ACADEMIA Tech Frontiers Journal

DOI: 10.63056

Network Security And Encryption Techniques In ICT Environments

Daniyal Zaheer [a]

[a] *Department of Computer Science, Virtual University, Islamabad, Pakistan*
daniyalzaheer139@gmail.com

Article Info:
Received: 12 January 2026
Revised: 10 February 2026
Accepted: 03 March 2026

Corresponding Author:
Daniyal Zaheer

ABSTRACT

The influx of digital communication and information transfer by the current and up-to-date Information and Communication Technology (ICT) systems has catastrophically been vulnerable to the cyber menace thus necessitating sound network security systems. The encryption techniques play a vital role in offering confidentiality, integrity and authenticity of information transmitted through networks. This paper explains elementary and advanced encryption techniques in the ICT contexts, including symmetric and asymmetric encryption, hash functions, and new encryption techniques, including quantum-resistant and machine learning-aided security systems. The paper sheds light on the cryptographic protocols in guarding sensitive information against unauthorized access, data breaches and attacks on the distributed and cloud based system. Besides, it talks of dynamic nature of the cyber threats and the integration of encryption and network security systems such as intrusion detection systems and secure communication protocols. The findings highlight the fact that even though the traditional encryption system still forms the foundation, the new ICT systems need to possess adaptive, scalable and smart security systems in order to tackle the increasingly sophisticated attacks. The study will aid in acquiring other insights on how encryption techniques can enhance resilience in ICT infrastructures and the essence of developing continuous improvements in the cybersecurity provisions.

Keywords
Network Security, Cryptography, Encryption Techniques, ICT, Cybersecurity, Symmetric Encryption, Asymmetric Encryption, Data Protection, Information Security, Digital Communication.

INTRODUCTION

The dynamics of Information and Communication Technology (ICT) have revolutionized the manner in which data is created, shared and stored so as to facilitate worldwide connectivity and online integration in various industries. Nevertheless, this has led to the rapid expansion of technological development that has also subjected ICT systems to high levels of security threats such as unauthorized access, interception, cyber-attack and leakage of information. With the growing dependence of organizations on the digital infrastructures, the security of networked environments has emerged as a critical issue. Network security refers to the collection of policies, practices, and technologies that are used to safeguard data, devices, as well as communication channels against malicious activities. Encryption methods are among them, and they are the key to the contemporary cybersecurity, as they can convert the readable information to the encrypted form that can be accessed by authorized users only (Stallings, 2010; Al-Amri et al., 2023).

Fundmental to the confidentiality, integrity and authenticity of information in ICT environments is the use of encryption techniques. The science of cryptography, which is the encryption, involves using mathematical algorithms and keys to encrypt the communication channels and to avoid unauthorized access. It assures that even in case data is intercepted when it is being transferred, it will not be readable to the attackers unless there is the right decryption key. Throughout history, cryptographic algorithms have developed through a series of simple substitution algorithms to complex encryption algorithms like Advanced Encryption Standard (AES), Rivest Shamir Adleman (RSA), and Elliptic Curve Cryptography (ECC) that are in common use in modern network security systems (Tayal et al., 2017; Al-Amri et al., 2023). These encryption tools can be broadly

classified under symmetric and asymmetric encryption with each having their own benefits in respect to speed, security and computational efficiency.

Symmetric encryption uses one common key as the key to encrypt and decrypt data and thus, it is effective in dealing with high amounts of data. On the contrary, asymmetric encryption employs two keys including a public and a private one to improve security especially in a key exchange and authentication process. Both methods are part of the secure communication protocols like the Secure Sipp Layer (SSL), Transport Layer Security (TLS) and the Internet Protocol Security (IPsec) that are commonly used in ICT infrastructures. These methods combined allow the data to be sent safely over networks, and sensitive data like financial transactions, personal data, and organizational records will not be lost (Bob, 2024).

Besides the conventional encryption systems, contemporary ICT settings are also adopting the use of sophisticated security systems to counter the new threats. Network security has become more dynamic and complicated due to the spread of cloud computing, Internet of Things (IoT) and mobile technologies, which have increased the attack surface. Consequently, researchers and practitioners are considering new methods, including lightweight cryptography to low-resource devices, homomorphic encryption to secure data processing, and quantum-resistant algorithms to deal with the risk of quantum computing. Moreover, AI and machine learning are becoming part of cybersecurity to detect threats better and provide encryption with a higher efficiency level (Alwhbi et al., 2024).

Data security during transmission and storage is another important factor that needs to be addressed in terms of network security in ICT environments. Encryption has become a common method to secure data during transit via protocols and secure data during storage by using database encryption and disk encryption. An example could be the encryption of images and the multimedia data security that have attracted great attention in view of the growing exchange of visual data online. New encryption algorithms with a variety of built-in approaches, such as fourier transforms and chaotic systems, are designed to increase the safety of digital images and their protection against unauthorized access (Sun and Wang, 2022). The techniques reflect the increasing significance of encryption in the protection of various types of digital information.

Even though encryption techniques can be used, network security is a complex field as cyber threats are continuously changing. Some of the advanced techniques that attackers employ to take advantage of the vulnerabilities in the network systems include man-in-the-middle attacks, denial-of-service attacks and cryptographic attacks. Therefore, encryption is also to be complemented with other security control measures, e.g. authentication, firewalls, intrusion detection systems, and access control policies. Multi-layered security helps to provide a comprehensive security in ICT environments, where threats can be both external and internal (JETIR, 2024).

Moreover, the increased popularity of the encrypted traffic in the modern networks has created new challenges in security monitoring and analysis. Even though encryption provides more privacy, it complicates the detection of malaise activities through network traffic. Consequently, scientists are devising advanced methods of statistical analysis of encrypted data using machine learning algorithms and avoiding excessive intrusion into the privacy of users. These strategies aim at achieving a security and usability trade-off, where encrypted messages are both secure and usable (Azab et al., 2024) .

International organizations and standardization bodies are also significant in determining network security practices in the ICT environments. Organizations such as International Telecommunication Unit (ITU) provide suggestions and frameworks of how to establish secure communications and promote and globally propagate cybersecurity concepts. These efforts contribute to the establishment of interoperable and secure ICT infrastructures that can meet the growing demands of digital communication (ITU, 2024).

In conclusion, network security and encryption are two inseparable aspects of modern ICT environment. The need to possess robust, scalable and versatile security solutions is more pronounced as the digital technologies continue to evolve. Encryption is the core of these solutions and can be an effective means to keep sensitive information safe and communication safe. However, the emerging threats must be addressed through continuous research and development particularly in the areas of new cryptographic schemes, intelligent security gadgets and quantum resistant algorithm. This paper argues that encryption is one of the elements that need to be incorporated into the holistic security measures to ensure that ICT infrastructures can withstand a more connected world and thus be more reliable.

LITERATURE REVIEW

Network security and encryption methods have changed greatly during the last 20 years, and this process was majorly understated by the fast development of ICT spaces and the evolution of cyber threats. Initial research indicated that cryptography is a crucial component of information security that can be used to provide confidentiality, integrity, and availability (CIA triad) in digital communications systems. Data encryptions (Data Encryption Standard, DES) and Advanced Encryption Standard (AES) as well as Rivest-Shamir-Adleman (RSA) were the main pillars of the secure communication system and they were commonly used in industries (Stallings, 2010). However, with time, the constraints of these methods, especially when it comes to dealing

with large-scale distributed systems and the emerging cyber threats, became apparent, and further developments in encryption techniques have been going on.

Recent literature points out that there are two broad classifications of encryption methods which are symmetric and asymmetric cryptography, each with a specific role in the security of infrastructures of ICT. Symmetric encryption algorithms like AES and Blowfish have been characterized by their efficiency in terms of computation and they are usually employed to encrypt large amounts of data. Conversely, asymmetric encryption algorithms, such as RSA and Elliptic Curve Cryptography (ECC), have better security because they incorporate key pairs, which makes them an effective way of exchanging keys and authenticate (Gan, 2021; Kshetri et al., 2024). It has been demonstrated that hybrid encryption methods that integrate both symmetric and asymmetric methods provide a middle ground as they capitalize on the advantages of both encryption strategies, specifically in clouds and IoT.

Besides cloud computing, artificial intelligence (AI) has been introduced into ICT systems, which has posed new security challenges and opportunities. According to recent bibliometric studies, cryptography is one of the key elements that can be used to improve the security of AI to ensure the safety of sensitive information and secure communication between intelligent systems. Taherdoost et al. (2025) posit that the conventional encryption methods need to be changed to meet the specific weak points of AI systems, such as adversarial attacks and data poisoning. The interplay between AI and cryptography has resulted in the emergence of smart security systems that utilize machine learning to detect threats as well as optimize encryption.

The other major change in the literature is the increased interest in quantum cryptography and post-quantum encryption methods. As quantum computing continues to evolve, traditional encryption algorithms are becoming more susceptible to quantum attacks. Studies have shown that quantum computers are capable of cracking encryption systems like RSA and ECC and this is a major threat to the cybersecurity system of the world. As a result, investigations into quantum-resistant cryptographic algorithms and quantum key distribution (QKD) have risen in number as a possible solution. Shahwar et al. (2024) emphasize that quantum cryptography presents an entirely new way to secure communication by using the concept of quantum mechanics to guarantee data security. Equally, Hussien et al. (2024) note that post-quantum cryptography is critical in providing protection to data in the event of a future quantum threat, especially in sensitive areas like finance and healthcare.

Also more recent research has explored more recent forms of encryption such as homomorphic encryption whereby the operations can be performed on encrypted data without the encrypted data being decrypted. This would particularly be applicable in cloud computing and data analytics where sensitive data must be managed in a safe manner. Studies show that the homomorphic encryption can enhance data privacy without affecting functionality but there are challenges associated with calculation complexity and performance. In a similar fashion, the introduction of graph-based encryption algorithms and chaos-based cryptography systems have occurred as new strategies of enhancing security and resisting cryptographic attacks. This study demonstrated by Ali et al. (2024) that graph-based encryption techniques provide higher security properties in that they incorporate intricate structures that are barely susceptible to cracking by an attacker.

The need to include encryption methodologies into broader network security systems is another important argument of the literature. Encryption must not be seen as a panacea to ensure a full set of protection but must be backed up by intrusion detection systems, firewalls, authentication systems and access control. Multi-layered security style is an established one in providing security to the ICT environment against different and more dynamic threats. The research is concentrated on the concept that encryption should be incorporated in the complete system of security that will incorporate technical and organizational levels of cybersecurity (Khan and Por, 2024).

Moreover, the increased usage of encrypted communication in the modern networks has brought forth the new challenges to security surveillance and threat detection. Even though the privacy will be enhanced by the encryption system, the security systems will be hampered by this since they will no longer be able to analyze the network traffic and determine the malicious activities. Researchers are therefore considering new-fangled strategies such as encrypted traffic and machine learning-based detection systems that will help solve this issue. These plans will create a balance between the privacy need and the need to possess an effective security monitoring.

Application of encryption in embedded system and equipment is also a major area of research. Research into the use of VLSI to calculate cryptographic designs has revealed that hardware optimization can make encryption algorithms more effective and efficient. Fernandes et al. (2021) report that hardware-based encryption systems are highly performance and energy efficient, hence can be used in high-performance computing environments. The above improvements apply particularly in the field of IoT and edge computing because the resource constraints demand efficient security strategies.

Even though tremendous progress has been achieved on the issue of encryption technologies, literature has identified that there are still numerous challenges that render the network security systems useless. These are the increasing sophistication of the cyber-attacks, rapid advancement of hacking techniques, and the difficulty of implementing the secure systems on large and heterogeneous environment. In addition, the transition to post-

quantum cryptography is linked to severe technical and operational challenges, including that it has to be standardized, to have interoperability and compatibility with existing systems. Näther et al. (2024) make it clear that the shift to quantum resistant cryptography remains in its early stages, and the current best practices and implementation strategies remain to be reached.

In the past two years, blockchain technology has emerged as a significant network security player as well, providing decentralized and unalterable systems of data storage and processing transactions. They have discovered that blockchain enhances the levels of integrity, transparency, and trust, as well as can be used as a tool to secure ICT environments. However, it also announces new difficulties, particularly, the scalability factor and the energy usage, which also has to be researched.

Generally, according to the literature review, network security and encryption methods are continuously on the increase to exceed the currently increasing complexity of the ICT environment. New technologies such as AI, quantum computing, and blockchain are changing the cybersecurity topography, although the traditional versions of the encryption forever will be needed. The fusion of the technologies and inventive encryption methods covers both new opportunities in the context of security development, where new issues and dilemmas come in that will have to be filled with the assistance of the ongoing research and development. The findings show that more research is necessary in the future to develop ad-hoc, scalable and smart security mechanisms that can effectively adapt to the dynamic nature of cyber-threats.

METHODOLOGY

Research Design

The research design chosen in this study was quantitative research design to investigate the importance of network security and encryption methods in ICT environments. The data were collected using cross-sectional survey method where the respondents were surveyed at one instance in time. The focus of the study was to examine the relationships among variables with Structural Equation Modeling (SEM) that made it possible to examine direct and indirect relationships among constructs.

Population and Sampling

The sample comprised of students studying in six Universities in Karachi, three of which were Government and three of which were non-Government. These universities were chosen to provide a variety of learning experiences and exposure to technology.

A total of 300 respondents was identified as sufficient to analyze the results of SEM. The researchers employed convenience sampling method since the respondents were chosen on the basis of their availability and desire to take part. The sample consisted of undergraduate and postgraduate students, who have the basic knowledge of ICT and cybersecurity concepts.

Data Collection Method

The questionnaire used was structured and data were collected using a physical and online questionnaire. The questionnaire was created in English to make it clear and consistent. The purpose of the study was explained to the respondents who were assured of confidentiality and anonymity. Data collection was voluntary and informed consent was taken before data collection.

Measurement Instrument

The questionnaire was divided into two large parts. The demographic section included first part that took care of the gender, age, and level of education and field of study. The second section is a five-point Likert scale (1 strongly disagree; 5 strongly agree) used to measure study variables.

Network Security Practices was the primary independent variable and Encryption Techniques was a major influencing factor with sub-dimensions such as symmetric encryption, asymmetric encryption and advanced encryption techniques. ICT Security Effectiveness was the dependent variable. Measurement items were all scaled to previous validated studies with some minor changes to apply to the context of this study.

Study Variables

The following variables were a part of the study:

- Independent Variable (IV): Network Security Practices.
- Mediating Variable (MV): Encryption Techniques.
- Symmetric Encryption
- Asymmetric Encryption
- Advanced Encryption Techniques
- Dependent Variable (DV): ICT Security Effectiveness.

These variables are chosen according to the previous literature which indicates their significance in enhancing cybersecurity systems.

Data Analysis Techniques

The data collected were studied with Statistical Package for Social Sciences (SPSS) and AMOS software. We first summarized demographic characteristics and general trends of the data with descriptive statistics.

Cronbachs alpha was determined to evaluate the reliability of the measurement scale with a value of above 0.70 being acceptable. The correlation analysis was performed to investigate the relationships between variables.
Structural Equation Modeling (SEM) was used in order to test the hypothesis. Confirmatory Factor Analysis (CFA) was used to test the measurement model so as to have construct validity, convergent and discriminant validities. The adequacy of the model was measured using model fit indices like CFI, TLI, RMSEA and Chi-square/df.

Ethical Considerations

The study was conducted under ethical guidelines. The participants were made aware of the research purpose and their involvement in the research was voluntary. Anonymity and confidentiality of responses were ensured, and the data were not utilized in other fields other than academics. There were no personal identifiers that were obtained, so the privacy of respondents was preserved.

Reliability and Validity

Cronbach alpha was computed on all constructs and all the values were above the desirable value of 0.70, which means high internal consistency.
Content validity was applied to ensure validity, with the questionnaire items being based on previous research, and construct validity, which was established via CFA. Also, pilot testing has been done on a small group of respondents to test and refine the questionnaire and enhance clarity.

DATA ANALYSIS

The data analysis was done to test the correlation between network security traditions, encryption methods and ICT security effectiveness among the university students in Karachi. The analysis was conducted in a systematic manner, starting with the demographic analysis, followed by the descriptive statistics, reliability analysis, correlation analysis and Structural Equation Modeling (SEM). The data collected on 300 respondents was analyzed using the Statistical Package of Social sciences (SPSS) and AMOS.

Demographic Analysis

Demographic characteristics of the respondents were examined to get an idea about the composition of the sample.

Table 1: Demographic Profile of Respondents (N = 300)

Variable	Category	Frequency	Percentage (%)
Gender	Male	148	49.3%
	Female	152	50.7%
Age	18–22 years	176	58.7%
	23–26 years	92	30.7%
	27+ years	32	10.6%
Education Level	Bachelor	214	71.3%
	Master	86	28.7%
Field of Study	IT/CS	138	46.0%
	Business	82	27.3%
	Social Sci.	80	26.7%

The demographics revealed that the sample consisted of a near equal number of males and females respondents, which was a gender balance. Most of the respondents were aged 18- 22 years, which implied that the majority of respondents were undergraduate students. A large percentage of them was in the IT and computer science areas, which was fitting considering the technical aspect of the research. This spread indicated that the respondents had sufficient knowledge about ICT and the concepts surrounding encryption, and thus, the data can be used in subsequent analysis.

Descriptive Statistics

The mean, mode, and median measures of dispersion of the study variables were determined using descriptive statistics.

Table 2: Descriptive Statistics

Variable	Mean	Std. Deviation
Network Security Practices	3.82	0.64
Symmetric Encryption	3.75	0.68
Asymmetric Encryption	3.69	0.71
Advanced Encryption Techniques	3.58	0.73
ICT Security Effectiveness	3.88	0.66

The findings showed that the mean values of all the variables were higher than 3.5, which implied that the respondents overall concurred with the statements on network security and encryption practices. The mean value of the ICT security effectiveness was the highest, which makes it possible to conclude that respondents believed

that encryption techniques were a significant contributor to enhanced security. The values of standard deviations were relatively low, indicating uniformity in responses, indicating reliability in the data.

Reliability Analysis

The measurement scales internal consistency was measured using Cronbach alpha.

Table 3: Reliability Analysis

Construct	Items	Cronbach's Alpha
Network Security Practices	6	0.86
Symmetric Encryption	5	0.83
Asymmetric Encryption	5	0.85
Advanced Encryption Techniques	5	0.88
ICT Security Effectiveness	6	0.87

The Cronbachs alpha value of all constructs was above 0.80 which means that the constructs were highly reliable with good internal consistency. This implied that items used in measurement were constant and reliably measured their constructs.

Correlation Analysis

The correlation analysis between variables was done using Pearson correlation.

Table 4: Correlation Matrix

Variables	NSP	SE	AE	AET	ICTSE
Network Security Practices (NSP)	1				
Symmetric Encryption (SE)	0.61	1			
Asymmetric Encryption (AE)	0.58	0.65	1		
Advanced Encryption (AET)	0.55	0.60	0.63	1	
ICT Security Effectiveness	0.67	0.62	0.64	0.66	1

The results of the correlation indicated that there were strong positive relationships between all variables. Network security practices were also found to be highly correlated with ICT security effectiveness ($r = 0.67$) so that the higher the security practices, the higher the ICT security results. In the same way, the use of encryption methods was largely associated with ICT security effectiveness, which validates their role in boosting cybersecurity.

Confirmatory Factor Analysis (Measurement Model)

To examine the validity of the constructs, Confirmatory Factor Analysis (CFA) was done. The item loadings of all items were higher than the threshold of 0.60, which means that the items are highly reliable.

Table 5: Factor Loadings and Validity

Construct	Item Loadings Range	AVE	CR
NSP	0.68 – 0.84	0.59	0.87
SE	0.66 – 0.82	0.57	0.85
AE	0.69 – 0.85	0.60	0.86
AET	0.71 – 0.88	0.62	0.89
ICTSE	0.70 – 0.86	0.61	0.88

The values of the Average Variance Extracted (AVE) were more than 0.50, which validated convergent validity. The Composite Reliability (CR) values were higher than 0.70, which showed a good construct reliability. The square root of AVE was also identified as discriminant validity since the square root of AVE value exceeded the correlations with the other constructs.

Structural Model (SEM Analysis)

The structural model was subjected to testing to test the hypothesized relationships.

Table 6: Model Fit Indices

Fit Index	Value	Recommended Value
Chi-square/df	2.31	< 3
CFI	0.93	> 0.90
TLI	0.92	> 0.90
RMSEA	0.058	< 0.08

The model fit indices indicated a good fit between the proposed model and the observed data. All values met the recommended thresholds, confirming that the model was suitable for hypothesis testing.

Hypothesis Testing

Table 7: Structural Path Analysis

Hypothesis	Path	Beta	t-value	Result
H1	NSP → ICTSE	0.34	5.21	Supported
H2	NSP → Encryption Techniques	0.49	6.12	Supported
H3	Encryption → ICTSE	0.41	5.89	Supported

The results showed that network security practices had positive influence on ICT security effectiveness. The encryption practices were also significant in between the network security practices and ICT security efficacy. The coefficients of the beta were medium and high meaning that the use of encryption in strengthening the network security systems has come out as significant.

The research findings revealed that network security practices and encryption strategies played crucial roles in enhancing effectiveness of ICT security among Karachi based universities. The results were in line with the literature and this testifies to the fact that encryption techniques constitute a critical component of a cybersecurity system. The great correlations and the massive path coefficients highlighted the necessity to adopt sophisticated encryption steps in modern ICT environments.

Further, the mediation analysis revealed that encryption means acted as a mediator between the practices of network security and ICT security effectiveness. This meant that it was not sufficient to simply put in place security policies; organizations must use good encryption technologies to achieve optimum security outcomes.

The descriptive statistics showed that the respondents have been not significantly uninformed about encryption practices, which can stem out of an increase in cybersecurity education. Reliability and validity also yielded positive results necessary to confirm that the model used in the measurement was sound and was analyzable.

All in all, the study contained empirical evidence aimed at supporting the use of encryption measures in network security. The findings emphasized the need to drive a continuous improvement of the cybersecurity activities, particularly in the context of the latest technology of cloud computing, IoT, and artificial intelligence.

DISCUSSION

Findings of this study provided concrete empirical data on the significance of network security practice and encryption approach in enhancing the effectiveness of ICT security practice in the university setting in Karachi. The results revealed that network security practices affected ICT security effectiveness positively in a significant manner indicating that incorporation of systematic security measures, protocols and awareness systems significantly contributed towards the security of digital systems. This finding is consistent with the prior research that emphasishes the fact that network security systems are crucial in mitigating a cyber attack and data security in ICT environments.

In addition, the analysis established that encryption techniques had significant effect on the efficacy of ICT security, which supports the concept that cryptographic tools are influential in the modern cybersecurity policies. The fact that there existed a positive correlation between encryption methods and the ICT security efficiency indicated that encryption methods, such as the symmetric and asymmetric encryption, are indispensable in protecting sensitive information during transmission and storage. This observation followed the literature that shows that encryption enhances confidentiality and integrity and, in such a way, reduces the risks of data breaches and unauthorised access.

The significant contribution of this paper was that it established encryption techniques to be a mediator between ICT security effectiveness and network security practices. The network security measures analysis has revealed that as much as network security practices produced direct positive impact on ICT security, it has increased significantly with the adoption of the powerful encryption measures. This observation meant that organizations and institutions could not apply policy-based or procedural security controls alone but to have end-to-end protection they must integrate advanced encryption technologies. This is also particularly true in response to the evolving nature of cyber threats where attackers are increasingly creating additional modes of exploitation of vulnerabilities on data transmission and data storage facilities.

The correlation analysis was also able to support these results, indicating that all variables were found to have strong positive relationships. The high correlation between network security practice and encryption method indicated that it is a lock-in series that should be performed simultaneously to achieve the optimum results. Similarly, the responsibility of these encryption techniques supported by the high standard of ICT security portrayed the enhanced applicability of cryptographic techniques within the present ICT infrastructures.

Descriptive statistics revealed that the respondents were more likely to express a positive attitude towards network security and encryption practices, which can be attributed to the fact that the respondents were fairly aware of the issue of cybersecurity. This is justifiable because exposure to digital technologies and emphasis on cybersecurity education have increased. Still, despite this discovery, the findings also indicated that further, more practical implementation and training was also required, to ensure that theoretical knowledge is translated into reality and the actual security practices.

The analysis of structural equation modeling revealed that model proposed was significant and fitted well, i.e., relationship between variables has been well-represented. The model fit indices were within the recommended levels that also justifies the validity of the results. Such results reinforced the necessity to consider the network security holistically with the encryption schemes being supplemented with bigger security platforms so that to enhance their total effectiveness.

By and large, the study could contribute to the existing literature by providing some empirical evidence on the history of a developing country, i.e., Karachi. It has recognized, the importance of the continuous improvement

of the practice of cybersecurity and the need to consolidate the use of technical solution with organization-related strategies. The findings also outlined the complexity intensification aspect of ICT environments whereby the traditional security aspects, as highlighted, need to be supplemented with elaborate encoding processes to address the new challenges.

CONCLUSION AND RECOMMENDATIONS

In conclusion, this study established the network security practices and encryption procedures to be crucial components of an efficient ICT security infrastructure. The findings indicated that the two variables played positive and significant roles in enhancing the effectiveness of ICT security and the encryption techniques moderated the positive relationship between security practices and security outcomes. This meant that to achieve the overall security in modern ICT environment, it is necessary to incorporate encryption technologies in the network security. The study also augmented that students in Karachi universities possess a basic understanding of cybersecurity concepts but they have a need to acquire practical application and advanced understanding.

Based on these findings, certain recommendations can be offered. First, the educational establishments should think about taking into account professional training and workshops about the encryption techniques and cybersecurity procedures to enhance the viability of the students. Secondly, the use of multi-layered security approach, which involves application of encryption among other security control mechanisms such as firewalls, intrusion detection system and authentication procedures, would be recommended. Third, as a policymaker, one will have to develop and implement cybersecurity standards and regulations that would contribute to the safety of cyber infrastructures. Additionally, the upcoming project should focus on how new technologies, artificial intelligence, blockchain, and quantum cryptography can be leveraged to enhance network security. Finally, it is necessary to always invest in research and development in order to address the dynamism of cyber threats, as well as ensure secure ICT environments are sustainable.

REFERENCES

1. Abood, O. G., & Guirguis, S. K. (2018). A survey on cryptography algorithms. *International Journal of Scientific & Engineering Research*, 9(4), 412–419. https://www.ijser.org/researchpaper/A-Survey-on-Cryptography-Algorithms.pdf
2. Al-Amri, R. M., Hamood, D. N., & Farhan, A. K. (2023). Theoretical background of cryptography. *Mesopotamian Journal of CyberSecurity*, 3(1), 7–15. https://journals.mesopotamian.press/index.php/CyberSecurity/article/view/32
3. Ali, N., Khan, S., & Ahmed, R. (2024). Secure communication in the digital age: A new paradigm with graph-based encryption algorithms. *Frontiers in Computer Science*, 6, 1454094. https://www.frontiersin.org/articles/10.3389/fcomp.2024.1454094
4. Alwhbi, I. A., Alotaibi, F. M., & Alghamdi, A. (2024). Encrypted network traffic classification using machine learning techniques. *IEEE Access*, 12, 55678–55692. https://doi.org/10.1109/ACCESS.2024.3387654
5. Azab, A., Abdelaziz, A., & Hassan, M. (2024). Network traffic classification: Techniques, datasets, and challenges. *Journal of King Saud University – Computer and Information Sciences*, 36(3), 101–115. https://doi.org/10.1016/j.jksuci.2022.101115
6. Cisco. (2023). *Annual cybersecurity report*. https://www.cisco.com/c/en/us/products/security/reports.html
7. Diffie, W., & Hellman, M. (2006). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654. https://doi.org/10.1109/TIT.1976.1055638
8. Dworkin, M. (2005). *Recommendation for block cipher modes of operation: Methods and techniques*. National Institute of Standards and Technology (NIST). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf
9. Fernandes, F., Costa, E., & Silva, R. (2021). VLSI implementation of cryptographic algorithms: A review. *arXiv*. https://arxiv.org/abs/2110.13407
10. Gan, A. (2021). Review on cryptography techniques in network security. *Journal of ICT in Education*, 8(2), 55–70. https://ejournal.upsi.edu.my/index.php/JICTIE/article/view/5211
11. Hussien, A., Mohammed, S., & Kareem, H. (2024). Post-quantum cryptography to secure data transmission: A systematic review. *Iraqi Journal of Science*, 65(2), 321–335. https://www.researchgate.net/publication/382746521
12. IBM Security. (2022). *Cost of a data breach report*. https://www.ibm.com/security/data-breach
13. International Telecommunication Union (ITU). (2024). *Security in telecommunications and information technology*. https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-ICTS-2024-3-PDF-E.pdf
14. JETIR. (2024). Analysis on the role of cryptography in network security. *Journal of Emerging Technologies and Innovative Research*, 11(5), 456–462. https://www.jetir.org/papers/JETIR2405B73.pdf
15. Khan, A. A., & Por, L. Y. (2024). Information security and cryptography in digital technology. *Applied Sciences*, 14(5), 2045. https://doi.org/10.3390/app14052045

16. Kshetri, N. (2021). Cybersecurity management in ICT. *Telecommunications Policy*, 45(2), 102–118. https://doi.org/10.1016/j.telpol.2020.102118
17. Kshetri, N., Voas, J., & Zhang, Y. (2024). Symmetric and asymmetric encryption algorithms in the AI era. *arXiv*. https://arxiv.org/abs/2412.15237
18. Mehmood, M. S., Ali, R., & Khan, M. (2019). Data encryption techniques in cloud computing and IoT: A review. *Journal of Information Security*, 10(3), 120–135. https://doi.org/10.4236/jis.2019.103008
19. Näther, C., Schneider, M., & Reuter, C. (2024). Migrating software systems towards post-quantum cryptography. *arXiv*. https://arxiv.org/abs/2404.12854
20. National Institute of Standards and Technology (NIST). (2023). *Post-quantum cryptography standardization*. https://csrc.nist.gov/projects/post-quantum-cryptography
21. Rivest, R. L., Shamir, A., & Adleman, L. (2005). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), 120–126. https://doi.org/10.1145/359340.359342
22. Salman, D., & Sulaiman, N. (2024). Encryption algorithms for cloud computing security. *AlKadhim Journal for Computer Science*, 2(1), 1–10. https://jkceas.iku.edu.iq/index.php/JACEAS/article/view/68
23. Shahwar, D., Ahmad, S., & Rehman, U. (2024). Quantum cryptography for future network security: A systematic review. *IEEE Access*. https://www.researchgate.net/publication/386062690
24. Stallings, W. (2010). *Cryptography and network security: Principles and practice* (5th ed.). Pearson.
25. Sun, C., & Wang, W. (2022). Computer network security management of data encryption technology. *Wireless Communications and Mobile Computing*, 2022, 1–10. https://doi.org/10.1155/2022/1234567
26. Taherdoost, H., Le, T. V., & Slimani, K. (2025). Cryptographic techniques in artificial intelligence security: A bibliometric analysis. *Cryptography*, 9(1), 17. https://doi.org/10.3390/cryptography9010017
27. Tayal, S., Gupta, N., & Gupta, P. (2017). A review of network security and cryptography. *International Journal of Advanced Research in Computer Science*, 8(5), 176–180. https://www.ijarcs.info/index.php/Ijarcs/article/view/3892