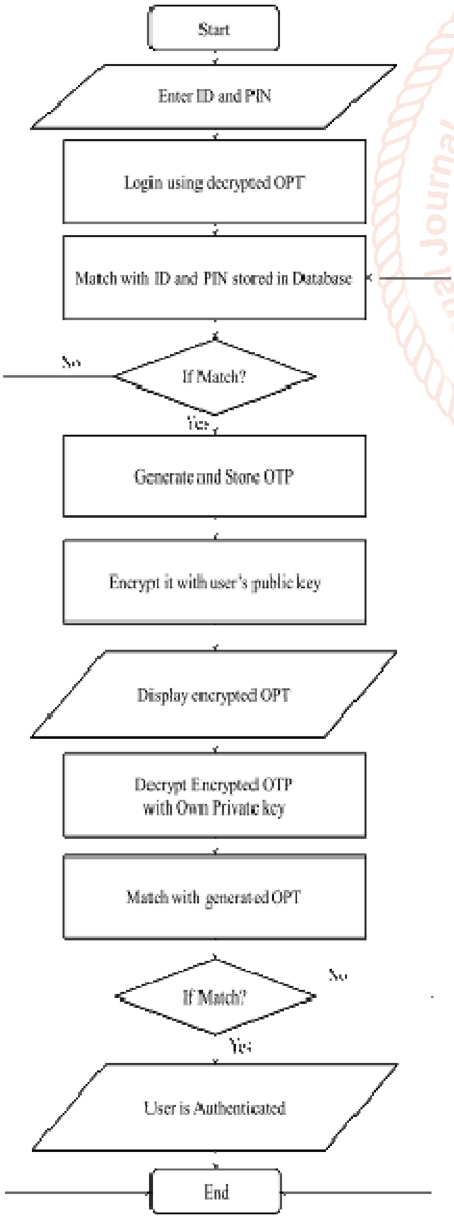

Figure3. Proposed System Flow

Advantages of proposed system over existing system are:

1. Proposed system is independent of third party (e.g. email, GSM mobile number).
2. Proposed system is highly secure based on key size.
3. Proposed system is more efficient.

Although this proposed system is designed for cloud authentication but also it can be used in other area which are describe bellow:

1. All the social networking sites: The proposed system will provide more secure authentication system compared to existing systems used by social networking sites.
2. All the electronic-commerce sites: The proposed system will provide more secure authentication system compared to existing systems used by electronic-commerce sites.
3. In the e-banking sectors also proposed system is very useful.

8. CONCLUSIONS

In this paper we used RSA public key cryptography for encrypting and decrypting One Time Password (OPT). In the proposed system encrypted OPT is directly send to user through the network. In the proposed system third party such as GSM mobile number or email is not required. The proposed system is designed to improve security, efficiency and to remove dependency on third party. Proposed system is highly secure and is dependent on the key size. The key pairs are generated with the help of public key cryptography algorithm.

9. REFERENCES

[1] H: B Kekre, V. A Bharadi, International Journal of Intelligent Information Technology Application, 2009, 2(6):279-285.

[2] Gururaj Ramachandra, Farrouka Aslam Khan, "A Comprehensive Survey on Security in Cloud Computing", The 3rd International Workshop on Cyber Security and Digital Investigation (CSDI 2017) Procedia Computer Science 110 (2017) 465–472.

[3] S. Lee, I. Ong, H. T. Lim, H. J. Lee, Two factor authentication for cloud computing, International Journal of KIMICS, vol 8, Pp. 427-432.-33

[4] M. S. Hwang, and L. H. Li, "A New Remote User Authentication Scheme using Smart Cards", IEEE Transactions on Consumer Electronics 46 (1) (2000) 28-30.

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

[6] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, New Delhi.

[7] https://aws.amazon.com/what-is-cloud-computing/

[8] https://searchsecurity.techtarget.com/definition/cryptography

[9] https://www.cloudflare.com/learning/ssl/how-does-public-key-encryption-work/