ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 19, April 2017

Safe and Secure File under Coercion

Sam Divine.P
Department of Information Technology,
Kings Engineering College,
Chennai,Tamilnadu,India,

Selva jenifa.R
Department of Information Technology,
Kings Engineering college,
Chennai, Tamilnadu,India

Mrs.Gracia Nissi S.
Assistant Professor of Information Technology,
Kings Engineering College,
cChennai, Tamilnadu, India,

Abstract—**The information on research is safely stored as documents in a web-based page which can be accessed by the scientific team in which has an Admin (team head).The encryption and decryption technique is based on the TrueCrypt Algorithm which is latest and more preferable. The encryption is based on the cipher concept. This concept implements the Grace wipe technique which is more securable in which the secured files cannot be accessed by coercion (threatening the user). For secure interaction the user receives a onetime password generated when user uses the correct password .The files can also be decrypted when required by the user. Files can also be shared among the users and Admin for better interaction of projects when the user specifically shares the documents. And there is a fake document which can be accessed when there is a wrong combination of real password. Hence, the secured files aresafer from coercion and can be accessed later. If there is a full wrong combination of real password the grace wipe deletes the real-password given to the specific user. We design grace wipe to design deletion of the real password and a new password is generated and sent to the registered mail-Id.**

Index Terms—**Coercion, full disk encryption, panic passwords, cryptographic data deletion.**

1. INTRODUCTION

Information security, sometimes shortened to Infuse, is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.The information forensics and security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs withintheir authority**.** Network security covers a

Variety of computer networks, both public and private that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password**.**

Plausibly deniable encryption describes encryption techniques where the existence of an encrypted file or message is deniable in the sense that an adversary cannot prove that the plaintext data exists. There are several methods and schemes to secure the files. But all those schemes have certain limitations. True Crypt is a discontinued source-available freeware utility used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file, or encrypt a partition or the whole storage device (pre-boot authentication).Even though if True Crypt is implemented a coercive attacker can punish a victim up till he or she reveals the actual password. This kind of coercion is called as rubber hose cryptanalysis. Multiple hidden volumes and also adding different security levels can also be broken if the adversary is untiring. The attacker can also encrypt the file by using password dictionary if he gets certain clues in order to encrypt it.

In order to save the sensitive information from the attacker the victim can delete/destroy the information/data when he or she is coerced. The deletion should be really very quick so that the attacker will not be able to stop the deletion by just cutting off the power. He can also make a backup copy of the sensitive files.

There are several cryptographic techniques which enable quick deletion and they are developed by several storage vendors called as SED. An SED is a self-encrypting hard drive with a circuit built into the disk drive controller chip that encrypts all data to the magnetic media and decrypts all the data from the media automatically. It allows overwriting of the data encryption key through an API call. But verifiable deletion is not possible with SED. It does undetectable deletion trigger but undetectable execution is not possible by SED. Since the calls to the deletion API can be diagnosed using SATA/IDE interface.

Grace wipe is a technique proposed by Zhao and Mann anis a solution implemented using True Crypt and SEDs which can possibly make the sensitive data permanently inaccessible. When the victim is coerced instead of using the actual password the victim will use pre-defined password which automatically deletes the hidden volume key. The coercer will not be able to distinguish between the actual password and the deletion password. To implement grace wipe they are using Trusted Platform Module (TPM) along with Intel trusted execution technology (TXT). But in Grace Wipe the key to decrypt sensitive data is deleted o the data is inaccessible to the user also.

In the existing system, the user cannot experience the Grace wipe concept more securable which makes dates unsecure. Attackers can break the security easily. Since the analysis of the encrypted data can be viewed. And the encryption used is also less secure. It has poor user interface environment. The encryption of the data is not as secured as required and the technique used is an old technique.

But we have used a technique based on the Grace wipe in which we can secure the file from the coercer and the file from being depleted by using duplicate dates. The main purpose of the project is to overcome the problem of coercion and unauthorised entry. The security level in web application is in week contributed. There many way to attack the target browse since several attacks target password key loggers, boot-nets. Document theft from corporate network Loss of private data which highly confidential dates are retriever by the unauthorised person. The grace wipetechnical is outlined for the designing framework original retirement of dates. Private confidential dates cannot be retrieved from the origin since wrong or unauthorized entry the fake user can retrieve the fake data which are as like as the original document.

Unknown entry will go to the fake page since the notification alert to the user, since the user knows original file the unknown does not have knowledge of original document.

II. METHODS IN EXISTING SYSTEM

In the existing system, it does not check the user’s ability. Same content could be displayed for each and every user. Attackers can break the security easily. Since the analysis of the encrypted data can be viewed. we couldn’t reviewed the approaches according to general categories such as thinking style, ratings etc.True crypt is implemented in current system since True crypt has been failed due to many reason. Methodology of measurement. Unlike Linux kernels do gettimeofday (), we lack a reliable clock source in the pre OS environment. We use CPU’s Time Stamp Counter (TSC) via the rat’s instruction. TSC stores the total number of machine cycles since the processor reset. We perform each measurement 15 times and use the R project to calculate statistics. Toot. The choice of using toot (as opposed to dealing with TXT with custom code) is justified by the fact that it has undergone sufficient public/expert scrutiny and thus is more reliable especially for the crucial TXT-handling logic. It also introduces an apparently acceptable level of latency. By default, toot enables debugging (to VGA, serial port or memory), which slows it down significantly, taking 30 seconds or more to complete. We disable debugging by passing necessary arguments. Our 15 independent measurements demonstrate coherent execution times: mean 1611.20ms, median 1611.96ms, standard deviation (sad) 6.08. DL-distance-based Grace wipe-XD.

True Crypt is about to be loaded. Our attempts to measure the DL-distance-based scheme result in an average. The basic Grace wipe. As the basic design tries to unlock the three defined indices in sequence until a success, we separately time the three cases Success at the first index (including By tamers can access data stored in a cloud anytime and anywhere using any device, without caring about a large amount of capital investment when deploying the underlying hardware infrastructures.

Promptness of deletion. We also measure the duration of the deletion operation (releasing and overwriting an NVRAM index). Where a user can read state data for a period of time. The domain name system (DNS) is one of the most popular applications that implement eventual consistency. The truecrypt design varies with the os functionality . [5] proposed a system in which FASTRA downloads and data transfers can be carried over a high speed internet network. On enhancement of the algorithm, the new algorithm holds the key for many new frontiers to be explored in case of congestion control. The congestion control algorithm is currently running on Linux platform. The Windows platform is the widely used one. By proper Simulation applications, in Windows we can implement the same congestion control algorithm for Windows platform also. The Torrents application which we are currently using can achieve speeds similar to or better than —Rapid share (premium user) application.

III. PROPOSED SYSTEM

Using secure storage on a Trusted Platform Module (TPM) and modern CPU's trusted execution mode (e.g., Intel TXT), we design Grace Wipe to enable secure and verifiable deletion of encryption keys through a special deletion password. An attacker cannot distinguish between a deletion and real. Here the files are get encrypted and decrypted with the pass phrase since the can be saved without the pass phrase for sample phrase assessment, since the encrypted and decrypted files cannot be accessed without the password.Security in web application with in particular group of users can not access
other without the knowledge of the sources file loader.

Here, we applied this concept in the corporate sector by communication between the corporate sectors through a central communicative function. The group of members who is added within functionality should be adding by the admin We design technical to maintain communication between the user and admin. The technical was shared among the user, where all the user is share their knowledge in the commonly shared area.If any changes are made in the grace wipe was notified to the other user are domains connected to the central maintenance area.The user has direct communication between them but they communicate each other by the shared area.The shared area files will be common to the entire user. The shared area is the common part for all the users.The user interacts by updating the files when they receive information from their own sources loader which could affect to others agents. Also, the user could receive an update of their file from the reasoning in the source loader.

When a new domain is joined to the maintenance architecture, it would also have the communication between them.Implemented in web application so that many members can access at the same time.

Grace wipe implementation ,since this provides different web pages with the password routing analysis correct password enters into correct web page.Wrongcombination enters into fake web page.
Complete wrong password will enter otherweb page.Admin can add the members so that no one can access without knowledge. Members can encrypt their fields and they can store it. For encryption passphrase entered so that no one cannot access without passphrase. Transferring file inside the member group.During Members addition their login password will be send to Gmail so that their password and encrypt password shared with mailing.

IV. STUDY OF THE SYSTEM

In the flexibility of uses the interface has been developed a web module in mind, associated through a module interface. The GUI's at the top level has been categorized as follows

1.Fake page

2.Orignal page

3.Decoy page

Module page has layouts for login, listing messages and announcements and displaying posts and replies.Moderator page should have layout to view the moderation queue.Admin page should have layouts to create announcements, maintain moderators and to view history.

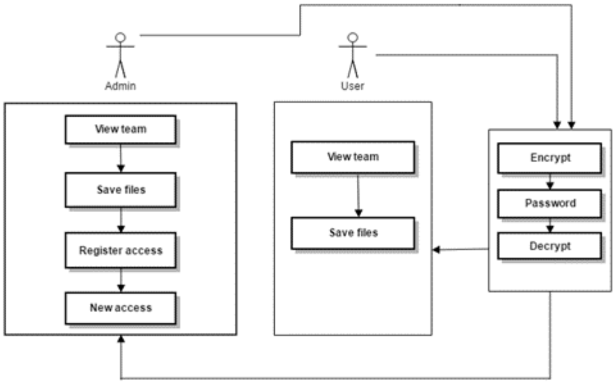


Fig.1.Diagram of the proposed method

NUMBER OF MODULES:

After careful analysis the system has been identified to have the following modules:

□Admin view implementation

□user

ENROLLMENT:

The users who has been registered by admin their details to the service provider accessing it are called enrollment. They have the following permissions. They are

□ View their details.

□ Upload and download the file.

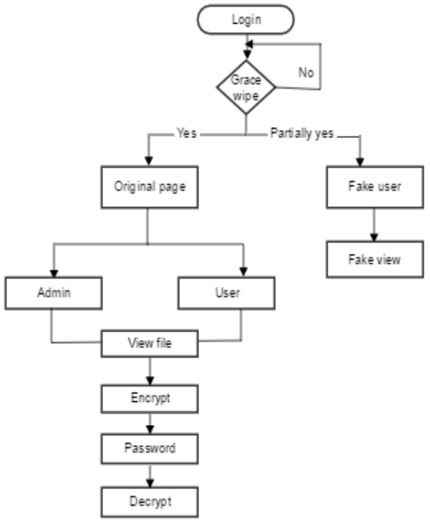
□ Encrypt and Decrypt secret file.

ADMIN VIEW IMPLEMENTATION:

Admin has the responsibility to maintain their employeedetails . They also have privileges to create an announcement that can be viewed by all the users. Their roles and responsibilities are

□ Add a new user.

□ Delete a user.



IV.SOFTWARE AND HADWARE REQUIREMENTS

Hardware Requirements

Developing Kit			
	Processor	**RAM**	**Disk Space**
Net Beans 8.0	Computer with a 2.6GHz processor or higher	512MB Minimum	Minimum 20 GB
Database			
MySQL	Intel Pentium processor at 2.6GHz or faster	Minimum 512 MB Physical Memory;1 GB Recommended	Minimum 20 GB

SOFTWARE INTERFACE:

- **Client on IDE:**Net Beans 8.0
- **Database Server:**MySQL
- **Database IDE:**HeidiSQL

V.RESULTS

Input and Output

The major inputs and outputs and major functions of the system are follows:

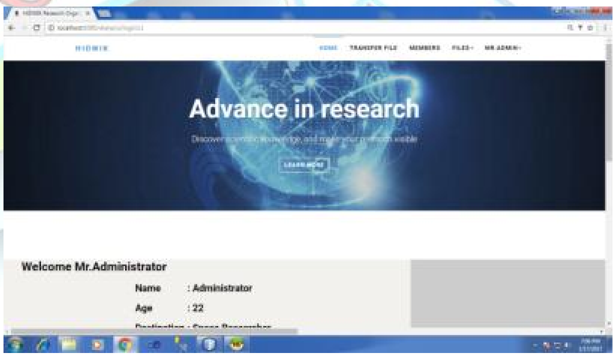
Input:
The admin enters his details like name, emailid, phone number, password and address. The emailid and password are for user login purpose.They can save their files. They can secure their secret details.The administrator can add a new member.Modification in user are done by admin.

Output:
The system performs login check. File are viewed by every user.Common file requiring the user comments is displayed to the registered user.Encrypted file accessed using pass phrase.

Input Design

Input design is a part of overall system design. The main objective during the input design as given below:
Encrypt and decrypt files . Input documentation and imagesType of Input can be image and document files.A source document differs from a turnaround document in that the former contains data that change the status of a resource while the latter is a machine readable document. Transaction throughput is the number of error-free transactions entered during a specified time period. A document should be concise because longer documents contain more data and so take longer to enter and have a greater chance of data entry errors. The more quickly an file is detected, the closer the file is to the person who generated it and so the pharse is more easily corrected.

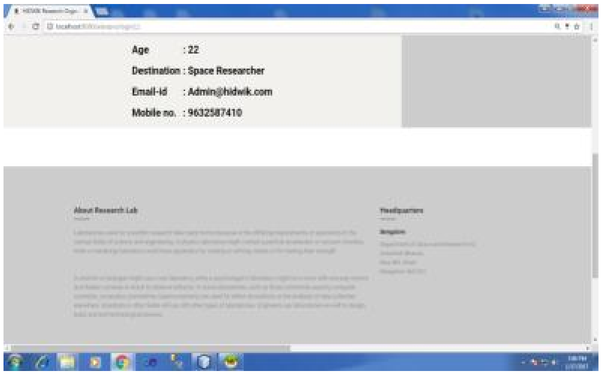
Admin login:



Welcome Mr.Administrator

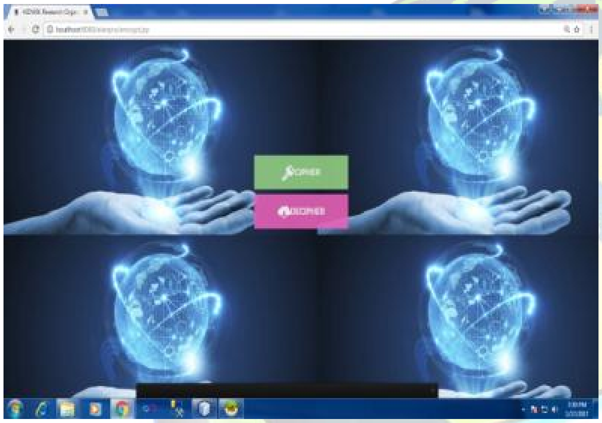
Name : Administrator
Age : 22
Destination : Space Researcher

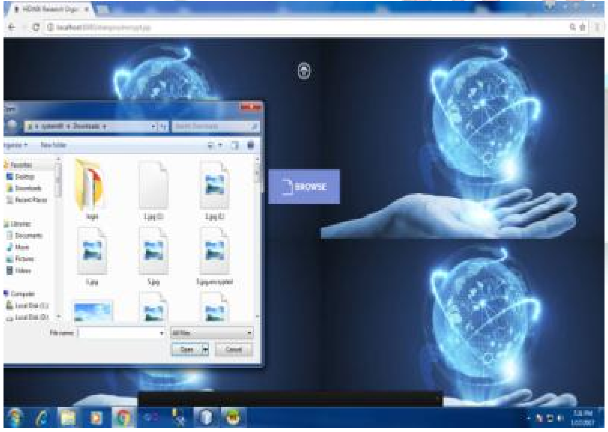
User Login Page:

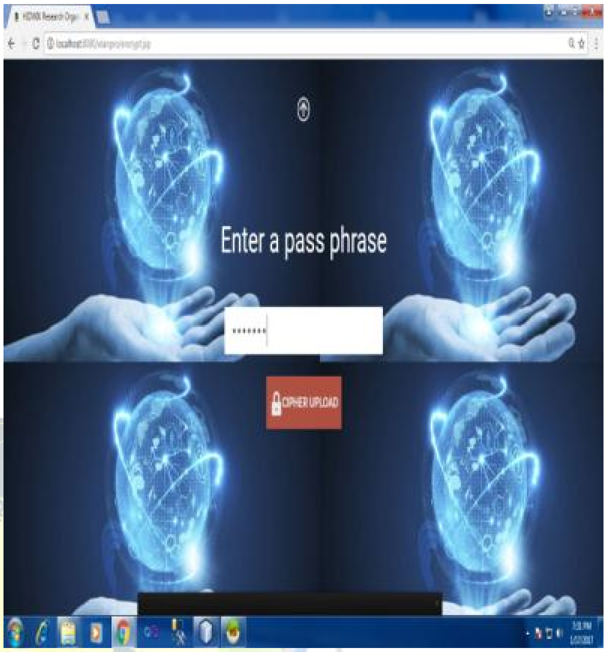


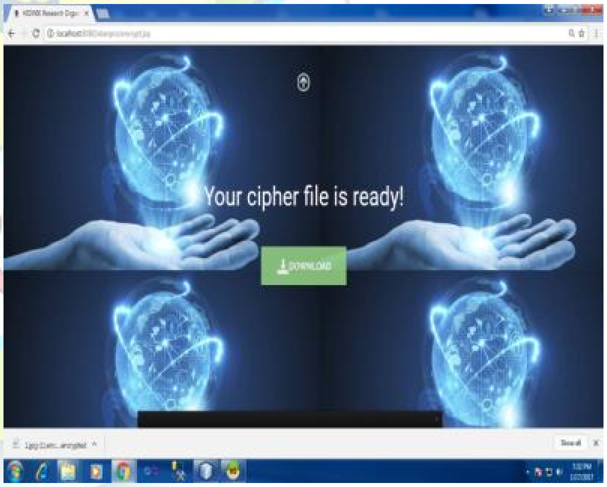
Age : 22
Destination : Space Researcher
Email-id : Admin@hidwik.com
Mobile no. : 9632587410

Encrypt a file:









VI.CONCLUSION

Thus the sensitive files are kept safe from the coercer by using a fake login page when they actually try to hack it or when they force the user to reveal the password.

VII.FUTURE ENHANCEMENT

In future, the tutor techniques can be used encrypt and decrypt both audio or video recognition.And the bugs in the gracewipe technique is fixed for better interface.so,the project can became more securable and reliable for better feasibility.

VIII.REFERENCES

. [1] Lianying Zhao, Mohammad Mannan ,"Deceptive Deletion Triggers Under Coercion", vol.11,no.12,Dec 2016.

[2] E.Rescorla, "Protecting Your Encrypted Data in the Face of Coercion" (Feb 11, 2012). [Online]. Available:http://www. educatedguesswork.org/2012/02/protecting_your_encrypted_data.html.

[3] J. Reardon, D. Basin, and S. Capkun, "SoK: Secure data deletion," in Proc. IEEE Symp. Secur. Privacy, SanFrancisco, CA, USA, May 2013.

[4] R. Geambasu, T. Kohno, A. A. Levy, and H. M. Levy, "Vanish: Increasing data privacy with self-destructingdata," in Proc. USENIX Secur. Symp., Montreal, QC, Canada, Aug. 2009

[5] Christo Ananth, A. Ramalakshmi, S. Velammal,B. Rajalakshmi Chmizh, M. Esakki Deepana, "FASTRA –SAFE AND SECURE", International Journal For Technological Research In Engineering (IJTRE), Volume 1, Issue 12, August-2014,pp: 1433-1438

[6] H. Bojinov, D. Sanchez, P. Reber, D. Boneh, and P. Lincoln, "Neuroscience meets cryptography: Designingcrypto primitives secure against rubber hose attacks," in Proc. USENIX Secur. Symp., Bellevue, WA, USA, Aug.2012.

[7] J. Reardon, S. Capkun, and D. Basin, "Data node encrypted file system: Efficient secure deletion for flashmemory," in Proc. USENIX Secur. Symp., Bellevue, WA, USA, Aug. 2012.