Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/



Research Paper Open Access

A Comparative Study Between Traditional And Modern Cyberattack Types and Cryptographic Defense Mechanisms

Dr. Audie Sabrie Abdalrazzak[1], Salam Mohsen AbdulKadhim[2]

[1] Prof. Department of Cybersecurity Technologies Engineering Islamic University of Babylon, Iraq. Emal: audiesabrie51@iu-babil.edu.iq
[2] Assist. Lect. Department of Computer Technical Engineering, Islamic University of Babylon, Email: Iraqsalam.mohsen@iu-babil.edu.iq

Abstract
The development of digital technologies is occurring at such a rapid pace that the complications and complexities of attacks are becoming more frequent. As a result, cybersecurity is becoming a major problem for information systems. This review gives a comparative analysis of the traditional cyber-attacks and modern cyber-attacks and the role of cryptography in security in detail. Malware and virus threats, phishing (social engineering) and fraud, network attacks, Denial-of-Service (DoS/DDoS), insider threats are some of the attacks that are dealt with here. Moreover, the study looks into the evolution of modern cyber threats such as Advanced Persistent Threats (APTs), Ransomware-as-a-Service (RaaS), zero-day exploits, AI-powered phishing, cloud security attacks, and IoT attacks and their growing sophistication, persistence, and ability to circumvent standard security mechanisms. Moreover, this review not only scrutinizes classical and symmetric techniques but also asymmetric and hybrid techniques with post-quantum cryptography to combat possible threats. In other words, it analyses a significant role of cryptography to secure digital assets. The characteristics of cyberattacks and cryptographic techniques are shown in tabular form for understanding of their strengths, limitations and applications. In addition, the document will explore best practices on cyber defense and promising future researches such as AI-based security, Zero Trust Architecture, cloud security and quantum-resistant crypto. The findings suggest the need for a combination of mean, advanced cryptographic techniques, smart threats detection systems, continuous monitoring and able security management for the confidentiality, integrity and availability of digital information as cyber threats become more sophisticated. This review is a comprehensive reference for researchers, practitioners, and cybersecurity professionals on the new cyber threats and the significance of cryptography in today's cybersecurity.

Keywords: Cybersecurity refers to defending computing and information technology devices from adversaries who published malicious code and engaged in technical attacks against electronic communications networks.

1. Introduction

The unprecedented advancement of digital technologies has redefined the modern world and enabled communications, cloud storage, artificial intelligence (AI), the internet of things (IoT) and one and all cyber-physical systems. The productivity as well as efficiency of businesses and access to information across several sectors like healthcare, finance, education, transport, manufacturing, and government department has improved due to these technological advances. The critical infrastructure increasingly relies on digital and technological systems for their functioning, but this trend has widened the cyber threat landscape with growing cyberattacks. Consequently, cyber-security has become the most serious challenge that organizations and governments encounter across the globe. To successfully contain it, constant augmentations of security strategies, technologies and regulatory measures are required [1]–[6].

Over the decades, cyberattacks have changed a lot in terms of their target, techniques, and sophisticated levels. Traditional cyber attacks like malicious programs, fishing, network attacks, denial of service (DoS/DDoS), and insider threats exploit known software vulnerabilities, weak authentication, system misconfigurations, and human errors of information systems. Despite ongoing enhancements to defensive technologies, these attacks continue to contribute to a significant proportion of data breaches, financial losses, and operational disruptions in both public and private organizations [4]–[16].

The quick progress of digital ecosystems also leads to a new generation of more intelligent, persistent, automated, and adaptable cyber threats. Sophisticated attack methods like Advanced Persistent Threats (APTs), Ransomware-as-a-Service (RaaS), zero-day exploits, AI phishing, cloud security attacks, and Internet of Things (IoT) attacks are very capable of defeating traditional security systems and maintain undetected in the system for a long time. In contrast to earlier attacks, today's attacks often combine multiple vectors; utilize artificial intelligence and machine learning; exploit cloud-based services and application programming interfaces (APIs); and affect critical infrastructures underpinning essential services. As a result, the organizations have to use advanced cybersecurity solutions that use intelligence, adaptability and proactivity to detect and mitigate old and new cyber threats [16]–[21].

According to a stakeholder expert, cryptography is one of the best cybersecurity technologies which protects digital information throughout its life cycle. Cryptographic methods provide protection of integrity, accessibility, authentication and non-refusal of communication and enable us to transfer information over an unprotected network. With the developments in classical ciphers to symmetric encryption, asymmetric encryption, hybrid cryptographic frameworks and post-quantum cryptographic algorithms, cryptography has strengthened the security of modern communication systems, cloud computing platforms, financial transactions, healthcare applications, and IoT environments. As cyber threats continue to evolve, improving cyber resilience more and more depends on embedding AI, Zero Trust Architecture and continuous monitoring with future cryptography. [1], [2], [22]–[24]

According to recent review studies dealing with cyber threats and attack techniques, on one side, and cryptographic methods and secure communication protocols on the other side [16], [17], [22], [24]. Most reviews talk about a specific subject such as malware, ransomware, IoT attacks, encryption algorithms, and post-quantum cryptography. Nonetheless, these studies discuss these issues separately, not providing a comparative analysis of the evolution of the cyberattack and the corresponding use of cryptography. Many studies focus on cybersecurity threat assessment and cryptographic techniques in isolation. However, a comparative study that can provide comparison between old and new cyber-attacks while emphasizing the role of cryptography will be very beneficial. Motivated by this gap, the present study offers the first integrated comparative study of traditional and modern cyberattacks to show how new cryptographic techniques can help protect our systems against cyber attacks.

This study primarily seeks to achieve the following.

1. Write an essay comparing and contrasting the nature of an ordinary cyberattack and a modern cyberattack.
2. The evolution of crypto system could be a classic symmetric asymmetric hybrid crypto system.
3. Study how cyber threats relate to their cryptographic countermeasures.
4. A comparative study of cyberattacks and cryptography techniques.
5. The Future of Cybersecurity: Best Practices and Solutions at the Present Time
6. The rest of the paper is arranged as follows. Section 2 will review traditional and modern cyberattacks by comparing and contrasting their features. Cryptography is an important area of the cybersecurity world, as section 3 of this interesting book mentions. It reviews classical, symmetric, asymmetric and hybrid encryption approaches.

It also offers comparative analyses, cybersecurity best practices, and future research proposals. In conclusion, the paper summarizes its findings and leading trends in the field of cybersecurity and cryptography research.

Research Contributions

Research Contributions

- An integrated comparative review of traditional and advanced cyberattacks, their evolution, nature and security issues
- By combining the analysis of cyberattacks with cryptographic art, it provides a comprehensive perspective on safeguarding cyber security.
- Explaining the strength, weakness and cyber security applications of symmetric, asymmetric, hybrid, hash and post quantum cryptographic techniques by comparing them with classical one.
- Finds underlying cybersecurity challenges as well as research avenues for the enhancement of the resilience and adaptiveness of cybersecurity.

2. Traditional Cybersecurity Attacks

Despite better technology defenses, conventional cyberattacks still threaten people and organizations. These attacks usually exploit software vulnerabilities, weak authentication, or human error 7 8.

2.1 Malware

Malware, also known as "malicious software" can disrupt computer operation, gather sensitive information, or gain access to computer systems and networks. The presence of this malware can jeopardize the confidentiality, integrity and availability of data.

- ❖ Viruses are malware programs that attach themselves to executable files and get spread on the computer by infecting other files.
- ❖ Worms are self-replicating malware programs that can propagate across a network without the need for user action.
- ❖ "It disguises as real software to fool the user into installation".
- ❖ Spyware: Recognizes information without user knowledge.
- ❖ Adware Shows Unwanted Advertisements.
- ❖ Rootkits gain privileged access to the operating system and hide malicious activities.
- ❖ Keystrokes are listened to by them so as to get the passwords, and financial data.
- ❖ A ransomware encrypts computer files and demands a ransom.

Of all these malwares, ransomware is probably one of the most damaging because it encrypts important information disrupting the overall functioning of an organization.

Illicit software can steal data, make financial losses, disrupt systems and steal identity. In order to protect against malware, organizations should use antivirus software, keep software updated, enforce strong authentication, maintain secure backups, and educate users on security.

2.2 Phishing

Phishing attacks occur when attackers use social engineering to trick a user into giving up his/her sensitive information like username, password, credit card number, etc. An entity is spoofing an email address or text message to trick you into doing something that compromises your security in a phishing attack.

Phishing began as an old-school social engineering attack, but it has become a huge threat because of artificial intelligence.

- ❖ Spear phishing targets specific individuals.
- ❖ Whaling: Targeting managers,
- ❖ Smishing refers to the practice of targeting mobile users with text messages.

Phishing can result in stolen credentials, financial fraud, malware installation, identity theft, and worse network infiltration.

Safeguarding your company needs combining tech measures like multi-factor authentication (MFA) and secure email gateways with multi-prong authentication and ongoing user awareness and cyber. [10], [11].

2.3 Network Attacks

Network Attacks are malicious attempt that executes inside a computer network. More precisely on a communication network, device or a data transmission channel. Cyber-attacks take place at any instance on the web in millions. These attacks highlight the poor security implementation in various domains. The Distributed Denial-of-Service (DDoS) attack, Man-in-the-Middle (MitM) attack, port scanning, packet injection, spoofing, and network intrusion attack is common. The challenge of sophisticated and zero-day attacks are diminishing the effectiveness of legacy signature detection mechanisms as the complexity of network traffic increases. In recent years, researchers are using deep learning techniques like CNNs and deep autoencoders for enhancing the efficacy and accuracy of network intrusion detection systems. Modern network security can benefit through the use of the intelligent systems that can automatically identify the abnormal traffic pattern and detect the known and zero-day attacks with a very high level of accuracy[12],[16],[17].

2.4 Denial-of-Service (DoS/DDoS)

Denial-of-Service (DoS) attacks stop a machine from functioning normally. Further, it stops communication links to a network. Moreover, it is overwhelming the target with unwanted traffic. Finally, they make the services useless for users. Another advanced type of attack is Distributed Denial-of-Service (DDoS). This attack uses compromised devices (botnets) to launch an attack at the same time. This is considerably harder to detect and stop.

The financial loss and service outages caused by these attacks can degrade the performance of the network and affect its reputation. This especially applies to cloud platfo Signature-based defense mechanisms alone are very hard to mitigate against DoS and DDoS as they are becoming bigger, more distributed and more automated.

The contemporary mitigation techniques that are used now include the use of an intelligent traffic analysis system, cloud-based mitigation services, artificial intelligence, rate limiting and much more. They will aid in the detection of malicious traffic during the Denial of Service attack while ensuring the services remain continuously available. Recent DDoS incidents show that these attacks have evolved to sophisticated ones and are targeted at different network layers, rather than just flooding them with bandwidth.

2.5 Insider Threats

Insider Threats is defined as the security risk that comes from individuals who have legitimate access to your organization's systems and data. These could be the employees, contractors, business partners, etc. Such threats may be [15].

- Intentional actions such as stealing sensitive data, abusing privileges, sabotaging systems.
- Accidental refers to any result caused by negligence, human error or violation of policy.

Since insiders possess authorized credentials and knowledge of organizational processes, their malicious activities mimic normal user behaviour and are often difficult to detect. Abuse of privilege, identity theft, and data leakage are frequent.

Recent techniques use deep learning along with the multi-head attention technique to analyze the user behaviour pattern to detect these attacks more efficiently than the previous approaches that used machine learning techniques.

To prevent insider threats, organizations should implement strict policies.

- The least privilege principle.
- Routine User Behaviour Tracking.
- Multi-Factor Authentication (MFA)
- Consistent Training for Security Awareness

3. Modern Cybersecurity Attacks

Cybersecurity attacks modern have increased in sophistication, adaptability, and persistence due to advances in cloud computing, artificial intelligence, the Internet of Things, and digital transformation. As compared to traditional attacks that invoke single simultaneous exploitation of vulnerability, modern attacks utilize multiple techniques for denial of detection, ensuring access and/ or causing maximum damage.

Types of common attack

- evolved threat.
- Malware Attack.
- AI-Powered Phishing.
- Exploits in zero days.
- Attacks on Supply Chain.
- attacks on the Cloud and API
- Cyber Assaults Subjected to Networked Devices

Malicious cyber threats attack critical infrastructure, government agencies, healthcare, financial institutions and enterprises that impact their data, service, finances and reputation.

The standard protection techniques such as signature-based antivirus, firewall, classic intrusion detection, etc. are mostly not enough. A multi-layered defense requires modern cyber security.

- Advanced crypto technology.
- Artificial Intelligence and Machine Learning
- Behavior analysis data.
- Intelligence surveillance.
- Zero Trust Framework
- Ongoing surveillance of your security.

This integrated approach effectively deters, detects, and responds through mitigation.

[16], [17].

3.1 Advanced Persistent Threats (APTs)

Advanced persistent threats (APT) are among the most deadly and powerful cyberattacks. APTs differ from most attacks in that they are not designed to disrupt or steal but rather to maintain covert access.

Target systems in order to steal intelligence and information from highly protected entities.

- Perform online spying activities.
- Appropriate intellectual property.
- Collect Strategic Information
- Disrupt widely used products.

APTs undergo a series of stages.

1. Research.
2. Preliminary agreement through phishing or zero-day attacks.
3. Privilege escalation
4. Lateral movement refers to traffic moving within a web or network.
5. persevering through trials
6. Hidden Information Theft

Attackers mimic the behavior of legitimate users and apply evasion techniques. This enables APTs to remain undetected for long periods. Consequently, they can inflict significant financial, operational, and reputational damage.

- ❖ Dealing with APTs needs a layered approach which includes.
- ❖ Top-notch encryption.
- ❖ Endpoint Detection and Response (EDR)
- ❖ Systems that Detect IntrusionThreat intelligence.
- ❖ Constant observation of network
- ❖ Neutralize Trust Strategy
- ❖ Detection of anomaly using artificial intelligence.

This all-encompassing strategy is useful to detect and monitor early APT activities [16].

3.2 Ransomware-as-a-Service (RaaS)

Ransomware-as-a-Service (RaaS) promotes ransomware cybercrime using subscription-based tactics similar to SaaS. In this model, developers of ransomware create and maintain the malicious software, while the affiliates lease or subscribe to launch attacks, splitting the ransom payments.

The RaaS module can arouse aspiration among cybercriminals, causing them to target government agencies, health care, financial institutions and private enterprises. Common attack methods include phishing emails, exploiting poor vulnerability management, and using stolen credentials. These attacks usually involve encrypting the data, as well as double-extortion by stealing information and threatening to release it publicly.

The growth of RaaS cryptocurrencies and darknet markets offer criminals easy-to-use tools to launch major cyberattacks.

Strong defenses consist of.

- ❖ Consistent physical backups.
- ❖ Prompt security renovations.
- ❖ Multi factor authentication
- ❖ Endpoint Detection and Response (EDR)
- ❖ Isolation of Networks.
- ❖ Ongoing security surveillance.
- ❖ Comprehensive training on user awareness.

3.3 Zero-Day Exploits

Zero-day Exploits are attacks that exploit a software or hardware vulnerability unknown to a vendor, so a patch is not available. Since there are no official patches or detection signatures available at the moment, these attacks are particularly dangerous and difficult to identify using conventional security tools. Attackers use zero-day exploits to[19].

1. Acquire illegal access
2. Carry out harmful code.
3. Increase Privileges
4. Use Ransomware.
5. Ensure Have Long-Term Persistence

These exploits occur in mature cyber-espionage campaigns, advanced persistent threats (APTs) and intrusions against crucial components, government agencies, financial institutions and enterprises. Recent intelligence indicates increasing targeting of enterprise technology including security devices, networking equipment and cloud services, indicating rising complexity of zero-day attacks. Recommended area of prevention includes spending and compiling intelligence on zero-day vulnerability types and usage. Analysis of previously patched zero-day exploits may also be useful in limiting new attacks. The focus on zero-day usage increases attack effectiveness approach.

- ❖ Regular software updates.
- ❖ Ongoing security flaw management.
- ❖ Detection of intrusion based on behavior.
- ❖ Danger Insights.
- ❖ Endpoint Detection and Response (EDR).
- ❖ Artificial intelligence has been used to detect unusual or strange activities.

3.4 AI-Driven Phishing

A new form of social engineering is a phishing scam where attackers use artificial intelligence (AI) and large language models (LLMs) to successfully send phishing messages.

Unlike conventional generic phishing emails, AI-enabled attacks scrutinize publicly available information and communication patterns and organizational hierarchy to produce messages that mimic legitimate entity communications closely. As more and more malware attack and succeed in their agenda of stealing credentials, business email compromise (BEC) through financial fraud, spreading financial fraud, detection continues to become tougher for the average internet user as well as traditional security solutions.

The phishing campaign automation, the realistic, error-free text generation, and the production of a deepfake voice or video for impersonation is also possible by AI [11][20].
Organizations must implement measures to combat threats.

- ❖ Sophisticated email protection systems
- ❖ Detection of phishing using Artificial Intelligence.
- ❖ Multi-factor authentication (MFA),
- ❖ Ongoing security awareness training.
- ❖ Behavioral analytics that identify anomalous communications.

These strategies deter AI-powered phishers from executing effective attacks.

3.5 Cloud Security Attacks

Attacks on Cloud Security targets vulnerabilities in the cloud infrastructure, applications, identity and access management (IAM), and storage. Understood by variation.

- ❖ Use of stolen credentials for access.
- ❖ Poorly Configured Cloud Storage
- ❖ APIs that are vulnerable.
- ❖ Hacking of official account
- ❖ Privilege escalation.
- ❖ Data breach.

Due to the shared responsibility model and variable and dispersed nature of cloud environments, attackers leverage configuration errors as well as weak authentication to gain access or move laterally crosswise services.
Consequences contain data leak, disruption of service, monetary loss and violation of regulation.
Organizations must implement to reduce these risks.

- Having a Strong Identity and Access Management
- Multi-factor authentication (MFA).
- The data will be encrypted when stored and transferred.
- Constantly ensure security monitoring.
- Ease of management.
- Periodic assessment of vulnerabilities.
- The tenets of Zero Trust security.

The security measures ensure reliability and accessibility of cloud systems and services.

3.6 Internet of Things (IoT) Attacks

The swiftly growing Internet of Things (IoT) is quickly expanding the cyberattack surface with billions of connected smart devices such as sensors, cameras, healthcare equipment, industrial control system devices, and home automation devices. Due to limited computational power, many IoT devices are poorly configured and come with outdated firmware, weak or no authentication mechanisms, default passwords, and insecure communication protocols. Due to these weaknesses, IoT devices make attractive targets for cybercriminals. A number of attacks are popular in the IoT world. These include DoS / DDoS attacks, Spoofing attacks, Malware and Botnet attacks, MitM attacks, and Credential-based attacks. Once hacked, IoT devices can be used for data theft, service disruption, or integrated into large botnets that execute widespread attacks. An optimal security for IoT environments includes strong authentication, encryption, regular firmware updates, network segmentation, intrusion detection systems, and security monitoring. Moreover, there is an increasing use of machine learning–based detection techniques to identify abnormal behaviour of devices to enhance the detection and prevention of IoT cyberattacks[21].

Table 1. Comparison Between Traditional and Modern Cyberattacks

Aspect	Traditional Cyberattacks	Modern Cyberattacks
Primary Objective	Disrupt systems, steal data, or gain unauthorized access.	Maintain persistent access, conduct cyber espionage, steal sensitive data, and cause large-scale disruption.
Attack Techniques	Viruses, worms, Trojans, phishing, DoS, packet sniffing, and insider attacks.	APTs, RaaS, AI-driven phishing, zero-day exploits, cloud attacks, API attacks, IoT attacks, and supply chain attacks.
Attack Complexity	Generally rely on known vulnerabilities and simple attack methods.	Employ multi-stage, adaptive, stealthy, and AI-assisted attack strategies.
Detection Difficulty	Easier to detect using signature-based antivirus and traditional IDS.	Difficult to detect due to encryption, polymorphism, fileless techniques, and AI-assisted evasion.
Attack Duration	Usually short-term and immediate.	Long-term, persistent, and capable of remaining hidden for months.
Target Scope	Individual computers, local networks, and small organizations.	Critical infrastructure, cloud platforms, IoT ecosystems, healthcare, finance, governments, and global enterprises.
Propagation Method	Email attachments, infected files, removable media, and local networks.	Cloud services, compromised identities, APIs, software supply chains, botnets, and AI-generated social engineering.
Authentication Exploitation	Weak passwords and user mistakes.	Identity theft, credential abuse, MFA bypass, privilege escalation, and identity-based attacks.
Typical Impact	Data corruption, malware infection, system crashes, and localized service disruption.	Massive data breaches, ransomware, operational shutdowns, financial losses, reputational damage, and national security risks.
Defense Mechanisms	Antivirus software, firewalls, software patching, and user awareness.	Zero Trust Architecture, AI/ML-based detection, EDR/XDR, threat intelligence, behavioral analytics, cloud security, encryption, and continuous monitoring.

4. Cryptography in Cybersecurity

It is a method to prevent the third parties from interfering with the users. It is the process to make sure that communications and products are secure. It can also be called the 2-step verification. It offers a host of vital security services like confidentiality, integrity, authentication and non-repudiation to users. As a result, it ensures secure communication over computer networks, cloud- computing platforms, monetary systems, and Internet of Things (IoT) environments. Cryptographic algorithms comprise symmetric-key, asymmetric-key, and hash-based techniques that support different security needs. However, the rapid advancement of quantum computing threatens to render public key cryptographic systems, like RSA and Elliptic Curve Cryptography (ECC), unsecure after some time as quantum computers may easily solve the mathematical problems behind them. In view of the above, researchers are working on the development of post-quantum cryptographic (PQC) algorithms including the lattice-based, hash-based, code-based, and multivariate cryptosystems for long-term quantum security. It is predicted that the implementation of quantum-resistant cryptography will be very important in protecting future digital communication systems and critical infrastructures against new cybersecurity risks.

4.1 Classical Cryptography

Classical cryptography is the first form of cryptography where the sender encrypts the data manually using a simple mathematical or linguistic technique. Classical cryptography aims to hide the content of the message by changing plain text to some cipher text by substitution or transposition method. In substitution ciphers, we replace each character in the plaintext with another character in accordance

with an established rule. Whereas, in transposition ciphers, we alter the position of the characters without changing the character itself. Famous examples, which have been widely used for military, diplomatic and governmental communications before the advent of modern digital encryption, include, Caesar cipher, Vigenere cipher and Playfair cipher. While they demonstrated the basic concepts of encryption and cryptanalysis, these methods offer little security due to their relatively small key space and vulnerability to frequency analysis and brute-force attacks. Although classical cryptography techniques have limited practicality today, they are still crucial for understanding the history and principles underlying modern cryptographic algorithms [1][22].

4.2 Symmetric Encryption

Symmetric encryption is one of the most commonly used techniques to protect digital information. A symmetric system is one that requires a single secret key for both encryption of the message at the sender side and decryption at the receiver side. Thus, the sender and the receiver need to securely share the same key before the commencement of the communication. On account of computational efficiency and quick processing speed, symmetric encryption is suitable for encrypting a large amount of data. For instance, it is used in cloud computing, database protection, file encryption, wireless communication, and VPNs. Modern symmetric encryption include Advanced Encryption Standard (AES), which is the current international standard, Data Encryption Standard (DES), 3DES, Blowfish. While symmetric encryption is performance efficient and provides good confidentiality, its major issue is key distribution and management in general large communication. As a result, symmetric encryption is frequently used with asymmetric cryptography to generate secure session keys to encrypt data efficiently [1], [22].

4.3 Asymmetric Encryption

Asymmetric encryption, also referred to as public key cryptography, is a cryptographic technique that involves the use of two keys that are mathematically related. A public key is used to encrypt a message, while a private key is necessary for decryption. As opposed to the symmetric encryption method, where the secret key is employed in both operations, the public key can be distributed openly in asymmetric encryption while the private key remain secret. This technique overcomes the problem of how to share secret keys securely, enabling communications to be on untrusted networks. The primary usage of asymmetric cryptography is for digital signatures, key exchange, authentication, Public Key Infrastructure (PKI), and secure communication protocols like Transport Layer Security (TLS) and Secure Sockets Layer (SSL). The asymmetric algorithms that are most commonly used are RSA, Elliptic Curve Cryptography (ECC), and ElGamal. Asymmetric encryption can scale better and securely manage keys than symmetric encryption, yet it is slower. Most up-to-date cybersecurity architectures use hybrid cryptography – that is the session key is exchanged and securely communicated through asymmetric encryption but the data is protected through symmetric encryption due to better processing. In addition, with the development of quantum computing, there have raised concerns as to the security of public-key algorithms, leading to efforts to develop post-quantum cryptographic (PQC) algorithms that can withstand quantum computer attacks [1]. [23][24].

4.4 Cryptographic Hash Functions

Cryptographic hash functions are one-way cryptographic algorithms which convert input data of fixed-size (message digest) from any size. Contrary to encryption, data hashing cannot be reversed to its original value from the hash that has been generated. Cryptographic hashes are chiefly used for checking data integrity, securely save passwords, supporting digital signatures, and message authentication. Modern-day hash algorithms like the SHA-256 and SHA-3 are collision and preimage-resistant. Further, they find usage in many applications today. On the flip side, older algorithms like MD5 and SHA-1 have been proven vulnerable to collision attacks and are deprecated for protecting critical systems [1], [22], [24].

Table 2. Comparison of Cryptographic Techniques

Cryptographic Technique	Key Characteristics	Advantages	Limitations	Common Applications
Classical Cryptography	Uses substitution and transposition methods with simple manual encryption techniques.	Easy to understand and implement; provides the foundation of modern cryptography.	Small key space; vulnerable to frequency analysis and brute-force attacks.	Historical communication systems, cryptography education, and algorithm demonstration.
Symmetric Encryption	Uses a single secret key for both encryption and decryption (e.g., AES, DES, 3DES, Blowfish).	High encryption speed, low computational cost, efficient for large datasets.	Secure key distribution and management remain major challenges.	File encryption, databases, cloud storage, VPNs, wireless networks, and disk encryption.
Asymmetric Encryption	Uses a public-private key pair (e.g., RSA, ECC, ElGamal).	Secure key exchange, digital signatures, authentication, and scalable key management.	Higher computational complexity and slower performance than symmetric encryption.	Secure web communication (TLS/SSL), Public Key Infrastructure (PKI), digital certificates, email security, and cryptocurrency.
Hash Functions	One-way mathematical functions that generate a fixed-length message digest (e.g., SHA-256, SHA-3).	Ensures data integrity, efficient verification, and secure password storage.	Does not provide encryption or confidentiality; vulnerable if weak hash algorithms are used.	Password hashing, digital signatures, blockchain, file integrity verification, and authentication.
Hybrid Cryptography	Combines symmetric and asymmetric encryption to exploit the strengths of both approaches.	High security with efficient performance; resolves the key distribution problem.	More complex implementation and key management than single-method systems.	HTTPS, secure cloud services, VPNs, secure messaging applications, and enterprise cybersecurity systems.
Post-Quantum Cryptography (PQC)	Designed to resist attacks from quantum computers using lattice-based, code-based, hash-based, or multivariate algorithms.	Provides long-term security against quantum attacks; supports future secure communications.	Higher computational overhead; standardization and deployment are still evolving.	Next-generation secure communications, government systems, financial services, IoT, and critical infrastructure.

5. Comparative Analysis of Cyberattacks

Over the past few decades, cyberattacks have grown more sophisticated in terms of execution and intent. Exploit of known software vulnerabilities, weak authentication, and human error, malware, phishing, network attack, Denial-of-Service (DoS/DDoS), or insider threat are cyberattacks that are traditional. Usually disable the service, obtain sensitive information or get access to the computer other than the owner. With simple attack patterns, many of these above mentioned threats can be detected and thwarted by conventional security solutions like firewalls, signature-based antivirus and intrusion detection systems (IDS) [1], [16].

On the other hand, modern cyberattacks have become more sophisticated. As new forms of attacks emerge, such as APTs (advanced persistent threats), RaaS (ransomware-as-a-service), AI-enabled phishing, zero-day exploits, cloud security attacks, and IoT attacks, we see the frequent convergence of attack techniques to evade security. Such attacks utilize elements of artificial intelligence (AI), automation, encrypted communications, complex technologies, evasion measures, and exploits to effect damage over an extended period of time. Furthermore, a significant assessment revealed a shift towards cloud services and digital transformation in Nigeria and globally, which is noteworthy in the evolution of cybercrime [15]. Modern cyber attacks are far more automated, scalable, and sophisticated than traditional attacks. Consequently, traditional defence mechanisms can no longer cope with today's cyber threats. Today's cybersecurity strategy consists of multi-layered security architecture which integrates advanced cryptography, artificial intelligence, machine learning, threat intelligence, Zero Trust Architecture, endpoint detection and response (EDR), and continuous security monitoring. Organizations can improve detection of threats, speed up incident response and improve resilience due to increasingly sophisticated cyberattacks [16], [17] .

Table 3. Comparative Analysis of Traditional and Modern Cyberattacks

Criterion	Traditional Cyberattacks	Modern Cyberattacks
Representative Attacks	Malware, phishing, network attacks, DoS/DDoS, insider threats	APTs, RaaS, zero-day exploits, AI-driven phishing, cloud attacks, IoT attacks
Primary Targets	Personal computers, local networks, databases	Cloud platforms, critical infrastructure, IoT ecosystems, APIs
Attack Methodology	Exploits known vulnerabilities and social engineering	Multi-stage attacks, AI-assisted techniques, zero-day exploits
Attack Complexity	Moderate	High
Persistence	Short-term	Long-term and stealthy
Automation	Limited	Extensive automation using AI and botnets
Detection Capability	Signature-based antivirus and IDS	AI-based detection, EDR/XDR, behavioral analytics
Impact	Localized disruption and data theft	Large-scale data breaches, ransomware, financial and operational losses
Defense Mechanisms	Firewalls, antivirus, patching	Zero Trust, MFA, AI-based security, advanced cryptography

5.1 Hybrid Cryptographic Framework

A hybrid cryptographic framework employs a combination of symmetric and asymmetric encryption that ensures security along with efficiency. This approach makes use of asymmetric cryptography for the secure exchange of a session key or to establish a secret session key to be used by the two communicating entities. Thereafter, symmetric encryption is used to encrypt the data which has a much faster processing speed and requires lower processing power. Consequently, this framework solves the main distribution problem of symmetric encryption without the performance cost of using asymmetric algorithms on large data. As a result, they became the backbone of many secure communication protocols, such as Transport Layer Security (TLS), Secure Sockets Layer (SSL), Virtual Private Network (VPN), secure email, cloud computing,

and electronic commerce. Recent developments have embedded even more AI, ML, and post-quantum cryptographic algorithms into hybrid architectures for enhanced threat detection, better key management, and improved resilience against quantum computing attacks.

Hybrid systems of cryptography may be able to meet the overall objective of confidentiality, integrity, authentication, scalability, and performance in different environments. [1], [23], [24].

5.2 Best Practices for Cyber Defense

To defend against cyber attacks, it is essential to adopt an integrated approach that combines technology, people and processes. As cyber attacks' sophistication and complexity rise, a single point of failure is no longer sufficient to be safe. Organizations should adopt a defense-in-depth approach that integrates preventive, detective, and responsive security controls for minimizing cyber risks and improving resiliency against threats.

To reduce the risk of unauthorized access, one of the best practices is implementing strong identity and access management (IAM) through multi-factor authentication (MFA), role-based access control and the principle of least privilege. Updating software regularly, assessing vulnerabilities and patching security threats are also effective methods for preventing the emergence of malware and zero-day exploits through already identified vulnerabilities. In addition, organizations should implement strong encryption to protect data at rest and in transit, as well as manage cryptographic keys securely.

Organizations can detect abnormal activity and take quick action on an incident through monitoring with SIEM platforms, EDR solutions, and IDS/IPS systems.

Artificial intelligence (AI) and machine learning (ML) offer cybersecurity solutions that help in improvement of threat detections using anomalous behaviour detection and predicting attacks to curb significantly damages.

The importance of employee awareness and cybersecurity training remains constant as human error continues to be among the leading causes of cyber-attacks successfully taking place especially phishing and so on. Regular use of security awareness, phishing simulation and incident response exercises enhance the security culture of organization. Finally, adopting new security frameworks (such as zero trust architecture), secure cloud security practices, regular data backups, network segmentation and comprehensive disaster recovery and business continuity plans greatly improves the resilience of the organization to modern and traditional cyber threats [16][1][24].

5.3 Future Research Directions

With the fast growing cyber threats and digital technologies, new challenges are emerging in cybersecurity research.

Future work needs to be done in order to create smart and adaptive defence mechanism against smart attacks. Such smart attacks will be targeted at cloud computing, Internet of Things (IoT) environment, artificial intelligence (AI) and critical infrastructure. Anticipated to be less reliable than traditional signature-based security devices, cyber-attacks will be more automated and sophisticated – which calls for new generation cybersecurity frameworks that include ML, DL, and real-time behavioral analytics.

Another key research avenue focuses on the innovation of post-quantum cryptography (PQC) to tackle issues regarding security in quantum computing. Because of these quantum computers' ability to break widely used public-key cryptographic algorithms, much effort is needed to design, analyse, and standardise quantum-proof encryption schemes to ensure the long-term confidentiality of data and secure communications. Future research is also recommended to explore efficient hybrid cryptographic frameworks of classical and post-quantum algorithms with acceptable overhead in cloud platforms, mobile devices and IoT systems.

There appear to be also several future research opportunities linked to greater use of ZTA, secure identity management and AI-assisted threat intelligence. Advanced security frameworks will contribute to cyber resilience by automatically analyzing, predicting, and responding to an attack in real-time to manage the situation. In addition, researchers specializing in cybersecurity, artificial intelligence, cloud computing services, and industries must work together with policymakers to devise cybersecurity solutions that are extensible and create secure, privacy-preserving, and sustainable solutions to tackle the ever-evolving threat landscape.

Conclusion

As cyberattacks grow in frequency, sophistication, and impact, cybersecurity is becoming an increasingly important part of digital infrastructures. This review analyzes the traditional and modern cyberattacks based on their characteristics, attack vectors as well as targets and impacts. Security threats such as malware, phishing, network attacks, Denial-of-Service (DoS/DDoS), and insider attacks remain traditional. The latest Advanced Persistent Threats (APTs), Ransomware-as-a-Service (RaaS), zero-day attacks, phishing powered by AI, attacks about cloud security and Internet of Things (IoT) attacks indicate the growing complexity of current cybersecurity threats.

The review also highlights the important role that cryptography plays in protecting the digital system. The theoretical basis of secure communication is classical cryptography. The practical symmetric, asymmetric and hybrid cryptographic systems for confidentiality, integrity, authentication and non-repudiation are modern information systems. Moreover, post-quantum cryptography development is promising to secure users against future attacks while providing an experience similar to today's security.

Modern cyberattacks are considerably different from pre-Internet attacks because they are more sophisticated, persistent, automated, and varied in target. Incorporating advanced cryptographic techniques, artificial intelligence and machine learning, Zero Trust Architecture, multi-factor authentication, constant security monitoring, and threat intelligence into an organization's cybersecurity strategy can augment cyber resilience.

With the ongoing acceleration of digital transformations across cloud computing, IoT, artificial intelligence and critical infrastructures, the field of cybersecurity research also needs to evolve to tackle these new challenges. The integration of smart defense systems, quantum resistant cryptographic layers, and flexible security systems will help secure future information systems (IS) and ensure confidentiality integral and availability of digital assets. The ongoing cooperation of researchers, cyber security professionals and policy makers in the industry will be crucial for developing innovative and sustainable cybersecurity solutions to tackle the changing cyber threats.

References

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed. Pearson, 2023.
[2] C. Paar and J. Pelzl, Understanding Cryptography, Springer, 2010.
[3] National Institute of Standards and Technology (NIST), Cybersecurity Framework (CSF) 2.0, Gaithersburg, MD, USA, 2024.
[4] Verizon, 2024 Data Breach Investigations Report (DBIR), 2024
[5] ENISA Threat Landscape, 2024.
[6] MITRE Corporation, MITRE ATT&CK Framework, 2024.
[7]R. Tahir, "A Study on Malware and Malware Detection Techniques," International Journal of Education and Management Engineering (IJEME), vol. 8, no. 2, pp. 20–30, Mar. 2018, doi:10.5815/ijeme.2018.02.03
[8] Symantec, Internet Security Threat Report, 2023.
[9] Cybersecurity and Infrastructure Security Agency (CISA), Ransomware Guide, 2023..
[10] C. Hadnagy, Social Engineering: The Science of Human Hacking, 2nd ed. Indianapolis, IN, USA: Wiley, 2018..
[11] S. K. Birthriya, P. Ahlawat, and A. K. Jain, "Detection and Prevention of Spear Phishing Attacks: A Comprehensive Survey," Computers & Security, vol. 151, 2025, Art. no. 104271.
[12] S. B. Selvakumar, M. Sivaanandh, K. Muneeswaran, and B. Lakshmanan, "Ensemble of Feature Augmented Convolutional Neural Network and Deep Autoencoder for Efficient Detection of Network Attacks," Scientific Reports, vol. 15, Art. no. 4267, Feb. 2025, doi: 10.1038/s41598-025-88243-6.
[13] M. A. Alnuaimi et al., "A comprehensive framework for detecting and mitigating Denial-of-Service attacks in modern networks," Array, vol. 29, 2025
[14] K. S. Alketbi and A. Mehmood, "A Comprehensive Survey of Explainable Artificial Intelligence Techniques for Malicious Insider Threat Detection," IEEE Access, vol. 13, pp. 109345–109390, 2025, doi: 10.1109/ACCESS.2025.3587114.

[15] T. Tian, C. Zhang, B. Jiang, H. Feng, and Z. Lu, "Insider Threat Detection for Specific Threat Scenarios," Cybersecurity, vol. 8, no. 1, Art. no. 17, 2025, doi: 10.1186/s42400-024-00321-w.
[16] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yılmaz, and E. Akın, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," Electronics, vol. 12, no. 6, Art. no. 1333, 2023, doi: 10.3390/electronics12061333.
[17] A. Shaheen, "Cybersecurity in the Modern Era: An Overview of Recent Trends," Journal of Engineering and Computational Intelligence Review (JECIR), vol. 1, no. 1, 2023.
[18] B. Wibowo, L. Hafiz, and T. Hidayat, "Unveiling the Cybercrime Ecosystem: Impact of Ransomware-as-a-Service (RaaS) in Indonesia," International Journal of Science Education and Cultural Studies, vol. 4, no. 1, pp. 11–21, Mar. 2025, doi: 10.58291/ijsecs.v4i1.320.
[19] N. Mohamed, H. Taherdoost, and M. Madanchian, "Comprehensive Review of Advanced Machine Learning Techniques for Detecting and Mitigating Zero-Day Exploits," EAI Endorsed Transactions on Scalable Information Systems, vol. 11, no. 6, 2024.
[20] C. S. Eze and L. Shamir, "Analysis and Prevention of AI-Based Phishing Email Attacks," Electronics, vol. 13, no. 10, Art. no. 1839, 2024, doi: 10.3390/electronics13101839.
[21] M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, H. Hamam, and H. Song, "The Rise of 'Internet of Things': Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks," Wireless Communications and Mobile Computing, vol. 2022, Art. ID 8669348, 2022, doi: 10.1155/2022/8669348.
[22] S. N. Tambe-Jagtap, "A Survey of Cryptographic Algorithms in Cybersecurity: From Classical Methods to Quantum-Resistant Solutions," SHIFRA, vol. 2023, pp. 43–52, 2023, doi: 10.70470/SHIFRA/2023/006.
[23] V. Hryshchuk, O. Korchenko, O. Yudin, V. Buriachok, Y. Khokhlachova, and V. Khoroshko, "Cryptographic Encoding in Modern Symmetric and Asymmetric Encryption," Procedia Computer Science, vol. 207, pp. 54–63, 2022, doi: 10.1016/j.procs.2022.09.037.
[24] A. Mehmood, A. Shafique, M. Alawida, and A. N. Khan, "Advances and Vulnerabilities in Modern Cryptographic Techniques: A Comprehensive Survey on Cybersecurity in the Domain of Machine/Deep Learning and Quantum Techniques," IEEE Access, vol. 12, pp. 26336–26374, 2024, doi: 10.1109/ACCESS.2024.3367232.