Trust Negotiations Using Cryptographic Approach

Sandeep.V

Student, M.tech[IT-Networking]
VIT University
Vellore, India

Gitanjali .J

Asst Prof ,SITE
VIT University
Vellore, India

***Abstract*-Security involves , any person or an organization has certain entities or attributes which cannot be disclosed directly to any other organization or third person , so the main idea of our project is to safe guard or encrypt the very sensitive entities of a person or organization by encrypting them by using the public key generated and decrypting them by using the private key which is generated at the initial key generation stage. After which public key is used for the encryption and generated private key pair is used at the time of decryption.**

***Keywords*- Key generation, Optimal Asymmetric encryption algorithm(OAEP),Encryption, Decryption.**

INTRODUCTION

As long as the online and the internet related transactions dominate this present world , security is always the compromised issue which has to be and need to be given the highest priority. There is every vulnerability of threat for the crucial data submitted by the user. Some of the crucial data and the sensitive data concerned to a person or entity include Name, Employee ID, salary, Passport number etc , so user or the customer has to be very cautious that the data which he has submitted is not subjected various attacks like Masquerade, SOURCE REPUDIAION , DESTINATION REPUDIATION and other form of active or passive attacks by the administrator or the external entities[1] . The main goal in this project is to avoid the user data from being attacked[2]. Initially a journey portal is maintained by the administrator having an account to himself and also facilitates services to other users by giving additional accounts to user also. First user creates to himself an account to himself by using user USER NAME AND PASSWORD , afterwards he submits his detailed profile which include some of the entities like NAME , AGE , SEX, PASSPORT NUMBER, ,SALARY . In these information submitted by the user which include some of the very sensitive entities which cannot be disclosed to the other user or even the administrator which include PASSPORT NUMBER , SALARY etc[6]. So is the responsibility of the administrator to encrypt these crucial information and should be disclosed by decrypting the information when ever required for carrying on to the subsequent process. Soon after the he registers his profile and submits his profile is submitted to the administrator with decrypted values and the even though after the user himself after registration wants to see his profile he has to submit the private key generated .

PROBLEM DEFINION

As long as the web based applications are dominating the present world security would be the pivotal and the central issue .The main issue which concerns is how effectively we provide this security so that attacker would not be able to obtain the illegal access with the user credentials which he has given. Majority of the threats which revolve

around tampering, compromising, illegal access to the sensitive information of the person. Current system which includes that in any online transaction strategy the administrator maintains the portal he could access all the crucial information pertaining to the user like the passport number, credit card number, salary so if the administrator is compromised, from him some one could access all the crucial information pertaining to the user . If not the administrator of some other person could retrieve the some of the sensitive information like the USER ID or PASSWORD of our account of our some applications he could access services stipulated to us illegally.

RELATED WORK

In order to address the above two problems and to give priority for the security issue the following strategy is used . The main crux of the project lies in the providing security includes identifying most important and sensitive fields given by the user .This could be done by selecting the most important and crucial field selected and there by encrypting it with the key and there by keeping this key as a referral for all other future negotiations .

The purpose of this negotiation is that it avoids the crucial issues to be blocked so that even the user cannot see his profile until he gives the key and the profile number correctly. So for the administrator even though if he refers to the profile of the user he could not get the real values since all the crucial values got encrypted. For the decryption methodology to be soon after the user posts his profile by selecting the important fields to be encrypted and submitted the profile immediately he will get an SMS getting his key and the profile number .So again after logging in when the user want to access the services he needs to give input of the key which is allotted to him immediately decryption algorithm activates and decrypts all the values which are decrypted and we will get the plain text values which are given at the time of the initial registration of the profile. The main advantage of this technique is either the administrator or the if other user intrudes into out account he could not use the services since he as to submit the profile number and the key correctly then only he could access the services.

OVERVIEW OF TECHNIQUES

Key generation

Before proceeding to the encryption or decryption step first we have to generate the public key and the private key . The plain text have to be encrypted with the public key generated and decrypted by using the private key .This private key and public key could be generated by using following methodologies .

First choose initially two large prime numbers p and q

Calculation of n= p*q

Now calculate f(n)= (p-1)(q-1)

Choose e in such a way e should be in between 1<e< f(n)

The value of e could be calculated in the following manner that GCD(f(n), e) =1 .

The GCD could be calculated by the Euclidean's algorithm. e and f(n) are cop rimes

Now e could be assumes a the public key component.

Now determining d could be done in the following manner $d = e^{-1} \bmod \varphi(n)$

d is the multiplicative inverse of e^{-1} mod φ(n)

This could be found by extended Euclidean's Algorithm

Now d could be used and a private key

A. Optimal Asymmetric **Encryption Algorithm(padding Scheme)**

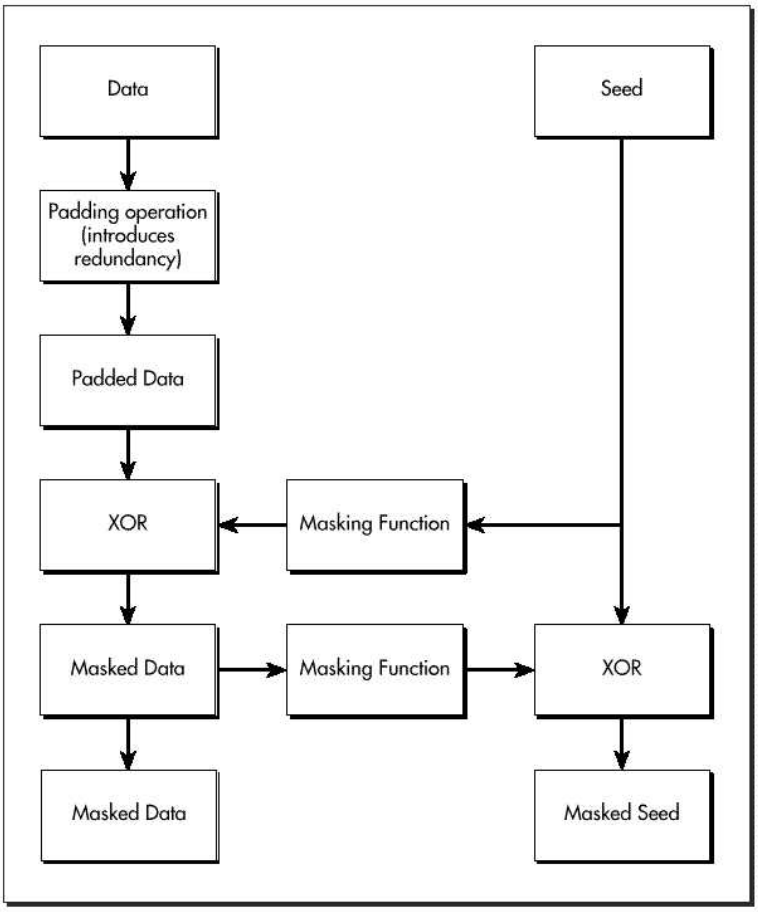
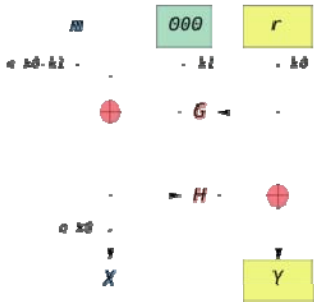


Figure1:The process of Optimal Asymmetric encryption padding.

This scheme is mainly used to calculate the value of m from the give plain text to convert into the cipher text as well to retrieve back the obtained plain text binary format after decryption into the original plain text format.



'N' is number of bits in the RSA module
k0 and k1 are fixed integers by protocol
m is a plain text message, an (n-k0-k1) bit string
G and H are the cryptographic hash functions prescribed by the algorithm.
To encode:
Messages are padded with k1 zero's to be n-k0 bits in length
r is random k0 bit string.
G expands k0 bits of r to n-k0 bits
$X = m00..0 \oplus G(r)$
H reduces n-k0 of X k0 bits
$Y = r \oplus H(X)$
X become the value of m

To Decode:

The decoding process to be activated when the decryption is carried out and the obtained plain text is in the binary format. This binary plain text could be retrieved back to the actual given text by using the following decoding techniques.

To recover random string could be calculated as $r = Y \oplus H(X)$

To recover main message as = $X \oplus G(r)$

B. Encryption

The encryption here could be defined as taking the public key set and converting the plain text into cipher text by using the public key This could be done by employing the following formula

$c = m^e \pmod{n}$.

C. Decryption:

Now the encrypted message could be decrypted by decrypting the message with user's private key. So when even ever the receiver give the correct pair of public and private key only he could decrypt the information. This could be done with following formula:

$m = c^d \pmod{n}$.

m could be obtained by reversing the padding scheme.

PROPOSED SYSTEM

In the existing scenario generally taking the exception from the financial and some other mercenary websites the other type of web sites which include shopping websites, and some other general purpose registration websites generally either the administrator is given the whole responsibility for the protection of the sensitive data provided by the or other user could intrude and tamper all the sensitive information provided by the user, this is generally the existing scenario and in the proposed system ,Soon after the user registers the profile , the sensitive attributes provided by the user are decrypted by using the public key generated and stored in the decrypted format in the database. Neither the authenticated user or the administrator could retrieve the original data supplied by the user unless until he supplies the valid key that used for encryption is supplied to it . So , this terminology clearly safeguards the sensitive information provide by the user without taking any external help of the other organization for the security . So clearly here sensitive information provided by the data is secured profoundly.

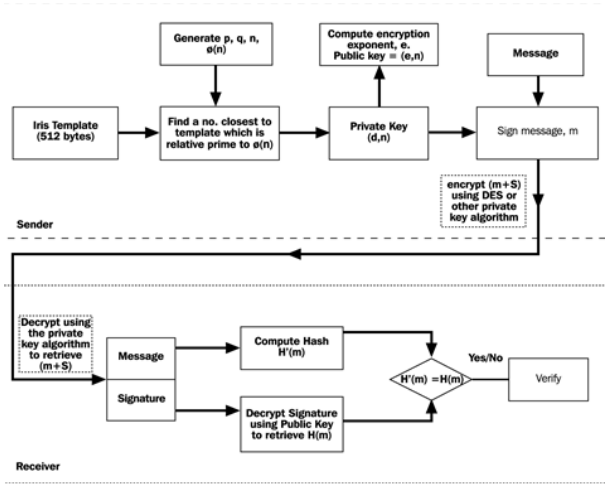


Figure2. Modular diagram for encryption and decryption methodologies.

RESULTS

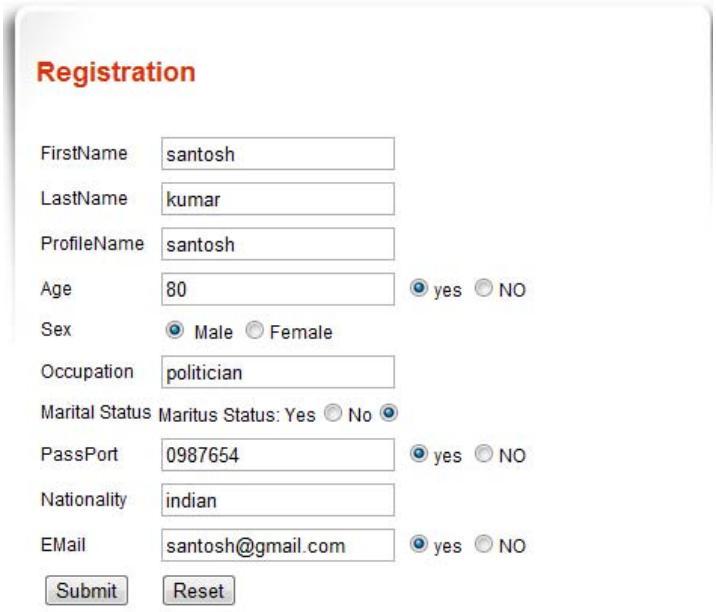


Figure3.Encryption of required values(Sensitive values with public key)

Figure4:Encryption with public key.

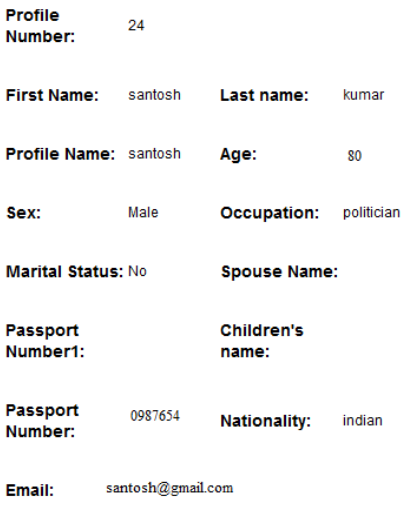


Figure5. Decrypting with the private key pair to get original values.

CONCLUSION

In this paper we have addressed the problem of privacy preserving in trust negotiations. We have introduced the concept of privacy preserving disclosures. These disclosures which include encrypting all the sensitive information that is specified by the user and disclosing the information whenever the user gives the correct private key is submitted . Hence privacy is preserved.

REFERENCES

[1] E. Bertino, E. Ferrari, and A. Squicciarini, "Privacy Preserving Trust Negotiations," Proc. Fourth Int'l Workshop Privacy Enhancing Technologies, 2004.
[2] E Bertino, E. Ferrari, and A. Squicciarini, "Trust-X—A Peer toPeer Framework for Trust Establishment," IEEE Trans. Knowledge and Data Eng., vol. 16, no. 7, pp. 827-842, Apr. 2004.
[3] E. Bertino, E. Ferrari, and A. Squicciarini, "Trust Negotiations: Concepts, Systems, and Languages," IEEE Computing in Science and Eng., vol. 6, no. 4, pp. 27-34, 2004.
[4] P. Bonatti and S. Kraus, "Foundations on Secure Deductive Databases," IEEE Trans. Knowledge and Data Eng., vol. 7, no. 3, pp. 406-422, 1995.
[5] P. Bonatti and P. Samarati, "Regulating Access Services and Information Release on the Web," Proc. Seventh ACM Conf.Computer and Comm. Security, 2000.
[6] S. Brands, Rethinking Public Key Infrastructure and Digital Credentials.MIT Press, 2000.
[7] A. Herzberg et al., "Access Control Meets Public Key Infrastructure,or: Assigning Roles to Strangers," Proc. IEEE Symp. Security and Privacy, 2000.
[8] R.D. Jarvis, "Selective Disclosure of Credential Content during Trust Negotiation," master of science thesis, Brigham Young Univ., Apr. 2003.
[9] M. Marchiori, L. Cranor, and M. Langheirich, "The Platform for Privacy Preferences 1.0 (p3p1.0) Specification," W3C Recommendation, Apr. 2002, http://www.w3.org/P3P/brochure.html.
[10] T. Yu and M. Winslett, " A Unified Scheme for Resource Protection in Automated Trust Negotiation," Proc. IEEE Symp. Security and Privacy, 2003.
[11] T. Yu, M. Winslett, and K.E. Seamons, "Supporting Structured Credentials and Sensitive Policies through Interoperable Strategies for Automated Trust Negotiation," ACM Trans. Information and System Security, vol. 6, no. 1, 2003 .