ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 8, August 2015**

# A New Concept on Key Based Secure File Transfer Mechanism

Anurag Singh[1], Siddharth Pandey[2]

B.E. Graduate, Dept. of Computer Engineering, Thakur College of Engineering and Technology, Mumbai, India[1,2]

**ABSTRACT:** As data is stored in digital format that is in the binary language, understood by machine has proved to be highly beneficial, allowing us to extract and search for particular content of data using various data mining algorithms. Multiple copies of the same data can be easily created for backup and future reuse. As our digital data can be copied and shared easily, it becomes vulnerable to data theft. Few mechanisms has been created to prevent data leaks that include securing our data by a password, encryption of data, but that too can prove to be ineffective by various other counter effective techniques such as brute force attack, etc. Tracking unauthorized users is yet a challenge. This paper presents a method that may help us to keep track of our data transfer along with tracking the unauthorised user and try to prevent data theft or leakage to a certain extent.

**KEYWORDS**: Data theft; Data leaks; secure file transfer; Tracking; read-only –no copy; one time file access.

## I. INTRODUCTION

In digital world the most precious asset is the data that may include highly confidential material. However due to the expansion of technology and internet, almost all the data is stored in the form of electronic digital data. Copying of this digital data is can be done very easily and hence it is alarming how easily one can access that confidential data without even getting traced. Even if a file is encrypted or password protected, by using sheer brute force and other techniques [5**].** One can simply though illegally gain access to that confidential digital data. A file that is password protected or encrypted is like a safe, and in digital world one can create another copy of that whole safe and then try to crack it. Tracking of such activity is a difficult aspect of the process as cracking is performed on a copy of original data.

Digital world unlike the actual world, allows us to copy the data in form of bits allowing us to create multiple copies in a flick. Here one can create almost unlimited copies, at our whim and never even keep track of the individual copies [2]. A hacker for example can install a password detection software on a computer that not only sees (copy of data) and records the passwords typed by the user but also sends it to the hacker (uncontrollable transfer of data) without the person even knowing that his passwords have been leaked.

Digital data can be copied very easily, as this feature is very handy but can be removed just easily allowing us to use digital data as real world objects. Real world object cannot be just cloned that easily, and require a whole process to do it. For example copying a piece of paper will first require it to be scanned (digital format) then be printed again. Creation of another car in a factory will require new assembly of new parts of the new car. So to prevent copy or even editing one can create a read-only –no copy mode by creating a new interface. Standard file explorers like Windows file explorer can be clubbed with third party applications (M File Anti-Copy) that secures a file and even prevents the whole file or a part of the file from being copied or renamed. So creation of a new file explorer interface that prevents copy command can be easily achieved. One can also achieve the task of determining how many times a file has been open. So one can say that one can delete the file if it has been opened once or n number of times by using a script program that is the part of the whole file explorer interface.

## II. RELATED WORK

In [1] authors have introduced secure RSA for secure file transmission. There are many cases where one needs secure file transmission for example in banking transactions, e-shopping etc . In this paper authors present modified RSA algorithm for secure file transmission. RSA algorithm is asymmetric key cryptography also called Public Key

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 8, August 2015**

cryptography. The paper focuses on file transfer using Secure RSA, which eliminates some loopholes of RSA that might prevent a hacker from stealing and misuse of data.

Paper [2] describes a general purpose trace back mechanism based on probabilistic packet marking in the network. Their approach allows a victim to identify the network path(s) traversed by attack traffic without requiring interactive operational support from Internet Service Providers (ISPs). Moreover, this trace back can be performed "post mortem"--after an attack has completed. The paper presents an implementation of this technology that is incrementally deployable, (mostly) backward compatible, and can be efficiently implemented using conventional technology.

In [3] authors have described a security system using for domestic applications Radio-frequency identification (RFID) is the wireless non-contact use of radio-frequency electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by and read at short ranges (a few meters) via magnetic fields (electromagnetic induction). We use the RFID reader for domestic applications using an Atmega 328(Arduino) microcontroller.

In paper [4], authors present a unique concept of combining different PPDM techniques which provides high level security and integrity to confidential data. One of the latest concept of PPDM called Slicing which preserves better data utility and authors have merged slicing with one of the best security mechanism that is Cryptography.

In [5] the authors present their view on current encryption algorithms, in particular on private key block ciphers which are widely used for bulk data and link encryption. The authors have initially surveyed some of the more popular and interesting algorithms currently in use. This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study all the techniques together as a literature survey. This study extends to the performance parameters used in encryption processes and analyzing on their security issues.

## III. RESEARCH CHALLENGES

Data loss, Privacy theft and many actions that compromise data confidentiality has been a potential threat to one's private data online. Various algorithms have been created that prevent data loss and provides privacy preserving of individual data [5]. Since data on internet can easily be copied and then manipulated, tracing such activities has been a challenge [4]. Original data can easily be prevented however on a copy of original data various manipulations can be done without letting the data owner know about these manipulations. Tracking of actions such as cut, copy or paste on a file is a big challenge as the file resides in network of networks.

The challenge of preventing a file from illegal or unwanted access can be easily explained with the help of an example. Suppose a person 'X' wants to send a file encrypted with a password to person 'Z' [5]. 'X' tells 'Z' the password and person 'Y' overhears 'X' telling him the password. Person 'Y' may then try to copy the file from X's computer by secretly accessing his computer, or by trying to hack X's or Z's emails. Y then creates a copy of that file in a matter of seconds and takes the file with him in an external storage device. X may not even know this that his data has gone into wrong hands and also he does not know that it was Y who did it.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 8, August 2015**

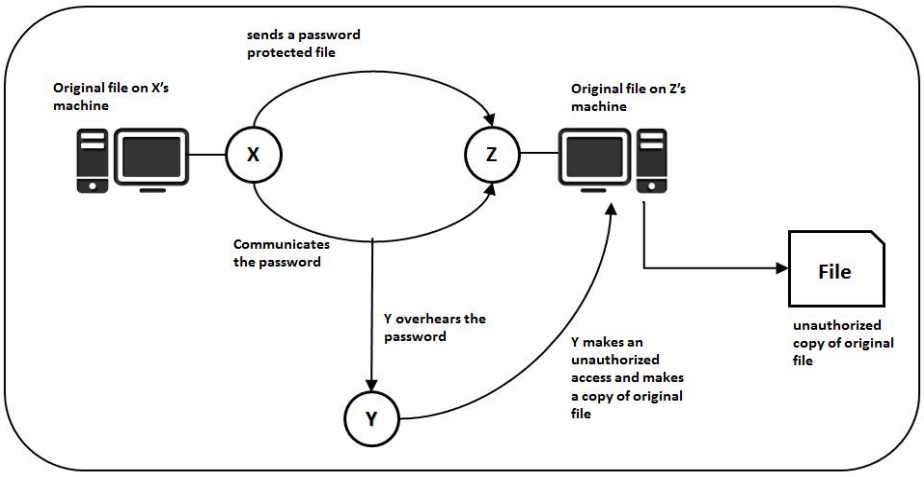


Fig. 1. Undetected File copying by unauthorized user

Even if one encrypts or protects his file using a password, allowing only limited attempts, one can simply create multiple copies of that same file and as one file collapses after all the attempts have been used, he can switch over to the next file. There are even more methods to try to crack into the file, as the data within that file that is being tried to be accessed. There needs to be a way of not only allowing access to person with the password but also keeping track of the person who accessed it [2]. Thus our aim is to keep track of file manipulations right from the basic actions of copy pasting and making it unusable after a set of operations performed on the file.

## IV. OUR PROPOSED METHODOLOGY

This method requires a creation of a new file explorer interface that does not allow copying of a file and can also additionally have a feature that allows deletion of a file that is once accessed. To download a file into the new explorer one requires a key to the file. The key provides an access to the file from a secure server created by third party, that tracks the usage of the keys and when the keys were used too.

A person X wants to send a confidential file to person Z. X first uploads the file onto the secure server telling the server the number of keys required as per the number of people he wants to send to. The server then sends the keys to X. Each key has a unique identity by which we can keep track which keys have been used. The key will also determine if the document can be accessed exactly once or will be deleted after a single access. The recipient of the key will use the key to download the file in the new interface. The new interface would then prevent the file to be copied or prevent multiple copies of the file. The user can read the file exactly once, as, if the file is read once it will be deleted from the interface. This feature would prevent the file from being accessed without being noticed. That is if an unauthorized person accesses the file in the interface it would be deleted from that interface, making the actual recipient know that the file was accessed.

The sender X can also put a password on the file preventing it from being accessed by unauthorized person. A key cannot be used twice as the server will know that from the unique identity the key has been assigned that the key has already been used. Additional security can also be put on the file by notifying the sender when the keys are being used and can additionally ask the sender for permission to allow the recipient to download the file from the server.

## V. CONCLUSION AND FUTURE SCOPE

Additionally we can add more number of protection mechanisms to this method. Like tracking of the IP address of the computer which downloaded the file can be stored by the server [2]. By this we can also see that exactly where the file has been downloaded by which we may be able to track the unauthorised user who has downloaded the file. The sender can also prevent the server from allowing anyone to download using the old keys and issue fresh keys for the same file

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

**Vol. 3, Issue 8, August 2015**

if he feels the need of it. An improvement in various aspects can be done on this existing methods to improve its efficiency and security.

## REFERENCES

1. Rajan.S.Jamgekar and Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA", *International Journal of Emerging Science and Engineering (IJESE)*, Volume. 1, Issue 4, February 2013.
2. Stefan Savage, David Wetherall, Anna Karlin, and Tom Anderson,"Network Support for IP Traceback", *IEEE/ACM Transactions on Networking*, Volume. 9, No. 3, June 2001.
3. Akshay Punjabi, Siddharth GV, Siddhant Singhal, K.V.N. Kavitha,"RFID security system for domestic applications ", *Publications of problems & application in engineering research - paper*, Volume. 4, Article 11062, pp. 318-321, December 2013.
4. Siddharth Pandey, Priya Singh, Rohan Patil,Harshali Patil,"An Enhanced Approach to Privacy-Preserving in Data Mining and its Techniques", *International Journal of Engineering Research & Technology (IJERT)*, Volume. 4, Issue 2, February 2015
5. E. Thambiraja, G. Ramesh, Dr. R. Umarani,"A Survey on Various Most Common Encryption Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE)*, Volume 02, Issue 7, July 2012.