A REVIEW OF DIFFERENT APPROACHES FOR IMPROVING NETWORK SECURITY IN CRYPTOGRAPHY

Chamkour Singh[1], Lovepreet Kaur[2]
[1,2]Guru Kashi University, Talwandi Sabo

ABSTRACT

Organizations all over the globe create a significant quantity of data on a daily basis, owing to the introduction of the World Wide Web and the advent of ecommerce apps and social networking sites. The most fundamental challenge both organizations and users face while ensuring secure data transfer over the internet is information security. As a society the more we are progressing towards an era of digital information, the more issues concerning network security are arising. While the number of people accessing the internet is increasing, cyber-attacks on the other hand are becoming increasingly common. It is necessary to safeguard computer and network security, which are both significant problems. The system is hampered by the parasitic hubs. It may make use of the assets of other hubs while still protecting its own. In this article, we have provided a brief introduction of network security and the different approaches that may be used to improve network security, such as cryptography.

Keywords: Security, Threats, Cryptography, Encryption, Decryption

I. INTRODUCTION

Because of the advancement of modern Internet technology and information technology, more individuals, businesses, schools, and government departments are joining the Internet, triggering more illegal users to attack and demolish the network at the same time by using fake websites, fake mail, Trojan horses, and backdoor viruses. Computers are the target of network attacks and intrusions, so if the attackers succeed, thousands of network computers will be rendered inoperable. Furthermore, some invaders with nefarious motivations see the military and government departments as targets, posing significant dangers to social and national security [1][2].

The term "cryptography" refers to the domain of encryption. Cryptography is the study of systems for secure communication. It is useful for analyzing the conventions associated with many perspectives in data security, such as authentication, information categorization, non-denial, and data uprightness.

The science of writing in secret code is known as cryptography. Modern cryptography is concerned with creating and analyzing protocols that stop attackers; [3] many elements of information security, such as data secrecy, data integrity, verification, and non-repudiation [4], are essential to the field. The testing problem is figuring out how to effectively communicate encrypted data. Encoding messages using an unmistakably safe key that is only known by the sender and recipient is a remarkable way to improve sensor security. The secure exchange of keys between sender and receiver is a difficult task in the asset critical sensor system.Clients should scramble information before sending it to a remote distributed storage service, and both information security and information access security should be guaranteed to the point where distributed storage specialist organizations are unable to decode the information, and when the client needs to search for a few sections of the entire information, the diversion should be avoided. This article examines several cryptography and system security techniques.

II. CRYPTOGRAPHY MECHANISM

Cryptography is a method of storing and sending data in a specified manner so that only those who need it may read and interpret it. The word is frequently associated with scrambling plaintext messages (standard content, also known as clear text) into cipher text (a process known as encryption), and then back again (known as decoding). There have been three types of cryptographic plans that are often employed to attain these goals: mystery key (or symmetric) cryptography, open key (or hilter kilter) cryptography, and hash works, all of which are depicted here.

Key: A key might be a unique figure or a numeric or alpha numeric text.\

Plain Text: is the introductory message sent by a person who desires to communicate with another person. For example, a guy called Alice desires to send the message "Hi Friend, how are you?" to Bob. "How are you doing?" is a simple quick message here.

Cipher Text: A message that no one can understand or a meaningless message is what we refer to as Cipher content. Suppose "Ajd672#@91ukl8*5%" is a Cipher Text for "How are you doing, Friend?" Cipher text is also known as jumbled or encoded data because it comprises a kind of basic plaintext that is undecipherable by a person or computer without any of the right figure to decode it. Decoding, or decryption backwards, is the process of converting cipher text into intelligible plaintext. Because the latter is a consequence of a code, not really a figure, cipher text should not be confused with code content.

Encryption: Encryption is the process of converting plain text into a graphical representation. This technique necessitates the use of an encryption computation as well as a key. The term "calculation" refers to the encryption technology that was used. Information is encrypted on the sender's side.

Decryption: Decryption is the reversal of an encryption operation. This method converts Cipher material into Plain content. A key and a decompiling computation are required for the decoding procedure. The term "calculation" refers to the procedure used in the process of decryption. Both computations are, for the most part, identical.

III. SYMMETRIC AND ASYMMETRIC ENCRYPTIONS

Asymmetric and symmetric encryption techniques are the most widely used approaches for encrypting and decrypting protected data.

Symmetric Encryption:

If Symmetric Encryption occurs, the plaintext is encrypted with the same cryptography keys as the figure content is unscrambled with the same cryptography keys. Symmetric encryption is faster and easier to use, but the main disadvantage is that certain clients must transfer their keys.

There is just one key that is used for data encryption and decryption.

Stream or block cyphers can be used for symmetric-key encryption. [4]. Stream cyphers encrypt a message's digits (usually bytes) one by one. Square figures gather a bunch of bits and combine them into a single unit, padding the plaintext so that it is not part of the piece measure. Squares with 64 bits were often used. 128-piece squares are used in the Advanced Encryption Standard (AES) computation, which was approved by NIST in December 2001, and the GCM piece figure mode of operation.

Asymmetric Encryption:

Since the user utilizes two keys: a public key that is shared with the public and a private key that can be accessed only by the user, asymmetric encryption is also known as Public Key Cryptography.

Key that is asymmetric Encryption, often known as public and private keys, is the process of encrypting and decrypting data.

Message data is encrypted using a recipient's public key in public key encryption. The Message can't be decoded by anybody who doesn't have the coordinating private key, who dares to be the owner of that key, or who is connected to the general public key. This is an attempt to ensure privacy. A digital signature is wherein a message is acknowledged with the sender's private key and can be confirmed by anybody with possession to the private key, therefore ensuring the Network's security.

IV. AES (ADVANCED ENCRYPTION ALGORITHM)

AES is an iterated symmetric piece figure that is shown as follows: the operation of AES is completed by repeating a similar drawn out steps under different conditions. AES is a computation that uses a mystery key to encrypt data. AES is based on predetermined bytes [5].

AES Implementation Which Works With the rapid growth of computerized information exchange via the electronic route, as well as data storage and transfer, data security is becoming increasingly important. Cryptography, which plays a critical role in data protection against various threats, now has a solution. As part of this security method, a few computations are done to scramble information into jumbled material that can only be deciphered or decoded by collecting those who have the relevant key. There are two types of cryptographic techniques in use: symmetric and hilter kilter. In this study, we used the AES (Advance encryption standard) symmetric cryptographic process with a 200-piece obstruct and a large key size. Furthermore, the 128-piece procedure is the same. For 200 pieces, the 5*5 Matrix AES computation is used. On two foci, the suggested work is compared to 256-piece, 192-bit, and 128- bit AES systems during execution. At both the encryption and decoding sides, these priorities are encryption and unscrambling time and throughput [5].

The communication is scrambled with a beneficiary's open key in open key encryption. The Message can't be decoded by anyone who doesn't even have coordinating private key, thus isn't allowed to be the owner of that key, or is associated with the general society key. This is an attempt to ensure categorization.

Efficient Data Hiding By Using AES & Advance Hill Cipher Algorithm:

We recommend an information concealing procedure based on the AES calculation in this paper. Steganography and cryptography are the two most used ways for conveying basic data secretly. Cryptography was proposed as a means of securing information. Because the jumbled communication is still available to the spy, cryptography cannot provide a superior security method. A requirement for information concealment arises.Along similar lines, security can be improved by combining steganography with cryptography. There are a variety of cryptography techniques available here, with 289 AES being one of the most effective. In cryptography, the use of an AES computation to encrypt a message with a 128-piece key conceals the message. The suggested solution makes use of the propel slope figure and AES to improve the security level, which could be assessed using various factors. This research found that a half-breed conspiracy produces better results than the past [6]

V. Network Security Model

The model of system security is shown in the diagram. Over some sort of Internet administration, a message will be sent from one group to the next. An outsider could be in authority of stealing the mysterious data and sending it to the sender and recipient while keeping it safe from competitors. The following should be taken into account while constructing a safe system.

1. Confidentiality:

It indicates that the data is not examined by the non-authenticated person.

2. Integrity:

It is an assurance that the information obtained by the collector has not really been changed or modified since the sender sent it.

There are two components to any security measures.

- A modification in the data to be sent that is relevant to security. The message should be jumbled by key in order for the enemy to be puzzled.
- An encryption key that is used in combination with the switch to scramble the information before sending and then decode it at the receiving end

When it's crucial or appealing to protect data transfer from a competitor who could pose a threat to categorization, veracity, or other factors, security considerations become critical.

V. Need for Key Management in Cloud

Encryption ensures the security of data, while key management allows access to that data. It is strongly recommended that information be encoded in very still transit over systems and on reinforcing medium. Specifically, they need knowledge to encode their own data. To assist protect apps and information stored in the Cloud, encryption and key management are required. The next sections look at the prerequisites for effective key management.

Protect key stores from obnoxious clients: Key stores must be protected from obnoxious clients. If a malicious client gains access to the private key, they will be able to access any encrypted information that the key is linked to. As a result, the key stores must be protected while travelling and on backup media.

Client access to key stores: Client access to key stores should be limited to those with access rights to information. To better control access, component partitioning should be used. The substance that utilizes a key should not be the same as the one that keeps it.

Key backup and recovery: Keys necessitate secure reinforcement and recovery plans. Loss of keys, although capable of completely destroying access to information, may be extremely damaging to a business, therefore Cloud providers must ensure that keys are not really lost via backup and recovery mechanisms.

VI. CONCLUSION

System and information security are becoming an inescapable issue for every organization whose internal private system is connected to the Internet, owing to the turbulent expansion of the Internet. The information's security has proven to be extremely important. The security of a client's data in the cloud is a major concern. Cryptographic designs are becoming more flexible as more scientific instruments are being developed, even though they frequently incorporate several keys for a single application. The study illustrates the several strategies that can be used in cryptography for network security purposes. Encoding messages using a strong secure key that is only known by the sender and recipient is a crucial aspect of cloud security. The secure interchange of keys between the sender and collector is a must-do task. Secret data from unauthorized customers is restricted by the key administration. It may also verify the validity of the exchanged message by checking its reliability.The use of cryptographic computations in system conventions and system applications is referred to as arrange security. Through this paper an attempt is made to briefly introduce the concept of PC security, by focusing on the threats to PC system security. Furthermore, how work on key circulation and administration, as well as optimal cryptography calculations for information security via mists, can be achieved has been suggested.

REFERENCES

[1] Zhijie Liu Xiaoyao Xie, Member , IEEE ,School of Mathematics and Computer Science and Zhen Wang, Key Laboratory of Information Computing Science of Guizhou Province , Guizhou Normal University Guiyang , China, The Research of Network Security Technologies.

[2] The Research of Firewall Technology in Computer Network Security, 2009 Second AsiaPacific Conference on Computational Intelligence and Industrial Applications by Xin Vue, Wei Chen, Yantao Wang, College of Computer and Information Engineering Heilongjiang Institute of Science and Technology Harbin, China.

[3] Shyam Nandan Kumar, “Technique for Security of Multimedia using Neural Network,” Paper id-IJRETM-2014-02-05-020, IJRETM, Vol: 02, Issue: 05, pp.1-7. Sep-2014

[4] Daemen, J., and Rijmen, V. "Rijndael: AES-The Advanced Encryption Standard, Springer, Heidelberg, March 2001

[5] Ritu Pahal, Vikas Kumar,”Efficient implementation of AES”, International journal of advanced research in computer science and software engineering, volume3, issue 7, july2013.

[6] N.Lalitha,P.Manimegalai,V.P.Muthu Kumar, M. Santha,”Efficient data hiding by using AES and advance Hill cipher algorithm ”, International journal of research in computer applications and Robotics, volume 2, issue 1 ,January 2014.