WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Basic Trends in Security of Cryptography Network

Vidya Vijayan [a]*, Deepthy S[b]*

[a*]ITM Vocational University, Faculty of Engineering and Technology, Waghodia, Gujarat, India
[b*]Kerala Technological University, Baselios Mathews II College of Engineering, Institute, Sasthamcotta, Kerala, India

A B S T R A C T

Network protection is for securing data through wireless transmission to ensure the contents of a message which are confidential . Data protection is the main aspects of secure data transmission over unreliable network. Network protection involves the authorization of access to data in a network, which is controlled by the network administrator. It is used in various computer network sectors such as private and public. Networks used in the organizations, enterprises, institutions, etc..are in the form of private and public. The task of network protection is not only ensuring the protection of end systems but also to the entire network. Network protection is used in various applications like Government agencies, Organization, Enterprises, Bank, Business etc. Cryptography nobody can understand the received message expect the one who has the decipher key, this is done when the sender includes a cryptography operation called hash function on the original message. A hash function is a mathematical representation of the information, when any information arrives to receiver, the receiver calculates the value of this hash function. protection of data is done by a technique called cryptography. So one can say that Cryptography is an emerging technology, which is important for network protection. In olden day's cryptography was used to keep the military information, diplomatic correspondence secure and in protecting the national protection but the usage was limited. Now-a-days, the range of cryptography applications have been expanded a lot in this modern area after the development of communication.

Keywords: Cryptography, Key, Encryption, Hash Function, Data

1. Introduction

During this pandemic, we all rely upon online for all our needs such as communication, sharing information, online shopping, net banking, work, storing personal information, etc… so we use the method called cryptography to secure the information that we share using a network. Network security is the protection of the access to files and directories in a computer network against hacking, misuse, and unauthorized changes to the system. [1] Network security acts as insurance for the stored resources. An example of network security is an anti-virus system. There are three components of network security: hardware, software, and cloud services.

The most common network vulnerabilities:

• Improperly installed hardware or software

• Operating systems or firmware that has not been updated

• Misused hardware or software

• Poor or a complete lack of physical security

• Insecure passwords

• Design flaws in a device's operating system or the network

While a vulnerability does not guarantee that a hacker, can easily gain access to our network information. Cryptography is the branch of network security. Cryptography is origin from the Greek word Kryptos meaning hidden, Cryptography is an application of mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode them. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and protect confidential transactions such as credit card and debit card transactions.

2. Process and Components of Cryptography

Components of Cryptography system are as follows:

A. Plain Text: The confidential data that should be secured while transmission is referred as plain text.

B. Cipher Text: The transformed plain texts that cannot be understand without applying encryption algorithm and encryption key over the plain text.

C. Encryption Algorithm: It is a mathematical process which is used to convert plain text into cipher text using some encryption key.

D. Decryption Algorithm: This is the reverse process of encryption algorithm. To produce the original text we use cipher text and encryption algorithm.

E. Encryption key: The value which is applied within encryption algorithm to get the cipher text from the plain text is called the encryption key. To make the cryptography system successful safeguarding of encryption key is important. The value of encryption key is known to both sender and receiver or only to the sender

F. Decryption key: To get the plain text back from the cipher text decryption key is applied within the decryption algorithm. The value of decryption key is known only to the receiver.

Network Security protects our network and data from breaches, intrusions and other threats. This is a vast and overarching term that describes hardware and software solutions as well as processes or rules and configurations relating to network use, accessibility and overall threat protection. Network Security involves access control, virus and antivirus software, application security, network analytics, types of network-related security [endpoint, web, wireless], firewalls, VPN encryption and many more. Network Security is the most vital component in information security because it is responsible for securing all the information passed through networked computer. Network Security refers to hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, administrative and management policy required to provide an acceptable level of protection for hardware and software in a network. Internet has become more widespread, if an unauthorized person is able to get access to this network, he can not only spy on us but he can easily mess upour lives. Network Security and Cryptography is a concept of protecting the network and data transmission over a wireless network. A Network Security system typically relies on layers of production and consists of multiple components including networking, monitoring and security software in addition to hardware's and appliances. All components work together to increase the overall security of the computer network. Security of data can be done by a technique called Cryptography.

Cryptography is the science of writing in secret code. Modern Cryptography exists at the intersection of the disciplines of mathematics, computer science, and electrical engineering. An application of cryptography includes ATM cards, computer password, and electronic commerce. The development of the World Wide Web resulted in broad use of cryptography for e-commerce and business applications. Cryptography is closely related to disciplines of cryptology and cryptanalysis. Techniques used for decrypting a message without any knowledge of the encryption details fail into the area of cryptanalysis. Cryptanalysis is what the layperson calls "breaking the code". The areas of cryptography and cryptanalysis together are called cryptology. Cryptography means "Hidden Secrets" is concerned with encryption.

3. Techniques

Model The following technologies can be used to reduce network attacks:

A. Authentication: All the received data must be authenticated if it is sent by the trusted sender or not

B. Antivirus: On a regular period of time we should install and update antivirus software in our system.

C. Firewalls: The inward and outward traffic of any system can be tracked using this software. This software also helps in informing the user about any unpermitted access and usage.

D. Access Controls: Each user must have their particular username and password to avoid unauthorized access.

E. Cryptography: The technique of encoding the plain text into cipher text to avoid the confidential data from getting stolen before transmitting it over channel is cryptography

4. Result and discussion

With the explosive growth in the Internet, network and data security have become an inevitable concern for any organization whose internal private network is connected to the Internet. The security for the data has become highly important. User's data privacy is a central question over cloud. With more mathematical tools, cryptographic schemes are getting more versatile and often involve multiple keys for a single application. The various schemes which are used in cryptography for Network security purpose. Encrypt message with strongly secure key which is known only by sending and recipient end, is a significant aspect to acquire robust security in cloud. The secure exchange of key between sender and receiver is an important task. The key management helps to maintain confidentiality of secret information from unauthorized users. It can also check the integrity of the exchanged message to verify the authenticity. Network security covers the use of cryptographic algorithms in network protocols and network applications. This paper briefly introduces the concept of computer security, focuses on the threats of computer network security. In the future, work can be done on key distribution and management as well as optimal cryptography algorithm for data security over clouds

Conclusion

Today everything is on the internet, thus security plays a very vital role. The older techniques are easy to attack. So, to keep the data secure cryptography is very important to save our data from unauthorized users. The key should be very confidential only to the sender and the receiver. Cryptography is useful for clients for the encryption of information and confirmation of different clients. Some cryptographic algorithms are used in network security to provide secured communication. Cryptography and network security is used in data communication over the internet to provide security. In this paper we have seen how cryptography make sure that the original data is not manipulated during any transmission. We also discussed about its goals. Network security can be prevented using various techniques like Cryptography, Firewalls, access controls and steganography etc. So to safeguard our confidential information we can say Cryptography is a must.

REFERENCES

Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington. Algorithms: http://www.cryptographyworld.com/algo.html, Data_Communication_and_Networking_by_Behrouz.A.Forouzan_4th.edition Bellare, Mihir; Canetti, Ran; Krawczyk, Hugo," Hash Functions for Message Authentication",1996.

William Stallings, "Cryptography and Network Security Principle and Practice", Fifth Edition,2011.

Diffie, W., Hellman, M.E.: New directions in cryptography. IEEE Transactions on Information Theory 22,644–654(1976).

Gross, T.,M ¨odersheim, S.: Vertical protocol composition. In:24th IEEE Computer Security Foundations Workshop(CSF2011). Publication197-Announcing the Advanced Encryption Standard (AES). Federal Information Processing Standards,26Nov.2001. Ralston, Anthony, Edwin D. Reilly, and David Hemmendinger. Encyclopedia of Computer Science. Fourthed. London, England: Nature Publishing Group,2000

Maurer, U.: Secret key agreement by public discussion from common information. IEEE Transactions on Information Theory39(3),733–742(1993) Shyam Nandan Kumar, "Technique for Security of Multimedia using NeuralNetwork," Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05,pp.1-7.Sep-2014

Preneel, B. (2010, September). Cryptography for network security: failures, successes and challenges. In International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security(pp.36-54).Springer, Berlin, Heidelberg.

Panda,M.(2014).Security in wireless sensor networks using cryptographic techniques. American Journal of Engineering Research(AJER),3(01),50-56. Dhamdhere Shubhangi .T., & Gumaste, S. V. Security in Wireless Sensor Network Using Cryptographic Techniques.

Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317-323.