International Journal of Grid and Distributed Computing
Vol. 10, No. 4 (2017), pp.1-8
http://dx.doi.org/10.14257/ijgdc.2017.10.4.01

Authentication using Unique Identification Number in Cloud Network using RSA Algorithm

Debabrata Sarddar[1], Mousumi Biswas[2], Priyajit Sen[3] and Rajat Pandit[4]

[1]*Assistant Professor, University of Kalyani, India*
[2]*M. Tech (Pursuing), Department of Computer Science and Engineering, University of Kalyani, India*
[3]*M. Tech (Pursuing), Department of Computer Science and Engineering, University of Kalyani, India*
[4]*Assistant Professor, Department of Computer Science, West Bengal State University, West Bengal, India*

Abstract

Each country would like to make its websites secure. Now a days each countrymen use internet moreover the cloud make it that much feasible. Every sensitive detail has been stored on cloud. The main problem that arises for cloud is the security issues regarding authentication. In this paper we have mentioned a way by which we could solve the authentication problem. We have used the unique identity number of a person which was provided by the trust worthy organization. Then applying the RSA algorithm on that unique ID the authentication process is improved.

Keyword: *Cloud Computing, Authentication, attacks on website, RSA algorithm, Terrorist attacks over internet*

1. Introduction

Technologies to organize recruit and spread propaganda by using Internet as a weapon. Internet increases the speed of communication so that huge number of people is attracted toward it. Even official works and secret information are propagated through internet. Terrorist always try to keep track of the official data/secret information of the organization. The terrorists focus on ordinary people is based on the fact that they are easy to reach and are susceptible to the deadly force. The hackers manage to acquire all the necessary secrets of a particular country by using loophole. To reach to the loophole the terrorist may use any account of a particular countryman by simply hacking it. To protect all the important information In today's world every country faces the threat of terrorism over the Internet in varying degree. The terrorist groups express their grievance through violence when their political desires and ambitions conflict with any organization. They find themselves engaged in an unofficial war for which they keep on destroying the innocent people besides property.

Each coin has its two sides likewise internet also shows its good side and bad side. It solely depends upon the user how they are going to use the internet. Terrorists use social media and other we need to remove the ambiguity. By applying a proper authentication method the data in cloud can be protected.

Security issues of web services: Before deploying the web service, it is always mandatory to have the knowledge about the security issues. If the service open up for everyone and anyone then security is must. There are few ways through which we can increase the security of web services. They are –

ISSN: 2005-4262 IJGDC
Copyright ⓒ 2017 SERSC

1. **Equipment Deployment:**
   Instead of using any software which can be replaced by hardware would be better for website security purpose.

2. **User Authentication:**
   Authentication is needed to learn the identity of the user. The identification number is used to make sure whether a person should have the access to the service. Identity number is also used to track user's activities.

3. **Application–level Authentication:**
   Users can identify themselves by the credentials supplied in the SOAP message.
   HTTP digest authentication: The hashed version of the basic authentication credentials are send to the server to decode.
   Client certification: During SSL authentication the client can proves its identity by using a certificate issued by a certificate authority.
   Windows authentication: IIS can project a user identity to areal windows user by other authentication (client certificate, HTTP basic/digest) process.

4. **Guarding Data:**
   Access control list can be used to guard files and SQL based security can be used to guard database.

5. **Tracking User Activity:**
   Using the IP address or other time to time activity of the user we can track the user activity on website.

2. Harm Caused by the Terrorists Over Internet:

Terrorism on the Internet is very dynamic phenomenon. As the network increases the crimes are also increasing. The term Cyber terrorism becomes a familiar; though it is a controversial term. There have been several definitions of the term Cyber terrorism. The phrase came from two different words Cyberspace and Terrorism. It is an unlawful attacks or threats of attacks against computers. The information that is stored on the cyberspace is mostly harmed by the terrorists. Furthermore, precisely if we want to define the cyber terrorism then one thing we need to consider here is that it results in violence against people and the properties. The main motivation is to harm people or generate enough fear to force the government to fulfill their intentions. Hacktivism is considered as some activities conducted online and secretly that reveals, manipulate or expose the vulnerabilities in computer operation system and other software. Hackers don't have any political agenda. The terrorists are somehow managing to use the hacking procedure to achieve their mission on cyberspace.

We have mentioned here few ways in which terrorists use the internet. They are like Psychological welfare, publicity purpose, data mining, fund raising, recruitment and mobilization, Networking, sharing information and co-ordination.

Types of Attacks:

The kinds of attacks that are faced by the websites are –

Injection Attacks:

Structured Query Language Injection (SQLI) is a technique where a code is injected into the query to modify the database. A PC and a little knowledge of database is enough for exploitation the database.

 Copyright ⓒ 2017 SERSC

Denial of Service (DDos) Attacks:

It occurs when multiple systems is flooded by the large number of fake external requests. In such a case the targeted resource bandwidth gets jammed. All other genuine requests get eliminated because of this congested condition.

Brute Force Attacks:

Here the attacker will try every possible type of username and password combination to get the access to the targeted website. That is why a strong password is always required to protect the account of a user. Otherwise from the users account the intruder will get the chance to enter into the website.

Cross Site Scripting:

Attackers will use Cross-site-Scripting (XSS) to inject malicious script into other trusted harmless websites so that the user of the website can execute the script. XSS is used to gain the access of a user's account of a particular website.

Why RSA algorithm is used:

Cloud computing is a new technology, it is a type of internet-based computing that provides shared computer processing data and resources to computers and other devices on demand. All the service is solely dependent on the internet so, security is a big challenge here. A proper authentication and authorization mistake can cause data loss, botnet, phising *etc*. Beforehand protection and prevention is the only way to solve the issue of security.

In 1977 Run Rivest, Adi Shamir and Len Adllman first introduce the RSA algorithm. RSA is a asymmetric key cryptography. It has two different keys for encryption and decryption. The key which is used for encryption is the public key but the decryption key is the private key. So, only the person with correct private key could only decrypt the encrypted data. RSA derives the security from the strenuous of factoring large integers that are the product of two large prime numbers. Multiplying two large numbers are easy but finding out the original prime number from the total factoring is considered infeasible because of the time factor even if we use today's super computers.

As the computation power is increasing it become easier to factor large numbers efficiently. The encryption strength is strongly tied to the key size. Doubling the key size would exponentially increase the effectiveness. Although it may impair performance. RSA keys size lies between 1024 to 2048 bit in length, which is a bit tough to break. Experts believe that 1024 bit keys could be broken in near future. That is why it will be beneficial if we could use 2048bit long keys from now.

3. Related Work

In cloud computing data is not on the same location it is distributed over the internet to various locations. Which data is travelling to which server it is hard to detect. Authentication is very important aspect here. Through which an intended person could get his data safely. There are few ways that are already available in the cloud computing process. In the paper "Authentication in the Clouds: A Framework and its Application to Mobile Users", Richard Chow et al have proposed Authentication frameworks, models and architecture oriented authentication. Here the model first collect the user's context and activities, and update the data aggregation regularly. Secondly at the time of authentication the reports were sent to the authentication engine. It is architecture oriented method.

In the paper "user security in cloud password authentication", Deepika Singh et al have proposed an algorithm where password will be generated depending on the username.

Copyright ⓒ 2017 SERSC

Password is always required to keep our data safe and secure. But, because we need to remember it, we keep it simple and short. This is not feasible at all. Smart cards are the pocket sized plastic card where integrated circuits are embedded. This card made the authentication process much stronger by providing additional security. In the paper "Secured biometric authentication in cloud sharing system" E. Sasi *et al.*, mentioned that, Biometric authentication is the most trusted process of authentication. By using this technique a user will enter the required biological features as the input, which cannot be copied by others. Then the input will be verified with the previously stored biometric features. Here the features may be the facial recognition, finger print recognition, Iris recognition.

The technique that have been used to make the data secure in cloud, in both "Providing Data Security in Cloud Computing using public key cryptography" and "An Efficient data storage security algorithm using RSA Algorithm" papers the writers have mentioned the RSA algorithm as an important feature.

4. Proposed Work:

Terrorism is the random use of violence to achieve political ends that inflicts damage on innocent people and property. Terrorists are always active on web to find out the ways to get the desired infrastructure for various purposes. One such example would be acquiring the sensitive information of a country. There are few websites of each country that contains the secret information of that country only. Eavesdropper will always try to tamper with those data. In this paper we try to restrict the access of those websites.

1st Level Authentication:

In this proposed work we need a particular unique ID which will be mandatory for each countryman and one more thing here we have to remember that the ID should be provided by the country government authority. The government should have to keep the record of the ID . [One more consideration should be there, if a person of country A wants to access a particular website of country B. Then the countryman of A need to prove that he/she is genuine one so he/she will verify his ID with country A and send the report to country B. country B verify it, then it provide a temporary random ID for that person].

Now, the estimated algorithm will goes on like –

Step 1: when a user tries to access a particular official website of a country it will ask for the user ID number.

Step 2: whenever ID number is entered the website will try to verify it.

Step 3: The ID number will be encrypted (RSA algorithm).

Step 4: ID number will be reached to a site for decryption.

Step 5: decrypted ID number send to the government maintained ID database for matching.

Step 6: if match found the access is accepted otherwise not.

2nd Level Authentication:

Here along with the ID number the biometric feature is also asked. It totally depends upon the user's access level of a website. If the user needs some sensitive information of a website then he/she has to enter the biometric features like facial recognition, finger print, iris recognition *etc*. The biometric feature will be compared to the saved biometric details of the government maintained database. But the main problem arises here is the device required for extracting the biometric features. They may not available to the user so it will be feasible if the image of the user could be send for verification using webcam by

 Copyright ⓒ 2017 SERSC

maintaining some specification. One thing we should consider here is that the user is already accessing the website. Only the additional verification is performed here.

The algorithm would be like -

Step 1: The website will ask for the current image through webcam by maintaining some specification.

Step 2: Facial image is send to the government maintained database.

Step 3: Matching operation is performed.

Step 4: If matching result is true further access is possible.

RSA Algorithm:

RSA algorithm is most popular asymmetric key cryptographic algorithm. RSA name is came from the first letter of the surname of the inventors in 1977.

The algorithm is like:

Step1: Two random large prime numbers P and Q should be chosen. [typical key size should be 1024 to 4096].

Step2: Compute N=P*Q and M = (P-1) (Q-1).

Step3: Factor M and select public key (i.e. the encryption key) E such that it is not a factor of M.

Step4: Compute the private key (i.e. the decryption key) D such that the following equation is true:

(D*E) mod M = 1

Step5: The cipher text (CT) will be

CT= (PT) ^E mod N

Step6: The plain text (PT) will be

PT= (CT) ^D mod N

Though it is a very secure process of encryption but the user should always use the fresh P, Q, N and E.

Example:

Step 1: To make the calculation easy we will pick two small prime number P=7 and Q=17.

Step 2: Now calculate N= (P*Q) =7*17=119 and

M= (P-1)*(Q-1) = (7-1)*(17-1) = 6*16=96.

Step 3: choose a number encryption key E (public key) in such a way that E should not be the factor of 96.

Lets choose E as 5.

Step 4: select a decryption key D (private key) such that (D*E) mod M = 1 equation is true.

That is, (D*5) mod (96) =1

After some calculation let us take D=77.

Copyright ⓒ 2017 SERSC

Step 5: calculate cipher text CT=PT^E mod N.

Let us assume the plain text is 10. So the Ct will be

CT= 10^5 mod 119 = 100000 mod 119 = 40

Step 6: The cipher text that has been sent to the receiver will be 40.

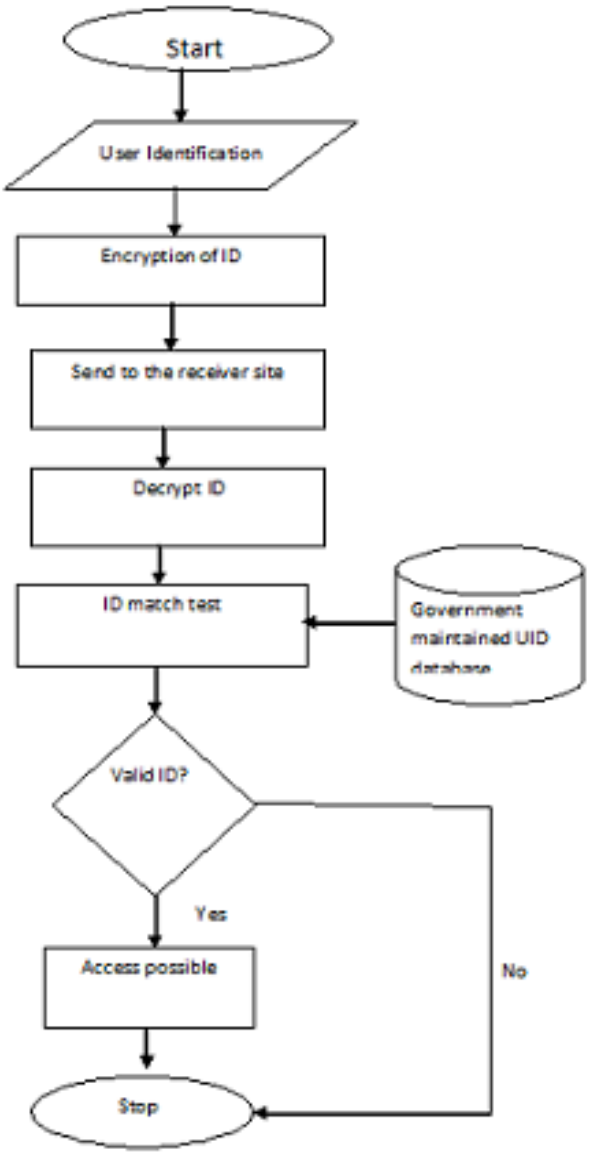
For decryption, calculate the plain text PT from cipher text CT by applying the equation

PT= (CT) ^D mod N

PT= (40) ^77 mod 119 =10

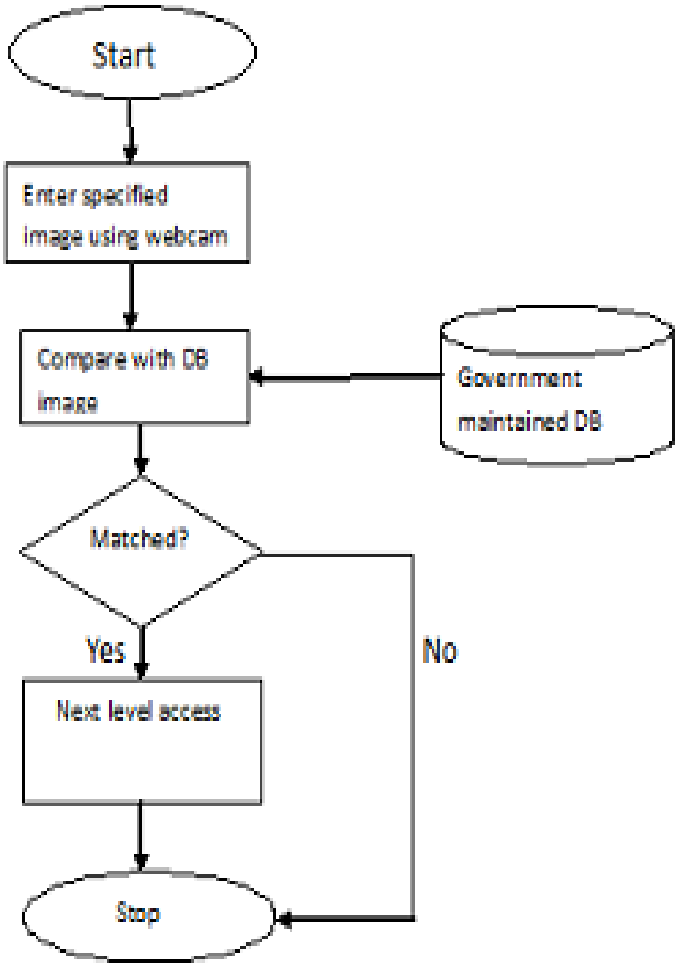
10 is the original plain text that is what we wanted back.

Level 1 Authentication Flowchart:



 Copyright ⓒ 2017 SERSC

Level 2 Authentication Flowchart:



5. Conclusion

In cloud computing authentication is a big factor. Here special care has always been taken to make the data secure. Various techniques are there to provide the security but in this paper we have a mentioned a technique which make the user as a unique user of a particular website. Each person will have only one identity which will be provided by the trusted third party of a country. So, when a person will try to access a government website he/she must enter an id. Then the id will be compared to the previously saved id of the person in a government maintained database, if the comparison gives a result as matched one; the person will be authenticated. Hence here we are not using any strict authentication method. Any terrorist if able to get an id will easily can access the website. Hence, here we will set a limited access for each user up to which they can access a website. If anyone wants details of any website he/she have to face the second level authentication, which will be somehow near to the biometric authentication. In all Identity cards few special features of their body parts are always given. i.e. the image, fingerprint, iris, retina *etc*. So, to do the second level of authentication we don't need to collect the users those biometric features, because those are all previously saved along with the ID number to the government maintained database. We only need here is the second level of authentication and perform the authentication process. By applying this technique we can

Copyright ⓒ 2017 SERSC

differentiate between the real and fake (terrorist) user. Therefore, the whole concept is that if a person has valid ID he/she can access a particular website.

References

[1] R. Prasad Padhy, M. Ranjan Patra and S. Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges", IJCSITS, **(2011)** December, pp. 136-146.
[2] M. Ahmed and M. Ashraf Hossain, "Cloud Computing and Security Issues in the Cloud", IJNSA, **(2014)** January, pp. 25-36.
[3] V. Ashktorab and S. Reza Taghizadeh, "Security Threats and Countermeasures in Cloud Computing", vol. 1, is. 2, **(2012)** October.
[4] R. M. Lomte and Prof. S. A. Bhura, "Survey of different Web Application Attacks & Its Preventive Measures", IOSR-JCE, **(2013)** October.
[5] J. Raiyn, "A survey of Cyber Attack Detection Strategies", IJSIA, pp. 247-256.
[6] S. Ziyad and S. Rehman, "Critical Review of Authentication Mechanisms in Cloud Computing", IJCSI, **(2014)** May.
[7] S. Sharma and U. Mittal, "Comparative Analysis of Various Authentication Techniques in Cloud Computing", IJIRS, **(2013)** April.
[8] R. Chow, M. Jakobsson and R. Masuoka, "Authentication in the Clouds: A Framework and its Application to Mobile Users", CCSW '10 Proceedings of the 2010 ACM workshop on Cloud computing security workshop, Chicago, Illinois, USA, **(2010)** October 08, pp. 1-6.
[9] D. Singh, P Gour and R. Thakur, "User Security in Cloud Using Password Authentication", ISSN: 2248-9622, vol. 4, Issue 6(Version 5), **(2014)** June, pp. 39-44.
[10] P. Kalpana and S. Singaraju, "Data Security in Cloud Computing using RSA Algorithm", IJRCCT, ISSN 2278-5841, vol. 1, Issue 4, **(2012)** September, pp. 143-146.
[11] N. Padmaja and P. Koduru, "Providing Data Security in Cloud Computing using public key cryptography", IJESR, ISSN:2230-8504, vol. 04, Special Issue 01, **(2013)**, pp. 1059-1063.
[12] E. Sasi and R. Saranyapriyadharshini, "Secured Biometric Authentication in Cloud Sharing System", IJCSME, **(2015)** March, pp. 572-577.
[13] A A. Pawle and V. P. Pawar, "Face Recognition System(FRS)on cloud computing for User Authentication", ISSN: 2231-2307, vol. 3, Issue 4, **(2013)** September.
[14] D. Sarddar, P. Sen and M. Kumar Sanyal, "Central Controller Framework for Mobile Cloud Computing", International Journal of Grid and Distributed Computing, vol. 9, no. 4, **(2016)**, pp. 233-240.

 Copyright ⓒ 2017 SERSC