IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

Computer Network Security Strategy Based on Data Encryption Technology

Mr. Pradeep Nayak[1], Mohammed Tamjeed[2], Mohammed Irshad[3], Namratha[4], Naveen Kumar[5]
Department of Computer Science and Engineering (IOT)[1-5]
Alva's Institute of Engineering and Technology, Mijar, Karnataka, India

Abstract: *Recently, there has been a lot of room for the security elements of computer networks due to the rapid proliferation of information. Hacking and data breaches are two security dangers that have already inserted themselves into the computer network security framework's jigsaw puzzle. One timely security measure for computer networks is data encryption technology. It reduces security threats and safeguards data availability, confidentiality, and integrity. The research development and application status of computer network security techniques based on data encryption technology were summarized in this paper using the literature review method, which involved evaluating and analyzing pertinent research material from different nations. It also looked at the benefits and importance of data encryption technology in network security, as well as its drawbacks and future directions. According to research, the TLS/SSL protocol raised email confidentiality breaches from 318 to 81 and decreased email integrity breaches from 378 to 73. This implies that our data security can be successfully safeguarded by data encryption technology. It offers a wide range of potential applications to enhance network security performance. The intricacy and speed of encryption algorithms, for example, are some of the drawbacks and restrictions of data encryption technology itself that require further research. Therefore, it is highly justified to investigate data encryption technology for application-based research in the future, bolstering it with this context for ever-increasing security.*

Keywords: computer network, access control, network security, and data encryption

I. INTRODUCTION

Information security problems are growing as computer networks are used more and more. Network communication, data storage, identity authentication, and other topics are all part of computer network security concerns. security flaws have the potential to result in major repercussions including data breaches, system paralysis, property losses, etc. Thus, maintaining computer network security is crucial for the benefit of people, businesses, and the nation as a whole.

One crucial security protection tool is data encryption, which can encrypt private information to stop unauthorized access and hacker attacks. Data encryption technology has been studied by numerous academics. Yazdeen A. A. examined the application of DES (Data Encryption Standard) and AES (Advanced Encryption Standard) for Field Programmable Gate Arrays (FPGA) and suggested using data security and integrity to safeguard user data sharing over unprotected networks [1]. A novel data encryption technique appropriate for Internet of Things (IoT) applications was put out by Sara č evi ć M

H. Catalan objects, also known as cryptographic keys, are the foundation of the cryptosystem and offer encryption based on a combination structure with non-cross or non-nested matching [2].

In order to offer more thorough and efficient guarantees for computer network security, this article sought to investigate data encryption- based computer network security strategies and examine the uses of data encryption technology in network communication, data storage, identity authentication, etc.

as well as 387

This article's primary research methodologies include survey analysis and literature review. First, by reviewing pertinent literature, this study was able to comprehend the fundamental ideas and techniques of data encryption technology. The benefits, drawbacks, and development trends of security methods based on data encryption technology were then

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

compiled by examining the cases of data storage, identity authentication, etc. This article's research findings might aid in a better comprehension of its function and benefits.

II. DATA ENCRYPTION TECHNOLOGY

Data breaches, network attacks, viruses, and other security issues can be successfully avoided by encrypting data while it is being transmitted across a network [3]. Simultaneously, network encryption technology can guarantee data security and integrity, preventing theft during transmission. More and more data must be sent via networks in contemporary network contexts, and network security problems are growing more complicated and significant. Consequently, the use of network encryption technologies has grown in significance. At the same time, given the extensive use of networks

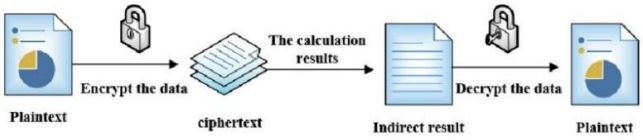

Fig: Encryption and Decryption in Data technology

A. Symmetric Encryption

Another name for symmetric encryption is shared secret encryption [4]. In the encryption process, a key is used to create ciphertext data from plain text data, and in the decryption process, the same key is used to decrypt the ciphertext data and return the original plain text data. High encryption efficiency is one of symmetric encryption's benefits, but it also has drawbacks, such as unsafe key transmission and challenging key management. Key agreement algorithms and key exchange algorithms are typically used to generate and distribute keys securely in order to address these issues.

B. Asymmetrc Encryption:

Public key Encryption is another name for asymmetric encryption. The terms "public key" and "private key" describe the various keys used for encryption and decryption in asymmetric encryption. Anyone can encrypt data using the public key that the encryption party makes available to the public, but only the owner of the private key can decode and retrieve the original content. Low Encryption and Decryption efficiency are two drawbacks of Asymmetric Encryption, but it also offers the benefits of secure key transfer and easy key management. DSA, or the digital Signature Algorithm, is one of the more widely used asymmetric encryption methods.

C. Node Encryption:

One method for encrypting data in distributed networks is node encryption [5–6]. Each node in node encryption has its own encryption key and decryption key, which it generates and maintains. In addition to preventing Man-in-the-Middle attacks and other dangers, node encryption can safeguard data security and privacy in distributed networks. Node encryption is typically implemented using asymmetric encryption technology, in which every node creates its own public and private keys and makes them available to other nodes over the network. Node encryption has applications in a number of domains, including distributed storage, blockchain technology, and Internet of Things security.
It can successfully increase data security and dependability while safeguarding sensitive data and user privacy.

III. SPECIFIC APPLICATIONS OF DATA ENCRYPTION TECHNOLOGY

The following are some particular application scenarios for data encryption technology, which has several uses in the realm of contemporary information technology:

- Network communication security: Hacker assaults and data breaches can be avoided by using data encryption technology to safeguard network communication security [7-8]. For instance, network data is encrypted and decrypted using data encryption technology via the SSL/TLS protocol.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

- Security of storage: Technology for data encryption can be employed to safeguard data storage security and stop unauthorized access and alteration. Hard disk encryption technology, for instance, can encrypt data that is kept on the hard drive so that only authorized users can access it.
- Mobile device security: Hacker assaults and data breaches can be avoided by using data encryption technologies to safeguard data on mobile devices. For instance, data encryption technology can be used by mobile device management software to both encrypt and decrypt data on mobile devices.
- Security of electronic payments: Data encryption technology can be utilized to safeguard electronic payment security and stop payment data from being altered or stolen. Electronic payment information, for instance, can be encrypted and decrypted using encryption technology.
- Database security: Hacker attacks and data breaches can be avoided using data encryption [9]. Data in a database, for instance, can be encrypted and decrypted using database encryption technology.

IV. NETWORK SECURITY PROTECTION STRATEGIES

A. Firewall Technology:

The best network security defense system available right now is a firewall. It has a very potent function. In addition to blocking unauthorized data packets from entering the network, it may also isolate the internal and external networks and even intercept and log unauthorized external network attacks. State detection, address translation, and packet filtering are the three main components of a firewall. The firewall's most crucial module is the packet filter. It filters all data packets between the intranet and the extranet and is an essential component of the complete firewall system. Firewalls are able to respond appropriately to data packets by classifying and processing them according to the various access reasons between internal and external networks.

B. Intrusion Detection System:

An active security protection solution that can monitor, assess, and react to intrusions from external systems or computer networks is an intrusion detection system (IDS) [12–13]. One or more programs that keep an eye on a computer network or system make up an intrusion detection system [14–15]. It has the ability to track and log regular network or system access and to sound an alert in the event that questionable activity is noticed. Generally speaking, there are two categories of intrusion detection systems they are network-based intrusion detection systems, or network intrusion detection systems, are the first kind. It alludes to a security tool that gathers data on computer usage from a network, examines it, and sounds an alert in the event that a hacker tries to access workstations or computers.

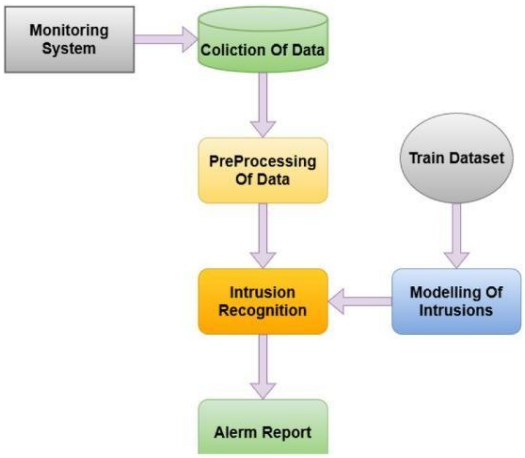

Fig: Intrusion Detection System Model

By examining the gathered data, this intrusion detection system ascertains whether a computer has been compromised. Host-based intrusion detection systems, or intrusion detection systems that use hosts for detection, are the second category. Numerous network- based intrusion detection systems are included in a network-based intrusion detection system, sometimes referred to as a network intrusion detection system. Computers, servers, or workstations can be

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

monitored, recorded, analyzed, and reported on in real time by this kind of IDS. The intrusion detection system model is displayed in Figure 2.

C. Antivirus System:

An antivirus program's main objective is to keep computers virus- free. It scans every file after analyzing the malware. It would clean it up if a virus was discovered. At the moment, antivirus technology come in three primary varieties:

Active defense technology: It guards against hacker attacks by eliminating any internal computer system weaknesses [16]. Firewalls are an example of this kind of technology.

Immune technology: This kind of technology views all computer programs as authentic and prevents viruses from infecting them.

Virus detection and removal technology: This involves installing specialist antivirus software on the computer system, which then automatically removes programs that have been contaminated with viruses.

D. Access Control Technology:

Token Ring Medium Access Control (TRMAC), an access control mechanism used to regulate the access privileges of devices in the Token Ring network, is the primary access control technique [17–18] covered in this section. Only the token-holding device in the Token Ring network is authorized to access network resources; other devices must wait for the token to be delivered to their location in order to do so. Token passing is used by TRMAC to manage the device's access privileges. A device must wait for the passage of the token to reach its destination before it may access network resources. TRMAC's primary benefit is its capacity to guarantee that network resources do not clash when used by numerous devices at once, enhancing the network's dependability and efficiency. Additionally, TRMAC can stop device conflicts and packet loss, enhancing network security and dependability. TRMAC does, however, have certain disadvantages. For instance, it is unable to stop device spoofing or spoofing, or stop hostile devices from using spoofing to obtain tokens and gain access to network resources. Furthermore, TRMAC is rarely utilized in practice since it necessitates specific hardware support. To put it briefly, the Token Ring network's devices' access privileges are managed using the TRMAC access control mechanism. Although there are certain security restrictions, it can increase the network's dependability and efficiency.

E. Digital Signature Technology:

A digital signature, sometimes referred to as a digital digest or hash function [19–20], is an encryption mechanism that uses a public key and a private key to digest data into a predetermined length.

Anyone can use the public key since it is publicly available. Only the owner of the private key can use it because it is encrypted. Data manipulation during transmission can be successfully avoided with the use of digital signature technology. The following outcomes could happen in network communication if digital signature technology is not used for encryption when data travels through a specific network segment: the data could be altered while being transmitted; the recipient might not receive all of the data; the data could be falsified; Digital signatures don't allow the sender and recipient of the message to identify each other.

V. COMPUTER NETWORK SECURITY CASE BASED ON, DATA ENCRYPTION TECHNOLOGY

One essential element of computer network security is data encryption technology. Data availability, confidentiality, and integrity can all be safeguarded by encryption. After that, 500 responders' email addresses were encrypted using the TLS/SSL protocol. The integrity and confidentiality of these 500 respondents' email addresses were examined and evaluated after 30 days. This paper examined data encryption-based computer network security scenarios.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

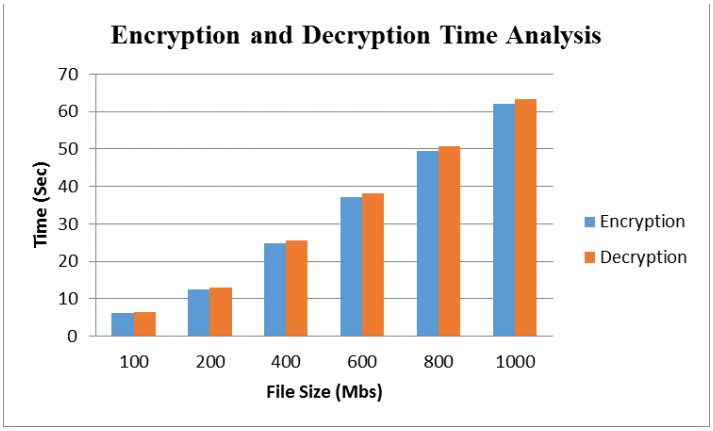

Fig: Encryption and Decryption Time Analysis

A. Design Experiments

TLS (Transport Layer Security) and its precursor SSL (Secure Socket Layer) are extensively used encryption protocols for preserving data security in network transmission. The TLS/SSL protocol is commonly used in scenarios such as websites, emails, and instant messaging to secure the confidentiality and integrity of data during transmission. Technology for encryption: The two primary encryption technologies used by the TLS/SSL protocol are symmetric encryption and public key encryption (like RSA and ECC). During the data transmission phase, both parties use session keys to encrypt the data, ensuring its confidentiality. This article randomly selected 500 email users who did not use TLS/SSL encryption technology and conducted a questionnaire survey to investigate the confidentiality and integrity of their email during transmission.

B. Experimental Results

It can be clearly seen from Figure 6 that after installing the TLS/SSL protocol, the security performance of email has been greatly improved. Both the confidentiality and integrity of emails have become more secure to some extent. However, its security is still limited and cannot fully guarantee the security of data. Therefore, the issue of data protection can be combined with authentication, access control and other security policies together to protect our data security.

VI. CONCLUSION

Traditional computer network security has a lot of information security vulnerabilities, vulnerable to malicious assaults and information leakage difficulties. The computer network security approach based on data encryption is a crucial security feature that can successfully safeguard sensitive data and information in computer networks from unauthorized access and attacks. The network's dependability and security can be increased by encrypting data to stop hackers and other malevolent people from taking it. Data encryption isn't the sole security technique, though. To provide more thorough protection and security in practice, further security mechanisms including intrusion detection and prevention, access control, security auditing, and authentication must be implemented. A computer network security plan based on data encryption must also take into account a number of crucial elements, including data transmission security, key management, encryption performance, and the security of data encryption methods. To guarantee adherence to pertinent laws and regulatory standards, it is also essential to take into account rules and regulations pertaining to data encryption, such as GDPR, HIPAA, etc. All things considered, data encryption-based computer network security techniques are a crucial security measure that can raise the network's dependability and security.

However, it is only a part of a complete security. strategy and must be used in conjunction with other security measures and standards to provide more comprehensive protection and security.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

REFERENCES

[1]. Yazdeen A A, Zeebaree S R M, Sadeeq M M, et al. "FPGA implementations for data encryption and decryption via concurrent and parallel computation: A review", Qubahan Academic Journal, 2021, 1(2): 8-16.

[2]. Saračević M H, Adamović S Z, Miškovic V A, et al. "Data encryption for Internet of Things applications based on catalan objects and two combinatorial structures", IEEE Transactions on Reliability, 2020, 70(2): 819-830.

[3]. Chevroen Washington, Phillip Yarbrough, Shavon Parker, Rafia Islam, Vardhan Patamsetti, Olatunde Abiona. "Information Assurance Technique for Mitigation of Data Breaches in the Human Service Sector", International Journal of Communication, Networking, Science,2022,15(2):15-30

[4]. Qingqing GAN, Joseph K. LIU, Xiaoming WANG, Xingliang YUAN, Shi-Feng SUN, Daxin HUANG, Cong ZUO, Jianfeng WANG. "Verifiable searchable symmetric encryption for conjunctive keyword queries in cloud storage", Frontiers of Computer Science in China: English Version,2022,16(6):103-121

[5]. Kritika Bansal, Pankaj Mukhija. Aperiodic Sampled-Data Control of Distributed Networked Control Systems Under Stochastic Cyber- Attacks[J]. journal of Edition,2020,7(4):1064-1073 Automation: English

[6]. Hongchao Ma,Yi Man, Xiao Xing, Zihan Zhuo, Mo Chen. "IOTA-Based Data Encryption Storage and Retrieval Method", Journal of Quantum Computing,2021,3(3):97-105

[7]. Manuel Muro, Aurelia Collados-Ros, Isabel Legaz. "Alcohol- related diseases and liver metastasis:Role of cell-free network communication", World Journal of Gastroenterology: English Edition,2022,28(30):4231-4234

[8]. Murali R Kuracha, Peter Thomas, Martin Tobi, Benita L McVicker. Role of cell-free network communication alcohol- associated disorders and liver metastasis[J]. World Journal of Gastroenterology: English Edition,2021,27(41):7080-7099

[9]. Yong Wang, Jinsong Xi, Tong Cheng. "The Overview of Database Security Threats' Solutions: Traditional and Machine Learning", Information Security (English),2021,12(1):34-55

[10]. Olivier Bonnaud. "Skills in Physics and Semiconductor Devices: A Global Challenge for Digital Society", Applied mathematics and Applied Physics,2021,9(11):2936-2946

[11]. O. Bonnaud. "The Challenges of Microelectronics for the Future Digital Society: The Roles of Thin Film Technologies and of the Higher Education", Materials Science and Chemical engineering,2019,7(12):47-56

[12]. Aiming Wu, Shanshan Tu, Muhammad Wagas, Yongjie Yang, Yihe Zhang, Xuetao Bai. "Intrusion Detection System Using a Distributed Ensemble Design Based Convolutional Neural Network in Fog Computing" Journal of Information Hiding and Privacy Protection,2022,4(1):25-39

[13]. Moody Alhanaya, Khalil Hamdi Ateyeh Al-Shqeerat. "Performance Analysis of Intrusion Detection System in the IoT Environment Using Feature Selection Technique", Intelligent Automation and Soft computing,2023(6):3709-3724.

[14]. Mariusz Ostrowski, Bartlomiej Blachowski, Bartosz Wójcik, Mateusz Zarski, Piotr Tauzowski, Tukasz Jankowski. "A framework for computer vision-based health monitoring of a truss structure subjected to unknown excitations", Earthquake engineering and Engineering Vibration: English,2023,22(1):1-17

[15]. Jon Karapetyan, Li Li, Eduard Geodakyan, Songyong Yuan, Roza Karapetyan. "Site survey and assessment for the planned seismogeodynamic monitoring network in the Republic of Armenia", Journal of Seismology: English,2022,35(6):510-518

[16]. Fei LIU, Xiwang DONG, Qingdong LI, Zhang REN. Cooperative differential games guidance laws for multiple attackers against an active defense target[J]. journal of Aeronautics and Astronautics of China: English Edition,2022,35(5):374-389

[17]. Hongyan Yin, Xiaokang Ren, Jinyu Liu, Shuo Zhang, Wenkun Liu. "User Station Security Protection Method Based on Random Domain Name Detection and Active Defense", Information Security (English),2023,14(1):39-51

[18]. Pablo Dorta-González, Data María Isabel Dorta-González. "Contribution of the Open Access Modality to the Impact of Hybrid Journals Controlling by Field and Time Effects", Journal of Edition,2022,7(2):57-83 Information Science: English

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 2, December 2024

[19]. AnJian-Cai Rang, Dawei Song. Tibetan Sorting Method Based on Hash Function[J]Journal (English),2022,4(2):85-98 of Artificial Intelligence

[20]. Xiaoling Huang, Youxia Dong, Guodong Ye, Wun-She Yap, Bok-Min Goi. Visually meaningful image encryption algorithm based on digital signature[J]. Digital Communication and Networking: English Version,2023,9(1):159-165