Data Authentication and Theft detection for USB Flash Drive

Shoaib Ahmad [1], Apoorva Mishra [2], Uthra R [3], Akshaya P [4], K Subha [5]
[1, 2, 3, 4] SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.
[5] Assistant Professor, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.

Abstract – The Internet of things (IoT) is the network of physical devices. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure. Data has always played the crucial part be it any field work. In the new, faster growing era of technology the data is being shared in numerous ways available - via USB flash drive being one of them and also most popular. The aim of this empirical study is to propose a more secured framework for data sharing via USB flash drive and also for the physical security of the device, using the classic security algorithm along with some theft detection techniques (like GPS, RFID) respectively.

Index Terms – RFID, GPS, IOT, USB.

1. INTRODUCTION

In this paper, the explanation, illustration, and the paradigm of RSA algorithm, IoT[4], RFID, GPS and Log Files are proposed and potential models that can implement *security and authenticity of data in USB* flash drive are analyzed. The system will identify the data provided by the user and according to the prescribed level of security and transfer of the file requested, the required process is run at the server (if necessary).

Rivest-Shamir Adleman (or RSA) is an asymmetric algorithm used by modern computers to encrypt and decrypt messages. Radio-Frequency Identification (RFID) is the use of radio waves to read and capture information stored on a tag attached to an object. A tag can be read from up to several feet away and does not need to be within direct line-of-sight of the reader to be tracked.

With the Use of RSA[1]one can generate Random keys, by using this Key we will make our Encryption and Decryption. Python is the programming language which is highly Object-oriented, interactive and easily interpreted. With the help of log files, the server's log files can easily identify numbers of visitors, the domains from which they're visiting, the number of requests for each page and usage patterns according to variables such as times of the day, week, month or year. In case of device theft, since the USB device is GPS enabled with RFID tags, it's location can be tracked easily by the server system.

2. RELATED WORK

Numerous efforts have been taken in securing the data. Some of the significant ones include using global positioning system (GPS), using general packet radio service (GPRS), use of encryption algorithms [1]. Most of these methods proved to be inefficient owing to the low level of security that they provide. The model proposed in this paper aims at reducing the risk of unauthorized access to data. Some of the notable advantages of the model is that it is user-friendly, highly portable and cost efficient.

3. PROPOSED MODEL

To ensure the security and authenticity of the data being shared widely through USB flash drive the proposed system uses RSA Algorithm. The Algorithm is used in sync with RFID and GPS technology to ensure the security of USB flash drive as well. The system will identify the user provide the data according to the prescribed level of security and transfer of the file requested and run the required process at the server (if necessary). The proposed system uses Arduino (An open source hardware and software), Log files(At servers) and python language to code the software.

The security is enhanced by double encryption with the use of El-gamal algorithm[2]. The security of the El-gamal algorithm depends on the difficulty of computing discrete logs in a large prime modulus. It has the advantage where the same plain text gives a different cipher text each time it is encrypted.

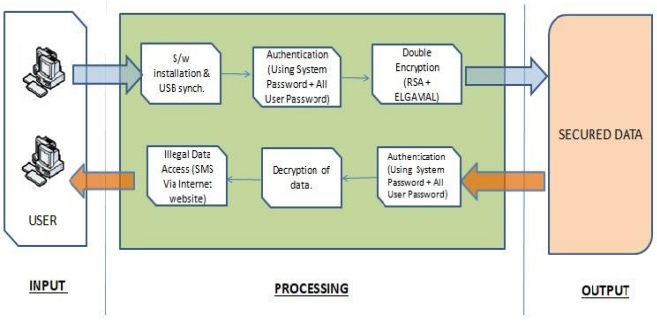

Figure-1 Proposed System

A. USB synchronization & Authentication

- The software installation will be done on the server computer. After installation, the RFID details of the USB flash drive will be saved in the database. The user needs to install the security software and the USB drive needs to be synchronized with the software in order to secure the data.
- After this process, the login credentials can be saved in the database to recognize authorized person for accessing the data later. User logs in using a password, if the password is correct, data can be accessed. In case of unauthorized access, user's IP details will be sent to the server system[5].

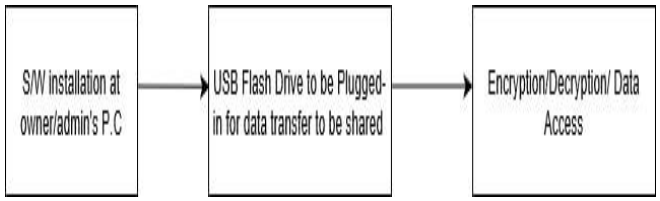

Figure-2 Synchronizing & Authentication

B. Encryption & Decryption

Encryption is one of the principal means to grantee the security of sensitive information[3]. It not only provides the mechanisms in information confidentiality, but also functioned with digital signature, authentication, secret sub-keeping, system security and etc. Therefore, the purpose of adopting encryption techniques is to ensure the information's confidentiality, integrity and certainty, prevent information from tampering, forgery and counterfeiting

Figure-3 Encryption

To access the data, the encrypted data undergoes the decryption process. Once decryption is over, data can be accessed.

For the purpose of double encryption, El-Gamal Algorithm is put to use. In cryptography, the El-Gamal[7] encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. The system provides an additional layer of security by asymmetrically encrypting keys previously used for symmetric message encryption. It was described by Taher El-gamal in 1985. El-Gamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm (DSA) is a variant of the El-Gamal signature scheme, which should not be confused with El-Gamal encryption.

In El-Gamal Algorithm, the public key is (p,g,A)(p,g,A), and the secret key is (a)(a), in order to encrypt some data, the sender generate a random k, where:

- (C1,C2)=m x A^k(modp),
- gk(modp) x (C1,C2) = (mxAk(modp),
- gk(modp) .

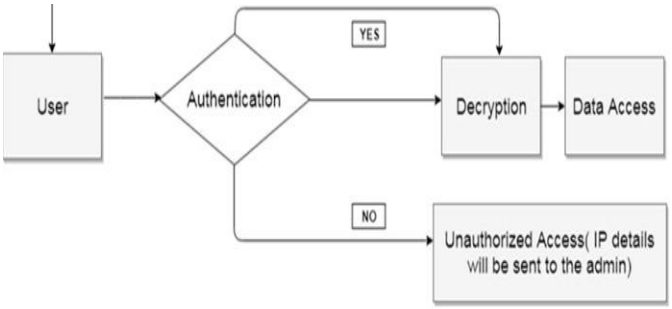

Figure-4 Decryption

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system[6]. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords.

C. Theft and Data theft Detection

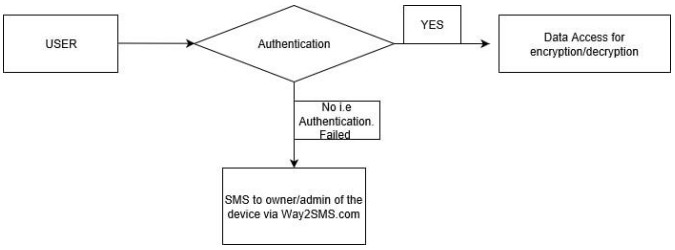

Figure-5 Theft and Data Theft Detection

An anti-theft system is any device or method used to prevent or deter the unauthorized appropriation of items considered valuable. Theft is one of the most common and oldest criminal behaviors. From the invention of the first lock and key to the introduction of RFID[3] tags and biometric identification, anti-theft systems have evolved to match the introduction of new inventions to society and the

resulting theft by others. For data theft if authentication failure occurs owner is informed via sms service through Way2SMS.com

4. RESULTS AND DISCUSSIONS

The analysis[2] of the proposed system is an essential parameter to check it's efficiency. Analysis was done based on the following parameters:

- Execution time
- Level of security of the algorithm.
- Block size
- Type of encryption technique.
- The size of input key.

The following table shows the comparison of the proposed architecture (Our code) with other traditional encryption and decryption techniques that are being implemented in and around the IT sector.

INPUT KEY SIZE	EXECUTION TIME	SECURITY LEVEL	BLOCK SIZE	ASYMMENTRIC	
49	6.456	Medium Level	64	Diffie-Hellman Key Exachage	AES ALGORITHM
36	3.976	High Security	64	RSAAsymmetric Algorithm	BLOW FISH
54	5.998	High Security	128	SHA-224	DES ALGORITHM
123	6.159	Medium Level	64	SHA-386	3DES ALGORITHM
256	0.6999999	Very High Security	64	SHA-256	OUR CODE

Table-1 Analysis of proposed solution

5. CONCLUSION

The system at hand helps in securing the data with the use of double encryption technique, thereby making sure that the data is accessed only by the authorized person. The system also helps in identifying the unauthorized access. Everytime a scenario involving unauthorized access of data, the admin is notified with the help of text message through a website. Hence, the proposed system ensures that safety of the data is not compromised.

REFERENCES

[1] Houtao Ji, Jianfeng Feng, Mingzhong Liu,Xianchao Yang, "Design of USB Storage Encryption Device Based on XTS-AES" in Proceedings of the 9th International Conference on Intelligent Human-Machine Systems and Cybernetics 2017
[2] Zhu Zhao, Zhongqi Dong, Yongge Wang, "Security analysis of a password-based authentication protocol," *IEEE*,Jan. 2013.
[3] Wuhan Vocational Coll. of Software & Eng., Wuhan, China, "The Research of IoT Based on RFID Technology", 2014 7th International Conference on Intelligent Computation Technology and Automation.
[4] K. Asha Rani, A. V. R. Mayuri, "Paper on Basics of Internet of Things," International Journal of Emerging Trends in Science and Technology, IJETST, 2016.
[5] SULI WANG, GANLAI LIU., "File encryption and decryption system based on RSA algorithm," in Proceedings of the International Conference on Computational & information services, 2011.
[6] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, Sirius: "Securing remote untrusted storage", in Proc. of NDSS03, 2003.
[7] The ElGamal Cryptosystem by Andreas V. Meier, JUNE-2005 (Survey Paper).