A Research Study on Java File Security System Using Rijndael Algorithm

Inuganti N.V.A.Pratyusha
Student (M.Tech), CSC,
Gokul Group of Institutions
Visakhapatnam, India.

K.R.Koteeswa Rao
Asst. Prof, CSC,
Gokul Group of Institutions
Visakhapatnam, India.

ABSTRACT:

In the recent electronic world, we are facing various types of dangers to the confidentiality of information. The information is saved on the secondary storage devices e. g. hard disks, compact disks, flash drives, floppy drives, etc. Some dangers are accidental, such as human error, while others are intended. Intended dangers are done by the persons for many reasons like causing harm, disturbance and other frauds. Among these frauds the common one is loss or theft of the storage devices. So, the majority of critical topics of computer world are security of information.

It is focused on preventing information from unauthorized access. Due to increase in the dangers to the important data which is possessed by the users and associations as the data loss results are shown in the thesis. There is a need of a robust solution to the danger of information security. But everyone has their own benefits and limitations. Some are inconvenient to the users or others have technical faults. To protect and secure the data is very much vital than forever. The existing protected file systems are not well used by us. Cryptographic is the technique which is used to secure the computer systems.

The encryption is the technique of the cryptography which is used and can gratify the necessary security needs of the users for computing machines, internet, and the data beside varied dangers set. There are three main security assumptions. These are integrity, availability and the confidentiality. Our main focus is on improving the two characteristics of security namely confidentiality as well as availability, due to the loss of the information and the neglecting the services is the two biggest one attacks.

I INTRODUCTION:

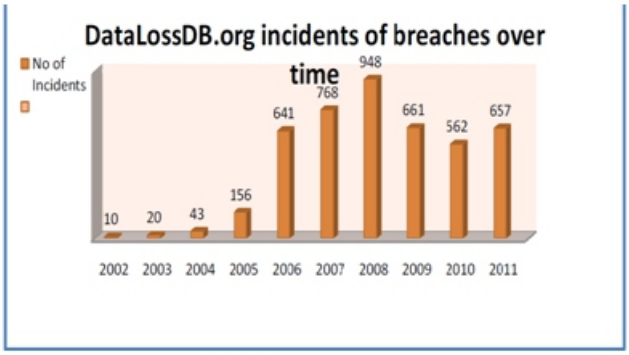
This portion of the thesis will commence the definitions of information, and information security. Also we will know about the significance of information security and the penalties of information security, if we will compromise it. The information is collected through the Data Loss DB (Open Security Foundation) association.

It is a non-profitable association of United States. Data Loss DB (http://datalossdb.org/) is a project of research of United States (but records also losses of worldwide data that include the United Kingdom and European countries) targeted to inform the events of losses of known data and world-wide retrieved.

These are the society's attempts to have knowledge about the great losses in the society. It is an open call to the society by the association that demands the contributors to contribute in their joint attempt to introduce the novel events of the data losses.

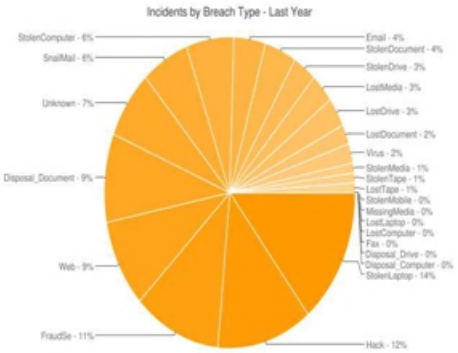
When information is not protected appropriate, it may be impaired and is this as an information or security breach well known. The penalties of an information break are heavy. For commercialization, a breach requires usually gigantic financial punishments, luxurious law processes, loss of the call and business.

For the personal point, a break to individuality stealing and harm can lead at financial story or credit worthiness. It takes so many years to recover from these breaks and is the gigantic costs.



In the starting year of study they were very less only 10 incidents in the complete year which are to be considered by the organization. And after that they st increase till 2008, the year of highest number of incidents takes place.

There is slight down fall till the year 2010. But again they start to increase in the current year 2011. The results are till the month of September, there may be more one till the end of year.



1.1 Cryptography:

It is the learning of numerical practice narrated to facets of information protection for example authentication of entity and data source, confidentialism as well as integration of data . It does not merely provide the information protection, but it is also a set of mathematical techniques.

It is the exercise and revision of covering securely to the information. Recent cryptography interconnects the subjects of mathematical studies, computing technology, and electrical technology. The cryptographical uses comprise Automatic Telling Machine cards, passwords, and e-commerce. At the very early stage it was simply the cipher text that was the nonsense data that is not read by the intruders.

It was only the simple conversion of the data to secure it. As for example it was like, the original word "happy", but after the treatment it was "ibqqz". Now a reasoning person can easily understand the data that it is the single character forward in the English alphabet. But some of the year passes it was much complex that it is not possible for the reasoning person to understand the information. But the computer age grows more the processors with very high speeds.

They can easily find the converted data to the original one. It becomes the challenge for the cryptologists to think about much more accurate and high attach bearers algorithms must be developed by the mathematicians that the computers cannot resolve them easily. There was the use of encryption keys of small size but they are also sorted out easily by the intruders with the help of computers.

Now there are so many algorithms which require the big size keys. At present there are the encryption keys of size 128 bytes, 152 bytes, and 256 bytes.

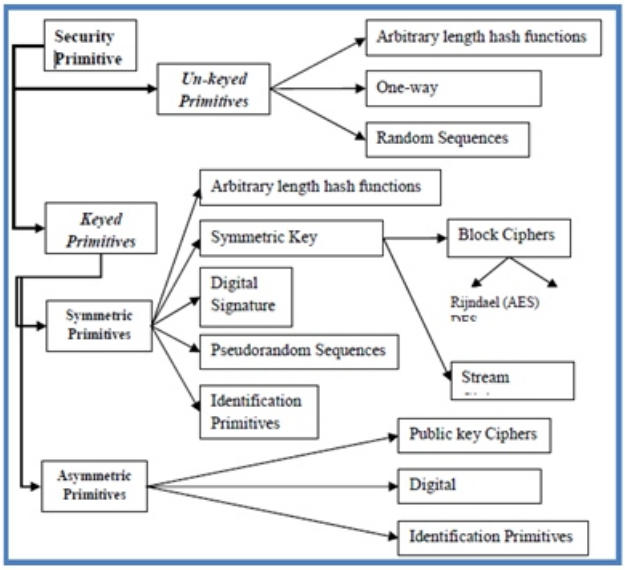
1.2 Steganography:

Steganogrphy is another way to protect the data from the intruders. The information is hided into the other images. It covers the vital information very efficiently that the intruders cannot easily recognize the available information. The terminology is taken from the Greek language. It is the art for communicating in which the availability of the communication is completely hidden. As we compare it with the cryptography where the intruders are permitted to see or intercept or detect or modify the communicating data. In the case of this technique "Steganography", the intruders have no knowledge about the presence of the information.

Cryptographic goals. These are the basic aims for the security providers that are as follows. These are privacy of data (data confidentiality), integrity of data, user authenticity, and non-repudiation. The first three are also very well discussed in the first chapter which is named as "Introduction".

The confidentiality is also called as the privacy of the data. The applications which provide the confidentiality mean they are keeping the data or information in the reach of their permitted users. And keep away the unauthorized users. It has another name that is the secrecy of data or information. It is provided through the use of various methodologies.

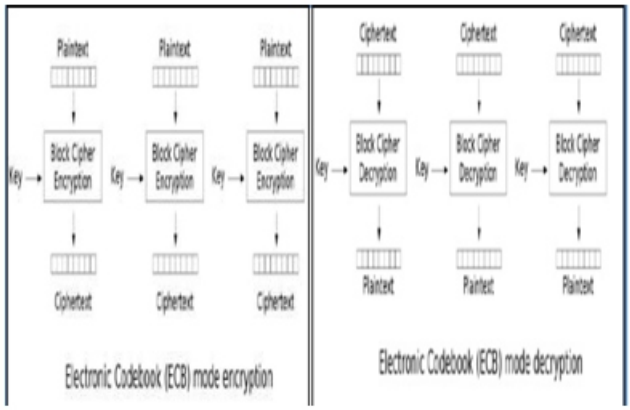
In it the physical security as well as the algorithmic conversions takes place. 2. Integrity of data tackles the problems of data alterations or data modifications. For ensuring the integrity of the data, we must spot the manipulations of data done by the intruders. Any type of data modification can take place like insertion of new data in between, or deletion of the exact data, or substitution of the communicated data.



1.3 Electronic Codebook (ECB):

In this mode of operation, each block is encrypted in the same way. This is the simplest mode of operation to implement, and is easy to do in parallel because there are no inter-block dependencies. The encryption simply runs the cipher block algorithm on each block in the data; see Figure 3.4 for the encrypting procedure, and the decrypting procedure.

This means that two identical plain texts will be encrypted to identical cipher texts. As mentioned it has a severe problem with security. We see in Figure 3.4 that it is possible to distinguish the original picture, and this shows that the encryption with ECB in some cases is not sufficient. One should however, note that even though ECB looks random, it is not a guarantee that the encryption is secure.



II FILE SYSTEM:

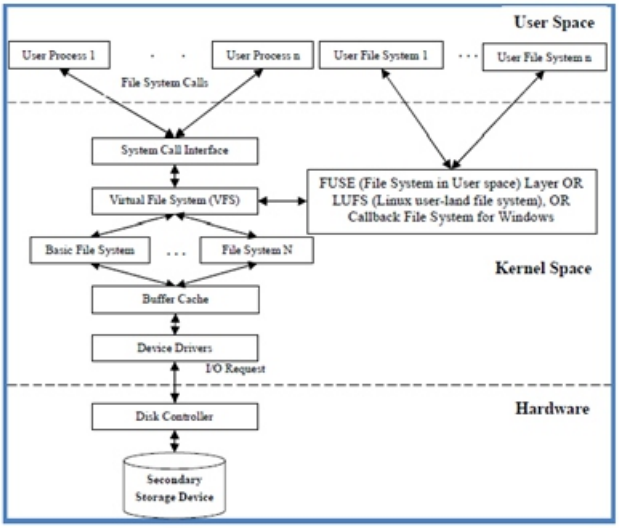
It is the way to store and access the stored data in the form of files that may be information or executatble programs. This chapter covers the high-level details of file systems and the concerned matters like the caches of the storage devices, the interfaces of the file systems, and the user-oriented Application Programming Interfaces which utilizes the file systems characteristics. This chapter will highlight the working of the file systems.

It is the main part of the OS. It is used to create, manipulate, store, and retrieve data. At the highest level, a file system is a way to manage information on a secondary storage medium. There are so many layers under and above the file system.

All the layers are to be fully described here. This paper will give the explanatory knowledge of the file system designers and the researchers in the area. Any file system is an important component of the operating systems. It is utilized to handle the storage devices.

The electronic media is controlled for the file to be stored on it in an efficient way. The media may be of any type like floppy disk, compact disk, hard disk, flash drives, etc. It has a very clear working at the very first look. But it not only stores the data, it also protects them from any type of hazards. There are so many file systems which are one the multiuser operating systems like UNIX operating system.

In such type of configurations the task becomes more typical to handle all the files of many users on a single storage space. For a perfect file system it is mandatory to cover the following tasks Totally control the electronic media which is very novel and it has not been maintained previously, The storage is utilized by the many processes which are the simultaneous one, Intrinsic synchronization is needed for all the processes on the system, The security and the protection are enforced that permits the comfortable data accessing, Management of the independent files by many process simultaneously, Differentiating of the problems within the physical media or rude use of the accessing ways by the operating system. It controls the data that has been lost because of hardware problems, An ordinary collection of the interface functioning must be given to the layers which are above of the file system in the operating system.



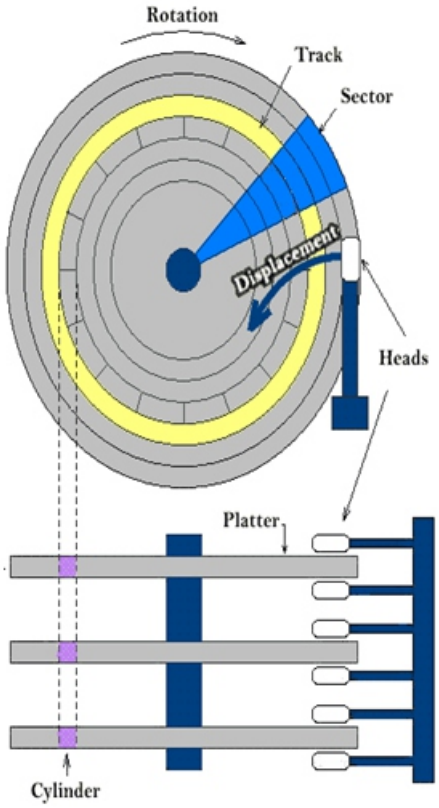
There may be many types of categories of the hard disk drives. These may be arbitrary accessing, digital nature, magnetic nature, and the non-volatile. In nineteen hundred and fifty six, the International Business Machine launched the hard disks. There are numerous names for the hard disk drives like hard drive, hard disk, disk drive etc. This device is utilized to store and access the digital data or information. It is a permanent storage media. It has one or more numbers of the discs which are also known as the platters. These platters are furred using the magnetic material.

These have some of the well arranged magnetic heads which are used for storing and accessing the data on the hard disk drives. Every platter has one or two surfaces for storage of the data. of the basic terminology is described here in this section which is used for the harddisks. In the Fig. 4.2, the basic components of the hard drive are displayed.

There is more than one platter in the hard drive. One or both of the surfaces are furred with the magnetic material. This magnetic material is used for the data storage. Every surface of the platters has on read and write head hovering on it. It is utilized for examining or recording of the data. A common axis is used for rotating all the platters. Usually the rotation speed is in between fifty four hundreds or seventy two hundreds numbers of rotations per minute.

There are also the higher performance hard disks in the market and their costs also increases with better speeds. The older versions of the hard disks have the less revolution speeds. The movements of the head are done along the radius of the platters. It is the combination of the movements done by the rotation head and the rotations of the platters.

There is a communication between the processor and the hard disk with the help of the disk controller that has been discussed previously. This hides the working of the drive from the rest of the applications. While the disk controllers for diverse kind of disk drives are prepared for the use of the similar interface. The controller is also utilized to work for other kind of jobs.



These are like the caching or removing of the bad sectors. From the above readings we can easily know the hardware workings. There are more concepts like the motor that is used to rotate the platters and the movements of the heads backward or forward. The electronics is used to maintain all the operations of the mechanical components. But there is no need to know such workings for us of the hard drive.

DiskController:

A storage device is the fundamental part of any computer system. Usually every computer system has the following storage media Floppy disk drive,Hard disk drive,CD-ROM disk drive,DVD disk drive USB flash drive All the devices are interconnected with the computer with the help of the IDE (Integrated Drive Electronics) interface. . Basically it is the normal path for the storage media to interconnect with the computer system. This is not the actual interface name as the IDE. The unique name for the same interface is the Advanced Technology Attachment (ATA).

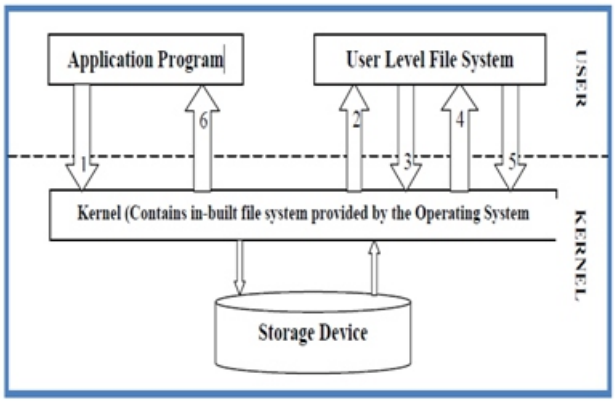
It was developed for the IBM AT machine. Basically the disk controller is a circuitry that is enabled with the processor for communicating with the all types of disks (hard, floppy, DVD, CD, etc.). There are so many types of disk controllers available in the market. Some of these are like Intelligent Drive Electronics (IDE) as well as Small computer system interconnects (SCSI). The IDE controllers are utilized in the desktop computers or personal computers or the standalone computers. Whereas the SCSI is utilized in soaring end personal computers, workstations for professionals and network file servers. All the disk controllers have their own individual processors with independent Random Access Memory buffers. There is also the availability of the Programmable Read Only Memory.

Laptop Hard drive
http://www.computerhope.com

III USER PROCESS FILE SYSTEM:

The idea of developing a file system as a user process is appealing for a variety of reasons not least of which being that it is simpler than other techniques. By developing the file system as a user level process, the complexity of kernel level programming can be avoided. This simplifies the development process enormously, as developing in the kernel is more restrictive than user level development.

The standard development, debugging tools and programming libraries can be used. This helps to reduce the time required to implement the file system. One of the most advantages of developing a file system as a user level process is that the file system can be installed by a user without the assistance of a system administrator. This provides the user with greater flexibility in how they use files. Figure 4.4 illustrates how a file system developed to run in user space interacts with the local and remote operating systems. A user process requests access to a file from a user-space file system. The request is routed through the kernel.



STORAGE ENCRYPTION AND JAVA FILE SECURITY SYSTEM:

Nowadays, the attacks are going to increase at the storage data systems. So the security systems are going to turn into a compulsory attribute of any storage data system. For the security purpose we are always dependent on the cryptography techniques. These techniques take the performance costs for the complete system. So we have proposed the Java File Security System(JFSS). It is based on the on-demand computing system concept, because of the performance issues. It is a greate comback for the system performance.

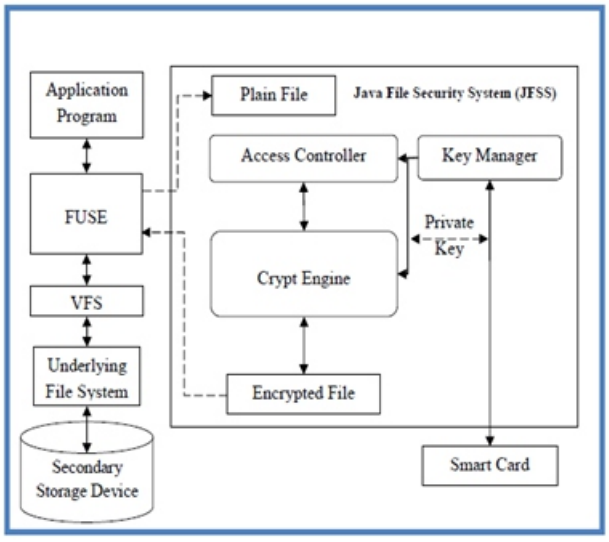
The concept is used because, we are not always in need the secure the files, but the selected one only. The concerned chapter shows the design of the Java File Security System on WindowsXP.

When we use the operating system, we have to secure some important data. The date is always stored in the files, so we secure the important files well. To check the proposed functionality, we experiment the above said system on the Windows operating system. With these experiments, we have found that the proposed system is working properly, according to the needs of the users.

The access control is one of the fundamental security services in the computer system. It is a mechanism for constraining the interaction between users and protected resources. File is one of the important resources of the computer system. That must be protected from the unauthorized access that it can't be tempered or stolen by intruders. The file security can enforced using cryptographic techniques. With the help of these techniques the important files are enciphered as well as authorization of consumers are provided suitable encryption keys.

The cryptographic techniques can be applied at any level of the storage systems because they use the layered architecture. The level may be the block or virtual one in the operating system. Basically, file management is an important task of the computer system. The suggested file security system storing encrypted files using Rijndael Algorithm (AES), so an unauthorized user can't access the important data.

The encryption takes place for the selected files (important ones which requires the security) only. We are using the concept of on-demand computing which results in the high performance of the computer system. The proposed system is working properly for all types of the files. In this chapter there are more sections. Next section is section II which is about the related works. In section III, the design of the system is shown. In section IV, the evaluation is done. In section V, there is conclusion.



TOWARDS THE FILE SYSTEMS PERFORMANCE

IV EVALUATION FRAMEWORKS:

This is the era of High Performance Computing (HPC). There is a great demand of the best performance evaluation techniques for the file systems. The task of evaluation is both necessary and hard. It gives in depth analysis of the target system and that becomes the decision points for the users. That is also helpful for the inventors or developers to find out the bottleneck in their systems. In this chapter many performance evaluation techniques are described for file and storage system evaluation and the main stress is given on the important one that is replay traces.

A survey has been done for the performance evaluation techniques used by the researchers and on the replay traces. And the taxonomy of the replay traces is described. The some of the popular replay traces are just like, Tracefs, //Trace, Replayfs and VFS Interceptor. At last we have concluded all the features that must be considered when we are going to develop the new tool for the replay traces.

The complete work of this chapter shows that the storage system developers must care about all the techniques which are utilized for the evaluations of the file storage systems. So they can develop highly efficient future file systems. File and storage system designs are being proposed in a little span of time because there is no robust file system is available which can perform all the functionalities according to the always changing user needs.

Every user has their specific needs or demands which are not common at all. One user may ask for the secure file system because he/she has important information that must be protected from the others which are not authorized. Some are demanding for highly portable file systems. Considering all these a novel Java File Security System (JFSS) has been developed. One user demands for the energy efficient file systems because he/she is using portable devices.

Because of such diverse requirements by the users it isvery typical to develop a robust file storage system. Consequently a lot of diverse kinds of file storage systems are available. The user has to choose one of them which are suitable for them. Here the question is which one is better for the selection? To make this judgment we require theevaluation tools. These tools are to be applied by the researchers on the file systems under study for the performance evaluation..

VI Conclusion:

Java File Security System (JFSS) offers an answer to the file storage system's main problems like the difficulty in the portability. This file storage security system is designed for single operating system as well as grouped in the previously loaded Virtual Machine. The users can execute the JFSS on any operating system. It can be utilized as a file storage system. We have presented a JFSS design with minimal performance overheads because of ondemand computing and noticeable semantic alterations for users.

File storage system semantics are preserved exclusive of file system alterations, therefore supports the existing file storage systems performances. We have contributed in designing and enlargement of a user space cryptographic file storage system. We have balanced the design goals like security, performance, convenient and independability of the system. We have achieved the high security by including the support of the Rijndeal Algorithm (AES) and we have saved the keys on the portable smart cards for the documents which are important.

The performance is achieved with the help of on-demand computing concept which is that we are not going to encrypt all the files on the computer system, but we are going to encrypt only the important documents only. It saves the performance overhead of the system. The system is very convenient to the users. And the independability is attained by the novel Java technology which is highly portable. So the complete system is a highly independent of the configuration. At the end of thesis, I would like to conclude that my design goals in the research have been achieved well.

The proposed system has better system performance as well as expands it for the existing file system. It is an independent File System (it does not require the modifications in the other file systems or user applications). It offers strong storage protection alongside of the very unimportant and reasonable attacks. It is compatible with the future technology for separate key management just like smart cards for storing the encryption keys which are directly in the possession of authorized users.

It is compatible with the existing file system services as the encrypted files should behave normally as of the other files within the system. This has been developed in a customer level space FS for convenience of users. All the design goals for the research study have been achieved.

VII REFERENCE:

[1.] A. Aranya, C. P. Wright, E. Zadok (2004), "Tracefs: A File System to Trace Them All", In Proc. of the 3rd USENIX Conf. on File and Storage Technologies, pp. 129-145.

[2.] A. Brown (1997), "Operating System Benchmarking in the Wake of Lmbench: A Case Study of the Performance of NetBSD on the Intel x86 Architecture", in the Proc. of Sigmetrics '97, Seattle, WA, pp. 214 – 224.

[3.] A. D. McDonald, and M. G. Kuhn (1999), "StegFS: A Steganographic File System for Linux", Information Hiding, LNCS 1768, Springer-Verlag, pp. 462- 477.

[4.] A. Grunbacher (2003), "POSIX Access Control Lists on Linux", in Proc. of the USENIX Annual Technical Conf. (FREENIX Track), San Antonio, Texas, pp. 259–272.

[5.] A. E. Papathanasiou, and M. L. Scott (2002), "Increasing Disk Burstiness for Energy Efficiency", Technical Report 792, University of Rochester, Rochester, NY, pp. 1-31.