Secret Sharing Key Management Protocol For Secure Data Sharing

M.Mahasakthi[1], S.Nandhini[2], N.Sindhuja[3], S.Kayathri[4]
[1, 2, 3] Dept of CSE
[4]Assistant professor, Dept of CSE
[1, 2, 3, 4] P.S.R.Rengasamy college of engineering for women

Abstract- *When ownership of mobile devices is becoming more common (e.g. a person owns several mobile devices), the need to provide safe and user-friendly security is becoming increasingly relevant. A significant number of identity-based user authentication methods for the mobile wireless world have been suggested. However, they are not usually meant for cases when a user private key and any other confidential data could be compromised when his or her mobile device is remotely or physically manipulated by an intruder. Secret sharing is one of the solutions to this issue, although it is constrained by the fact that there should be an honest third party to keep the full key until the secret restoration process. Therefore, in this article, we consider the special case where only two devices (i.e. no honest party) on the user side jointly perform user authentication with the server, and neither system can effectively complete the authentication process on its own. In addition, key reconstruction is not needed during authentication so that neither system can hold a full key. The proposed scheme is composed by SECURE SECURITY GENERATION KEY ALGORITHM. The efficiency review of the proposed scheme is also presented in order to illustrate its practicality.*

Keywords- Authentication, Confidential, Intruders , Secret sharing , Private key.

I. INTRODUCTION

It is necessary to provide a secure transfer of information between the sender and recipient, so the process of encryption is one of the mechanisms that provide information security when data is transmitted, a secure method must be provide because today security has become an important resource. The main purpose of security is to transfer important and sensitive information protected and unreadable only by an authorised or recipient persons. Data protection is an important way to provide a powerful tool is the use of encryption, which depends on many of the security mechanisms in the process of encryption and decryption of information. Encryption allows us to store sensitive data securely or transmit it over networks that are insecure that cannot be understood by anyone just the recipient. To gain privacy, integrity and data integrity, the use of encryption is a powerful tool. Encryption distinguishes between two types of public encryption and private encryption, which has an ancient history, one secret key is used for encryption and decryption in this symmetric encryption and two keys are used in an asymmetric encryption, one public and the other private. However, asymmetric encryption is one of the coding techniques, which is thousand times slower than analogy, because it requires more computational processing. ECC used for an asymmetric key generation for the recipient. Moreover the key size of ECC is very small comparing with other methods and it is easy to generate and share data quickly.

II. LITERATURE SURVEY

Abdul hadi bin sulaiman generated a novel secret key based an image link, one of the main problems with this symmetric encryption is key distribution especially when involving large number of users i.e.,identical keys at different locations.

Amirudhin, Riri fitri constructed and analysis of generation algorithm for privacy preservation, Linear algorithm cryptography key is the most important factor for supporting encryption of confidential data before it is transmitted in a communication network. Cryptographic key has properties of random sequence and long period.

Isratjahan, Mohammad asif was improved RSA cryptosystem based on the study of number theory and public key cryptosystem security is required to transmit confidential information over the network. Security is also demanding a wide range of applications.

III. PROPOSED SCHEME

Secret sharing key is the method of sharing common temporary key to reduce the information leakage. Information was encrypted to provide more security. This temporary key can be used only once. Key size will be reduced by use of ECC algorithm.

Modules

1.Data sharing middleware

The systems that are in place to ensure that the data is kept to private and secure.

2.Key generation

How keys are created and for whom.

3.Secure data sharing

Ensures that the data is kept secure at all times, using either software or hardware isms.

4.Access control

Ensures that the data is used as per the rules set by the data owner.

5.Sender

User can send message to other user by using division algorithm.

6.Receiver

Receivers login with username and password. Receiver needs to enter secret key and they can get the original message.

IV. ALGORITHMS USED

SSGK

It is used to protect the communication between user through mail by providing private key for secure data sharing.

DIVISION

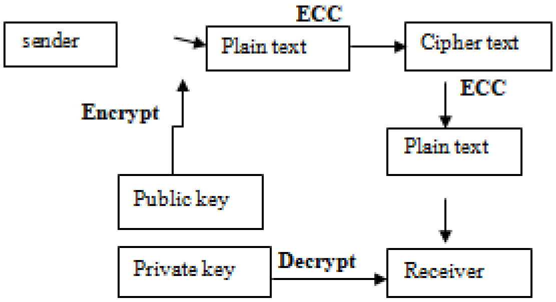
Division algorithm is an algorithm which given two integers N and D, computes their quotient and/or remainder, the result of Euclidean division. Some are applied by hand, while others are employed by digital circuit designs and software.

Formula :$a = bq + r, 0\leq r < b$.

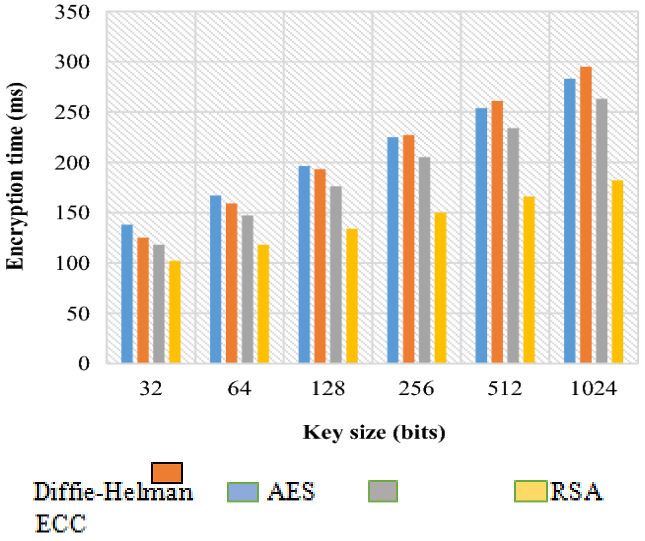
ECC

ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA and Diffie-Hellman.

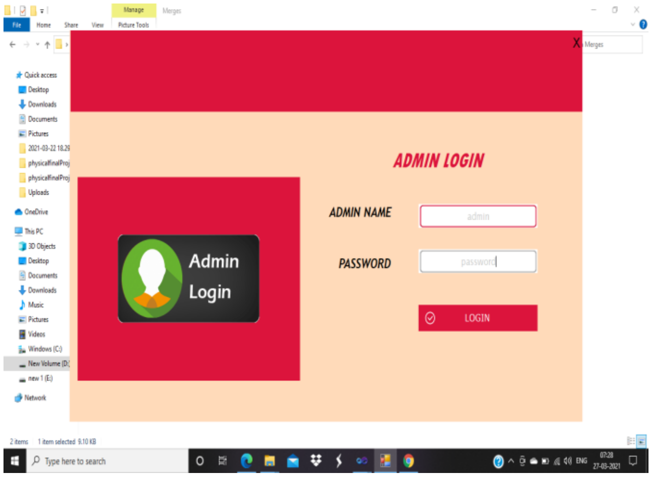
Formula : $y^2=x^3+ax+b$.

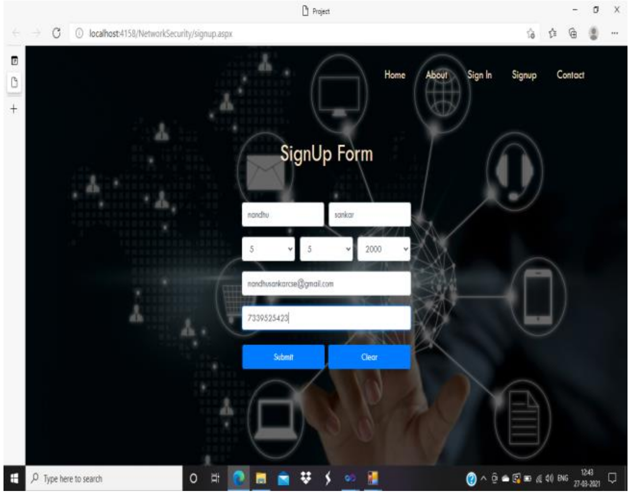


(Architecture)



V. RESULT





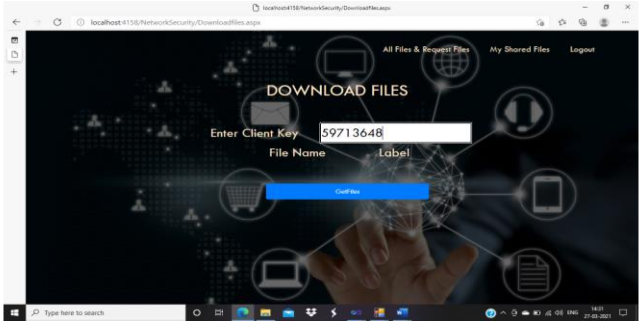
SignUp Form

nandhu sankar

5 5 2000

nandhusankarcse@gmail.com

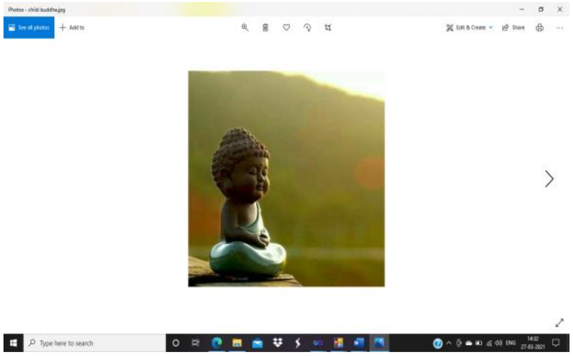
7339525423


localhost:4158/NetworkSecurity/Downloadfiles.aspx
All Files & Request Files
My Shared Files
Logout
Type here to search

DOWNLOAD FILES

Enter Client Key 59713648

File Name Label



VI. CONCLUSION AND FUTURE WORK

We reviewed a different key generation for different algorithm. The main problem arise while sharing data is security problem. We proved the generation of private key solves the problem of security loss with small temporary key and less time complexity. Possibilities of developing secret key as an application in mobile devices using java successfully.

REFRENCES

[1] Zijie Ji, Hao Yin – 2020 : “Vulnerabilities of Physical Layer Secret Key Generation Against Environment Reconstruction Based Attacks”.

[2] S. Chen et al., - 2019 : “Learning-based remote channel inference: Feasibility analysis and case study,” IEEE Trans. Wireless Communication

[3] E. V. Belmega and A. Chorti - 2018, “Protecting secret key generation systems against jamming: Energy harvesting and channel hopping approaches”.

[4] J. Zhang,R. Woods - 2016, “On the key generation from correlated wireless channels,” .

[5] J. Zhang, A. Marshall-2016, “Key generation from wireless channels: A review,”.

[6] C. Wang, and W. Wang - 2015, “On the 3-D MIMO channel model based on regular-shaped geometry-based stochastic model,”

[7] H. Liu, J. Yang-2014, “Group secret key generation via received signal strength: Protocols, achievable rates , and implementation, .

[8] S. N. Premnath et al-2013, “Secret key extraction from wireless signal strength in real environments,”,.

[9] J. W. Wallace and R. K. Sharma-2010, “Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis,” .

[10] Hardjono T. and Dondeti L. (2005). Security inWireless LANS and MANS.