International Journal of Scientific Research and Modern Technology (IJSRMT) *ijsrmt.com*
Volume 4, Issue 10, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i10.872

When Encryption Meets Efficiency: Analysing the Performance Impact of Data Security Techniques

Yousef Elzidani[1]

[1]BSc of Cybersecurity and Digital Forensics University of West of England (UWE) Bristol, England.

Publishing Date: 14/10/2025

Abstract

These days, computer networks are used in a wide variety of home and business settings worldwide. Computer networks play a crucial role in corporate organisations. Device-to-device communication is at risk since hackers can fetch this data without authorisation. As a result, data is encrypted to protect it from online threats. When this encryption procedure is used across a network, it presents serious difficulties. Because it uses a lot of extra network resources to do complex computations, such as encrypting and decrypting data. As a result, it affects computer network performance, which results in a very poor user experience. Finding the best and most suitable solution is crucial to maintaining the robustness and integrity of data security as well as increasing network efficiency. This paper's findings include an evaluation of how encryption affects network performance. Additionally, strategies to lessen the effect of data encryption on computer network performance are included. Through future study, more effective data encryption methods can be developed.

Keywords: *Encryption, Data Security, Network Performance, Encryption Algorithms.*

I. INTRODUCTION

Nowadays, in this digital era, the world relies on the transmission of data from one place to another through computer networks. Computer networks have applications in every sector and field. Computer networks are perceived as the backbone of technological and business growth. In current times, there is a significant increase in cyberattacks. These hacking experts fetch the important data of business organisations through computer networks illicitly, which makes their data compromised. Consequently, there can be serious ramifications of cyber assaults for companies [1]. As a result, the information is required to be protected by safeguarding its transmission to make sure that its secrecy and integrity is maintained. Therefore, encryption is required to be carried out to make data secure. Data encryption has some merits as well as demerits. It makes data secure, but it has some impact on the performance of networks, which depends on various factors, including type, level of encryption and order of processes. The focus of global debate is on the impact of encryption on the performance of networks, as it is impacting global business community massively [2].

II. LITERATURE REVIEW

- *Data Encryption*

It is the process of converting information into an indecipherable form through an algorithm. The encrypted information can be changed to its original form by means of the key. The person who possesses the key can get the decrypted information [3].

- *Sorts of Data Encryption*

Data encryption has two major types. Symmetric encryption and asymmetric encryption are these two sorts [4]. In symmetric encryption, those who possess authorisation and receive information have the private key, which can be used to encrypt and decrypt information. It is a basic method, but it is not recommended for commercial applications as it sends the key with data, which is not secure [5]. Asymmetric encryption is comprised of two keys, I-e, public and private keys. Public key is publicly available to everyone, while the private key is only available to authorised people. A mathematical formula is employed to decrypt data, which requires both keys. The private key can decrypt the information which is encrypted by the public key [6].

Elzidani, Y. (2025). When Encryption Meets Efficiency: Analysing the Performance Impact of Data Security Techniques: A Systematic Review of Network Encryption Performance. *International Journal of Scientific Research and Modern Technology, 4*(10), 1–8.
https://doi.org/10.38124/ijsrmt.v4i10.872

➢ *Determinants of Encryption Performance*

Encryption is a critical approach for ensuring the integrity and confidentiality of data. However, there are different factors which impact the performance of encryption.

➢ *Technique and Mode*

The selection of mode and algorithm has a significant impact on the efficiency of encryption and its scalability [7]. There are some pros and cons of different algorithms of encryption. These algorithms vary in terms of speed, protection and usage of resources. For example, Advanced Encryption Standard (AES) has greater speed and better security as compared to Data Encryption Standard (DES). In contrast, AES has greater memory and processing power requirements than DES [7].

➢ *Management of Key*

Key management is the other main component of encryption, which impacts the efficiency and scale of encryption. During the procedure of encryption, the keys are produced, saved and shared [8]. The safety of keys, accessibility and compatibility with various systems are some of the main problems of key management. The impact of key management on the efficiency and speed of encryption and decryption techniques depends on the size, type and frequency of variations in the key [8].

➢ *Hardware and Software*

The hardware and software of networking appliances have an impact on the efficiency as well as scalability of encryption. The physical components incorporate processors, network cards and memory. The software is the programs which employ algorithms to carry out the encryption and decryption process [11]. These programs include libraries, frameworks, and protocols. The impact of hardware and software on encryption's efficiency and scalability is in terms of configuration, enhancement and synchronisation. For example, the hardware can accelerate the sort of task which can be expedited by it. Moreover, this can reduce the computational load on the central processing unit. However, the synchronisation and utility of encryption can be reduced if there is incompatibility between software components and encryption [9].

➢ *Data Size and Frequency*

The greater size of data and high frequency can impact the performance and scale of encryption. The information is transmitted in the form of packets, documents, and texts [13]. The rate at which encryption and decryption should be carried out is keyword data frequency. The impact of frequency and size of information on the performance and scale can be measured in latency, output and bandwidth [10].

➢ *Security Requirements*

The higher data protection requirements are based on the type, value, and sensitivity of information and applicable regulations. It can have an effect on the functioning and scale of encryption [15]. Appropriate algorithms, modes and key management are essential to comply with protection requirements. The high security reduces the efficiency and frequency of the encryption procedure badly [11].

➢ *System Design*

The method of integration of encryption into the system can impact the working of encryption with other components of the system. The different components are sources of information, flows of data and data conversions. The usage of resources of system nodes, including servers and clients, can vary as it depends on the way encryption is scaled in the system. The level of integration with the system can influence how well it will adapt to the requirements and changes in the system, such as load, growth and productivity [12].

➢ *Ways to Minimise Performance Impact*

The enhancement of encrypted communication is the major requirement to mitigate the impact on performance. There are various approaches which can be employed to make the plain text data secure from possible threats, and encryption incorporates the conversion of the data into "*Ciphertext*" [13].

➢ *Selection of Appropriate Encryption Algorithms*

Appropriate algorithm selection is quite significant. Every algorithm requires a different magnitude of computational intricacy. Enterprises are balancing between protection and efficiency by assessing the network's requirements and the significance of data.

➢ *Hardware-based Acceleration*

The encryption efficiency is elevated through hardware accelerators. These accelerators are developed to perform cryptographic processes effectively. It reduces the load on the main CPU [14]. The major impact of encryption on networks is minimised through incorporating accelerators in servers that enhance performance.

➢ *Perfect Forward Secrecy*

The current as well as future communication has not employed a "*Cryptographic Key*" for decryption as per the concept of perfect forward secrecy. It is an important data security feature, but it impacts the encryption efficiency. The deployment of perfect forward secrecy comprises attentive deliberation regarding computational load and key exchange techniques to balance between protection and efficiency [20].

➢ *Compression Approaches*

The reduction of noise is carried out by compression before transmitting the data. It allows to transmit data appropriately, enhances the performance of the network and reduces the transmission time [21].

➢ *Load Balancing and Traffic Shaping*

This enhancement approach enhances the performance of the network by easing congestion and reducing delays. The encryption normally consumes the majority of network resources. This technique still enhances performance. It employs Traffic Shaping approaches to convert Plaintext to Ciphertext. It is carried

out to transmit data which is time sensitive. It enhances flexibility and precision depending on the data, which is encrypted [15].

➢ *Content Delivery Networks*

These sorts of networks have elevated the network performance significantly. CDNs transfer the computation load to scattered servers which are near the users while transmitting the main data. Content delivery networks are employing an important encryption approach for making the confidential information secure during transmission [16].

III. METHODOLOGY

➢ *Research Design*

The methodology of this research paper is comprised of a systematic review of relevant and latest literature for exploring the impact of encryption on the performance of computer networks, including the way it enhances the security of data, contributing factors, and ways to reduce the impact of data encryption on network [17].

➢ *Search Strategies*

The systematic review conducted in this research paper abides by the framework of Petticrew and Roberts [18]. The search in numerous research journals and repositories is carried through employing relevant key terms. For collecting diverse literature, the reference lists and in-text references are checked. Moreover, the titles, abstracts, and keywords of different publications checked to explore more pertinent publications [19]. For conducting the pertinent research and fulfilling the requirements of the current paper, the major term used is 'impact of encryption'. By means of this key term, different research repositories are checked. These repositories include Research Gate, Scopus, Web of Science, Grey Literature, and Science Direct. The other relevant key terms which are used include ‘encryption’, ‘encryption and network performance’, ‘demerits of encryption’, ‘disadvantages of encryption’, ‘factors impacting network performance’, ‘ways to minimise network performance impact’, and ‘techniques to reduce encryption impact on network’.

During the search the complete focus was on finding the pertinent literature to the topic of this paper I-e impact of data encryption on network performance. These all terms are used to get the highly pertinent, authentic and latest information. The focus remained on research papers, reports, and conference proceedings. By means of inclusion criteria, peer-reviewed papers are incorporated. The papers need to have relevance with cybersecurity, networking and encryption [20].

Due to exclusion criteria, some publications are overlooked. In includes the publications which are not pertinent to networking. Moreover, the publications which fall in the networking field but remain irrelevant to encryption, data transmission, and network performance are considered not pertinent. In addition, the key terms ‘encryption’ or ‘network performance’ or ‘impact on network performance’ are incorporated in publications 1-4 times. First, 52 publications are considered. In contrast, 13 of the irrelevant ones are excluded. Therefore, the remaining 39 are shortlisted. The publications’ references, and in-text references are assessed. Moreover, backwards and forward references are assessed. The number of publications which are shortlisted as a result of backwards searches is 5. Additionally, the 'cited by' feature is used in carrying out forward searches of 39 papers. It is conducted by checking the titles, abstracts, and keywords. Therefore, another 7 papers are included. The 3 papers were similar and were excluded. Therefore, the total number of papers shortlisted for systematic review is 48. The literature is checked twice to ensure the pertinence and authenticity of the literature.

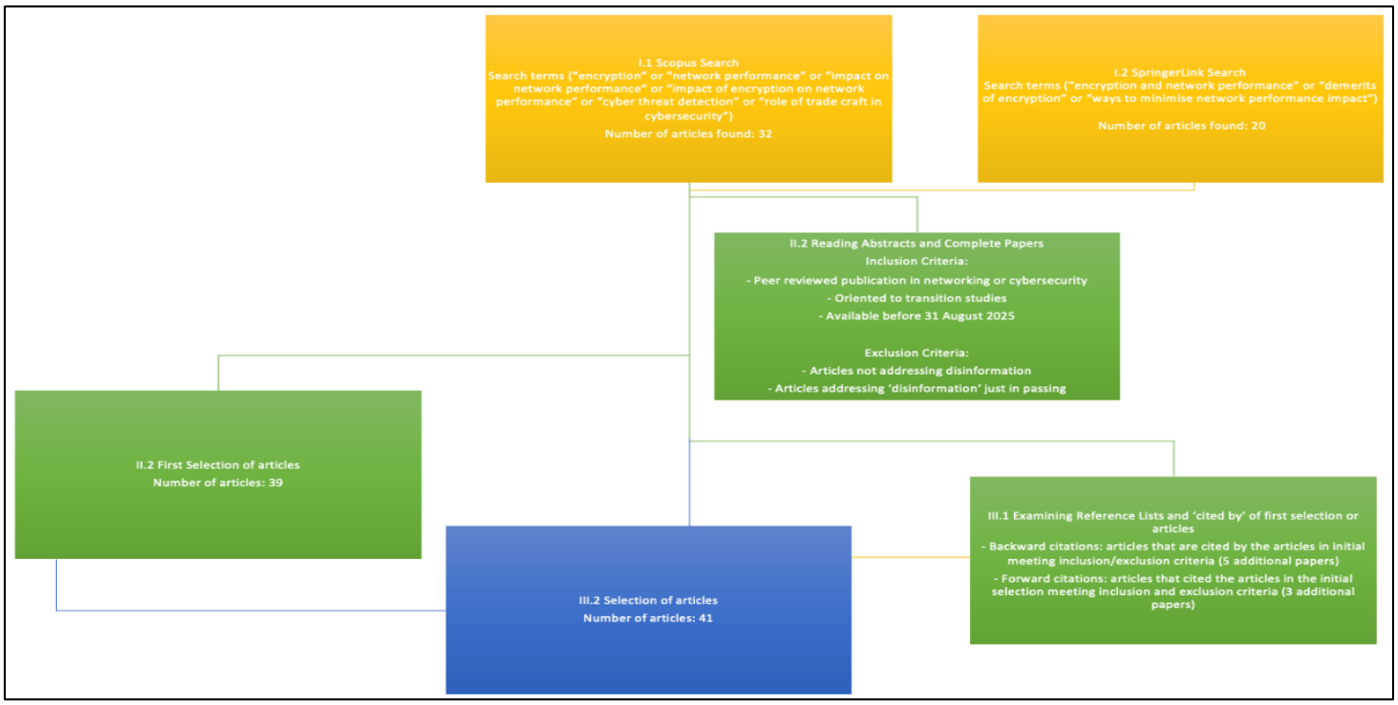

Fig 1 Flow of Systematic Review

IV. FINDINGS

➢ *Encryption's Role in Data Protection*

The most effective and appropriate technique to make the information safe is encryption. A good encryption technique is one which does not impact work, which can be accomplished by protecting data and having a balance between productivity as well as security [28]. Furthermore, the processing should be expedited when data is being encrypted and decrypted. It will minimise the response time. The information must be encrypted and decrypted fairly and accessible to people who are authorised [21].

In addition, the encrypted database' size must not be increased to a greater extent. The protection of information is completely dependent on the secrecy of encryption keys. Consequently, the key management has paramount significance [23]. The key generation should be carried out in such a manner that it cannot be predicted, even if the algorithm, configuration and generated key are fetched, no one can anticipate or trace the future keys [23].

By means of data encryption, an authorised resource can store the information securely by keeping it separate from the system. This encryption procedure ensures that no unauthorised person can fetch information when it is in an idle state. After encryption, the authorised person can even send the encrypted data through a medium that is not secure [22].

This process of making information encrypted is a comprehensive errand as it involves the generation of a number of keys in order to make data protected. Although the key storage and management is quite strenuous. If any key is illegally fetched by a hacker then the owner of the information will not be able to possess it [26].

Secrecy, availability and integrity of information are critical components of making information protected. It is difficult to attain secrecy as well as availability at the same time [27]. The reason is that data can be protected by encryption by the database, so once it is protected, it cannot be completely available. Consequently, it is required to carry out a balance between secrecy and availability [21].

The process of encrypting data impedes the efficacy of traditional data techniques. It is strenuous to trace unusual patterns in the encrypted traffic. Furthermore, the tools which are employed to prevent the loss of data cannot check and protect the illicit transmission of secret data. The malicious assaults exploit it, actually, which encrypt information prior exfiltration or encryption of communications among command-and-control and system which is assaulted [22].

The best method is to perform TLS evaluation, start encrypted traffic with a private TLS certificate and spot harmful elements in decrypted traffic. In this case no end-to-end encryption will be available. In this case, trusting third-party firms and a TLS inspection box will be an available option to oversee the network traffic [36]. This is not recommended when information is quite critical and private. Decryption and assessment of the payload make confidentiality compromised if the user does not know the technicalities. As the network engineers carry out device configuration to make intermediate certificates reliable without informing the users [36].

In the current technological landscape, the main difficult errand is to ensure conformity in end-to-end protection, adhering clientele confidentiality and fetching adequate information of network traffic prior to potential threats and dedicate resources accordingly and make them save. It is a strenuous challenge, so the substitute techniques need to be investigated to identify threats which can make the secrecy of the user secure. Artificial intelligence-driven and machine learning-based modern technologies can be built [38].

The transmitted information can be protected through cryptographic algorithms through turning data into an encrypted text such as ciphertext. It can just be deciphered by people who possess authorisation. This will not permit people who don't possess permission to get secret information. The cryptographic encryption techniques provide an added protection layer to counter digital threats, securing the identity-based information and secrecy of those who are senders and receivers. The AI and ML-driven approaches can be used to carry out encryption of data, identify abnormalities and access control systems in an efficient manner [23].

The potential digital threats can be anticipated and decreased through leveraging AI and ML by identifying the data access patterns appropriately. In similar fashion, AI and ML-based technologies can allow recognising malicious things and automating the security of information. Accordingly, encrypting the information hides it. Therefore, encrypting data has a major impact in identification and scanning network traffic [40].

➢ *Encryption's Impact on the Network Performance*

The functioning of encryption impacts the performance of the network. Consequently, the right encryption approach is required to be adapted. The companies need to maintain a balance between the requirement to make data secure and up-to-the-mark performance [25].

The overhead impact of data encryption is on TCP. It is an internet protocol. It is liable to transmit information over the networks. The data is transformed from text into ciphertext by encryption for protecting it. Though it enhances the data size [26].

The data which is not encrypted has a smaller transfer time. In case the size of information which is not encrypted increases, the transfer time increases in a consistent manner. Nevertheless, in case the size of encrypted information increases the transfer time changes in an

inconsistent manner. Furthermore, it is observed that transfer time of encrypted information normally remains considerably high [43].

Normally, the cryptographic algorithms make the information highly secure that they allow senders to send the information over the mediums which are considered unreliable. Although intricate cryptographic procedures consume high technical resources and cause considerable network overhead. It is linked with significant costs such as overhead costs [28]. For the major range of node densities, AES outweighed DES standard in terms of latency, packet delivery proportion and data yield. Although there is the greatest packet loss due to the Advanced Encryption Standard cryptographic algorithm. In contrast, there is minimal packet loss in DES. Consequently, there are sizeable overheads and related costs caused by encryption [27].

AES gives a matchless network performance. AES requires the fewest rounds, that guides to a small deployment time while remaining random. Although Triple Data Encryption Standard requires a comparatively high number of rounds for verification. Therefore, it uses a higher authentication time. Consequently, AES provides quite lower deployment times and reduced intricacy while remaining random and protected from malicious activities [28].

It becomes difficult to analyse the traffic and performance of the network because of encryption. The technical staff normally relies on the capacity of the application to evaluate and understand the traffic's components to supervise potential issues and gain detailed insights about the network's performance as well as protection [29]. The tools which sniff network and trace packets are leveraged to troubleshoot the network-related difficulties. These tools scan traffic through by analysing packets as well as load. Furthermore, data flow is assessed by means of network flow analysers. These tools provide details regarding network performance, bandwidth and type of traffic. Tools related to network performance management supervise and scan network performance to find out and solve malfunctions which is impacting the network performance. Such applications are leveraged to highlight and diagnose issues including higher delay, less network access and poor performance [48].

The functioning and efficiency of network flow analysers is impacted by encryption. As they employ transmitted data to enhance the visibility of the network with tool information. Therefore, tools don't have the capacity to scan network packet payloads for checking the traffic, as encryption of data payload is carried out. Consequently, the technical staff remain able to receive handsome traffic details through leveraging SSL/TLS decrypting or obtaining the HTTP header from encryption certificates to identify traffic [49].

If the lengths of keys are different, the substantial length of encryption keys enables considerable changes in consumption of power and time. Hence, encryption shrinks the network performance massively [30].

- *Recommendations to Lessen the Effect of Encryption on the Performance of Networks*

The appropriate way to protect important information and make sure efficiency of networks is to carryout encryption of information at the DB level. Normally, the information is encrypted at the levels of file and the application. The two major types of encryption incorporate approaches that can be utilised to lessen the encryption's overhead and number of procedures and stages in encryption [25].

Furthermore, there is quite an intricacy in issues related to efficiency and protection. Consequently, the services of various technical and network professionals need to be taken who possess a complete comprehension of available choices as well as the end user or organisation's certain environment. As dependency on perimeter security and DB access control will not be adequate for the needed security. The tools related to packaged database encryption have significant efficacy in making the sensitive information secure [51].

It requires attentive oversight and enhancement of results while encrypting data to keep a balance between information protection and network performance. The performance of encryption can be assessed through different frameworks and metrics. It incorporates encryption rate, latency, quality, and security. Furthermore, there are a number of techniques through which encryption's productivity can be made better [31].

Such techniques manage factors, leverage parallel processing and perform hardware-powered and software-powered acceleration. The requirement is to find the desired balance between various variables. These variables include time, size, quality, and protection, fine-tune variables like level, mode, packet's size, or key's size. The multi-cores, multi-threads, or multi-nodes can help in enhancing the scale, efficiency and outcome. Additionally, the performance of networks can be significantly elevated by employing dedicated chipsets, GPUs or frameworks while maintaining interoperability and reliability [53].

The systems which carry out encryption need to be upgraded in order to enhance capacity and capability, so encrypting information can be considerably costly. Without the latest and cutting-edge systems, the number of steps in encrypting information will be on the higher side [22].

CDN reduces end-to-end delivery time towards the end-users. Furthermore, it removes loads of content providers that allow to ensure security against Distributed Denial of Service threats. It consists of a gigantic number of nodes that help users to gain information from close by nodes. Such networks elevate the user experience through sharing information to end-users by means of the appropriate usage of resources of network. CDNs preserve content in caches in locations close to end-users, send

fetched content to those locations and send information to end-users [32].

The symmetric wireless networks will revolutionise cellular communication systems. The way to enhance resource distribution, data transmission rate, time, and various competencies is a significant thing to deliberate on due to micro base stations' minute assets in the wireless networks. There is a need to have an appropriate heuristic information communication and relocation approach with load balancing. It is an adaptive data traffic control method. The main theme behind it is to segregate the traffic of network links and micro base stations for maintaining traffic. As it has more traffic in the symmetric wireless network [33].

V. CONCLUSION

The way encryption works, it affects network performance. As a result, the appropriate encryption technique must be deployed. A balance between the need to ensure data security and high-quality performance must be maintained. Data encryption has an overhead effect on TCP. To safeguard the data, encryption converts it from text to ciphertext. Even so, it increases the size of the data. Additionally, it has been shown that the transfer time of encrypted data typically stays incredibly long. Information is typically so secure thanks to cryptographic algorithms that they enable senders to transmit it over unreliable channels. However, complex cryptographic processes demand a lot of technological resources and result in significant network overhead and expenses.

AES provides unmatched network performance since it uses the fewest rounds possible, resulting in a short deployment time while maintaining randomness. As a result, it takes longer to authenticate. As a result, AES offers significantly shorter deployment times and less complexity while maintaining randomness and security against malicious activity. Because of encryption, it becomes challenging to assess network traffic and performance. Encryption affects the effectiveness and operation of network flow analysers. Using tool information, technical resources use communicated data to improve network visibility. The significant length of encryption keys allows for significant changes in power and time consumption if the key lengths differ. Security, quality, latency, and encryption rate can all be used to evaluate an encryption's performance.

Additionally, encryption's efficiency can be increased by utilising parallel processing and accelerating it using both software and hardware. Finding the ideal balance between time, size, quality, and protection is necessary. You must also adjust variables like level, mode, packet size, or key size. The scale, efficiency, and result can be improved with the use of several cores, threads, or nodes. Additionally, using dedicated chipsets, GPUs, or frameworks can greatly improve network performance while preserving compatibility and dependability. End-to-end delivery time to end users is shortened via CDN. Additionally, it eliminates load content providers that enable protection against threats such as Distributed Denial of Service.

Encrypting data at the database level is the proper method to safeguard sensitive data and ensure network efficiency. The technologies associated with packaged database encryption are quite effective at protecting sensitive data. Cellular communication systems will undergo a revolution thanks to symmetric wireless networks. Given the tiny assets of micro base stations in wireless networks, it is important to consider how to improve resource allocation, data transmission rate, time, and other abilities. A suitable heuristic information, communication and relocation strategy with load balancing is required. This method of data traffic control is adaptive. The primary idea is to preserve traffic by separating network connections and micro base station traffic due to the symmetric wireless network's increased load. As a result, encryption significantly reduces network performance, which must be fixed. Furthermore, more efficient data encryption techniques can be explored through further research.

REFERENCES

[1]. C. Eromosele, “Evaluating the Impact of AES-256 Encryption on Network Performance: An Analysis of Transfer Time, Latency and Throughput,” IJSRMT, vol. 4, no. 1, 2025.

[2]. D. &. Z. W. Xu, “Application of Data Encryption Technology in Network Information Security Sharing,” Security and Communication Networks, 2022.

[3]. IBM, “What is encryption?,” [Online]. Available: http://ibm.com/think/topics/encryption.

[4]. J. Lackey, “Understanding Factors That Impact Encryption Performance,” 2017. [Online]. Available: https://www.keysight.com/blogs/tech/traf-gen/2020/05/22/understanding-factors-that-impact-encryption-performance.

[5]. M. R. M. &. L. W. Ramachandra, “An Efficient and Secure Big Data Storage in Cloud Environment by Using Triple Data Encryption Standard,” Big Data Cogn. Comput., vol. 6, no. 4, p. 101, 2022.

[6]. J. Vandersteen, “The Disadvantages of Encrypted Files,” 2016. [Online]. Available: https://itstillworks.com/disadvantages-encrypted-files-2597.html.

[7]. H. Sakr, “Evaluation of Encryption Algorithms: A Comparative Approach over 6G Networks,” Nile Journal of Communication & Computer Science, vol. 8, 2024.

[8]. M. H. H. Baig, “A Comparative Analysis of AES, RSA, and 3DES Encryption Standards based on Speed and Performance,” Computer Security and Reliability, 2024.

[9]. Y. Y. N. &. Z. R. He, “Analysis of Data Encryption Algorithms for Telecommunication Network-Computer Network Communication

Security," Wireless Communications and Mobile Computing, 2021.
[10]. S. Orrin, "The Future of Data Encryption: What You Need to Know Now," 2021. [Online]. Available: https://fedtechmagazine.com/article/2021/07/future-data-encryption-what-you-need-know-now.
[11]. M. T. S. &. Q. M. Qureshi, "Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud," vol. 14, no. 4, p. 695, 2022.
[12]. M. Mock, "Industry Sectors That Need Data Encryption," 2022. [Online]. Available: https://www.kiteworks.com/cybersecurity-risk-management/industry-sectors-data-encryption/.
[13]. A. P. S. &. G. R. Mondal, "Cloud computing security issues & challenges: A review. In Proceedings of the 2020," in International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020.
[14]. M. Allan, "6 Types of Encryption That You Must Know About," 2023. [Online]. Available: https://www.goodcore.co.uk/blog/types-of-encryption/.
[15]. N. &. H. Z. Khanezaei, "A framework based on RSA and AES encryption algorithms for cloud computing services," in In Proceedings of the Systems, Process and Control (ICSPC), Kuala Lumpur, Malaysia, 2014.
[16]. A. Dhingra, "Encryption and Network Security: Striking a Balance Between Data Protection and Network Visibility," 2023. [Online]. Available: https://www.thefastmode.com/technology-solutions/30066-encryption-and-network-security-striking-a-balance-between-data-protection-and-network-visibility.
[17]. S. Pate, "Encryption as an enabler: the top 10 benefits," 2013. [Online]. Available: https://www.networkworld.com/article/2165740/encryption-as-an-enabler--the-top-10-benefits.html.
[18]. K. &. K. R. Manjunath, "A Robust Reversible Data Hiding Framework for Video Steganography Applications," International Journal of Advanced Computer Science and Applications, vol. 13, no. 3, 2022.
[19]. R. E. Ś. e. al, "The Latest Advances in Wireless Communication in Aviation," vol. 7, no. 1, 2022.
[20]. S. &. B. M. Abha, "Cloud computing security using AES algorithm," Int. J. Comput. Appl., vol. 67, p. 19–23, 2013.
[21]. Z. A. A. &. K. H. Kartit, "Applying encryption algorithm for data security in cloud storage.," Adv. Ubiquitous Netw. Lect. Notes Electr. Eng., vol. 366, p. 141–154, 2015.
[22]. S. H. V. &. K. S. Talasila, "Load Balancing Techniques for Efficient Traffic Management in Cloud Environment," International Journal of Electrical and Computer Engineering (IJECE), vol. 6, no. 3, pp. 963-973, 2016.
[23]. A. &. G. A. George, "The Evolution of Content Delivery Network: How it Enhances Video Services, Streaming, Games, e-commerce, and Advertising," International Journal of Advanced Research in Electrical Electronics and Instrumentation Engineering, vol. 0, no. 7, pp. 10435 - 10442, 2021.
[24]. K. Swarooprani, "An Study of Research Methodology," International Journal of Scientific Research in Science Engineering and Technology, 2022.
[25]. M. &. R. H. Petticrew, Systematic Reviews in the Social Sciences: A Practical Guide, 2006.
[26]. A. A. C.-R. O. W. &. L. F. Carrera-Rivera, "How-to conduct a systematic literature review: A quick guide for computer science research," MethodsX, vol. 9, p. 101895, 2022.
[27]. K. K. R. &. K. J. Khan, "Five steps to conducting a systematic review," JRSM, vol. 96, no. 3, p. 118–121, 2003.
[28]. D. Salama, "Improving the security of cloud computing by building new hybrid cryptography algorithms," Int. J. Electron. Inf. Eng., vol. 8, p. 40–48, 2018.
[29]. G. Liu, "The Application of Data Encryption Technology in Computer Network Communication Security," Mobile Information Systems, 2022.
[30]. C. Eromosele, "Evaluating the Impact of AES-256 Encryption on Network Performance: An Analysis of Transfer Time, Latency and Throughput," International Journal of Scientific Research and Modern Technology (IJSRMT), vol. 4, no. 1, 2025.
[31]. P. T. M. &. I. M. Nayak, "Computer Network Security Strategy Based on Data Encryption Technology," IJARSCT, vol. 4, no. 2, 2024.
[32]. M. S., M. &. T. S. Bilal, "Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud," vol. 14, no. 4, p. 695, 2022.
[33]. D. P. J. &. W. Y. Bian, "Study of Encrypted Transmission of Private Data During Network Communication: Performance Comparison of Advanced Encryption Standard and Data Encryption Standard Algorithms," Journal of Cyber Security and Mobility, vol. 11, no. 5, p. 713–726, 2022.
[34]. F. Chen, "Data Transmission Security in Computer Network Communication," Journal of Physics: Conference Series, Volume, The 2nd International Conference on Computing and Data, p. 1881, 2021.
[35]. P. F. J. &. M. N. Dimou, "ENCRYPTED TRAFFIC ANALYSIS," ENISA, 2019.
[36]. M. H. S. &. G. A. Tebaa, "Homomorphic encryption method applied to Cloud Computing," in In Proceedings of the 2012 National Days of Network Security and Systems, Marrakech, Morocco, 2012.
[37]. N. &. S. R. Murthy, "Security issues and challenges in cloud computing.," Int. Adv. Res. J. Sci. Eng. Technol., vol. 2, no. 12, 2015.
[38]. V. &. T. B. Naresh, "A study on data storage security issues in cloud computing," Procedia Comput. Sci., vol. 92, p. 128–135, 2016.
[39]. M. &. K. M. Khader, "Assessing the Effectiveness of Masking and Encryption in Safeguarding the

Identity of Social Media Publishers from Advanced Metadata Analysis," vol. 8, no. 6, p. 105, 2023.
[40]. R. &. S. K. Rao, "Data security challenges and its solutions in cloud computing.," 2015.
[41]. U. Mattsson, "Database Encryption - How to Balance Security with Performance," SSRN Electronic Journal, 2005.
[42]. O. O. A. &. O. A. Abolade, "Overhead effects of data encryption on TCP throughput across IPSEC secured network," Scientific African, vol. 13, 2021.
[43]. R. I. &. F. K. Gururaj, "A comprehensive survey on security in cloud computing," in Procedia Comput. Sci., 2017.
[44]. S. Y. W. &. G. E. Asare, "Evaluating the Impact of Cryptographic Algorithms on Network Performance," International Journal of Cloud Applications and Computing, vol. 12, no. 1, 2022.
[45]. W. A. S. &. G. E. Yaokumah, "Evaluating the Impact of Cryptographic Algorithms on Network Performance," International Journal of Cloud Applications and Computing, vol. 12, no. 1, pp. 1-15, 2022.
[46]. J. Kumawat, "Network Performance of different Encryption and Authentication Algorithm," Journal of Scientific and Engineering Research, vol. 2, no. 2, pp. 94-98, 2015.
[47]. Z. &. C. Kuang, "Research on smart city data encryption and communication efficiency improvement under federated learning framework," Egyptian Informatics Journal, vol. 24, no. 2, pp. 217-227, 2023.
[48]. A. F. A. &. M. H. Khalil, "Cloud computing security challenges in higher educational institutions—A survey.," Int. J. Comput. Appl., vol. 161, p. 22–29, 2017.
[49]. S. Hussain and U. S. &. U. M., "A Comprehensive Survey on Signcryption Security Mechanisms in Wireless Body Area Networks.," Sensors, p. 1072, 2022.
[50]. C. &. U. A. Ezeofor, "Analysis of Network Data Encryption & Decryption Techniques in Communication Systems," International Journal of Innovative Research in Science, vol. 3, no. 12, 2014.
[51]. M. K. A. &. J. A. Uddin, "Next-Generation Blockchain-Enabled Virtualized Cloud Security Solutions: Review and Open Challenges," Electronics, vol. 10, p. 2493, 2021.
[52]. A. S. C. Gomes, "Database Encryption for Balance Between Performance and Security," IBIMA Business Review, pp. 1-9, 2021.
[53]. A. P. &. A. R. Yanes, "Towards automated aquaponics: A review on monitoring, IoT, and smart systems," J. Clean. Prod., vol. 263, p. 121571, 2020.
[54]. S. A. &. R. G. Cui, "Multi-CDN: Towards Privacy in Content Delivery Networks," IEEETRANSACTIONSONDEPENDABLEANDSECURECOMPUTING, 2017.
[55]. J. B. H. &. W. H. Zhang, "When LLMs Meet Cybersecurity: A Systematic Literature Review," A Systematic Literature Review., 2024.
[56]. W. Zhang, "A Two-Level Cache for Distributed Information Retrieval in Search Engines," Recent Advances in Information Technology, 2013.