IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Advanced Cloud Security using RSA and variable length OTP with mixture of numeric, alphanumeric and special character.

Rahul Karmakar[1], Samrat Banerjee[2], Anirban Ray[3]

Assistant Professor, Dept. Of Computer, Burdwan University, India[1]

Final Semester Student, MSc (Computer Science), Burdwan University, India[2,3]

Abstract: Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. With the migration of the data and the applications into the cloud, new security issues appear, with the fact that services are accessible anywhere any time lead to several potential risks. The most serious concerns are the possibility of lack of confidentiality and data security issues among the cloud users remain the principal inhibitor in adopting Cloud Computing Service. In this paper we have proposed new authentication system for cloud platform based on Multi level authentication having variable length onetime password (OTP) with mixture of numeric, alphanumeric and special character(s) for enhanced security in cloud authentication.

Keywords: Cryptography, Cloud Computing, OTP, RSA, AES.

I. INTRODUCTION

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (such as networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. In the cloud computing system, both application software and database are moved to the large data centres, when data should not be secure in hands providers. The main benefit of Cloud Computing is the high-availability storage of data, but also the high parallel computing resources. For enterprises, the Cloud offers an alternative to the on-premises infrastructure to an off-premises one which means costs savings and accelerate adaptation for new applications and resources requirements.

This technology provides services with one of the three services:

1) SaaS (software as a service) -- In IaaS, you outsource the hardware. In such cases, it is not just the computing power that you rent; it also includes power, cooling, networking, and cloud storage. When you choose to run your applications at this cloud service level, you are responsible for everything on the stack that is required to operate above it.

2) PaaS (platform as a service) - In the middle, we have Platform as a Service, or PaaS. At this service level, the vendor takes care of the underlying infrastructure for you, giving you only a platform with which to build and host your application(s).

3) IaaS (Infrastructure as a service) - Software applications that are available only over the internet, fall into the Software as a Service category, or SaaS. The simplest example to understand is email.

The three primary types of cloud models are:

1. Public - Available to the general public or a large industry group and owned by an organization selling cloud services
2. Private - On or off premises cloud infrastructure operated solely for an organization and managed by the organization or a third party
3. Hybrid- Traditional IT and clouds (public and private) that remain separate but are bound together by technology that enables data and application portability

Fig 1: Cloud Computing Characteristics and Models

II. OTP

A one-time password (OTP) is a password that is valid for only one login session or transaction, on a computer system or other digital device. The most important advantage that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks. This means that a potential intruder who manages to record an OTP that was already used to log into a service or to conduct a transaction will not be able to abuse it, since it will no longer be valid. A second major advantage

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

is that a user who uses the same (or similar) password for multiple systems, is not made vulnerable on all of them, if the password for one of these is gained by an attacker. A number of OTP systems also aim to ensure that a session cannot easily be intercepted or impersonated without knowledge of unpredictable data created during the previous session, thus reducing the attack surface further. OTP generation algorithms typically make use of pseudo randomness or randomness.

Two way one time authentication works as follows:

Step 1. User send a login request server with its ID and pin (Static password)

Step 2. If ID and PIN match with the ID and PIN stored in database, server generate a one-time password (OTP) and send it through SMS or email to the user.

Step 3. Server request user for OTP.

Step 4. User enters OTP and if it match then user is authenticated.

III. CRYPTOGRAPHY

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. 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)

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) Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)
4) 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)

IV. THE RSA ALGORITHM

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.

The Rivest-Shamir-Adleman (RSA) algorithm is one of the most popular and secure public-key encryption methods. The algorithm capitalizes on the fact that there is no efficient way to factor very large (100-200 digit) numbers.

Using an encryption key (e,n), the algorithm is as follows:

1. Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.
2. Encrypt the message by raising it to the eth power modulo n. The result is a ciphertext message C.
3. To decrypt ciphertext message C, raise it to another power d modulo n

The encryption key (e,n) is made public. The decryption key (d,n) is kept private by the user.

How to Determine Appropriate Values for e, d, and n

1. Choose two very large (100+ digit) prime numbers. Denote these numbers as p and q.
2. Set n equal to p * q.
3. Choose any large integer, d, such that GCD(d, ((p-1) * (q-1))) = 1
4. Find e such that e * d = 1 (mod ((p-1) * (q-1)))

V. THE AES ALGORITHM

AES, short for Advanced Encryption Standard, is a widely adopted symmetric encryption scheme used, for instance, to secure electronic communication and messages. AES – as its name implies - has been the outcome of standardization and evaluation process which took years to select from the best encryption algorithms. Finally, in 2001, the Rijndael algorithm has been chosen as winner by the US National Institute of Standards and Technology (NIST) to be implemented as underlying security algorithm of the AES standard which as of the these days has largely replaced its predecessor and derivates of DES (Data Encryption Standard) which is longer considered secure due to its small 56-bit key length for example.

The Rijndael algorithm, invented by two cryptographers Vincent Rijmen and Joan Daemen, implements the mathematical operations substitution, transposition, as well as permutation to plaintext, the term used to describe input in the cryptography domain. The AES Advanced Encryption Standard uses 10 rounds of these algebraic operations in a complex scheme to produce encrypted output, or cipher text as it is called in expert terms. AES-192 and AES-256 have 12 and 14 rounds, respectively.

In the AES implementation of Rijndael the algorithm operates on 128 bits block ciphers, and comprises key lengths of 128, 192 and 256 bits

VI. EXISTING TECHNOLOGY

Several researches were proposed in cloud in recent times. But only authenticating the real user does not always guarantee unauthorized access to data. One of the main troubles with passwords is that most users either don't understand how to make strong and memorable passwords or underestimate the need for security. Extra rules that increase complexity are seen to drive call volumes for password-related issues to help desks proportionately. This problem can result in IT and management letting password standards slip and as a result passwords of shorter length and complexity tend to happen, such as simple seven

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

character words. These passwords can be cracked in a matter of a few short minutes making them almost as ineffective as no password at all or a password that is discovered from a sticky note, either in use or carelessly discarded. With the speeds of CPUs today, brute force attacks pose a real threat to passwords. With developments like massive parallel general purpose graphics processing (GPGPU) password cracking and rainbow tables,[10] it's possible for hackers to produce more than 500,000,000 passwords per second, even on lower end gaming hardware. Depending on the particular software, rainbow tables can be used to crack 14-character alphanumeric passwords in about 160 seconds.

OTP generation depends on the factors utilized to configure the OTP or on the algorithm employed to generate the OTP. Most OTP systems are susceptible to real-time replay and social engineering attacks. OTPs are also indirectly susceptible to man in the middle (MITM) and man in the browser (MITB) attacks. Real-time replay attack is a form of an MITM attack. In this attack, malware sitting on the browser captures user credentials. The malware forwards these details to the attackers, and simultaneously blocks the user request. The user receives an error message which reports a failure. The attacker can perform an immediate replay with the same credentials. These tokens are usually valid for 60 seconds (+/- 10 seconds). OTP is weak when it depends on a random number [7]. Ku proposed algorithm to generate OTP is a hash based strong pass word however, later researches proved that the algorithm is not secure enough [8].Several other researchers proposed algorithms to generate OTPs based on password; however, they are not very secure as they used fixed length (mostly numeric) OTP.[9]

VII. PROPOSED SYSTEM AND ALGORITHM

In out proposed model we have used the following security algorithms:-

1) RSA algorithm for secured asymmetric communication.
2) Variable length One Time Password (OTP) with mixture of numeric, alphanumeric and special character.
3) OTP can't be accepted more than once (even by legitimate user) within an allowable time period (approx.1-2 minute) if somehow the user gives it wrong at the first time.
4) User will be logged out even from the 1St level of authentication i.e. login based on static password- if wrong OTP is provided.

In the proposed security model 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 password. [3]

If the user provided data matches with the data stored in database, the server generates an OTP.

In our proposed system, Variable length one time password has been used for authenticating the user. The variable length password should be of min 6 character and max 10 character in length.

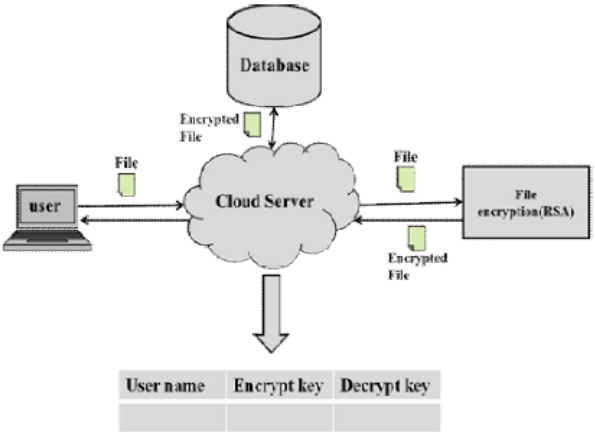

Figure 2: Encryption of file using RSA [6]

The OTP should be a proper mixture of Upper Case character, Lower case character, Numeric and Special symbol. The user should not be knowing the length of variable OTP and its combination that would be provided by the server for that particular session. This method will enhance the security and pose further trouble for hackers and intruders because it will nullify the fixed pattern being generated in a conventional OTP.

Besides, the variable length OTP should be valid for a very short span of time (1-2 minutes, configurable from server side).Generally within that time frame if the user gives wrong OTP, an error message is being displayed citing that wrong OTP had been entered. But the user can still login if he can provide the correct OTP within that time frame.

But in our proposed system it has been so designed, - OTP can't be accepted more than once (even by legitimate user) within an allowable time period (approx.1-2 minute) if somehow the user gives it wrong at the first time, user will be logged out even from the 1St level of authentication i.e. login based on static password- if wrong OTP is provided, so that the intruder doesn't have any chance to block the real user and retry the OTP on their behalf. The user has to start again.

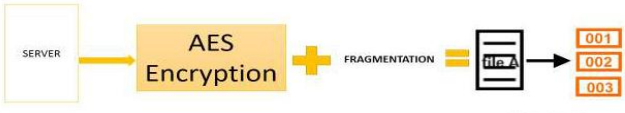

Fig 3 Server side encryption using AES [5]

In the server side Cloud provider will receive the file and will store it in the different zones for security purposes. Cloud provider will also replicate the data on the backup server [5]

VIII. STEPS OF OUR PROPOSED CLOUD AUTHENTICATION USING RSA AND VARIABLE LENGTH OTP.

1. User will provide the user id and PIN (static password)
2. The cloud provider would verify the credentials from stored in its database. If the matching is successful, server will generate a variable length onetime password (OTP) with mixture of numeric, alphanumeric and special character and send the encrypted OTP to user

3. User will decrypt the OTP and send the result back to the cloud server.
4. Cloud server will verify the OTP, if found successful the user will be logged in else error message will be displayed, ending the session and logging out from the 1st level authentication also (user id and password based).

IX. FUTURE SCOPE

Future scope includes improving the processor performance and integrating OTP with biometric authentication. Besides, the concept of digital signature can also implemented along with authentication in another multilevel authentication system in cloud so that the user and server exactly knew to whom they are communicating.

X. CONCLUSION

With the continuous growth and expansion of cloud computing, security has become one of the serious issues. The protection of the data stored in the Cloud face new vulnerabilities. So one must be very careful to understand the security risks and challenges posed in utilizing cloud technologies. Cloud computing brings us the approximately infinite computing capability, good scalability, service on-demand and so on, also challenges at security, privacy, legal issues.

Static password are susceptible to easy threats and in modern cloud architecture they alone are not at all sufficient to thwart data hacking and mishandling. One time password is designed to prevent replay attacks which has an upper hand over static password based authentication. In this paper we have proposed new authentication system for cloud platform based on Multi level authentication having variable length onetime password (OTP) with mixture of numeric, alphanumeric and special character(s) for enhanced security in cloud authentication over and above the conventional OTP generation. In this paper we used public key cryptography (RSAalgorithm) for encrypting and decrypting one time password. Moreover, OTP can't be accepted more than once (even by legitimate user) within an allowable time period (approx.1-2 minute) if somehow the user gives it wrong at the first time. In that case will be logged out even from the 1St level of authentication i.e. login based on static password- if wrong OTP is provided and needs to start afresh. This framework is highly secure in comparison with the existing similar cloud authentication techniques. In today's requirement it is very helpful in keeping the cloud security intact.

REFERENCES

1. http://en.wikipedia.org/wiki/Cloud_computing
2. Atul Kahate , Cryptography and Network Security, Tata McGraw-Hill Publishing Company Limited.
3 Geetanjali Choudhury et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 4077-4080
4. A Novel Approach to Provide Dynamic Authentication & Data Integrity in Public Cloud Environment: Using MD5, RSA and Enhanced OTP
5. Amandeep Kaur, Mr. Pawan Luthra, A Novel approach of hybrid model of encryption algorithms and fragmentation to ensure cloud security
6. Ankita Patil,, Kiran ZambareE, Preeti Yadav, Pankaj Wasulkar, Nisha Kimmatkar, Integration Of encryption of file and One Time Password for secure file access on cloud
7. Yu tao, F. and S. Gui ping, Design of Two-Way One-Time-Password Authentication Scheme Based on True Random Numbers, in Second International Workshop on Computer Science and Engineering2009,
8. Neng-Wen Wang and Yueh-Min Huang, User's Authentication in Media Services by using One-Time Password Authentication Scheme, in Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing2007,
9. Yang Jingbo and Shen Pingping, A secure strong password authentication protocol in 2nd International Conference on Software Technology and Engineering(ICSTE)2010
10. A Review of One Time Password mobile verification by Shally & Gaganjeet Singh Aujla

BIOGRAPHIES

Mr. Rahul Karmakar, B.Tech, M.Tech, Assistant Professor, Dept. Of CS, BU, W.B

Mr Samrat Banerjee, BCA (Hons), MSc (Computer Science-Final Semester)**,** Senior Software Engineer**,** IBM India Pvt Ltd

Mr. Anirban Ray, MSc (Computer Science- Final Semester Student)

.

.

DOI 10.17148/IJARCCE.2016.5139