A Web Based Framework for Data Confidentiality in Removable Media ensuring safe cyber space

Neel N. Shah, Gardas Naresh Kumar, Jigar A. Raval

Abstract— **In this era of technology, Data is considered to be the most important entity and hence loss of sensitive confidential data can therefore be a major weakness which leads an organization involving huge volume of data transformation daily to experience a major security threat. Many Research institutes are involved in experimenting new things which requires large amount of data to be processed. Hence protecting such data is of utmost important which involves nation's security. It is also observed that most of the data transmission within an organization or an institute involved in research uses a portable Removable media as a primary source without considering their risks and vulnerabilities which are responsible for committing cyber-crimes. Removable Media devices are prone to theft, information leakage and hence are used as a major weapon for dumping the confidential data and committing Cyber Crimes by launching a Cyber Attack exploiting the vulnerabilities they possess. Data Loss is therefore considered as one of the major cyber threats today. This paper discusses about some of the cyber threats which are in existence today, the risks and vulnerabilities associated with Removable Media, some of the existing frameworks and techniques used today for USB security and finally a web based framework whose major focus is on Data Loss cyber threat describes how the data within the removable media should be transferred and used so as to prevent them from being used as a weapon for Cyber Attacks today that will help in creating a secure cyber space.**

Index Terms—**Cryptography, Cyber Attacks, Cyber Space, Information security, Removable media, USB security.**

I. INTRODUCTION

Cryptography is one of the main pillar of information security. In the present scenario, the data is being used extensively and the amount of data transmission over the network is increasing exponentially. Due to this, safeguarding confidential data is becoming a challenging task as data transmitted over the network is in bulk which leads to possibilities of data theft and data leakage. Data confidentiality is defined as protecting the privacy of data so that it does not get disclosed to an unauthorized entity. Data created from research institutes are valuable resources for scientific and educational purposes in future [5]. Disclosure of data from any research organization may well cause harm to national security. Hence, researchers of almost all the domains are expected to remain proactive during their research, to ensure that the privacy of an individual research subjects are protected and the information about their respective domains remains confidential [5].

Removable or portable USB devices gives user a convenient access to official data. Hence as their use increases so is the security risks associated with them. Portable removable devices increases the risks of data loss, data exposure to and from any system it is connected with and also are prone to theft. It is also found that most of the malwares today are spreading through removable USB devices leading to cyber-attacks.

Many Research organizations denies the usage of Removable media within their respective working premises due to the security risks associated with them. Many open source encryption tools and techniques are available to safeguard data confidentiality. But to do that it is necessary for an individual to have an awareness and good knowledge about computer and security aspects related with it. Sometimes it may also be possible that removable device can be misplaced or lost, hence the data or information within the device is accessible to an unauthorized entity at that time. Hence removable media devices can therefore be used as a major weapon for cyber-attack leading to a cyber-crime.

In order to mitigate the risks and vulnerabilities related to portable removable media devices that can lead to a cyberattack and disrupt the ongoing confidential operations of many research institutes and private organizations, This paper summarizes some of the risks and vulnerabilities related with portable removable media devices and a Framework that describes how the data within the removable media should be transferred and used so as to prevent them from being used as a weapon for launching Cyber Attacks today.

II. CYBER THREATS

A. Data Loss

Most of the data today is being transferred to and fro within the organization using portable Removable media devices and hence it is necessary to safeguard its usage to launch the outsiders and even insider attacks (Cyber Attacks). As Removable Medias are portable devices they might get lost or Can be stolen. Many research and private organizations today are not allowing the use of portable removable devices within their respective premises because of the threat these devices

Manuscript received April, 2015.

Neel N. Shah*, Computer Engineering (IT Systems & Network Security), Gujarat Technological University, Ahmedabad, India.*

Gardas Naresh Kumar*, Coordinator, Centre for Development of Advanced Computing., Pune, India,*

Neel N. Shah, Computer Engineering (IT Systems & Network Security),

Jigar A. Raval*, Incharge Computer Centre, Physical Research Laboratory, Ahmedabad, India.*

ISSN: 2278 – 7798

can produce. One of the common and most widely used technique to prevent data loss or data theft from being compromised is using Encryption for scrambling the original data so that it would not get disclosed even if it gets compromised.

B. Malware

Malware is a short name for Malicious Software. Malware includes viruses, worms, spyware, Trojan horse programs like RATs (Remote Access Trojans) [10]. Hence in order to be safe from such malwares, organizations restricts its usage in their respective working premises because if Removable USB devices are not controlled in a proper way then it may well cause harm by spreading infected files into the local network from the computer system in which they are inserted. In this way they can be a major cyber threat and can well be the reason for Cyber Attacks. Some common mitigation methods against malware today includes Antivirus Software, Regular Patch Management, Restricting the usage of Removable Media devices.

C. Internet Attacks

Today Internet is used as a major medium for promoting and delivering the services by many organizations. By moving to the Internet, we are expanding our threat landscape from local or regional threats to global threats. We must be diligent to take the care needed to protect ourselves and our customers from unwanted attacks [10]. Major mitigating controls against internet attacks include multifactor authentication, secure website, technical controls like firewalls, IDS (Intrusion Detection Systems) etc.

Now we will discuss about some of **the risks and vulnerabilities associated with removable media devices, existing USB security practices and finally the framework that will help us to mitigate the risks and vulnerabilities and can help many organizations that processes sensitive data on regular basis thus helping in creating a safe cyber space.**

III. RISKS AND VULNERABILITIES WITH REMOVABLE MEDIA DEVICES

A. Risks with Removable Media Devices

Data Loss: Data within the Removable Media may well get lost if it gets infected and compromised with the malwares existing today.

- **Data Exposure**: Data within the USB Devices can well get exposed as data within the removable devices are usually stored in the plain text.
- **Data Theft**: It is a major risk as once the Removable device gets stolen so is the data within the device. So a proper way for maintaining the data within the Removable media confidential even if it gets theft is to be defined.

B. Vulnerabilities in Removable Media devices

Malware Infections: It is a major vulnerability that can cause many disruptions to a removable media devices. This type of vulnerabilities are responsible for data theft and data loss.

Data Leakage: Removable Media devices usually carry the data in plain text. Hence they are likely to be vulnerable to data leakage.

IV. EXISTING USB SECURITY FRAMEWORKS AND TECHNIQUES

Below mentioned are the existing Frameworks and techniques existing today:

A. Data Encryption Techniques for USBs

Authors **Shivanku Mahna and Sravan CH** briefs about USB and its significance evolvement in this era of technology where data is the most important entity. Authors mentioned that usage of USB for storing sensitive data lacks in security as any person that is not authorized can access the sensitive data of others. Hence, they proposed the following methods in order to overcome the security weakness related with using USB as a mass storage device.

- **Mutual Encryption**: In this technique data is stored in the USB device only after it is encrypted. The advantage of doing it is that whenever the removable device (USB) is lost or misplaced, the sensitive data within it is protected from any unauthorized access. Hence the data remains confidential due to encryption.
- **Key Match**: In this technique RSA algorithm is used in which a public key is generated by an authentication server (AS) and transferred to client. Keys (RSA public key and randomly generated key from AS when user inputs his/her credentials) are used for the encryption and decryption of messages. Keys exchanged between the client and AS might well be vulnerable to hack as receiving entity do not know that the message received is from the legitimate sender or not. Hence password for confirming the identity is required for protecting the sensitive data. Schnorr's digital signature method was used for the overall security of using this technique.

B. The use of two Authentication Factors to enhance the security of Mass Storage Devices

Authors **Mohamed Hamdy Eldefrawy, Muhammad Khurram Khan and Hassan Elkamchouchi** recognizes that for providing the security in removable media an authentication server is used as a trusted third party, but they are vulnerable to insider attacks and server impersonation attacks. Hence, authors proposed an access-authentication algorithm which overcomes the security issues associated with using Authentication server as a trusted third party. The proposed access authentication algorithm uses smart phone as a second authentication factor.

This algorithm works in two phases:

- **Registration**: The registration phase is conducted through a secure communication session using a wired connection (i.e., a USB cable) between the PC and the SP. In this phase, the client (PC) obtains the unique identification of the removable storage media, IDm, plus the user id and pwd from the user and transfers (id, hpw), hpw= h (pwd || IDm) to the user SP using the wired connection. Now, the smart phone SP will calculate r = (hpwk mod p) using some random number k and uses its private key x to calculate s = (k-e*x) mod q and then it signs the SIGsp, m and delivers it to PC to

ISSN: 2278 – 7798

be saved on the mass storage device. Before saving client must check e = h (id || r || gk mod p).

- **Verification**: The user inserts the mass storage device into the client computer and types the correct id and pwd to extract its IDm. Then, client (PC) computes h (pwd, IDm). Then, the client selects a random number rc to calculate u = hpw. yrc mod p and w = grc mod p. Finally, the client sends (id, e, s, u, w) to the SP. Then, SP calculates hpw = (u / wx mod p) and k = (s + e.x mod q) using its long term private key x. SP then calculates r = hpwk mod p. Then, AS verifies whether e = h (id, r, gs ye mod p) or not. If yes access to USB is allowed else communication is terminated.

C. *Existing Software and Techniques for USB Encryption*

TABLE I
EXISTING SOFTWARE SOLUTIONS AND TECHNIQUES

Solution	Algorithm	Web-Based	Limitations
TrueCrypt	AES, Twofish	NO	Project closed
USB Safeguard	AES	NO	Max 2 GB
AESCrypt	AES	NO	Max 2 GB
SecurStick	AES	NO	Max 47 MB
DiskCryptor	AES, Twofish	NO	Time consuming
Rohos Mini Drive	AES	NO	Max 4 GB
Encryptur	AES	Yes	No user Authentication

From above table it can be understood that all the existing software works within the USB and hence the processing within the USB removable media exceeds to a large amount and therefore it is not a good countermeasure to safeguard the device with such a huge processing within itself as removable media devices might well get crashed if it cannot withstand the processing within the media itself. So **the main objectives** that needs to be defined are:

To Ensure:

- Data in the Removable media is more important than the device itself.
- Data doesn't get disclosed to an unauthorized entity.

To Propose:

- An Impartial web based Framework that will help in mitigating the risks and vulnerabilities of Removable devices.
- It should differentiate the existing techniques available today.

V. PROPOSED WEB BASED FRAMEWORK FOR INFORMATION SECURITY IN REMOVABLE MEDIA

Proposed Framework for maintaining Information security in Removable Media devices basically will help in the following way to the user:

1) User can connect to the URL of web server locally and can encrypt their confidential data within the USB that they will be carrying to other research institutes or any organization for their respective work or assigned tasks.
Once User encrypts the confidential data locally within the institute then he can carry that data to other institutes and can follow the same procedure in order to receive the original file and can continue his/her assigned task for which they have been asked to visit the different location or institute.

The Framework described below will basically work in two phases as discussed below:

A. *PHASE-1 [Local Site]*

Following procedure is carried out at Local site:

- User inserts the Removable media and opens the web Server link for authentication.
- User will now input his/her Login Credentials.
- Web Server checks at backend and authenticates the user with correct credentials.
- User now can upload the file for Encryption.
- Now on clicking an upload button, a Script at server is invoked and will check **whether the uploaded file is Encrypted or readable to anyone.**
- Script will reverse the file from encrypted to plaintext and vice versa.
- Then a prompt for downloading the Encrypted or decrypted file will appear.
- User then can download the required file by clicking on the **SAVE FILES** button.

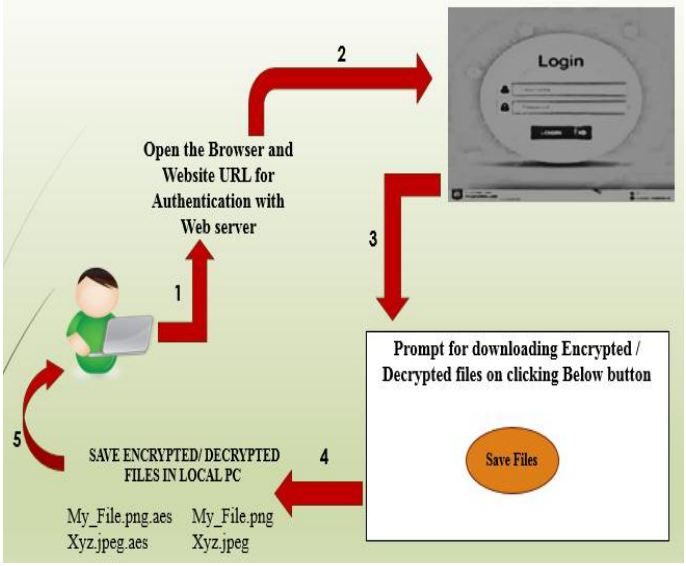

Fig. 1. Proposed Web-Based Framework for Information Security in Removable Media devices

ISSN: 2278 – 7798

B. *PHASE-2 [Remote Sites]*

At Remote Site:

- User have to follow the same steps followed at local site in order to decrypt the encrypted data within the Removable media
- Once user decrypts and uses the data that he carried in encrypted format,
- User can again encrypt the same data and can move at the local site from where the user started.

VI. PROPOSED WORKFLOW

The Framework discussed above will follow the below mentioned workflow steps:

- Click on the file to view
- User will be redirected to the server and asked to fill up his/her credentials for authentication
- Web Server checks the credentials and allows user to encrypt/decrypt their respective files if authenticated.

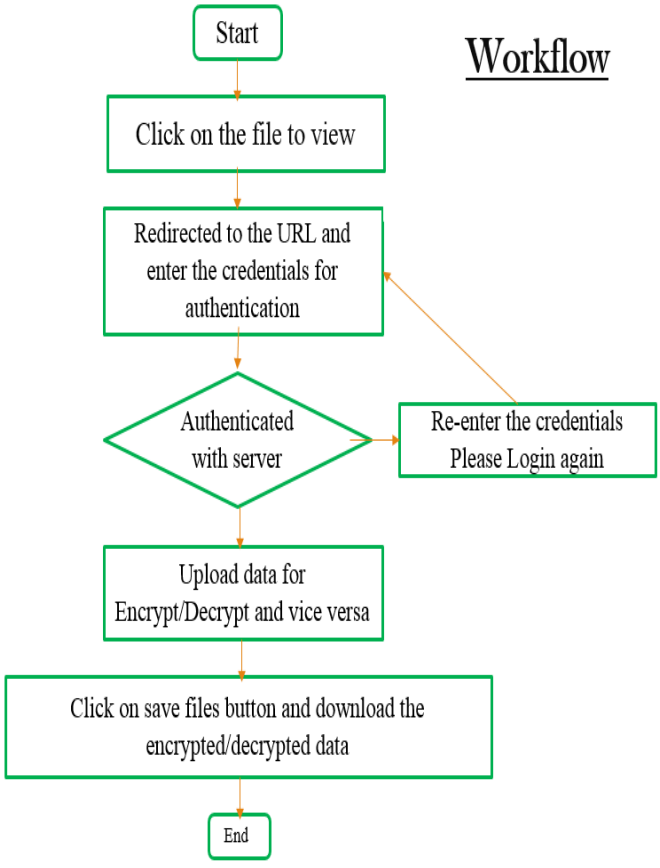

Fig. 2. Proposed Workflow

- User then can download their files by simply clicking on **SAVE** files button.

VII. RESULTS

Below Tables shows the time comparison between Encryptur and Proposed Framework (PRL-Crypto) taken for encrypting and decrypting the files up to maximum size of 20 MB.

TABLE II
ENCRYPTION TIME COMPARISON

File Size (MB)	Encryptur (milliseconds)	PRL-Crypto (milliseconds)
1.7	1235.467	782.398
7.4	2567.608	2182.539
11.8	4896.736	4151.723
17.9	7862.385	6375.451
23.4	9436.189	7963.650

TABLE III
DECRYPTION TIME COMPARISON

File Size (MB)	Encryptur (milliseconds)	PRL-Crypto (milliseconds)
1.7	578.657	521.828
7.4	2377.816	1872.672
11.8	4593.284	4070.546
17.9	7247.361	6207.409
23.4	8523.926	7589.867

VIII. EXPERIMENTAL RESULT COMPARISON OF ENCRYPTUR AND PROPOSED WEB BASED FRAMEWORK

Performance for both encryption and decryption of our work is carried out and tested on **linux – CentOS6.4** platform.

Encryption and Decryption of file sizes was carried out and accordingly the time ENCRYPTUR and PRL-Crypto (Proposed Web Based Framework) took to perform the same task is plotted and compared.

The performance is calculated based on maximum file size of 20 MB.

Below Two graphs shows the comparison based on time spent for encryption and decryption.

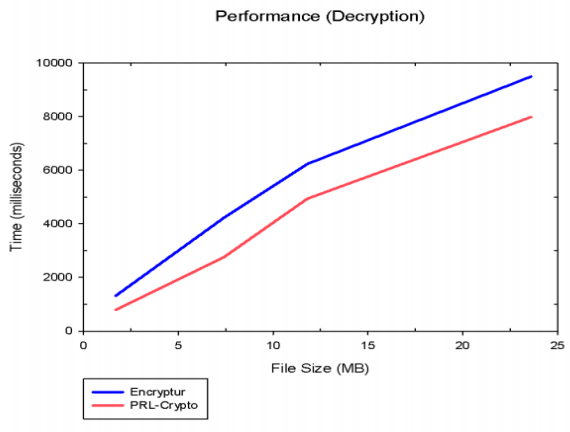

Fig. 3. Encryption Time Comparison

ISSN: 2278 – 7798

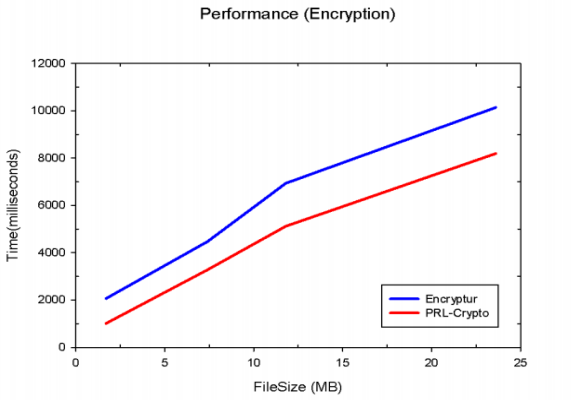

Fig. 4. Decryption Time Comparison

IX. Conclusion

Web Based Framework proposed ensures no data disclosure to an unauthorized user. The Proposed Framework differentiates the existing techniques available today. This approach can be used for Large Research and private organizations or institutes having different departments and sites where users carry their confidential information to and fro within the local premises or at remote sites. This approach also solves the issue of Data Theft and Data Loss from the Removable media as well as the risk of getting them misplaced or stolen. Because the DATA cannot be disclosed without an authentication and also the key used to encrypt and decrypt the users sensitive and confidential data cannot be easily guessed and cracked.

The Proposed Framework also takes lesser time in for encryption and decryption of files as shown and compared in graphs above.

Appendix

- IDm Unique Identification of USB
- p, q Two large primes p and q
- x Authentication server's private key
- id User's Identification Disclosure
- pwd User's Password
- y Authentication Server's Public key
- SP Smart Phone

Acknowledgment

We would like to express our deepest gratitude to **Mr. Samuel Johnson, Scientist/Engineer, PRL, Ahmedabad,** for his constant encouragement and guidance which helped us in learning cryptography concepts.

References

[1] Shivanku Mahna, Sravan CH, "Data Encryption Techniques for USB", International Journal of Computer Applications, IJCA (0975 – 8887) Volume 104 – No.7, October 2014.

[2] Mohamed Hamdy Eldefrawy, Muhammad Khurram Khan1 and Hassan Elkamchouchi, "The Use of Two Authentication factors to enhance the Security of Mass Storage Devices", IEEE 11th International Conference on Information Technology: New Generations, 2014.

[3] Charru, Paramjeet singh, Shaveta Rani," Efficient Text Data Encryption System to Optimize Execution Time and Data Security", International Journal of Advanced Research in Computer Science and Software Engineering IJARCSSE Volume 4, Issue 7, July 2014.

[4] Md Asif Mushtaque, "Comparative Analysis on Different parameters of Encryption Algorithms for Information Security", International Journal of Computer Sciences and Engineering IJCSE (ISSN: 2347-2693) Volume-2, Issue-4, April 2014.

[5] 5-best free usb encryption software. [Online] http://www.ilovefreesoftware.com/12/featured/5-best-free-usb encryption-software.html.

[6] USB flash drive security. Wikipedia. [Online] http://en.wikipedia.org/wiki/USB_flash_drive_security.

[7] AES Crypt. [Online] https://www.aescrypt.com/

[8] Privacy and Confidentiality – current issues in research ethics. [Online] http://ccnmtl.columbia.edu/projects/cire/pac/foundation/

[9] Information Security. Wikipedia. [Online] http://en.wikipedia.org/wiki/Information_security

[10] The Risks of Using Portable Devices [Online] https://www.uscert.gov/sites/default/files/publications/RisksOfPortableDevices.pdf

[11] Top 5 Emerging Cyber Threats [Online] https://www.conetrix.com/articles/top-5-emerging-cyber-threats.aspx

[12] Cyberspace. Wikipedia [Online] http://en.wikipedia.org/wiki/Cyberspace

[13] Encryptur [Online] http://www.encryptur.com

ISSN: 2278 – 7798