

A COMPREHENSIVE REVIEW ON CYBER SECURITY

Naila Anwar^{*1}, Iram Shahzadi²

^{*1}Associate lecturer, University of Gujrat, Pakistan

²Associate Lecturer, University of Gujrat

^{*1}naila.anwwar@uog.edu.pk, ²iram.shahzadi@uog.edu.pk

DOI: <https://doi.org/10.5281/zenodo.22747977>

Keywords

Cyber threats, confidentiality, zero trust, Cryptography, data Encryption

Article History

Received: 01 June 2026

Accepted: 23 August 2026

Published: 14 September 2026

Copyright @Author

Corresponding Author: *

Naila Anwar

Abstract

Cybersecurity has emerged as a critical security concern in modern digital world due to the rapid growth of internet, internet-connected systems, rise in cloud computing, artificial intelligence and digital services. The increasing use of internet and information technology have resulted in an increase of cyber threats, malware, phishing, ransomware, data breaches, identity theft and denial of service attack which result in financial loss, privacy violations and operational disruption. The research reviews major cyber threats, their impact and commonly used strategies for mitigation of cyber threats. Cryptography and Zero trust are two strategies discussed to mitigate cyber threats. Cryptography is a method of protecting data from threats by using encryption. Cryptographic algorithms like AES, DSA, RSA have been discussed. Zero Trust is an approach to cybersecurity which follows the principle of "never trust, always verify," requiring continuous authentication and authorization of users and devices.

1. INTRODUCTION:

Internet has seen explosive growth over the past few decades, fundamentally transforming society, economy, culture and technology infrastructure. This digital revolution, often referred to as "cyber civilization," has revolutionized way we communicate, conduct business, and access information. The speed and scale of transformation have made Internet an indispensable source of information exchange and cornerstone for modern digital world [1]. People Cyber threats are widely spreading creating challenges for organizations and individuals for protection against cybercrimes. In today's world, increasing threats and severity of cyber-attacks have prompted the necessity to develop more dynamic and creative solutions for cybersecurity.

and organizations use technology for business-critical tasks like banking, health sectors, educational, human resources management and smart cities [5].

In a world where over 61 % of the industry and social interactions occur online, ensuring high-security standards to facilitate seamless, efficient and secure interactions is very important. The key concepts for high-security are data protection, privacy concerns, reliability, availability and cyber threats [5].

Cyber threats have several categories like cyberbullying, Identity theft, phishing, wireless Sensor Networks [7].

Cyber threats come in many forms with varying complexity and potential damage like malware, viruses, worms and ransomware which

compromise millions of devices worldwide. Phishing tricks people by sharing personal data while denial-of-Service (DoS) and Distributed

Denial-of-Service (DDoS) attacks overload networks causing service disruptions [15].

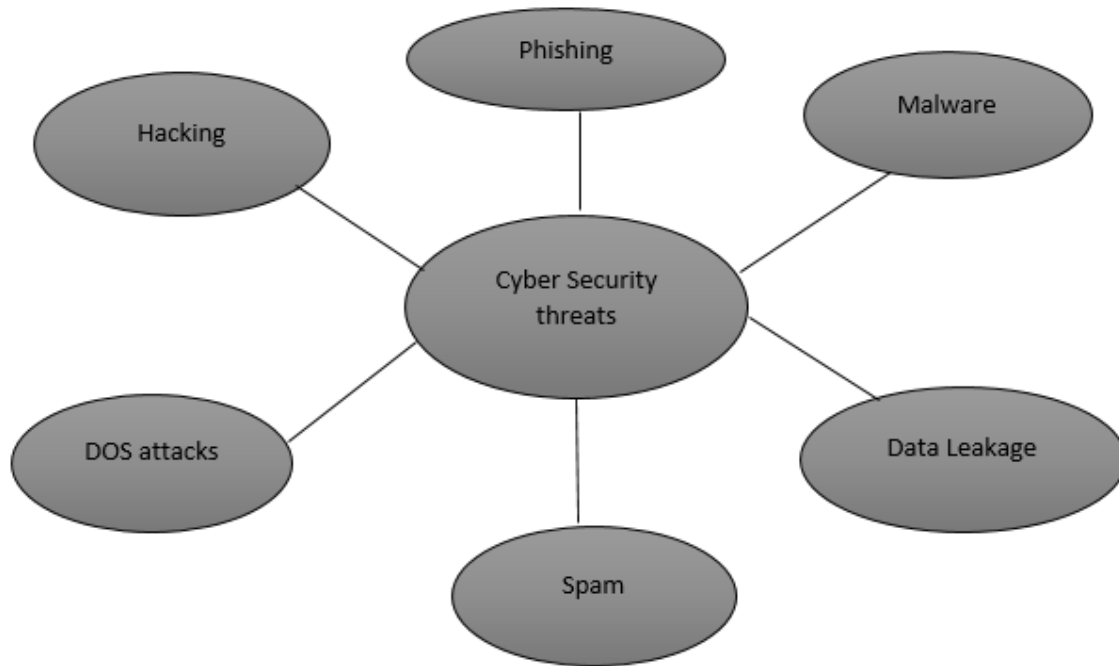


Figure 1: Cyber threats

In the digital age mitigating cyber risks is critical for organizations, governments and individuals. Proliferation of internet and digital devices have increased the volume and sophistication of cyber-attacks, making it important to apply advanced defense mechanisms. Cybercriminals seek out vulnerabilities in systems and networks to execute malicious activities ranging from stealing sensitive data to disrupting critical infrastructure. Zero-day attacks are among the most dangerous threats which exploit vulnerabilities, leaving defenders with no time to react before attack begins. So, securing information systems is a fundamental aspect of modern cybersecurity [15].

Rapid proliferation of Internet of Things (IoT) across smart homes, healthcare, industrial networks and smart cities have raised critical security concerns, particularly regarding device authentication. IoT devices are characterized by limited computational power, constrained memory and restricted energy which make

deployment of traditional cryptographic protocols infeasible, leading to better authentication as basic requirement. The central challenge in IoT authentication is achieving an appropriate balance between security strength and operational feasibility [14].

Authentication constitutes first line of defense in IoT security, ensuring only authorized devices and users can access network resources and communicate. Traditional authentication algorithms like RSA, Diffie-Hellman key exchange and certificate-based Public Key Infrastructure (PKI) offer strong security assurance but impose computational and energy constraints [14].

The core principles of data security are confidentiality, integrity and availability. Various sorts of cryptographic algorithms and digital signatures are used to maintain these principles. The strength of cryptographic algorithms to conventional attacks is ensured by computational difficulties and enormous amount of computation

to break them. In other words, the underlying principle of all cryptographic algorithms is that breaking them, even using the most powerful computers in the world, will take so long that the useful life of the encrypted data is over before the breaking [11].

According to International standard organization and international electrotechnical commission in ISO/IEC 27032 Cyber security is “Preservation of confidentiality, integrity and availability of information in cyber space” [12].

Cyber security means protecting Integrity, Confidentiality, and Availability (ICA) of

computing assets of an organization or another organization’s network. Due to increase of cyber threats, many researchers believe and urge organizations to educate new generations about concepts of cyber-security. Effective cyber security means using firewalls, encryption, multi-factor authentication and frequent software updates. Threat intelligence is a branch of cyber security which gathers and analyzes data about potential cyber threats to help organizations forecast and prevent attacks before they occur [2].

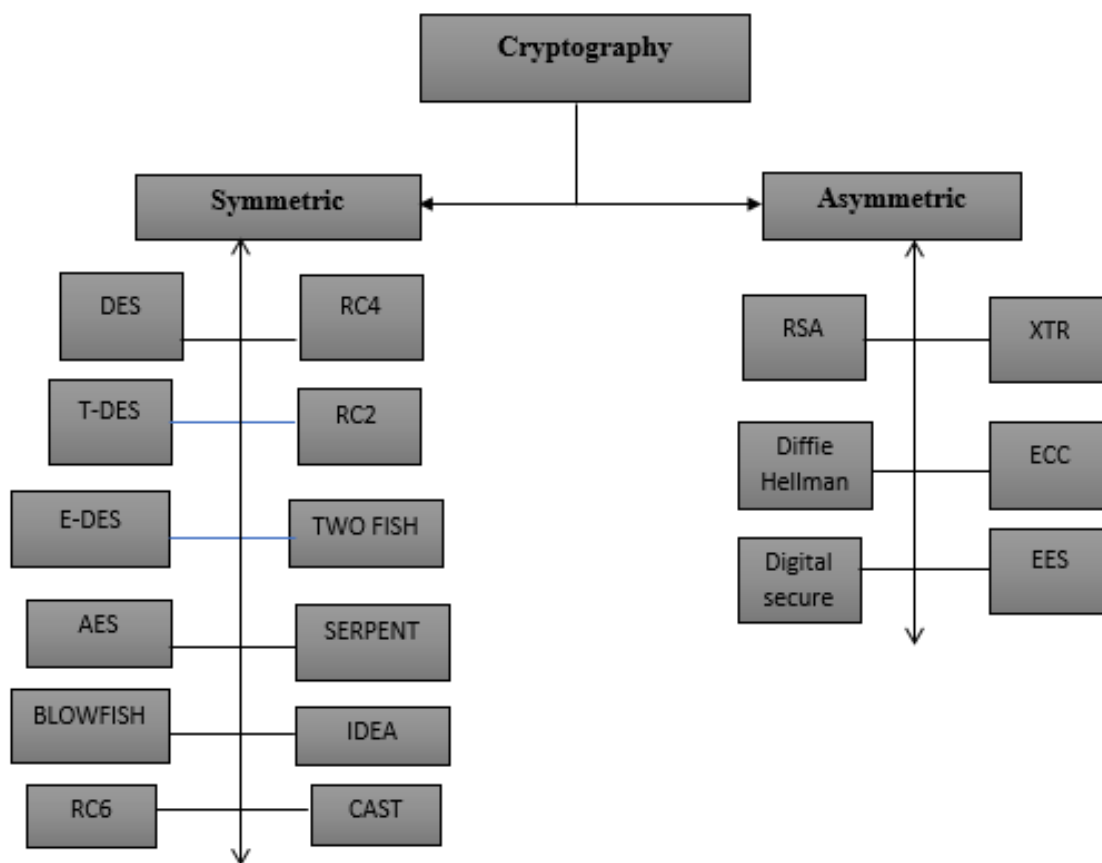


Figure 2: Types of cryptography

Data encoding is the process of protecting data by changing form of data to certain symbols by the use of codes. The process of encoding and decoding depends on a key which is called public

key or private key for Encryption and Decryption. Double cipher modes are tackled by a symmetric algorithm: block cipher and stream ciphers [13].

Cryptography falls in two categories Symmetric and Asymmetric.

The concept of Zero trust originated with the work of Jericho Forum, a security consortium, in 2003. However, the term was officially used by Forrester in 2010 and has since gained widespread recognition. In the zero-trust model, trust is not given blindly to entities seeking access to network

resources, even after undergoing initial authentication and authorization. This approach, which prioritizes data and identity awareness, views trust points as potential weaknesses. Key components of zero trust architecture are Policy Enforcement Point, Policy Administrator, Policy Engine and resource [17].

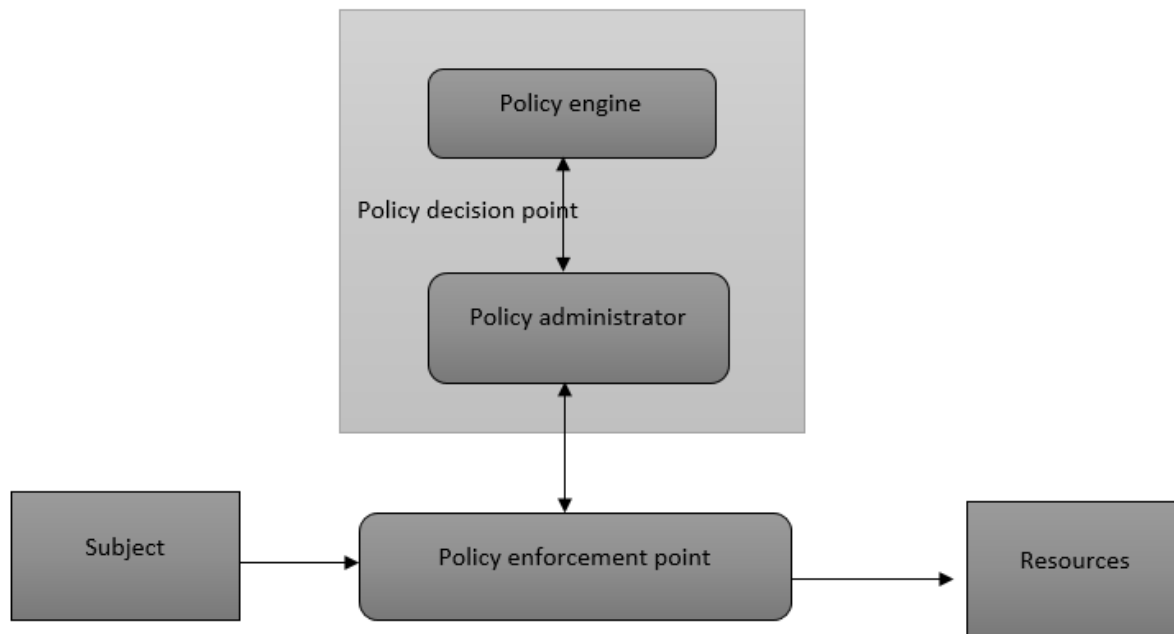


Figure 3: Zero trust architecture

2. Literature review:

Internet security has become very important after development of new technologies, services, and policies. Fighting cybercrime requires a comprehensive and safe approach. This means that cyber security does not occur with technical measures only. It is important that law enforcement agencies effectively investigate and prosecute cybercrime [5]. Making internet safer and protecting internet clients is critical. As digital landscape continues to expand and integrate with almost every aspect ensuring safe and secure online environment leads to positive effect for individuals, businesses and nations [5].

Cybersecurity measures are essential in safeguarding technology infrastructure, security, privacy, society and public safety. As a result, governments are investing significantly in cybersecurity, recognizing its vitalness in fighting threats and ensuring comprehensive protection of their citizens, infrastructure and future sustainability [7].

Data security, whether in transmission or storage, is important to all individuals and organizations. According to the report published by White House Office of Management and Budget on budget of the United States government for 2024, the allocated budget to Cybersecurity and Infrastructure Security Agency for 2024 was \$3.1

billion, representing a \$145 million increase as compared to previous year. The purpose of this Increasing frequency of zero-day attacks and data breaches have complicated cybersecurity. In the last ten years, hackers have stolen 14 billion data records. This is worrying and threatens digital security. Given this, intrusion detection is a crucial element of network security. Sophisticated systems excel in detecting and identifying abnormal network behavior, spanning from well-known attacks to new threats, undisclosed weaknesses, exploits and secret attack methods [9].

Zero trust security is based on the principle of “never trust, always verify, which means that no implicit trust is given to assets or user accounts just because of their physical or network location. A zero-trust architecture does not grant access to resources unless user/device, asset, or workload is confirmed through robust authentication and authorization process. The verification takes into account various factors and sources of information, like access privileges, device information and user behavior. Zero trust is also known as perimeter less security, as it shifts focus from network devices to assets [16].

Encryption is a cornerstone of data privacy and security, with its adoption driven by increasing security concerns and strict regulatory frameworks [1]. The rapid escalation of encrypted internet traffic has impacted network security, with recent data indicating that as of 2023, approximately 95% of web traffic is encrypted using HTTPS protocols [3]. In encrypted traffic, network security can be divided into two points Security and privacy. Security focuses on protecting network infrastructure from unauthorized access and attacks while privacy emphasizes protecting data confidentiality. Both aspects are vital for ensuring overall integrity of network communications [4].

Cryptography is the backbone of information security because it aids in safeguarding valuable data from unauthorized access. Since 1920s cryptography has been the most effective tool for secure communication. It transforms human-readable data called plaintext into ciphertext. Computer security includes CIA model, i.e., Confidentiality (authorized access), Integrity (data

increment was to make United States cyberspace more safe, resilient and defensible [11].

correctness and accuracy), and Availability (ready access for authorized entities) [5].

Key based cryptographic algorithms are divided into two categories: Symmetric- and asymmetric. In symmetric-key, there is one key for both encryption and decryption. Both sender and receiver have access to this key and must be kept confidential. One of the most well-known symmetric-key cryptographic algorithms is the Advanced Encryption Standard (AES) [11].

In the second category, each user possesses a pair of keys: Public key and private key. Public keys are non-confidential and shared with others, while private keys remain confidential and securely owned by owners. Data encrypted with the public key can be decrypted by corresponding private key. Conversely, a private key is used to create a digital signature, which can be verified using corresponding public key. That is why such algorithms are called asymmetric-key algorithms. The corresponding private and public keys are different but mathematically associated to each other. It is not possible to derive from the other [11].

2.1 Cyber security algorithms:

2.1.1 DES:

DES was once a primary symmetric-key algorithm published in 1977. Initially, DES worked with a 64-bit block size with a 56-bit key. DES works on equal block size and uses both confusion and diffusion in algorithm. In 1999, Electronic Frontier Foundation in collaboration with distributed.net broke the DES key in less than 24 hours using brute force attack. There are various other attacks (Biham and Shamir, 2012, Matsui, 1993, Biham, 1994, Biham and Biryukov, 1997) that can break the DES with less time complexity than brute force [7].

2.1.2 Advanced Encryption standard:

AES is an up-to-date ciphering strategy suggested by NIST to substitute DES in 2001. During encryption-decryption, the AES process encodes 10 rounds for 128-bit keys, 12 rounds for 192-bit

keys and 14 rounds to 256-bit keys for last encoded message [6]. AES allows 128-bit information length that can be split into 4 fundamental active blocks. Those parts are dealt with a line of bytes and combine a matrix of 4*4 named “the state”.

2.1.3 RSA algorithm:

RSA(Rivest-Shamir-Adleman) Algorithm is an asymmetric or public-key cryptography algorithm which means that it works on two different keys i.e., Public and Private Key. The Public Key is used for encryption and is known to everyone, while the Private Key is used for decryption and must be kept secret by receiver. RSA Algorithm is named after Ron Rivest, Adi Shamir and Leonard Adleman, who published the algorithm in 1977.

3.0 Discussion:

Human behavior has caused major issue in cyber security like social engineering, DOS attacks, data loss and phishing. High-profile breaches like 2020 Twitter hack demonstrate how attackers bypass advanced technological safeguards through human vulnerabilities. These incidents impose the need for adopting a human-centric approach like zero trust, encryption algorithms and AI trusted mechanisms for improving cyber security. Organizations need a combination of technical controls, security policies, employee awareness,

continuous monitoring, risk management and ongoing research for improving their internal security. As cyber threats continue to evolve, approaches like cryptography, Zero Trust and AI-assisted mechanisms can play an important role in protecting digital infrastructure.

4.0 Conclusion:

Cyber security is critically important in protecting information, ensuring trust and maintaining security for protection from unauthorized access, modification, and data interception. Algorithms like AES, RSA, ECC, and SHA provide essential security services like confidentiality, integrity, authentication and digital signatures. Symmetric algorithms offer efficient encryption for large amounts of data, while asymmetric algorithms support secure communication, key exchange and authentication. Zero trust model is a mechanism for ensuring security by giving limited access to users. Adopting Zero Trust security model can significantly strengthen cybersecurity by ensuring that every user and device is continuously verified before access is granted.

Ultimately, cybersecurity is not one-time solution but an ongoing process that requires continuous monitoring, vigilance, and collaboration. Strengthening cybersecurity practices today is crucial for building a safer and more resilient digital future.

REFERENCES:

- D. V. Trung, N. D. Minh, T. N. B. Hoang, and D. T. Son, “A comprehensive survey on cybersecurity threats and defense mechanisms in IoT networks,” *arXiv preprint arXiv:2511.xxxxx*, 2025
- M. Uddin, M. S. Irshad, I. A. Kandhro, F. Alanazi, F. Ahmed, M. Maaz, S. Hussain, and S. S. Ullah, “Generative AI revolution in cybersecurity: A comprehensive review of threat intelligence and operations,” *Artificial Intelligence Review*, vol. 58, no. 8, Art. no. 236, 2025, doi: 10.1007/s10462-025-11219-5
- A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, “On blockchain and its integration with IoT: Challenges and opportunities,” *Future Generation Computer Systems*, vol. 88, pp. 173–190, 2018, doi: 10.1016/j.future.2018.05.046
- A. Sharma and A. H. Lashkari, “A survey on encrypted network traffic: A comprehensive survey of identification/classification techniques, challenges, and future directions,” *Computer Networks*, vol. 257, Art. no. 110984, Feb. 2025, doi: 10.1016/j.comnet.2024.110984

- W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Security and Applications*, vol. 2, Art. no. 100031, 2024, doi: 10.1016/j.csa.2023.100031.
- M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol. 169, Art. no. 107094, 2020, doi: 10.1016/j.comnet.2019.107094.
- J. Kaur and K. R. Ramkumar, "The recent trends in cyber security: A review," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 8, Part B, pp. 5766–5781, Sep. 2022, doi: 10.1016/j.jksuci.2021.01.018.
- P. Dixit and S. Silakari, "Deep learning algorithms for cybersecurity applications: A technological and status review," *Computer Science Review*, vol. 39, Feb. 2021, Art. no. 100317, doi: 10.1016/j.cosrev.2020.100317.
- Y. Li, Z. Li, and M. Li, "A comprehensive survey on intrusion detection algorithms," *Computers and Electrical Engineering*, vol. 121, Art. no. 109863, Jan. 2025, doi: 10.1016/j.compeleceng.2024.109863.
- S. Chakraborty and V. Kumar, "A study and implementation of RSA cryptosystem," arXiv preprint arXiv:1506.04265 [cs.CR], Jun. 13, 2015.
- S. M. Hosseini and H. Pilaram, "A comprehensive review of post-quantum cryptography: Challenges and advances," *International Journal of Data and Network Science*, vol. 9, no. 2, pp. 267–288, 2025, doi: 10.5267/j.ijdns.2024.12.003.
- International Organization for Standardization and International Electrotechnical Commission, *Information technology–Security techniques–Guidelines for cybersecurity*, ISO/IEC 27032:2012, Geneva, Switzerland, 2012.
- O. G. Abood and S. K. Guirguis, "A survey on cryptography algorithms," *International Journal of Scientific and Research Publications*, vol. 8, no. 7, pp. 495–516, Jul. 2018, doi: 10.29322/IJSRP.8.7.2018.p7978.
- R. Alenzi, R. Aldoghan, and M. M. H. Rahman, "Lightweight Secure Authentication for IoT Devices: A Systematic Literature Review," *Journal of Cyber Security*, vol. 8, no. 1, pp. 373–396, 2026.
- S. A. Alansary, S. M. Ayyad, F. M. Talaat, et al., "Emerging AI threats in cybercrime: A review of zero-day attacks via machine, deep, and federated learning," *Knowledge and Information Systems*, vol. 67, pp. 10951–10987, 2025.
- C. Liu, R. Tan, Y. Wu, et al., "Dissecting zero trust: research landscape and its implementation in IoT," *Cybersecurity*, vol. 7, art. no. 20, 2024.
- L. Chunwen, T. Ru, W. Yang, F. Yun, J. Ze, Z. Fangjiao, L. Yuling, and L. Qixu, "Dissecting zero trust: Research landscape and its implementation in IoT," *Cybersecurity*, vol. 7, no. 1, Art. no. 20, 2024, doi: 10.1186/s42400-024-00212-0.