OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

A CERTIFICATE VALIDATION SYSTEM USING PKI

Prof. R. T. Waghmode[1], Mayuri Miniyar[2], Shivani Sonawane[3], Shreya Mirashi[4], Pratiksha Tiwari[5]

Zeal College of Engineering and Research, *Pune.*[1,2,3,4]

Abstract: ***According to the educational statistics there are about one million graduate students in one year. Due to lack of effective anti-forge mechanism, causes the certificates to be forged .To solve this digital certificates system using public key infrastructure is proposed. Public Key Infrastructure (PKI) is used for the secure communication in the network. Digital certificates need to validate very quickly and securely. For this PKI is used for security. As per the current popular validation system, it delivers the validation information to the client's .Due to which clients system suffers from high overhead. Motivated by this observations we present the effective validation system. Our implementation of the Certificate Validation System using QR Code is able to validate the digital certificate in short period of time and in low cost. It also provides security of the user's documents. QR Code is basically used for accessing the documents easily and a database is also provided in our system to store the data of the student in it.***

Keywords *– PKI, Certificate validation system, Network security, QR Code.*

----------∴∴∴----------

I INTRODUCTION

Public key cryptography is the base of the Public Key Infrastructure (PKI).PKI aims to provide the network security for the various networks like AD-hoc, VANET.PKI works by using two different cryptographic keys- public and private key. Public key is available to everyone who wants to send or receive messages. Private Key is a unique key which is kept secure and secret. Many protocols like SSL and TLS,PKI is successfully implemented in other systems. Registration Authority (RA) is used for providing digital certificates to users. PKI uses symmetric and asymmetric encryption and decryption.CA-Certificate Authorities is one of the main component of the PKI. Digitally signed certificates are published with help of CA. This certificates binds its identity with the public key. Certificate Revocation List (CRL) is the list in which the invalid certificates are listed . The CA is also responsible for the revocation of the certificate .CRL are blacklisted certificates which can't be trusted for any process.CA publishes the CRL in time interval. Clients need to download the CRLs while validating the certificates. The invalid certificates should not be proceed for any process in any of the system. While downloading the CRLs in low-speed network takes so much time which leads to time consuming disadvantage.

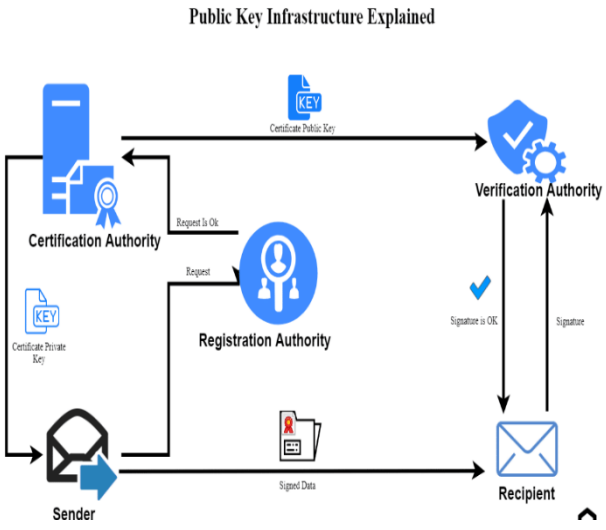

Figure: 1 Public key infrastructure

Any certificate validation system must follow the following propertied:

- Response time: The clients should get informed the updated revocation list as soon as possible.
- Security: Clients should be informed about the updated list of certificates so that client will not accept the invalid certificates.
- Availability: The system should be available for any platform and on any devices.

In recent popular system the CRLs are published over the radio stations of the clients which is costly for the client. This system fails to achieve some of the properties of above. This issue motivated us for developing the better performance system for the certificate validation process.

In our system we use the QR code for the accessing the information of the student which is stored in the database. We are using Public Key Infrastructure for the secure communication over the network. The central idea for proposing the paper is to propose the Certificate validation system using PKI along with the QR code which is for accessibility of the data as well as for keeping the data away from unauthorized access. QR Code is basically used for accessing the documents easily and a database is also provided in our system to store the data of the student in it.

The rest of the paper is arranged as follows**.** In Section 2 we have discussed the background of the recent certificate validation systems and in Section 3 we review the design of the system. We have presented its implementation and evaluation in Section 4.An analysis on security related to PKI takes place in Section 5 along with a conclusion in Section 6.

Background

In this section we will first discuss the background of this system, previously and recently proposed systems along with their limitations.

Certificate Revocation List (CRL): the most common technique for validation is CRL. in CRL the CA has authority to check the certificate is valid or not and id it is not valid then that certificate should be in revocation list and that list will be published to the liens . This technique suffers time dely CRLfile also consume more bandwidth to distribute because of the size.

Online certificate Status Protocol: Single certificate status is checked by using this technique. OSCP responder server plays a vital role in it. OSCP server is accepts the OSCP requests of client for certificate status. Then server checks in CRLs and then respond to client about the certificate status i.e the certificate is valid, invalid or unknown. In this technique clients need to communicate with the third party for the validation of digital certificate .this is time consuming and if client doesn't get respond then he/she can terminate the session. Web traffic is one of the limitation of OSCP.

Short-lived certificate: In this HTTP protocol is used as web service is used for the validation. It updated the certificates for apache web-servers automatically. Expiry date of the certificate is checked and CA issue the new one for the same. Google chrome URL and plug-in are used in this as the number of issued certificates increases the resources on server side need to increase to fetch and send the certificates . More number of the issued certificates increases the significant amount of network is required from CA side.

Rev-cast - Private certificate revocation:

As the previous systems broadcast the revoked certificate over the internet links. To update the lists of same need more time and software. In this technique the revoked certificate list is broadcasted privately over the FM radio. The revocation list is broadcasted over the radio stations of the clients. But to implement this the client need to have different hardware .if client have PC then it must have receiver, if smart phones then it must be integrated with the FM antenna to receive the information distributed by the CA .practically it is possible only in metropolitan areas where the coverage of FM towers is available.

II SYSTEM DESIGN

The design of the system is most important for implementation of any system. Our system is has frontend as java and the database is created in Mysql our system has three main modules as students, company and the collage.

Electronic Certificate system is at collage and the student will apply for the E-Certificate to the collage. Collage will create the E – Certificate and it will provide the E-Certificate serial number and QR-code to the student.

Collage will update the database of it with student name along with its certificate number for future reference.

When student apply for any company for the job .he has to submit the documents of it to the company for verification of the Student. Student will submit its E-certificate serial number along with QR-Code.

Then company will verify the student's documents using his serial number and it will verify it with the collage.

When the serial number will come to the collage for verification then the collage will check it into its database

and after verifying the information collage will send the review message to company about the information.

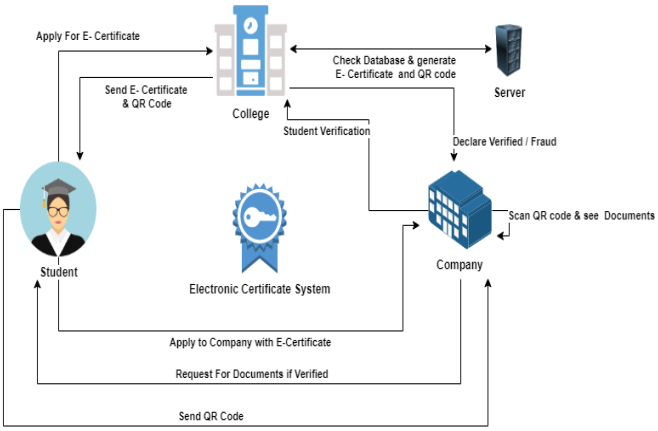

Figure 2: Design

III IMPLEMENTATION

A. Algorithms

I) AES (Advanced Encryption Standard)

AES algorithm is a fast and secure form of encryption. Earlier DES (data encryption standard) was used but it had only 56 bit key, as the attackers can easily crack the code, therefore AES algorithm is used now-a-days. AES uses maximum of 256 bit of block size. Here, we have used block size of 128 bits, there are 10 number of rounds. Output of encryption is a cipher text of 128 bits, keysize is 128 bits and there are 44 sub-keys. Each round has 4 sub-keys and size of a sub-key is one word that is of 32 bits.

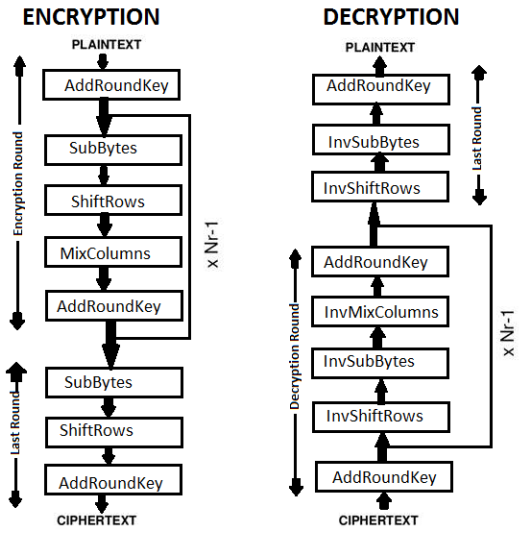

Figure 3. Structure of AES algorithm

Plaintext is represented as an input array and is divided into 16 blocks of total 16 bytes, each block contains 1 byte.

Therefore, Plaintext is of 128 bits equals to 4 words. As shown in fig 2. In add round key operation xoring is done between plaintext and sub-key of pre-round R0 that is w[0,3].

For 10 rounds sub-keys are:

R0(pre-round):w[0,3]

R1: w[4,7]	R2: w[8,11]
R3: w[12,15]	R4: w[16,19]
R5: w[20,23]	R6: w[24,27]
R7: w[28,31]	R8: w[32,35]
R9: w[36,39]	R10: w[40,43]

Output of xoring is given to first round that is Substitute bytes ,Shift-Rows, Mix-columns and again output of these operations are xored with sub-key w[4,7] for add round key. This process of rounds are repeated till completion of ninth round and then output of ninth round is given to tenth round. In the tenth round substitute bytes, Shift Rows and Add Round Key operations are performed and Cipher text of 128 bits is generated.

For Decryption same key of 128 bits is used and all the round operations are inversed and cipher text is converted to plaintext of 128 bits.

This algorithm is often used by the government, militaries, and social media to keep confidential information secure.

ii) MD5 (Message Digest five)

Hashing or hash function is a mathematical function that takes any variable length of information and converts it into fixed size of hash values or message digest. Different hash functions are MD2, MD4, and MD5. Here, we are using MD5 as the block size is of 512 bits. Output size (hash size) is of 128 bits. There are 4 rounds. It follows 5 steps for finding message digest or hash value:

1. Append padding bits

2. Append length

3. Initialize MD buffer

4. Process message in 16 word blocks

5. Output (message digest)

Here, digital signature is a hash value that is encrypted with student's private key and it generates digitally signed file and

digital signature. Further decryption is done by company using student's public key and they verify it by accepting or rejecting it.

B. Public Key Infrastructure (PKI), which is built on public key cryptography, aims to provide secure communications for various applications such as those supported by the Vehicular Ad-Hoc Networks (VANET).In this section we describe the concept implementation of certificate validation and its performance. The implementation of the project is performed in two modules: (A) Admin (B) Student.

For the admin to issue a certificate to the user the system implementation step is perform by admin and student are as follows:

Admin:

(1) Login.

(2) Add database with updated form.

(3)Add company details.

(4) Show result how many student can attend the particular company.

(5) Store company details.

(6) Database containing student past academic record.

Student:

To appear for the company process the student need to add the percentage of the academic years and special skills for the certificate generation of the individual user.

The certificate issued contain a public key for individual which can be accessed by the company to encrypt data of the student.

Security Analysis

Public Key Infrastructure (PKI) is a system designed to manage the creation, distribution, identification, and revocation of public keys. To ensure secure transfer of data from one end to another end and to ensure that public key is used only by its user. On one end a person encrypts a message using a public key, and another person at the other end decrypts the message using his private key. In this we developed a decentralized application and designed a certificate system based PKI. This technology was selected because it is incorruptible, encrypted, and track able and permits data synchronization. The system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates. A public key certificate, known as digital certificate, is a electronic document which proves the owner of the particular public key. The certificate contain information about the public and the private key, information about the identity of the owner whose certificate is generated and the digital signature of an owner documents. The certificate is an electronic document that contains the company information and the public key. The certificate holder accepts the request, which helps to produce a public certificate. During browsing, this public certificate is served to any web browser that connects to the company site and proves to the web browser that the certificate holder believes it has issued a certificate to the owner of the company site. In practice, a desired user gets a certificate by applying to a higher authority with certificate sign request.

IV RESULTS:

Here in this paper we are presented the new technique by using the QR-code generation library (Zxing) in java .In last technique the secure guard is designed to provide faster and efficient validation of certificate.

CRL is used and sent to the client then it is up to client to download the CRL and update yourself.

In our system we are not sending the CRL to the client we are giving the E_ certificate along with QR-code to the client .

Client will scan the QR-code and can see the documents of his.

V CONCLUSION

In this paper, we intensively analyze and study a certificate validation system using PKI, a validation system that resolves many limitations exhibiting in current certificate validation method. This system can be used for validating any certificate for its genuineness, by validating the certificate the end user (company) can be sure about the authenticity of the client (students).

Data security is one of the major features of public key infrastructure technology. It's a large and open-access online ledger in which each node saves and verifies the same data. Using the proposed public key frastructure-based system reduces the likelihood of certificate forgery. The process of certificate application and automated Certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security.

REFERENCES

[1] Towards Short-lived certificate by E.Topalvic, B.saeta in 2015.

[2] RevCast: Fast, Private Certificate Revocation over FM Radio by Aaron Schulman , Dave Levin , Neil Spring in 2014.

[3] Analysis of SSL Certificate Reissues and Revocations in the Wake of Heartbleed by LiangZhang ,DavidChoffnes in 2014.

[4] ARPKI:At-tack Resilient Public-Key Infrastructure by David Basin ,CasCremers in 2014.

[5] SecureGuard: A Certificate Validation System in Public Key Infrastructure by Arwa alrawais ,Jiguo Yu in 2018