# ENHANCEMENT OF NETWORK SECURITY CONSIDERING PERFORMANCE FACTORS

**Suman**, **Princy ,** Department of Computer Science, Sat Kabir Institute of Technology and Management,Ladrawan, Bahadurgarh, Haryana

**Abstract:** Due to rapid use of network operations there remains need to enhance the security. There are different factors that are influencing network security and performance. Researches related to network security have been considered and issues in existing research work are considered to propose efficient approach. The discoveries of the reproduction show that the arranged work will give an expanded degree of security. Dangers to the working of networks have taken many structures, remembering person for the center assaults, beast force assaults, and refusal of administration assaults, among others. All togetherto prevent attacks of this kind, the study that was recommended has produced an advanced network security system. This system encrypts the data and makes use of user-defined ports to give protection. In addition, a compression mechanism has been included in order to increase speed while also incorporating security measures. According to the findings, the work that was suggested is more resistant to assault and has a lower mistake rate. The suggested work performs much better than the techniques that are typically used.

**Keywords:** Network, Security, Performance, Encryption, Data transmission, External attacks

## [1] Introduction

With the increasing reliance of businesses on IT-based infrastructures, network security has emerged as a critical issue in the area of information security. Without proper precautions, a company's IT infrastructure might be compromised, resulting in losses that would be difficult, if not impossible, to recover from.

The primary goal of network security is to shield systems from harm that might result from unauthorised access to or manipulation of data. If network security is not done effectively, a variety of issues may arise. There is always sensitive information that a company must protect from its rivals. Loss of data may reduce the value of the manufacturing and selling processes, resulting in a loss of profit. Inadequate safeguards for monetary data can pose a threat, since it is possible for misleading information to replace the real path forward in company and product promotion. Thus, the absence of security measures in the web of data may result in breaches of confidentiality in the various enterprises and marketing of goods. Therefore, it is crucial for the administrator of any network, no matter the size or kind, to use stringent regulations to minimise possible losses. Network security refers to the measures used to keep data on computer networks and the resources available through such networks safe from illegal use, modification, or restriction.

### 1.1 NETWORK CONCEPTS

A network is a collection of interconnected computers, phones, or other devices that communicate with one another through a wired or wireless connection in order to pool their resources, such as data storage and printing, or their services, such access to the Internet. There are many different types of nodes in a network, but they all serve the same purpose: to transmit and receive data created by other devices on the network (see Figure-1). In wireless networks, the paths via which messages travel between nodes are known as communication channels.

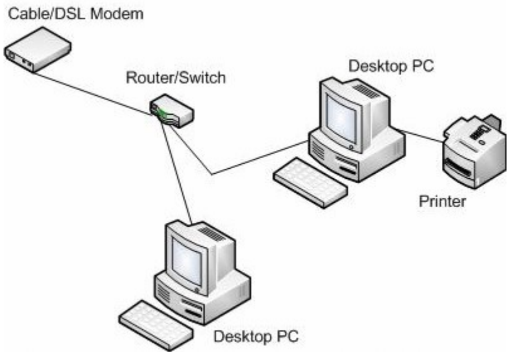

Fig 1 Basic network concept

Several security risks and difficulties are coming to light as networks grow more widespread. Many of the technologies that are now employed on the Internet are not safe. When it comes to protecting networks against intrusion, awareness is the key. Sometimes a network is set up such that it seems to the average user to be composed of only two nodes and a single link between them. This kind of thinking is usually right from a functional standpoint, but it may be misleading since it overlooks important details in the design, such as how a notion like a network is really implemented and managed.

### 1.2 Security issues in networks

With the proliferation of the Internet and the rise of digital processes that need a safe and encrypted connection, network security is now indispensable. As operating systems and software are utilised, they grow more functional and greater in size, which opens the door to a wider variety of threat sources, including software vulnerabilities. Users' sensitive and valuable data may be stolen by unauthorised parties if they get access to the network. Several security flaws are starting to emerge as networks grow more widespread. Unsafe antivirus and network security tools exist. There is "developing trend, pointing to development in both level and complexity of threats," the National Research Council said in 1991. We may have reached a breaking point; historical data on computer security is not very helpful for predicting the future. The years after 1991 have shown that this was really the case.

Consequences of security threats are always a topic of conversation. Attackers are increasingly drawn to the convenience of going after networks that transport and store data from all over the globe. The proliferation of networks has increased the number of possible attackers and hence the number of targets. Network risks, like computer system threats, endanger the privacy and security of connected devices and the information they contain.

In a digital setting, attackers' goals and methods for targeting and harming networks vary. One who is smart enough to strike first does so by researching and preparing. The information the attacker has is their most potent tool. A trusted insider might steal permitted access data and pass it along to an outsider. Outside attackers employ social engineering and other techniques to gain access to networks and steal sensitive data. Further, a port scan, an IP-specific application that reports whether ports reply to messages and which of many known vulnerabilities seem to be present, is a simple approach to collect network data. Since a port is a way for data to enter and leave a computer, port scanning is used to find unsecured entry points. While port scanning has its place in network administration, it may also be used maliciously by hackers on the lookout for vulnerable entry points.

### 1.3 Network security techniques

#### Firewall

It wasn't until the early '90s that the first firewalls were on the market. They provide an impassable barrier between floors, limiting the spread of fire from one area to another. A network firewall, in a similar vein, is a barrier that is erected between an internal network or subnetwork and the Internet. All traffic must travel via the firewall, only traffic approved by the inner network's security policy is allowed to pass, and the firewall cannot be breached; these are the aims of a firewall, according to the literature.

**Packet filtering**

Firewalls at the network layer, or packet filtering, are designed to allow only certain types of data to flow past the firewall. The interface's ruleset is checked against each incoming packet for compliance. Both incoming and outgoing packets may be governed by rules. The IP and transport protocol headers provide the foundation for the rules.

### 1.4 THREATS TO SECURITY

Cybersecurity threats are real and organisations need to be prepared. The Cloud Security Alliance identified the following as the top threats to cloud computing:

**a) Data breaches**

Information such as health, financial, personal identification, intellectual property, and other sensitive data might be the primary target of an attack in which sensitive information is accessed, stolen, or exploited by an unauthorized user.

**b) Insufficient identity, credential and access management**

Credentials might be vulnerable to attacks if they are not adequately protected. Data might be accessed, modified, or deleted by an unauthorized person.

**c) Insecure interfaces and APIs**

In order to administer and engage with cloud services, companies employ a set of software user interfaces or APIs provided by cloud service providers. In addition, these interfaces are frequently used by customers and third-party users to provide services to their consumers. They can be accessed and reused by an unauthorized person. It's possible that they'll be able to send data, receive permissions, and keep records.

**d) System vulnerability**

Exploitable flaws in applications running on a system can lead to security breaches. An attacker might get access to sensitive information or disrupt service operations by infiltrating the system.

**e) Account or service hijacking – using stolen passwords**

High-level privilege accounts can be abused through the use of account or service hijacking. Stolen passwords are commonly used in fraud, phishing, and other forms of attack that take advantage of security flaws in software.

**f) Malicious insider**

A malevolent insider can get access to the system administrator's critical data or even take control of the cloud services at a higher level, all without being noticed. Brand harm, financial losses, and productivity losses can all be caused by a malevolent insider.

**g) Data loss**

The risk of data loss in the cloud is a result of interactions between the cloud's inherent dangers and the cloud application's architectural features. Organizational records can be deleted or altered by anybody who has access to the data.

**h) Lack of due diligence**

When researching cloud technology, most cloud providers have a strong framework in place for doing due diligence. Due diligence exposes companies to dangers when they pick service providers without thoroughly assessing the technology and the hazards associated with it.

**i) Abuse and nefarious use of cloud services**

Using cloud computing resources to attack customers, businesses, and other cloud providers is referred to as a "threat." As a starting point, some of the most common methods include conducting DDoS assaults, email spam, phishing, and accessing credential databases.

**j) Shared technology vulnerabilities**

To provide their services, cloud providers pool resources, such as software or infrastructure. To provide strong isolation features, the components that form the infrastructure for cloud technology as a service may be inadequate. To put it another way, a common technology may include vulnerabilities that may be exploited in any delivery style.

## [2] Literature review

Our work was informed by a comprehensive literature evaluation of relevant papers and publications. The three most important problems are cryptography, network security, and data security. The following is a brief overview of each:.

All of the cryptographic methods are described at length by A. Krishna et al. (2020). Because of the importance of network security, storing data online safely is a time-consuming process nowadays. The purpose of cryptography is to conceal information during transmission. As with any kind of art, there is a skill involved in mastering the art of data concealment. With the exponential development of technology, the need of protecting sensitive information during transmission has skyrocketed. Multiple cryptographic techniques are used for confidential transmission. The application's security is guaranteed by the use of cryptography and a variety of methods. Encryption and decryption are two sides of the same coin that make up cryptography. [1]

Three laboratory studies using the free, open-source tool CrypTool 2 were presented by M. Alahmed (2019). These lab exercises are meant to complement the student's theoretical classroom lectures on network security. Cryptographic methods, including encryption algorithms and cryptanalysis software, are difficult to grasp without a solid grounding in mathematics. Learning these cryptographic methods is greatly aided by a combination of hands-on experimentation and theoretical foundation. Simple theoretical hand-on exercises, however, are insufficient in the face of the presence of complex cryptography systems. Over the last several years, there has been a marked improvement in all types of educational software, and cryptography software is no exception. The goal of cryptographic software is to help students better comprehend the complex algorithms by displaying them in an intuitive manner. [2]

The work by K. Vanitha et al. (2018) is a concise introduction to cryptography that analyses various cryptographic approaches and explains the basic ideas behind encryption and decoding. Services like information privacy, authentication, and data integrity immediately spring to mind when talking about data security (has not been altered) Both symmetric and asymmetric cryptography, using the public key cryptographic method RSA, are described in depth in this work. [3]

The security of computing systems was explored by N. Amalina et al. (2013), and the methods for doing so were outlined. This article focuses on the many security issues plaguing modern computer networks and demonstrates how firewalls can identify and block them. Different types of firewalls, such as Packet Filtering, Application Gateways, and Personal Firewall, are described and contrasted at the conclusion, with each kind being discussed in light of a specific network scenario. In addition, a novel architecture for managing threats to networks and keeping them secure is proposed in this study. [4]

Network security procedures were explored by R. Dastres et al. (2021) to lessen the likelihood that hackers would get access to the encrypted data. To offer a secure and risk-free means of communication for its users, a network must be protected against intrusion and misuse. This study presents a survey of the current literature on the evolution of network threats and security countermeasures, and it makes recommendations for future studies in this area. To better safeguard the data web, we explore various network assaults and how to gauge security in response to them. Research may be advanced by examining the existing papers and presenting novel concepts for network security solutions. [5]

Miguel Morales-Sandoval et al. (2018) created the AES4SeC, a cryptographic key pair-based security method. Experiments evaluating ciphertexts, private keys, and signatures have been conducted using this method extensively. When testing speed and memory requirements, AES4SeC developers found that type 3 pairs over type F elliptic curves offered the best overall results. The implementation results support this. The discovery of Type 1 pairing (symmetric) over Type A curves, which had a lower success rate, was crucial to the ABE and SSign systems. [6]

Yuan Zhang et al. (2018) planned a solid and safe information provenance methodology for a framework they called ESP to resolve these multifaceted issues. Secure and productive information reevaluating administrations are given by ESP due to its use of a blockchain-based provenance record chain to approve the integrity and idealness of provenance records. The WoL model might be utilized to assess the adequacy of secure provenance. The appraisal group presumed that ESP was secure and achievable due to its short WoL. [7]

According to Ioannis Konstantinidis and his coworkers, blockchain is the foundation of Coinbase's technology (2018). The fact that almost any transaction may be made without the need for a trusted third party has contributed to the widespread interest in this technology. Although blockchain technology was still in its infancy, much research and development was being done to expand its applicability outside the financial services industry. This paper analyses efforts by both governments and businesses to use blockchain technology into emerging products and services. Concerns regarding blockchain's possible impact on several sectors were voiced. [8]

Due to the explosion of mobile communications and networking, Guozhen Zhang et al. (2018) have developed a very complex system. utilises AI for autonomous network operation (AI). In order to get the most of AI, it is important that mobile network providers can communicate with one another. The purpose of this study was to remove barriers to sharing information by establishing a reliable network that could be relied upon by all parties involved. The system was built around the immutability and decentralised character of blockchain technology. A prototype is being constructed using Hyperledger Fabric. Smart contracts, which combined oversight with fine-grained data access limitations, required the creation of a trustless data transfer environment. They found that their system outperformed the current methods of data exchange during testing. [9]

Aiqing Zhang et al. (2018) demonstrate the potential advantages of BSPP (blockchain-based secure and private PHI sharing) for e-Health diagnostic systems like EHRs. Private and consortium blockchains' data formats and consensus processes were developed first. The protected health information itself was stored on a private blockchain, and the consortium blockchain was used only to keep track of cryptographically-protected indexes to that data. Patient health information (PHI), search terms, and individual user identities must all be encrypted with a public key before being sent to a search engine. Because of the importance of the system always being up, block producers are required to provide proof of conformance before they may add blocks to the blockchain. The security evaluation confirmed that the proposed process would work to accomplish the desired protection levels. Effectiveness of the proposed approach was measured using JUICE. [10]

The blockchain-based medical DPS was offered to Hongyu Li, et al. (2018) after they expressed interest in such a system. Users' information is kept in a secure, distributed ledger built on blockchain technology. DPS allows users to verify the integrity of data and save it permanently, even if it has been tampered with. An opponent who steals the data uses a number of cryptographic techniques to make the plain language of the data difficult to understand. Ethereum, a legitimate blockchain network, is used for the DPS prototype. The results of a comprehensive analysis of the proposed system show that it is effective and efficient. Concerns about data security were raised when Kristen N. Griggs, et al. (2018) examined the growing use of remote patient monitoring systems and Internet of Things (IoT) devices. Securely analysing and managing sensitive health data gathered by medical sensors would be achievable with the help of smart contracts implemented on the blockchain (PHI). Using a plethora of sensors, an Ethereum-based smart contract monitors the situation in real time. This smart contract system would be useful for real-time patient monitoring and medical treatments, since it could notify patients and medical staff of events and securely record the person who initiated these actions. HIPAA-compliant notification systems may improve the safety of remote patient monitoring by instantly notifying relevant parties of any potential threats. [12]

## [3] Problem statement

Encryption is the foundation for many of the security mechanisms used in networks. Research along these lines has a significant bearing on the cryptography used in network security as well as the data protection that it provides. The processing speed, dependability, and safety of these investigations are all areas in which there is room for improvement. It is necessary to have a network security system that is both more effective and accurate.

## [4] Proposed work

Cryptography, network security, and data security were all topics that were investigated in the study that was recommended. After that point, the issue was identified and resolved. There is a significant decrease in accuracy, as well as speed and safety. It has been argued that one solution to reduce the quantity of data would be to compress it, and another would be to encrypt it. Notwithstanding, the utilization of encryption brought about upgrades in both efficiency and security. Correlations have been made between the proposed model and the run of the mill model with respect to execution, botch rate, and resistance to outer connection.

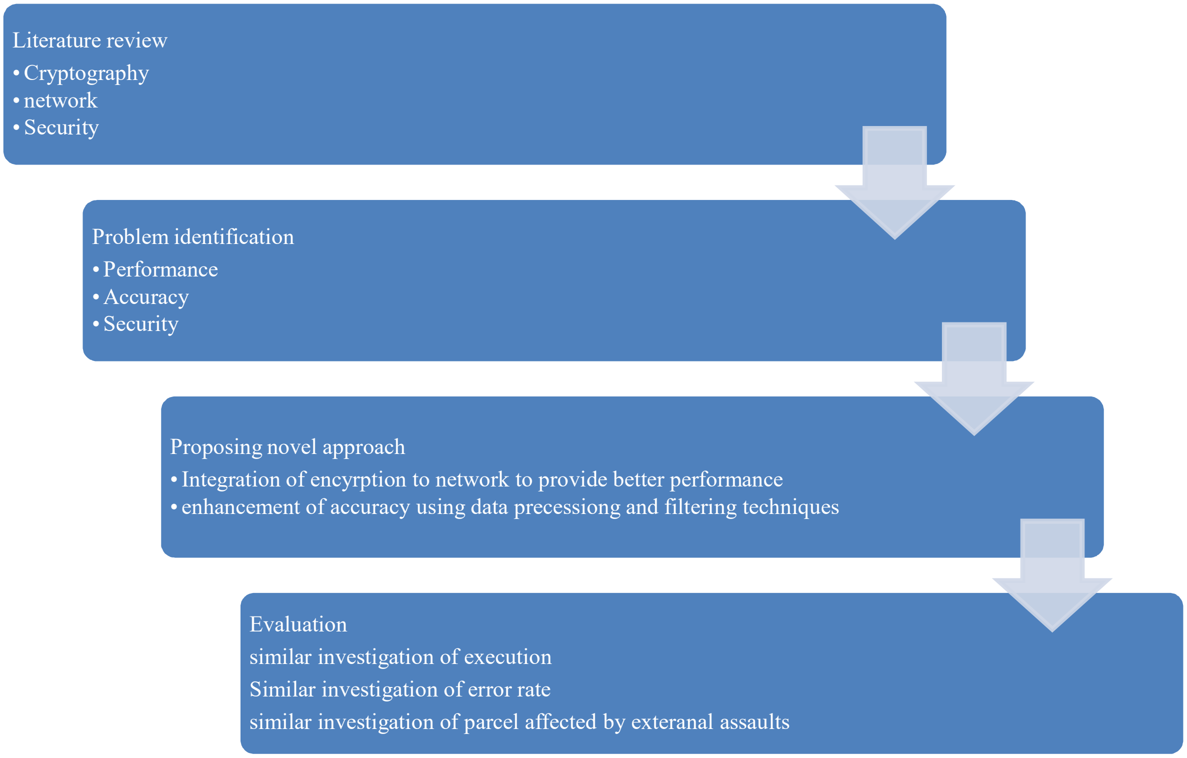
Literature review
• Cryptography
• network
• Security
Problem identification
• Performance
• Accuracy
• Security
Proposing novel approach
• Integration of encyrption to network to provide better performance
• enhancement of accuracy using data precessiong and filtering techniques
Evaluation
similar investigation of execution
Similar investigation of error rate
similar investigation of parcel affected by exteranal assaults

**Fig 2 Proposed Research Methodology**

## [5] Result and Discussion

### 1.5.1 Comparative analysis of performance

Simulates how long it takes to process a block of data in this area. There has been evidence to suggest that examining the number of blocks at 10-block intervals reduces block processing time.

**Table 1.1 Comparative analysis of performance**

| Number of blocks | Conventional processing time | Proposed processing time |
|---|---|---|
| 10 | 1.7 | 0.1 |
| 20 | 2.5 | 0.4 |
| 30 | 3.2 | 1.0 |
| 40 | 4.1 | 1.9 |
| 50 | 5.7 | 3.0 |
| 60 | 6.4 | 3.4 |
| 70 | 7.2 | 4.1 |
| 80 | 7.9 | 5.1 |
| 90 | 9.4 | 5.4 |
| 100 | 10.1 | 6.6 |

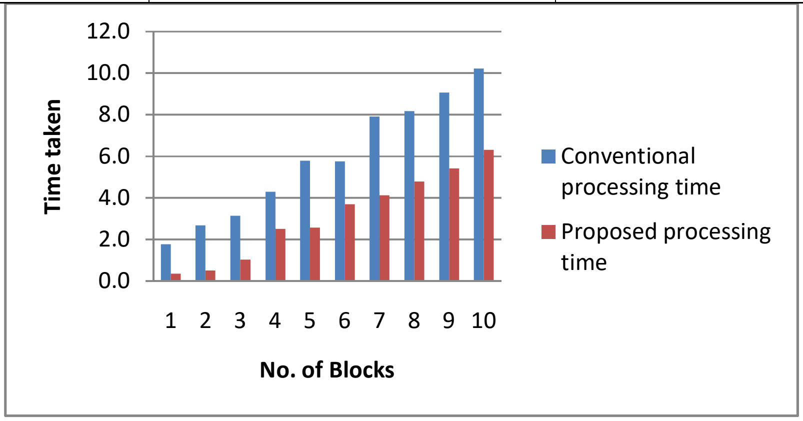

**Fig 1.6 comparative analysis of performance**

### 1.5.2 Comparative analysis of error rate

For the sake of this section, we've included a portion that accounts for simulated mistakes. When comparing block numbers every 10 blocks, there have been fewer errors than when using the usual technique.

**Table 1.2 Near investigation of Error rate**

| Number of Packet | Conventional Scheme | Proposed scheme |
|---|---|---|
| 1 | 4 | 2 |
| 2 | 6 | 2 |
| 3 | 9 | 3 |
| 4 | 11 | 4 |
| 5 | 14 | 4 |
| 6 | 16 | 5 |
| 7 | 19 | 5 |
| 8 | 21 | 6 |
| 9 | 24 | 7 |
| 10 | 26 | 7 |

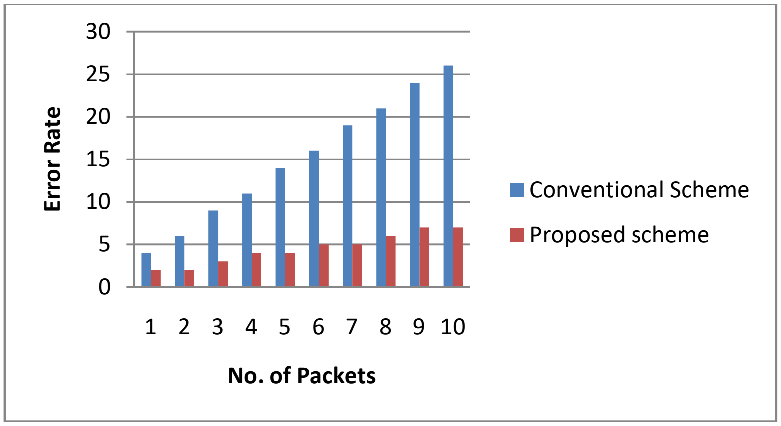

**Fig 1.7 Near investigation of Error rate**

### 1.5.3 Examination of Blocks impacted by outside assaults

In this section, an external attack has been simulated. A study found that when blocks are numbered in tens, the number of blocks that are susceptible to an outside attack is fewer than in an usual arrangement.

**Table 1.3 Comparative analysis of Blocks affected by external attacks**

| Number of blocks | Conventional Scheme | Proposed scheme |
|---|---|---|
| 1 | 4 | 3 |
| 2 | 6 | 5 |
| 3 | 7 | 6 |
| 4 | 10 | 9 |
| 5 | 10 | 9 |
| 6 | 14 | 12 |
| 7 | 14 | 13 |
| 8 | 16 | 14 |
| 9 | 18 | 15 |
| 10 | 21 | 18 |

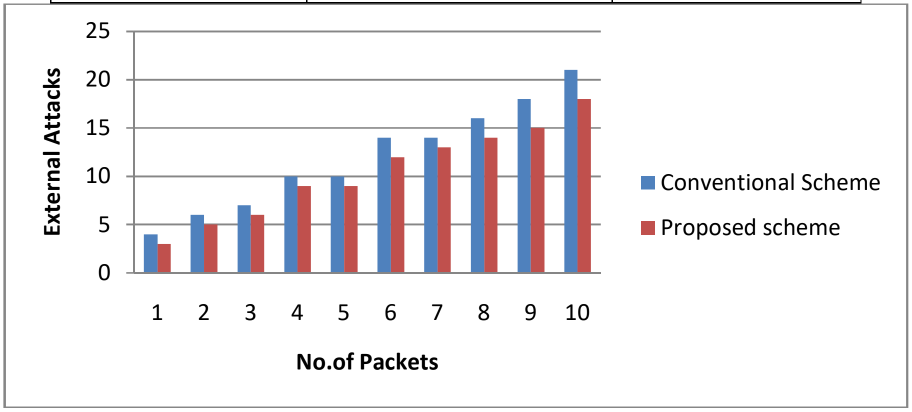

**Fig 1.8 examination of Blocks impacted by outside assaults**

## [6] Conclusion

Simulation results conclude that proposed work is providing enhanced security. There have been different types of network work threats such man in middle attack, brute force attack and services denial. In order to restrict such attack proposed research has provided advance network security system that is making use of user defined port along with data encryption. Moreover in order to improve the performance while integrating security compression mechanism has been integrated.

Results shows that proposed work is more immune to attack and is providing less error rate. The performance of proposed work is better than conventional approaches.

## [7] Scope of work

The essential objective of network security is Confidentiality, Integrity, and Accessibility. These three mainstays of Network Security are frequently addressed as CIA triangle. Data security safeguards touchy data from unapproved exercises, including review, change, recording, and any interruption or obliteration. The goal is to ensure the prosperity and security of fundamental data, for instance, client account nuances, money related data or safeguarded development.Information is an important resource that creates, gets, saves, and trades for any organization. Shielding it from inward or outside defilement and unlawful access safeguards an organization from monetary misfortune, reputational hurt, customer trust debasement, and brand disintegration. Like a wall around confidential land or a lock on an entryway, network security oversees admittance to a network by preventing different dangers from entering and spreading through a framework. Cybersecurity means to safeguard Web associated frameworks and networks from starting assaults like a hacker or a virus.

## Reference

[1] A. Krishna A and L. C. Manikandan, "A Study on Cryptographic Techniques," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 3307, pp. 321–327, 2020, doi: 10.32628/cseit206453.

[2] M. Alahmed, "Cryptographic Techniques for Network Security Academic Year 15 / 16 Cryptographic Techniques for Network Security This report is submitted in partial submission for the degree of Master of Science In Communication Network Planning and Management By Mohammed Alahmed Supervisor : Mr . Rallis Papademetriou Moderator : Dr Shikun Zhou School of Engineer," no. March, 2019, doi: 10.13140/RG.2.2.21913.06248.

[3] K. Vanitha, K. Anitha, Z. Rahaman, and M. Musthafa, "ANALYSIS OF CRYPTOGRAPHICTECHNIQUESIN Network Security," *J. Appl. Sci. Comput.*, vol. 5, no. 8, pp. 155–163, 2018.

[4] N. Amalina, R. Alsaqour, M. Uddin, O. Alsaqour, and M. Al-Hubaishi, "Enhanced network security system using firewalls," *ARPN J. Eng. Appl. Sci.*, vol. 8, no. 12, pp. 999–1004, 2013.

[5] R. Dastres and M. Soori, "A Review in Recent Development of Network Threats and Security Measures," *Int. J. Comput. Inf. Sci.*, vol. 115, no. 1, pp. 75–81, 2021, [Online]. Available: https://www.researchgate.net/publication/348676738_A_Review_in_Recent_Development_of_Network_Threats_and_Security_Measures.

[6] Morales-sandoval, M., Sosa-sosa, V. J., & Diaz-perez, J. L. G. A. (2017). A pairing-based cryptographic approach for data security in the cloud. *International Journal of Information Security*. https://doi.org/10.1007/s10207-017-0375-z

[7] B, Y. Z., Lin, X., & Xu, C. (2018). *Blockchain-Based Secure Data Provenance for Cloud Storage* (Vol. 1, Issue 2017). Springer International Publishing. https://doi.org/10.1007/978-3-030-01950-1

[8] Konstantinidis, I., Siaminos, G., Timplalexis, C., Zervas, P., Peristeras, V., & Decker, S. (2018). *Blockchain for Business Applications :* Springer International Publishing. https://doi.org/10.1007/978-3-319-93931-5

[9] Zhang, G., Li, T., Li, Y., Hui, P., & Jin, D. (2018). Blockchain-Based Data Sharing System for AI-Powered Network Operations. *Journal of Communications and Information Networks*, *3*(3), 1–8. https://doi.org/10.1007/s41650-018-0024-3

[10] Zhang, A., & Lin, X. (2018). Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *Journal of Medical Systems*, *42*(8). https://doi.org/10.1007/s10916-018-0995-5

[11] Li, H., Zhu, L., Shen, M., Gao, F., Tao, X., & Liu, S. (2018). Blockchain-Based Data Preservation System for Medical Data. *Journal of Medical Systems*, *42*(8), 1–13. https://doi.org/10.1007/s10916-018-0997-3

[12] Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems*, *42*(7), 1–7. https://doi.org/10.1007/s10916-018-0982-x

[13] Deng, R., B, N. R., Jin, R., Lu, Y., Jia, W., & Su, C. (2019). *Information Security and Cryptology - 14th International Conference, Inscrypt 2018, Fuzhou, China, December 14-17, 2018, Revised Selected Papers* (Vol. 11449). Springer International Publishing. https://doi.org/10.1007/978-3-030-14234-6

[14] Bonneau, J. (2019). Hostile Blockchain Takeovers. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 10958 LNCS*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-58820-8_7

[15] Li, D., Cai, Z., Deng, L., Yao, X., & Wang, H. H. (2019). Information security model of block chain based on intrusion sensing in the IoT environment. *Cluster Computing*, *22*, 451–468. https://doi.org/10.1007/s10586-018-2516-1

[16] Cheng, X., Chen, F., Xie, D., Sun, H., & Huang, C. (2020). Design of a Secure Medical Data Sharing Scheme Based on Blockchain. *Journal of Medical Systems*, *44*(2), 1–11. https://doi.org/10.1007/s10916-019-1468-1.

[17] Ishmaev, G. (2020). Sovereignty , privacy , and ethics in blockchain - based identity management systems. *Ethics and Information Technology*, *0123456789*. https://doi.org/10.1007/s10676-020-09563-x.

[18] Elisa, N., Yang, L., Chao, F., & Cao, Y. (2020). A framework of blockchain-based secure and privacy-preserving E-government system. *Wireless Networks*, *0*. https://doi.org/10.1007/s11276-018-1883-0

[19] Alam, S., Abdullah, H., Ayoub, Y., Abdulhaq, R., Alshaikh, A., & Hayawi, A. (2021). A Blockchain-based framework for secure Educational Credentials. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, *12*(10), 5157–5167.

[20] Sarier, N. D. (2021). Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management. *Computers and Security*, *105*, 102243. https://doi.org/10.1016/j.cose.2021.102243

[21] Rathee, T., & Singh, P. (2021). Secure data sharing using Merkle hash digest based blockchain identity management. *Peer-to-Peer Networking and Applications*. https://doi.org/10.1007/s12083-021-01212-4.

[22] Idrees, S. M., Nowostawski, M., Jameel, R., & Mourya, A. K. (2021). Security Aspects of Blockchain Technology Intended for. *Electronics*, *10*(951), 2–24.

[23] Li, C., Xiao, J., Dai, X., & Jin, H. (2021). AMVchain: authority management mechanism on blockchain-based voting systems. *Peer-to-Peer Networking and Applications*, *14*(5), 2801–2812. https://doi.org/10.1007/s12083-021-01100-x

[24] Namasudra, S., Deka, G. C., Johri, P., Hosseinpour, M., & Gandomi, A. H. (2021). The Revolution of Blockchain: State-of-the-Art and Research Challenges. *Archives of Computational Methods in Engineering*, *28*(3), 1497–1515. https://doi.org/10.1007/s11831-020-09426-0

[25] Liu, Y., Lu, Q., Zhu, C., & Yu, Q. (2021). A blockchain-based platform architecture for multimedia data management. *Multimedia Tools and Applications*, *80*(20), 30707–30723. https://doi.org/10.1007/s11042-021-10558-z

[26] Khettry, A. R., Patil, K. R., & Basavaraju, A. C. (2021). A Detailed Review on Blockchain and Its Applications. *SN Computer Science*, *2*(1), 1–9. https://doi.org/10.1007/s42979-020-00366-x

[27] Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, *0123456789*. https://doi.org/10.1007/s00521-020-05519-w

[28] Liang, W., & Ji, N. (2021). Privacy challenges of IoT-based blockchain: a systematic review. *Cluster Computing*, *0*. https://doi.org/10.1007/s10586-021-03260-0

[29] Jabbar, S., Lloyd, H., Hammoudeh, M., Adebisi, B., & Raza, U. (2021). Blockchain-enabled supply chain: analysis, challenges, and future directions. *Multimedia Systems*, *27*(4), 787–806. https://doi.org/10.1007/s00530-020-00687-0

[30] Ullah, F., & Al-Turjman, F. (2021). A conceptual framework for blockchain smart contract adoption to manage real estate deals in smart cities. *Neural Computing and Applications*, *6*. https://doi.org/10.1007/s00521-021-05800-6

[31] Ranjith Kumar, M. V., & Bhalaji, N. (2021). Blockchain Based Chameleon Hashing Technique for Privacy Preservation in E-Governance System. *Wireless Personal Communications*, *117*(2), 987–1006. https://doi.org/10.1007/s11277-020-07907-w

[32] Sun, X., Zou, J., Li, L., & Luo, M. (2021). A blockchain-based online language learning system. *Telecommunication Systems*, *76*(2), 155–166. https://doi.org/10.1007/s11235-020-00699-1

[33] Wang, D., Wang, H., & Fu, Y. (2021). Blockchain-based IoT device identification and management in 5G smart grid. *Eurasip Journal on Wireless Communications and Networking*, *2021*(1). https://doi.org/10.1186/s13638-021-01966-8

[34] Rathee, G., Balasaraswathi, M., Chandran, K. P., Gupta, S. D., & Boopathi, C. S. (2021). A secure IoT sensors communication in industry 4.0 using blockchain technology. *Journal of Ambient Intelligence and Humanized Computing*, *12*(1), 533–545. https://doi.org/10.1007/s12652-020-02017-8

[35] Pandey, P., & Litoriya, R. (2021). Promoting Trustless Computation Through Blockchain Technology. *National Academy Science Letters*, *44*(3), 225–231. https://doi.org/10.1007/s40009-020-00978-0

[36] Banupriya, S., Kottursamy, K., & Bashir, A. K. (2021). Privacy-preserving hierarchical deterministic key generation based on a lattice of rings in public blockchain. *Peer-to-Peer Networking and Applications*, *14*(5), 2813–2825. https://doi.org/10.1007/s12083-021-01117-2

[37] Rathee, T., & Singh, P. (2021). A systematic literature mapping on secure identity management using blockchain technology. *Journal of King Saud University - Computer and Information Sciences*, *xxxx*. https://doi.org/10.1016/j.jksuci.2021.03.005

[38]Hardjono, T., & Smith, N. (2021). Towards an attestation architecture for blockchain networks. *World Wide Web*, *24*(5), 1587–1615. https://doi.org/10.1007/s11280-021-00869-4

[39] Sen Gupta, Y., Mukherjee, S., Dutta, R., & Bhattacharya, S. (2021). A blockchain-based approach using smart contracts to develop a smart waste management system. *International Journal of Environmental Science and Technology*, *0123456789*. https://doi.org/10.1007/s13762-021-03507-8

[40] Garba, A., Dwivedi, A. D., Kamal, M., Srivastava, G., Tariq, M., Hasan, M. A., & Chen, Z. (2021). A digital rights management system based on a scalable blockchain. *Peer-to-Peer Networking and Applications*, *14*(5), 2665–2680. https://doi.org/10.1007/s12083-020-01023-z

[41] Rouhani, S., Belchior, R., Cruz, R. S., & Deters, R. (2021). Distributed attribute-based access control system using permissioned blockchain. *World Wide Web*, *24*(5), 1617–1644. https://doi.org/10.1007/s11280-021-00874-7