ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

Securing Valued Data by using Encryption Algorithms with the help of Inference Engine and Knowledge Base

Astha Gautam[1], Aatish Jaret[2]

Assistant Professor, Department of Computer Science & Engineering, LRIET, H.P., India

U.G. Student, Department of Computer Science & Engineering, LRIET, H.P., India

ABSTRACT: Today security is a main concern in information technology. Technology is upgrading day by day, we are getting ease of using the upgraded technology with a trust of security. But the fact is to know if we really are secure in the context of the data or not. Number of algorithms are there have been proposed on the basis of the level of security we needed so are the techniques too. Techniques such as steganography, cryptography etc. already are under research from ancient period of time, but still there are number of loop holes which are always a matter of concern. Different algorithms provide different sort of security which depends on the value of the information or data.In this paper we have proposed a technique of selecting a particular encryption algorithm depending on module with the help of Inference Engine. This will help selecting the type of algorithm according to the value of the data and thus providing security accordingly.

KEYWORDS: Cryptography, Confidentiality, Integrity, Inference Engine, Knowledge Base.

I. INTRODUCTION

Cryptography is an art of protecting information by transforming it or we can say that encrypting it into an unreadable format. That unreadable format is known as cipher text & the original text is known as Plain Text in technical term. Encryption is done with the help of key & the cipher text can only be decrypt if the person having the key to open it. Sometime cryptanalysis is performed that is code breaking or an attack to the cipher text. As the internet & other forms of electronic communication become more prevalent, electronic security is becoming increasingly important. Cryptology is used to protect e-mail messages, credit card information and corporate data. There are number of cryptology algorithms & system. [1]

Cryptography is an important part of preventing private data from being stolen.

Functions performed by cryptography:

1) Cryptography can also be used to authenticate that the sender of a message is the actual sender & not an imposter & even the receiver of that message is the actual receiver.Encryption also provides for repudiation, which is similar to authentication, & is used to prove that someone actually sent a message or performed an action.
2) Cryptography ensures confidentiality because only a reader with the correct deciphering algorithm or key can read the encrypted message.
3) Cryptography can protect the integrity of information by ensuring that message has not been altered.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

4) Cryptology in general means "hidden writing".It converts readable data or clear text into encoded data i.e Cipher Text. We can define cryptology as science of hiding information so that unauthorized users cannot read it. Encryption is absolutely necessary when transmitting sensitive data over unsecure medium like internet. [2]

II. NEED OF CRYPTOGRAPHY

Cryptography is needed in any situation which warrants privacy or secrecy to protect data, trade secrets or embarrassing situations. Examples include business transactions, e-commerce, political campaigns and government actions. [3]

Cryptography is the study & implementation of techniques to hide information or to protect it from being read. The information i.e. protected can be written text, electronic signals such telex or speech, or all kinds of digital information like computer files, e-mail messages or data transmissions. The unprocessed readable information is called Plain Text or plain data. A cryptographic algorithms works is controlled by a secret key, sometimes called password, the key is known only to those who are authorized to read the information without knowing the key, it should be impossible to reverse the encryption process, at the time to attempt to reverse the process should required take so much time that the information would become useless.

Cryptanalysis or cryptanalysis is the study and analysis of exiting ciphers or encryption algorithms, in order to assess their quality, to find weakness or to find a way to reverse the encryption process without having the key. Decryption without a key (often also without authorization) is a cryptanalytic attack, referred to as breaking or cracking a cipher. A cryptanalytic attack can exploit weakness in the algorithm or crypto device itself, exploit its implementation procedures or try all possible keys (brute-force attack).

2 types of attack:

1) Cipher Text-only attack: where the cryptanalyst or attacker ha access only to the Cipher Text.
2) Known plain Text Attack: Where the cryptanalyst has access to both Cipher Text & its corresponding Plain Text or assumed Plain Text, to retrieve the corresponding key.

Cryptology comprises both cryptography (making) & cryptanalysis (breaking). The expressions, 'code', 'encoding' & 'decoding' are frequency used in cryptology. A code, however is a simple replacement of information with other information & doesn't use an algorithm. Cryptography used an algorithm to manipulate the information. Ever since mankind has existed, people have had secrets and other people have wanted to know these secrets. The earliest form of cryptography were performed by pencil & paper & of course were available only to those who had access to proper education. These classical ciphers were mainly transposition ciphers, which rearrange the letters in a message & substitution cipher, which replaced letters, groups or words with other letters, groups or words.

Generally computer security introduces three key objectives that can also be considered as the heart of computer security: Confidentiality, Integrity and Availability. Together they are referred to as the CIA triad. [5]

a) **Confidentiality:**It assures that the confidential information is not disclosed to any unauthorized individuals.
b) **Integrity:** It ensures the data or information send by the sender is received unaltered by the receiver.
c) **Availability:** It assures that system works promptly and the services are not denied to any unauthorized user.

Cryptography Today:

Today cryptography is embedded in all aspects of our life to protect our privacy. When we connect our computers to internet to browse, to e-mail. Or login onto your private social network that connection is secured by TLS (Transport layer security).TLS protocol uses strong cryptography to prevent eavesdropping, tampering & message forgery. And it's not only our personal computer that uses encryption. If we go shopping, our customer card is scanned & cryptography protects the personal data of the customers.The most important benefit of

cryptography is indeed privacy. Today our lives are completely digitized. Nearly all our private information is stored in one of the many databases from the government, police, city service, banks, commercial holdings, health care services & so on. All this information can get exposed to unauthorized people. We need to stay in control of the technology that ensures our privacy.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

Cryptography protects the right to privacy & the right to communicate confidentiality. Secure communication can protect one's intimate private life, his business relations, & his social or political activities. [4]

III. PROPOSED TECHNIQUE

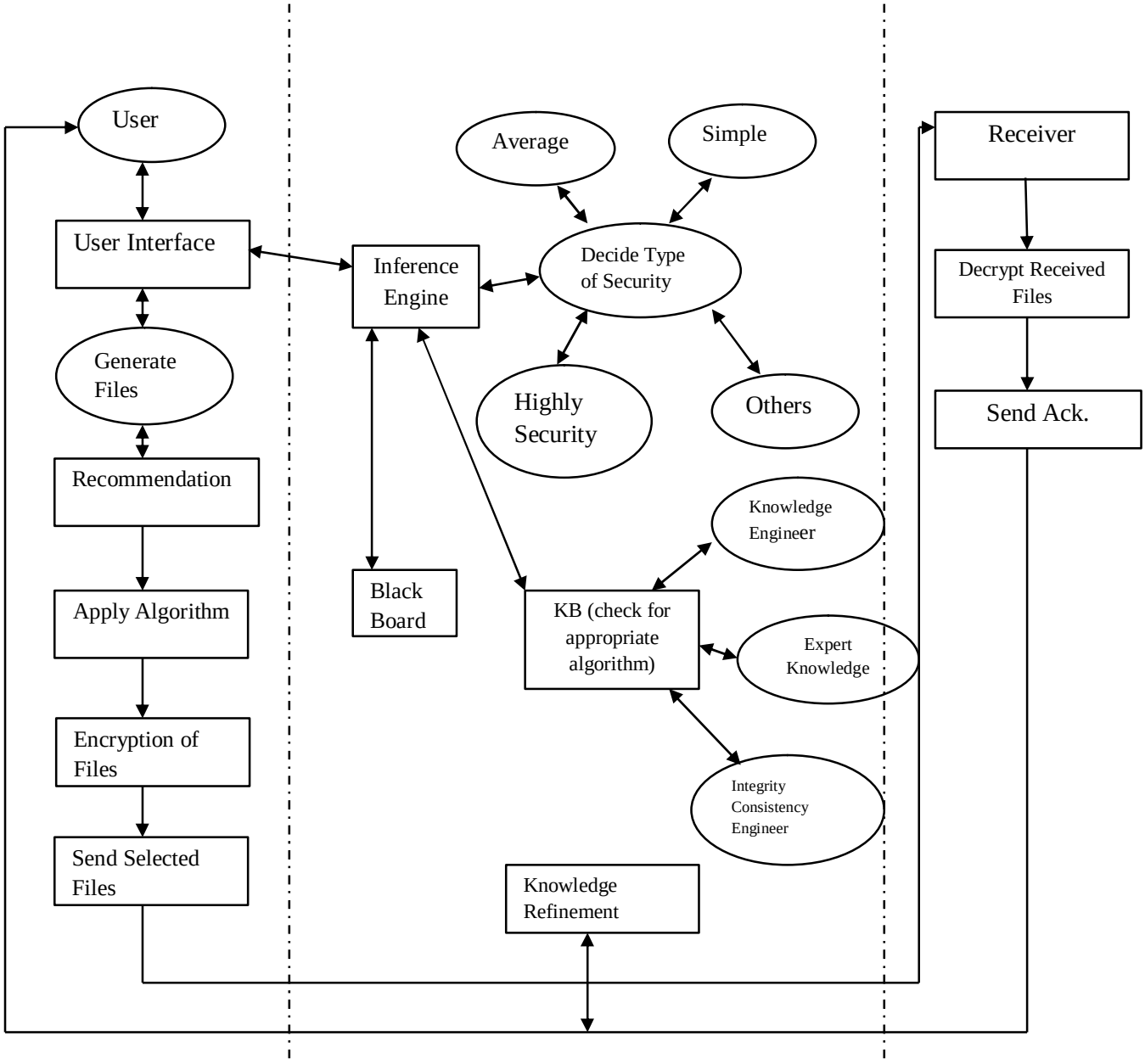

Fig. 1 Securing Information by decision making with the help of KB

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

- It is a technique of applying the appropriate encryption with the help of Inference Engine.

In general the way of transmitting the mail over the network is:

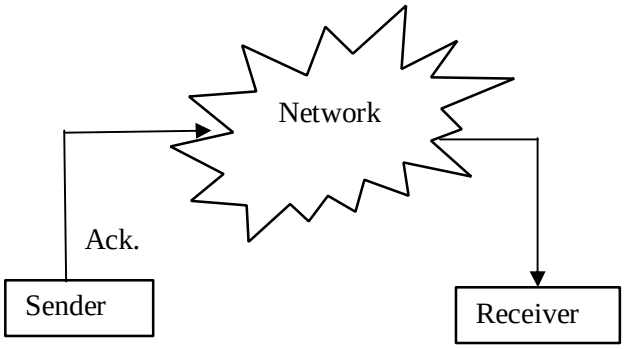

Fig. 2 Transmission of mail over network

- This is the very general way of transmission of files but it is not secure over the network. Intruder can attack the files.
- The problem is when sender has to send some secret or confidential files to receiver and the sender don't want anyone to download or open these files, expect the actual receiver.
- For such type of problem encryption is done of the files i.e. a key is used to encryption these files & even to decrypt the files the key is used i.e. known by only sender & receiver.
- After receiving the files, receiver has to send acknowledgment to the sender.

The general way of that our network is:

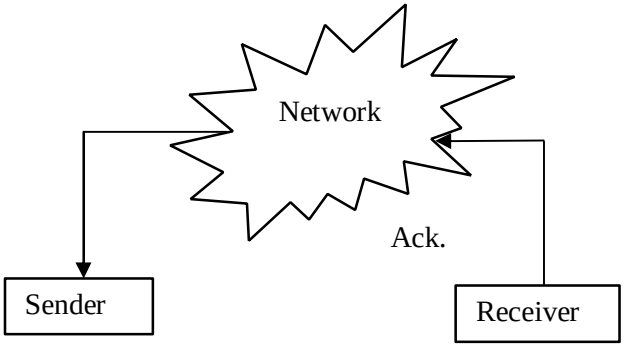

Fig. 3 Receiving of Mail by Receiver

- The problem arises if the intruder received the files & obviously if he can decrypt the file he can even send the acknowledgment.
- There are number of problems concerned with that of the type of security required, type of cryptography required, type of algorithms to be used.

ISSN (Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 4, April 2019

- Therefore, according to our proposed techniques, we are using the number of algorithms depending on the requirement, with the help of Inference Engine.
- There are number of aspects we can use in this technique. In very small aspect let us take an example we are considering 3 types of algorithms depending on various modes.
- Here modes are like we have to send a mail to the receiver, but we require the high security, high confidentiality, high integrity, high authentication etc.
- Number of factors can be there; therefore, depending on the factors or modules, it will choose the appropriate algorithm that has to apply to the message for the purpose of encryption. It will take the help of Knowledge Base for this.
- Various algorithms will be divided into the categories of low, medium and high security. Algorithms such as MD4, MD5, DES, Triple DES, Hash algorithms, Blow Fish algorithm and so on can be categorized accordingly depending on their features and properties.
- The main aim of KB is to check for appropriate algorithm i.e. best suited according to the factors available. It will trace out the algorithm & gives recommendation of that.
- Further the algorithm will be encrypted with that recommended algorithm & send to the receiver over the internet.
- At receiver side the decryption is performed and the acknowledgement is send to the receiver by applying the same encryption algorithm.
- The main concept is that the modules may vary. Some of the text may require less security, less confidentiality, high authenticity, less time or some may be very simple very average security, average confidentiality, high authenticity & less time.
- Therefore, the choice of an algorithm is based on such modules.

The inference engine will play a notable role in selecting the appropriate algorithm and recommended the same to apply into the system. Further the black board will iteratively be updated by a diverse group of specialist knowledge sources, starting with the value of the data and ending with there commended algorithm as a solution. Each knowledge source updates the blackboard with a solution when its internal constraints match the blackboard state.

IV. CONCLUSION

This paper focuses on selecting the appropriate algorithm depending on the value of the data or information. This paper helps to secure the data based on the value, as if the data value is high, it needs to be more secure and hence the more precise algorithm which can encrypt the data before sending it over to any communication network. The process of encryption and decryption is time taken and needs more sophisticated keys to work on it. This paper idea works on the concept that may be entire data which we send over the network may not be that much important for which the highly secure algorithm needed to be applied. If we apply same algorithm all time, this may increase time value first for encrypting and then for decrypting the data. This work can also be done manually, but the problem is, every time we may not select the appropriate algorithm precisely. For this reason the work is done by with the help of Inference Engine and knowledge base. So that they can choose the suitable algorithm based on the expertise knowledge and the previous decision making concept.

REFERENCES

[1] VangieBeal,Cryptography,Webopedia, www.webopedia.com/TERM/C/cryptography.html, [Accessed on: 19-04-2019]
[2] Computer Network Security, What is cryptography, www.Computer_network_security_training.com/what is cryptography, [Accessed on :02-06-2018]
[3] Internet Security and Privacy, Computer Security, Why do you need cryptography, wiki.answers.com/Q/Why_do_you_need_cryptography, [Accessed on :12-03-2019]
[4] Cryptography, users.telnet.be/d.rijneenants/en/cryptography.html, [Accessed on :2-11-2018]
[5] Stallings William, Cryptography and Network Security, Principles and Practice, Fifth Edition, Computer Security Concepts.