International
Journal
Of Advanced Research in Engineering & Management (IJAREM)

Security Supporting Mechanism for Exchange of File

Komal Sonkamble[1], Sagar Mudgal[2], Jyoti Vidhate[3], Aakash Mehta[4]
** (Department of Computer Engineering, Savitribai Phule Pune University, India)*
*** (Department of Computer Engineering, Savitribai Phule Pune University, India)*
**** (Department of Computer Engineering, Savitribai Phule Pune University, India)*
***** (Department of Computer Engineering, Savitribai Phule Pune University, India)*

ABSTRACT: *In today's information world despite the increasing awareness of security, malicious failures are inevitable in the modern world. Sharing of data has boosted information exchange on both the personal and business levels. There is a need of the authentication of messages sent by a group of individuals to another group. Due to unreliability of a single entity in an information environment we want to create the trust relation between the groups of entities. So transferring file securely has become and necessity. In most of the situation the sharing of file sharing happens between two entities.*

A secret sharing scheme allows one to distribute a piece of secret information between several entities. Following some ideas of the File Transfer scheme has been tried to enhance using some encryption technique and tried to improve the use of such protocol in regular life.

Keywords: *Compression, Cryptanalysis, Cyberannoyance, DES (Data encryption standard), EasySMS, Encryption, SafeChat.*

I. INTRODUCTION

In the ever changing world of global data communications, inexpensive Internet connections, and fast-growing software development, security is becoming more and more of an issue. Security is now a basic requirement because global computing is insecure. As your data goes from point A to point B on the Internet, for example, it may pass through several other points along the way, giving other users the opportunity to interrupt and even alter it. It does nothing to protect your data center, other servers in your network, or a malicious user with physical access to your system. The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents.

Encryption

Cryptography is used whenever someone want to send a secret message to someone else, in a situation where anyone might be able to get hold of the message and read it. It was often used by generals to send orders to their armies, or to send messages between lovers.

Decryption

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer are able to read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.

II. PROBLEM DEFINITION

In today's information world despite the increasing awareness of security, malicious failures are inevitable in the modern world. So sharing the file is essential. Most of the time physical medium is used such as Pen Drive, CD etc. So to improve the efficiency to transfer file we can use File Transfer Protocol to share the file if the computers are connected in the network.

III. PROPOSEDSYSTEM

As we have seen that now a day's security is the main aspect of concern in the digital world and transferring file from one place to the other is an important issues which mostly concerns the individual. To avoid unauthorized

access to the file we are trying our best to implement the best security to the file so that no un-authorized access is permitted to the file.
As the DES is the basic and fast to implement we will try to use and focus on boosting the security mechanism of the file by adding extra measures to it. As the DES will try to handle the little security measures.

We will also try to compress the data so that the time required to encrypt the file will reduce and so on the decryption time this will result in the boost in the performance of the system. With the help of the reduction in the data due to the compression will also give the added advantage in transferring in the file, as the file will be compressed so the size will get reduce so the network traffic it will require will also get reduce. So, this compression will give added advantage of speed in the network as well as the performance boost of the system to handle the file in the encryption and the decryption process. For exchange of keys we will be trying to try use the algorithm defined in the EasySMS.

After the handling performing some of the data manipulation on file we might achieve the more security than just use of the DES Algorithm.

But to improve we are planning also to introduce the time stamp system in the project, which will help to increase the security and also provide us whether the file is received to the legitimate user or not. As the introduction of time stamp will allow the user to know whether they are providing the file to another legitimate user or some other autonomous bot which is trying to breach the system. The time stamp will be in such a way that it will be decided by the sender and the receiver will need to enter the pass key in the given amount of time only else the file received by the user will be deleted or it will get converted into the unreadable format.

IV. IMPLEMENTATION

Implementation consists of the overall procedure and methodologies involve in creating a new system. Proper implementation is necessary to develop an efficient and reliable system to fulfil organization requirements.

1. Modules

1.1. File Manipulation:
This is the main module of the system, it deals with the core concept that is the transfer mechanism of the file from one user to the other. In this the basic exchange of file is performed.

1.2. Encryption/Decryption:
This is the section which deals with the encryption and the decryption work, in this we have used DES algorithm for encryption and decryption purpose, as it is simple it implement and its speed is fast
If the decryption fails then the notification is sent to the sender, that the decryption was unsuccessful, else the success message will be transmitted.

1.3. Timer:
This is the constraint which is imposed to enter the key, for the decryption. The user should enter the key in the given time, else the file obtained will not be decrypted.

1.4. Chatting :
This module has also been added in the system so that the users can communicate with each other in the ease.
There are 2 types of chat, Group Chat and Private Chat.

V. CONCLUSION

We have tried to ease the use of File Transfer mechanism, and also tried to secure the exchange of the File over the network. Also to improve the security the time constraint as also been added. As well to ease and provide extra facility to the users we have also added the chat feature, in which groups chat as well as individual chatting can be performed.

VI. FUTURE SCOPE

We can try to improve the encryption and decryption speed, by improving the algorithms. Also some key exchange algorithm can also be added to exchange of keys.

Acknowledgements

It is with great pleasure that we acknowledge the enormous assistance excellent co-operation extended to by the following respected personalities. Firstly we would like to express our sincere thanks to our respected Principal Prof. Dr. Sachin Admane sir for providing us the necessary infrastructure, laboratories, requirement and providing us an opportunity to do research work on “Security Supporting Mechanism for Exchange of File”.

We are greatly indebted to, Head of Computer Department, Prof. S.R.Todmal for providing valuable guidance. We would like to express our sincere thanks to our respected Guide Prof. Sonali Tidke for her valuable guidance.

REFERENCES

[1] Neetesh Saxena, Member, IEEE, and Narendra S. Chaudhari, Senior Member, IEEE , *" EasySMS: A Protocol for End-to-End Secure Transmission of SMS "* , *Information Forensics and Security, vol.9 ed.7, pp. 1157-1168, July. 2014*

[2] G¨unter Fahrnberger [University of Hagen], Deveeshree Nayak [University of Memphis, Tennessee, Mountain View, California] , " *SafeChat: A Tool To Shield Children's Communication From Explicit Messages* " , *Innovations for Community Services 2014 (14th International Conference), 2014, pp. 80-86*

[3] Atul Kahate, " Cryptography and Network Security", Second Edition, 2009, pp. 59-60,100-120,121-131

[4] J. Daemenand .V. Rijmen, The Design of Rijndael: *AES - The Advanced Encryption Standard*, SpringerVerlag, Berlin, 2002.

[5] E. Biham and A. Shamir, Differential cryptanalysis of DES-like cryptosystems, J. Cryptology, 4, 1991, pp.3–72.