A Review: Security of Data using Encryption and Decryption Techniques

Harmeet Kaur[1] Ravneet Kaur[2]
[1]Research Fellow [2]Asst. Professor
[1, 2] Sri Guru Granth Sahib World University, Fatehgarh sahib, Punjab.

Abstract---While transmitting any confidential information across network, some unauthorized user tend to steal or corrupt the data. To prevent this interruption, security of data is needed. As Data security is needed for protecting data from unauthorized users and destructive forces, some security techniques are used. Encryption is one such technique which is used to protect the database from unauthorized accesses and unwanted actions of external clients. It is used to secure the confidential information from unauthorized user by converting the data in to that format that is only understandable by the authorized receiver that knows the respective decryption to obtain the original data or information. Various techniques have been implemented to ensure the security of data. In this paper, we have studied symmetric, asymmetric encryption and some other techniques.

Keywords: Data security, Encryption, Decryption

I. INTRODUCTION

Data Security means to protect a database from destructive forces and the unwanted actions of unauthorized clients. Encryption is technique that is basically used to secure the confidential information from unauthorized user by converting the data in to the understandable form that is only understandable by the authorized user that knows the respective decryption to obtain the original data or information. In their work, they used Attribute-based encryption (ABE) public-key based one to many encryption which will allow users to encrypt and decrypt data based on user selected attributes. Existing scheme would be enhanced by using Hill cipher. Hill cipher is a multi-letter cipher and the encryption technique takes m successive plaintext letters and substitutes for m cipher text letters [13].

In cryptography technique, encryption is the method of encoding messages (or data) in such a way that third user cannot read it, but only authenticated user can do it. Encryption doesn't control hacking but it can control the hacker from reading the data that is encrypted. In encryption scheme, the message or information is encrypted using an encryption algorithm, converting it into an unreadable ciphertext. This is done with the use of an encrypted key, which will specify how the message has to be encoded. An adversary that can see the ciphertext should not be able to determine anything about the original input message. An authorized user is able to decode the ciphertext using a decryption algorithm, that usually requires a secret decryption key that adversaries do not have access to. Decryption is the reverse process of encryption to get back the original data [9].

Cryptography is used to secure the data. It is easy to imagine situations in ancienttimes where a writer who sent a message via courier would want to make sure that if the runner were intercepted, the interceptors could not read the message. Cryptography and encryption havebeen particularly important

Throughout history in times of war when a general would not want the enemy to figure out the plans he was distributing amonghis troops. Recently, the uses of cryptography have grown drastically [7].

Cryptography is still important in times of war, but with the advent of computers and with it the vast amount of information being shared on the internet, there has been a need to create better, more efficient encryption strategies to protect private information, such as credit card numbers, private communications, and so on. If protection of confidential information is to be done then cryptography is provide high level of privacy of individuals and groups. Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information.

II. ENCRYPTION AND DECRYPTION

Encryption is the process of converting information into an encrypted form, so that it is intelligible only to someone who knows how to 'decrypt' it to obtain the original message. It is used in connection with electronic data, whether stored on a computer or transmitted over an unsecured network such as the Internet. Encryption tools are available and can be used to secure:

- Stored data, from single files to entire hard disks;
- Computer code such as computer operating systems;
- Information transmitted over the Internet, including e-mails and internet telephony (Voice over Internet Protocol or VoIP);
- Entire communications infrastructures, such as wireless networks (including mobile telephony).

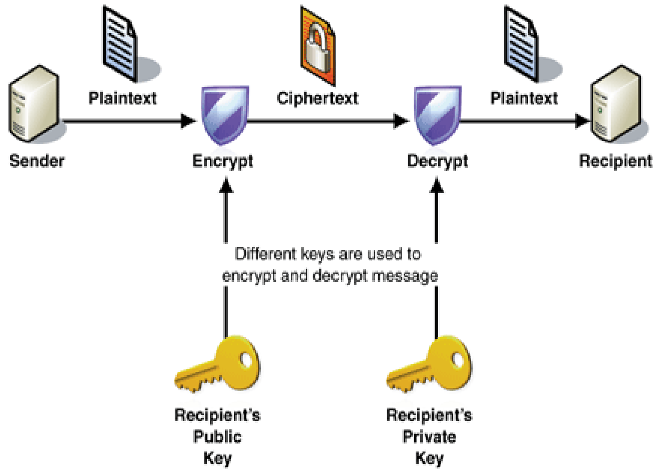

Fig. 1: Cryptography (Encryption & Decryption)

There are basically two types of encryption techniques used. Both the encryption techniques are described below.

A. *Symmetric Encryption*

In Symmetric-key method, the encryption and decryption keys are identical. Therefore communicating users must agree on a secret key before they wish to communicate. Symmetric encryption uses a single key to encrypt and decrypt the message. When user encrypt the message they provide key to the recipient user before decrypt it [9].for using symmetric encryption, the sender encode the message and, if the recipient does not already have a key, then sender sends the key and cipher text separately to the recipient user. The message then decode by recipient key. This method is very easy and fast to implement but has weaknesses.This means that the algorithm that is used to encode the message is easier for attackers to understand, enabling them to more easily decode the message.

B. *Asymmetric encryption*

In public-key encryption schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving user has access to the decryption key and is capable of reading the encrypted messages. Public-key encryption is a relatively recent invention, all encryption schemes have been symmetric-key (also called private-key) schemes[9].Asymmetric encryption is also known as Public-Key encryption that uses two different keys -a public key to encrypt the message and a private key to decrypt it. The public key is used to encrypt and private key to decrypt. One can easily distribute the public key to communicate because only with private key one can decrypt it. To protect the message between users the sender encrypts it by public key. Then receiver decrypts it by private key. Only recipient can decrypt the message in this technique of encryptions.

Decryption is the process of converting the cipher text into plain text or getting back the original data. A reverse process of encryption is called as Decryption. The process of decryption requires two things-a decryption algorithm and a key. A decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

III. RELATED WORK

In the paper [1] authors consider a new requirement of ABE with outsourced decryption: verifiability. Informally, verifiability guarantees that a user can efficiently check if the transformation is done correctly. They give the formal model of ABE with verifiable outsourced decryption and propose a concrete scheme. They prove that their new scheme is both secure and verifiable, without relying on random oracles. Finally, they show an implementation of their scheme and result of performance measurements, which indicates a significant reduction on computing resources imposed on users.

In the paper [2] profiles the execution time and the energy of each transformation within the AES decryption process and propose a novel analytic model for predicting the time and energy that are required to decrypt the content at a mobile receiver. The model uses the cross-layer information, including the characteristics of error control in the MAC layer and the varying conditions of the fading channel in the physical layer. In particular, they find that the decryption time varies significantly with the condition of the physical channel. Rate control is, therefore, required to smooth out these variations in the decryption time. For this purpose, they propose the introduction of a jitter buffer into the security layer and estimate the size of this jitter buffer to provide seamless multimedia services.

In the paper [3] proposed and implementation of four phase. First phase, image is renovated into binary matrix. Afterward matrix is apportioning into equal blocks. Two phases, each block is then encoded into DNA sequences and DNA sequence addition operation is used to add these blocks. For that result of added matrix is achieved by using two Logistic maps. At the time of decoding the DNA sequence matrix is complemented and they encrypt that result by using DES then they get encrypted image. Their paper has a novel encryption technique for the security to image. They have proposed an algorithm based on proper encryption method.

In the paper [4] developed a new cryptography algorithm which is based on block cipher concept. In this algorithm they have used logical operation like XOR and shifting operation. Experimental results show that proposed algorithm is very efficient and secured. To write this paper they have Study about information security using cryptography technique. After the detailed study of Network security using cryptography, they are presenting their proposed work. This paper is dividing in four sections. In this, they are presenting just basic introduction about Information Security using cryptography, in this, they are presenting detailed description of Information security using cryptography and various algorithms, in this, they are presenting their proposed algorithm, and in this they are presenting summary and references where they have completed their research. The proposed algorithm has the batter speed compared with the comparing encryption algorithm. Nevertheless, the proposed algorithm improves encryption security by inserting the symmetric layer. The proposed algorithm will be useful to the applications which require the same procedure of encryption and decryption.

In the paper [5] survey the security of database. This is an area of substantial interest in database because they know that, the use of database is becoming very important into day's enterprise and databases contains information that is major enterprise asset. This survey was conducted to identify the issues and threats in database security, requirements of database security, and how encryption is used at different levels to provide the security.

In the paper [6] implemented a set of encryption/decryption methods which include Hill Cipher, Caesar Cipher and Transposition Cipher & RSA. These methods are used to convert a given text into secret code it to another user & vice-versa. Further another possibility of finding out a text when a secret code is found out without knowing about the key, the sender has used to encrypt it. Hence they provide a way for encryption, decryption and an attack on any file and thus get the way for a secured communication between users.

In the paper [7] develop a security solutions that are transparent by design. Transparent Data .It is easy and effective protection of stored data by transparently encrypting data. Transparent Data Encryption can be used to provide high levels of security to columns, table and table space that is database files stored on hard drives or floppy disks or CD's, and other information that requires protection. It is the technology used by Microsoft SQL Server 2008 to encrypt database contents. The term encryption means the piece of information encoded in such a way that it can only be decoded read and understood by people for whom the information is intended. The study deals with ways to create Master Key, creation of certificate protected by the master key, creation of database master key and protection by the certificate and ways to set the database to use encryption in Microsoft SQL Server 2008.

In the paper [8] aimed at implementation of data encryption and decryption algorithm for information security. Internet and network application are growing very fast. So the importance and the value of the exchanged data over the internet are increasing. Information security has been very important issue in data communication. Any loss or threat to information can prove to be great loss to the organization. Information has to be protected when transmitting it. Cryptography plays a vital role in the field of network security. Various Cryptography techniques can be used for hiding the data during transmission so sometimes it can create little bit confusion to select best one. From the literature review the blowfish algorithm is found superior than the other algorithms.

IV. CONCLUSION

Now a days, security of data on web has become very important factor to be considered. As there are so many techniques available for the data security, so we must ensure the security of data by using the most efficient and appropriate technique. Many other techniques have been implemented till now. In this paper, we have explained encryption standards including symmetric and asymmetric techniques. Till

Now so many researches have been done on the same but still enhancements are required. For future work, we will be using hill cipher technique for the generation of cipher text so that we can enhance security based on encryption and decryption. An algorithm must be introduced using hill cipher technique.

REFERENCES

[1] Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng, "Attribute-Based Encryption with Verifiable Outsourced Decryption" IEEE Transactions on Information Forensics and Security, Vol. 8, NO. 8, August 2013.

[2] Kyungtae Kang, Junhee Ryu, Dong Kun Noh, "Accommodating the Variable Timing of Software AES Decryption on Mobile Receivers" IEEE Systems Journal, (Volume: PP, Issue: 99), pp. 1, 15 January 2013.

[3] Ranu Soni, Arun Johar, Vishakha Soni, "An Encryption and Decryption Algorithm for Image Based on DNA", BIC-TA '09. Fourth International Conference on Bio-Inspired Computing, pp. 1 – 5, 16-19 Oct. 2009.

[4] Vishwa gupta, Gajendra Singh, Ravindra Gupta, "Advance cryptography algorithm for improving data security", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012.

[5] Iqra Basharat, Farooque Azam, Abdul Wahab Muzaffar, "Database Security and Encryption: A Survey Study" International Journal of Computer Applications, Volume 47– No.12, June 2012.

[6] Rizwan Ali, Ashish Kumar, Esh Narayan, "Encryption/decryption tool with cryptanalysis", International Journal of Computer Science & Engineering Technology (IJCSET).

[7] Dr. Anwar Pasha Abdul Gafoor Deshmukh, Dr. Riyazuddin Qureshi, "Transparent Data Encryption- Solution for Security of Database Contents" IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.3, March 2011.

[8] Sweta K. Parmar, K.C. Dave, "Implementation of Data Encryption and Decryption Algorithm for Information Security" http://iraj.in/up_proc/pdf/10-137706677825-28.pdf.

[9] Melissa Chase, Sherman S.M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", http://research.microsoft.com/en-us/um/people/melissac/multiabe2.pdf.

[10] Bryan Parno, Mariana Raykova, Vinod Vaikuntanathan, "How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption", http://eprint.iacr.org/2011/597.pdf.