International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# A Review Study on Simplified Approach to Cyberattacks, Their Algorithms, Applications, and Challenges

**R. Shriya[1], P. Ramya[2]**

[1]Third year B.Tech, Department of Information Technology, Sri Krishna College of Technology, Kovaipudur, Coimbatore,
[2]Assistant Professor, Department of Computer Science and Engineering, Sona College of Technology, Salem

**Abstract**
The innovation of various technologies across domains tends to protect digital assets from cyber analytics, preventing data breaches and security attacks. For each domain, say for example defense, medical, business, e-commerce, personnel utilization, industries that include manufacturing, retail, transportation, etc., the emerging trends and technologies arise, and also demands crypto attackers have governance policies and standards. In the world, 61% of industry and social interaction depend on the internet, which requires high security standards to ensure ease of use, efficacy, privacy, reliability, availability, and cyber security. Cybersecurity prevents cybercrime and cyberattacks. Internet security is a part of the development of new technologies, services, and government policies. It needs an agency to safeguard those services. The review study states cyber attacks, detailed algorithms, possible solutions, and challenges.

**Keywords:** Cyber Security, Cyber Crime, Cyber Attack

## 1. INTRODUCTION

Cyber security plays a significant role in the modern digital world. Its innovation is not restricted to individuals, organizations, societies, industries, or government agencies. It has wider applications in healthcare, the military, the financial sector, the education domain, government agencies, human resource systems, smart cities, etc. As per research, over 60% of technical information security demands antivirus software, virtual private networks, firewalls, intrusion detection systems, vulnerability management, and data encryption in transit quoted by [271](Diptiben Ghelani,2022).The advancement in communication and information poses enormous security challenges that must be handled by stakeholders involved in it[3]. To address security challenges, educational awareness, ethical behavior, security campaigns, etc. are conducted. Security vulnerabilities are available that may lead to financial loss, reputation harm infrastructure fatalities, etc. is proposed by [23](Tanenbaum,2021). Artificial Intelligence(AI) and Machine Learning (ML) techniques are highly contributed in cyberattacks.AI automates certain tasks such as Intrusion Detection System, Malware Detection System, and Vulnerability Assessment.ML techniques serve as effective tools for various cyber attacks. It must guarantee confidentiality, integrity, availability, and reliability. Confidentiality ensures only sensitive

information is accessed by permissible users. Integrity ensures the data is protected from unauthorized access so that deleting, updating, and modifying the data can be prevented. Availability ensures the data, services, and computer system are provided whenever needed by authorized users. Here, reliability means computer systems and security tools perform consistently, oppose attack, and stay available without causing unexpected outages.


**Fig.1 CIA Triad**

## 2. Possible Cyber Attacks

These are the most common cyber attacks that prevail in the system where the hacker easily tricks legitimate users to obtain their credentials, sensitive information, credit card details, etc are listed by [1285](Yuchong Liu et al., 2021).

### 2.1 Phishing

Phishing is a cyber-attack that disguise the user by pretending email, message or website as legitimate one and make the user to provide confidential information such as passwords, account number etc.

### 2.2 Ransomware

Ransomware is malicious software that encrypts victim's file or system by holding the hostage until the victim make a payment by exchange of decrypt key.

### 2.3 Malware

Software that breaks or damage the system by means of virus, worms, Trojan horse

- **Virus**

A malicious type of software attached to clean files targeted to a system copies itself that spread the system or network when an infected file is executed.

- **Worms**

Unlike virus, Worms are standalone programs not requires host program the spread without any human intervention

- **Trojan Horse**

Trojan horse mimics as a safe and legitimate program that tricks the users to download and run it. Once, it get into the system either steal the data or damage the system.

### 2.3 Man_in_the_middle attack

In this type of attack, bad actor secretly listens and does changes the messages during the conversion of two parties. But the parties' legitimate sender and receiver are unaware of intermediate personnel who can steal password, credit card details etc.

### 2.4 Denial of Service

This type of cyber threat that floods unsolicited mails or messages to the targeted system to slow down its processes or crash it. The distributed denial of service targeted many computers and perform the same processes at the same time.

### 2.5 SQL Injection

A hacker enter malicious code as input into the websites and execute commands in the database allow steal private data, do change data and take control of the system.

### 2.6 Password Attack

It is the malicious attack in which hacker gain unauthorized attack to steal, guess or crack the legitimate user login credentials.

### 2.7 Spoofing

A hacker or a program disguises as a trusted source trick the people to share the sensitive data by clicking malicious link or granting unauthorized network access.

### 2.8 Insider Threat

The employee in the organization does the malicious activity by mistake or on purpose.

### 2.10 Zero day Attack

A Zero day attack is a cyberattack that they are unaware of security flaw in software or hardware. The creator of the software has zero days to resolve the problem. There is no authorized patch or defense when the attack happens.

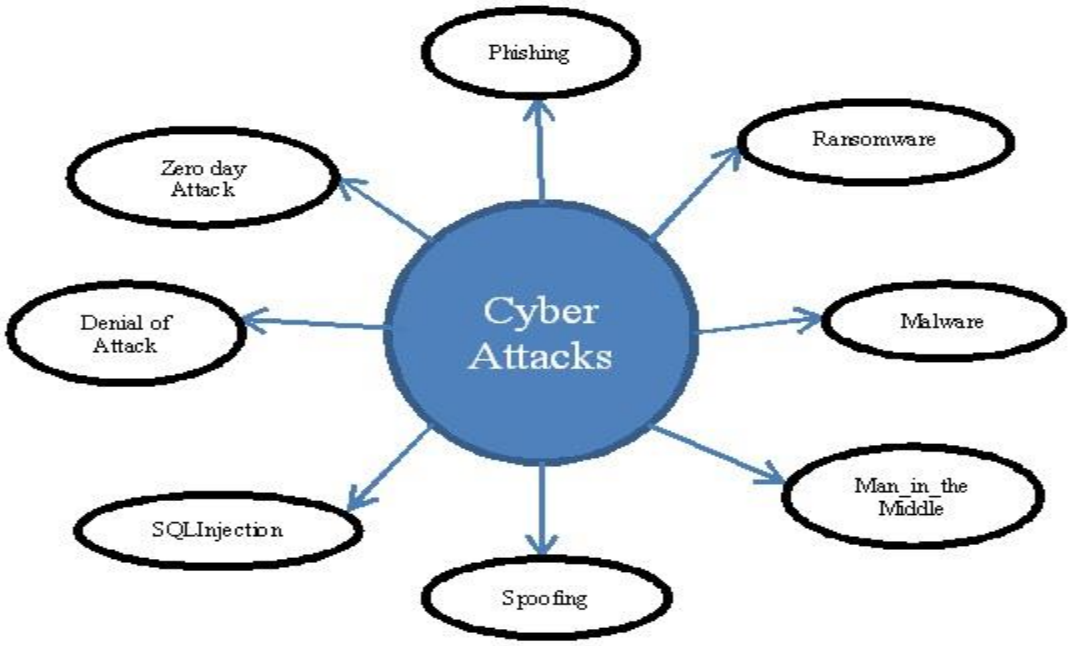


**Fig. 2 Most Common Cyber Attacks**

## 3. Cryptography

Cryptography is a process of transmitting data or information from source to destination across networks without any security breaches and cyber attacks. The transmitted data may be text image that have to be

disguised from others. Otherwise, adversaries can easily track and detect the data. For instance, Cryptography is a branch of study that is entirely dedicated to securing the data from identification, detection, and prevention by hackers. Cryptography is classified into two types based on key sizes and cryptography protocols. They are Symmetric Cryptography and Asymmetric Cryptography.

### 3.1 Symmetric cryptography

Symmetric cryptography uses a single key at both the sender and receiver ends. Whenever the sender wants to send a data, it encrypts the data that becomes ciphertext; nobody can reveal it. Only the recipient of the text message uses the private key to decrypt it. The process of transforming the encrypted text back to the original form is known as deciphering. Ciphering is the process of encrypting the text message. Deciphering is the reverse process of ciphering. AES, DES, Blowfish, TripleDES are examples of symmetric cryptography those are elaborated by [87](Sourabh Chandra et al.,2014).

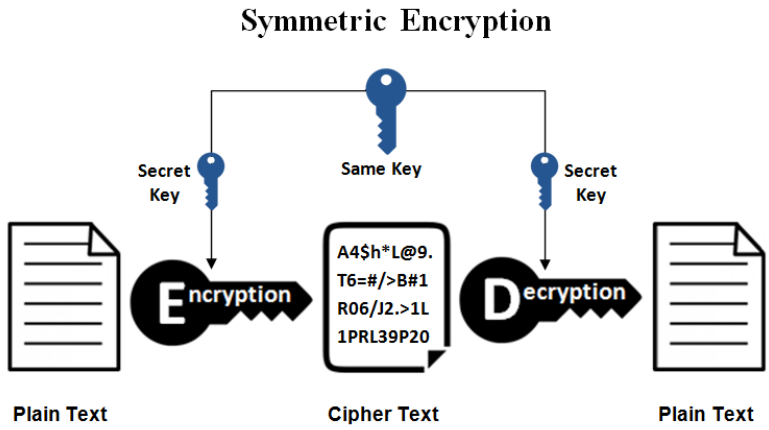


**Fig. 3 Symmetric Cryptography**

In symmetric key cryptography, both the sender and the recipient share the secret key with each other. For instance, the combination of messy text and plaintext is transmitted to the recipient. The recipient uses the secret key to uncover the unreadable format into a readable format. A single secret key is transferred between the source and destination.

There are two main types. They are,

Block Ciphers -A Block Cipher groups the data into fixed chunks and encrypts the chunks at a time using the AES.

Stream Ciphers -A Stream Cipher encrypts one bit or byte at a time using a continuous pseudo-random key stream.

There are different types of symmetric Key cryptography. They are,

#### 3.1.1 Advanced Encryption Standard (AES)

It was developed by NIST.It is faster and more robust than DES. Minimum block size is 128 bits which it first substitutes bytes, shifts rows then mixes columns and finally add the round key. It is widely used for encryption and decryption. It is used for transmitting sensitive information. Block size is 128 bits. The structure is a substitution-permutation network running 10 rounds. Key length may be 128,192,256 bits. It is used in Wi-Fi, messaging apps, and secure websites.

#### 3.1.2 Data Encryption Standard (DES)

The DES algorithm is deployed by IBM, whose block size is 64 bits. The encryption is divided into 16 stages comprising 8 S blocks. It shuffles bits first, and then proceeds with non-linear substitution.

Finally employ XOR operation to obtain the result. The sub key of the particular round is combined with the result using exclusive XOR. The decryption process is in reverse order of sub keys. The structure is a Feistel Cipher structure running through 16 rounds. Key length is 56 bits active key size. Block size is 64 bits. Insecure. Easily broken.

### 3.1.3 TripleDES

The triple DES key is an enhanced version of the DES key. It has an overall key length of 192 bits. It divides the key into 3 sub keys of 64 key bits in each. The first key is encrypted the data by first then it is decrypted by second sub key. Finally, the data is encrypted by the third sub key. It does not protect the data very securely.

### 3.1.4 Blowfish Algorithm

It is an efficient algorithm whose key length ranges from 32 bits to 448 bits. The block size is 64 bits. The procedure has two stages. They are at first, key expansion is performed. The P key has 18 sub keys, each of which is 32 bits. The Sbox has four 32 bits each of which 256 entries. The data encryption is done by the XOR operation. It applies to various domains whose keys are not changed[8].

## 3.2 Asymmetric Cryptography

In Asymmetric cryptography or Public key Cryptography, there exist key-pairs at both sides. Sender has both private key and public key, same way recipient has both private and public keys.

For instance, Uma wants to send a message to Shriya. She encrypts the message with the public key to make it unreadable before transferring the message to Shriya. On the recipient side, the message is decrypted with the private key to obtain the message. RSA, Diffie-Hellman, Elgammal and Elliptic curve Cryptography are public-key cryptography.

The security mechanism mainly focuses on three factors. They are Confidentiality, Data Integrity, and Availability. In Cryptography, the transfer of data from one individual, network, or organization to another must be reliable. The source has got acknowledgement that the message has reached the recipients. The confidentiality of data must be attainable. Only authenticated persons can view the message. The data integrity represents the correctness of the transmitted text message. The text message sent between the sender and receiver must be the same. It remains immutable during the data exchange process.

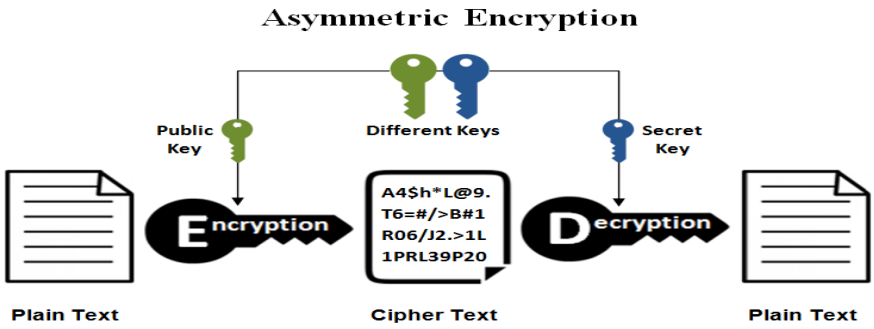


**Fig. 4 Asymmetric Cryptography**

In Asymmetric Key Cryptography, the key pairs are available to the sender and recipient parties[7]. Several Asymmetric key cryptography schemes are described as follows,

### 3.2.1 RSA Algorithm

RSA is named after Ron Rivest, Adi Shamir, and Leonard Adleman. It is widely used in key exchanges, Virtual Private Network, web browser, digital signature, chat application e-mails etc. in data

transmission. It highly relies on the practical difficulty of finding two prime numbers. It is slow as it directly encrypts data and shares keys in encryption and decryption. It is not easily breakable unless the key is shorter; hence, key enhancement is the target of crypto researchers.
There are two keys available in the RSA algorithm. They are,

**Key Pair Generation:**
Two keys that are uniquely generated using math behind.
**Public Key**: It is open to anyone who wants to send a message can use the key and encrypt the message.
**Private Key**: The private key unlocks the text message; only the owner who holds it can use it.

- **Working principle of RSA**

The underlying math behind the principle of RSA is prime factoring. It uses two keys It lock the data using public key and unlock the data using private keys.
It works as follows, provided with an example,
Step 1: Choose two large prime numbers (61, 53) randomly and name them p and q, also kept secret.
Step 2: Multiply $n= p \times q=61\times 53=3233$ (1)

- n is part of the public key and private key.
- The bit length of the key is 2048.
- Security completely relies on the factoring problem. It takes billions of years to reverse p and q if it only knows n.

Step 3: Compute Euler totient $\Phi(n)$

- $\Phi$: how many numbers smaller than n that share any common factors with n
- $\Phi(n) =(p-1) \times (q-1)$ (2)

The value is a trapdoor. It links mathematically private to public key and must be kept secret.

- $\Phi(n)=(61-1) \times (53-1)=3120$ (3)

Step 4: Choosing public expotent

- Select a small odd integer to serve as encryption exponent as it follows rules,
- It must be in the range $1<e< \Phi(n)$
- It must be co-prime to $\Phi(n)$ meaning GCD(e, $\Phi(n)$)=1 as they share no common factors except 1
- Its Purpose is for Scrambling in Real World Scenario**,** System does not guess. They almost use prime number $2^{16}+1=65537$ because it contains two 1s in binary make fast in computation and encrypt in safe.
- In the example. 17 is prime number that is not divisible 17 is coprime of 3120, Hence e=17

**Step 5: Compute private exponent**

- The decryption exponent, which acts mathematically inverse e,
- $d \times e \equiv 1 \mod (\Phi (n))$ (4)
- To find d, extended Euclidean algorithm is used by performing sequential long division of $\Phi$ (n) and e to find the Greatest Common Divisor (GCD) and then work backwards to isolate coefficients.
- $(d\times 17)(\mod 3120)=1$ yield d=2753 (5)

### 3.2.2 Diffie-Hellman Algorithm (Di-Hi)

It is a public key cryptography. Simple but easy to interpret as it is mathematically-oriented rather than lacking sender identity. Instead of directly encrypting the plain text, this algorithm chose shared secret

key between both parties on data transmission. Each one chose a secret key on their own and shared it in an insecure (key exchange) protocol. Then compute the public key with the shared key to reveal the data. It is susceptible to a Wireless Sensor Network (WSN) as it broadcasts the message to all nodes that are integrated with it. Key generation is easy to interpret in forward pass, but reverse back to the form is hard. Man-in-the-Middle is more common in this algorithm, as there is no authentication of either sender; the adversary in the middle can decrypt all traffic by manipulating the underlying math.

A step-wise approach of Diffie-Hellman algorithm is as follows,

It highly relies on modular exponentiation

- **Working principles of Di-Hi as follows,**

Step 1: Set up public key parameters. For instance, Uma and Shriya agree on two large numbers

- P=A large prime number (modulus); p=23
- g= A primitive root modulo p(base or generator) g=5

To find a primitive root modulo with an example as follows

- Calculate p =7; p -1=6
- Prime factors p are 2 and 3
- Test r=2,
  - Compute exponents (p-1) ÷ 2=3,
  - (p-1) ÷ 2=3 (6)
  - Check $2^3$ mod7=1 (7)

(since 1, not a primitive root)

- Test r=3
  - Check $3^3$ mod 7=2 ≠1 (8)
  - Check $3^2$ mod7 (9)

Hence a primitive root

Step 2: Generate Private keys

- Each party generate private key on their own randomly and never share with one another.
  - Uma chooses a private key a=4
  - Shriya chooses a private key b=3

Step 3: Compute and public key exchange.

- Each party generate public key using secret key later they exchanges both the keys with one another across the network during data communication.
- Uma generates the public key.
  - $A=g^a$ mod p (10)

    $5^4$ mod 23=625 mod 23=4 (11)

- Shriya generates a public key.
  - $B=g^b$ mod p (12)

    $5^3$ mod 23=125 mod 23=10 (13)

Step 4: After receiving the public key, both parties need to compute identical private keys.

- Uma calculates
  - $K=B^a$ mod p (14)
  - $10^4$ mod 23=10000 mod 23=18 (15)

- Shriya calculates,
  - $K=A^b \bmod p$ (16)
  - $43 \bmod 23 = 64 \bmod 23=18$ (17)

Both sender and recipient receive the shared secret key as 18. Diffie-Hellman is based on the Discrete Algorithmic Problem.

It is easy to determine forward math,

- $A=g^a \bmod p$ (18)

But even if g, A, p, and B are known, it is hard to find out or calculate the private exponents A and B if p is large.

## 4. Technological Advancement

In this work, the existing system of RSA and its variants for extensive applications, integrated based RSA on varying applications and domains, and hybrid model, parallelization, implementing RSA with various security parameters such as key length, security complication, execution time, decryption, encryption, space or memory, key constraints etc. Previously its usage is restricted with in traditional computer network approach and resource constraint mobile application. Now it has been enhanced to Internet of Thing that is Internet enabled systems applications, cloud storages, images, multiple keys ,Chinese remainder theorem, digital signatures, K-Nearest Theorem, Batch, wireless and smart gadgets which in turn use extensively[7].

The explosion of technological improvement, many data driven kits also be incrementally upcoming. The current proliferation of gadgets is not enough to get rid of data breaches and security attacks. The antivirus and malware kits do not get rid of those attacks. To compensate, the innovation of cryptographic algorithms are in demand to sort out each and every problem such as privacy, authenticity, security etc.AI-driven cyber-attack; a branch of study is emerged. As the name implies, Artificial Intelligence uses human intelligence and behavioral the advanced computer networks. It proactively identifies the congestion takes place region in prior and settle down the conflict that caused by traffic during data transfer in computer networks. It also identifies hackers predominantly based on unusual behaviors of end-users. Not only, it identifies, detects and prevents such kind of adversaries' before-in-hand and reduces the theft happening in the online repositories. In the Big data era, the sensitive information is exchanged between users via digitally, lots of AI generative tools are increased parallel facilitates the extracting such data is becoming easy for adversaries. Tools such as chatbot, botnet, etc. replace the human intervention in those business activities make ease of utilization of those tools to identify, detect and extract sensitive information without the knowledge of authorized users.

## 5. Applications of Cyber security

Cyber security has wider applications in various domains are briefly explained by [563](Wasyihun Sema Admass et al.,2023)..To enhance the services in terms of security, confidentiality, data integrity, availability and reliability [11].

### 5.1 Cyber security in smart grid infrastructure

A power system optimizes the generation, distribution, and consumption of electricity with high efficiency and reliability, as it consists of many interconnected electronic components are described by [9](Ahmad Aliet al.,2026). The renewable energy system supplies energy, distributes intelligence, and supports demand response [2].

### 5.2 Cyber security in smart e-Health system

The e-Health Infrastructure provided by (Michael Winter et al., 2026) that uses smartphones, devices, and IoT devices to obtain and manage patient records, monitor their health, and prevent them from severe problems [4].

### 5.3 Cyber security in smart city

Smart City is proposed by [70] (Nataliia Neshenko, 2020) that protects water, transportation, power, and communications. It preserves personal information by ensuring privacy. It also protects the disaster recovery system associated with the city[5].

### 5.4 Cyber security in smart vehicular system

As suggested by [130](Abdulrahman Abu Elkhail et al.,2021) , Vehicular Communication Infrastructure includes road units, traffic control centers, secure software and hardware controls of vehicles such as Electronic Control Units, namely sensors, actuators, protecting the privacy and personal information of drivers and passengers, such as location, driving behavior, health, etc., guaranteeing vehicular communication system in emergencies[1].

## 6. Possible Technical and Non-Technical Solutions

Cybercrime includes threats, vulnerabilities, and cyber attacks, which are classified into non-technical and technical approaches.

### 6.1 Non-technical Approach

Non-technical security lays in the hands of administrators and Cyber security Professionals. Policies, standards, risk assessments, vendor management, and assigned responsibilities are important concepts while dealt with cyber attacks.

### 6.2 Technical Approach

The technical approach involves technology-wise and platform-based tools, and applying AI and data science are listed by [1270] (Ömer Aslan et al., 2023)

- The blooming technologies, big data, virtualization, and blockchain are used in cyber security. Blockchain validates data consistency and identifies complex attacks.
- Virtualization separates the software application and hardware components to increase software usability, thereby reducing downtime attacks.
- Cloud computing: a service provider provides proactive threat management, advanced data security, scalability, high availability, and effective data recovery.
- Access Control List tools (ACL) and firewalls filter of Internet Protocol (IP) address, ports and protocols also reduce DDoS attack.Intrustion Detection System (IDS) and Intrusion Prevention System (IPS) are for detection of signatures and anomalies on computer networks. Virtual Private Network (VPN), Internet Protocol Security (IPSec), Transport Layer Security (TLS), Secure Socket Layer (SSL) are for data confidentiality and protection during data transmission across networks[6].

## 7. Challenges

There are enormous challenges are available and are listed by [1270] (Ömer Aslan et al., 2023).

- A lot of time needs to be spent designing a secure system; often seen as a barrier.
- Security Professionals often see all vulnerabilities in the designed system; otherwise, the attacker can crack the system through a loophole
- Detecting and preventing attacks is unknown, particularly if data is huge.
- Complexity of attack is increasing incrementally.

- Attacks can be automated
- Intelligent attacks bypass the detection of a system.
- ML models assume the data; chances of prone to bias, not possible to handle outliers all the time, and are increasing day by day.
- Classifying millions of networks is challenging
- High-dimensional data are time-consuming and tedious
- Data pre-processing is complicated as they are in multiple formats[12].

## 8. Conclusion

Internet is a global communication network in this digital world. Lots of People are striving to digitalize the data. As they are comfortable in storing, managing, updating, transferring, and maintaining the data on the Internet, Security is the major concern to protect the data. As per (Umakant Dinkar Butkar, 2026), Cyber security professionals build effective design systems in different domains. Same way the Cyber attackers are increasing day by day to create loopholes in the generated system. There are various solutions that are customized by the cyber security professionals both technically and non-technically while they are delivering the system to vendors. In this way, cyber attacks are reduced considerably. Social Engineering is a major area where cyber attacks largely occur. To convince the legitimate users, even then the attackers trick them easily stealth, damage, disrupt and harm the system [10].

## 9. Acknowledgement:

The author renders her thanks to the Almighty and Guide for the continuous support and encouragement in contributing to this work.

## References

1. Abdulrahman Abu Elkhail, Rafi Ud Daula Refat , Ricardo Habre , Azeem Hafeez , Anys Bacha , Hafiz Malik , Vehicle Security: A Survey of Security Issues and Vulnerabilities, Malware Attacks and Defenses, IEEEAccess,November 2021,(9), 162401-162437,https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9625934.
2. Ahmad Ali, Mohammed Wadi ,Wisam Elmasry, Cyber security in Smart Grids and Other Application Fields: A Review Paper, MDPI energies , 2026,*19*(1),246,1-46, https://www.mdpi.com/19961073/19/1/246/pdf?version=1767255056.
3. Diptiben Ghelani, Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review, American Journal of Science, Engineering and Technology, 2022, 1-8 https://www.authorea.com/doi/pdf/10.22541/au.166385207.73483369/v1 .
4. Michael Winter, Robin Kraft, Pascal Leber, Manfred Reichert, Helmut Greger, Johannes Muhr, et al., Cybersecurity in eHealth: A Scoping Review of Current Research and Trends, IEEE Journal of Biomedical and Health Informatics, 2025 ,1-19, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=11493882 .
5. Nataliia Neshenko, Christelle Nader, A survey of methods supporting cyber situational awareness in the context of smart cities, Journal of Big data, 2020, 7(92),1-41, https://link.springer.com/article/10.1186/s40537-020-00363-0 .

6. Ömer Aslan , Semih Serkant Aktug,Merve Ozkan –Okay,Abdullah Asim Yilmaz,Erdal Akin A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions, MDPI Electronics,2023, https://www.mdpi.com/2079-9292/12/6/1333 .
7. Raza Imam, Qazi Mohammad Areeb, Abdulrahman Alturki, Faisal,Anwer Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes:Past and Present Status, IEEEAccess,2021,155949155976https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=962007.
8. Sourabh Chandra; Siddhartha Bhattacharyya; Smita Paira; Sk Safikul Alam, A Study and Analysis on Symmetric Cryptography, International Conference on Science, Engineering and Management Research (ICSEMR 2014),2014, https://doi.org/10.1109/ICSEMR.2014.7043664 .
9. Tanenbaum, Weterall, Computer Networks, Pearson Higher Ed, sixth edition book, ISBN-13**:** 978-0137523214, 2021.
10. Umakant Dinkar Butkar, Cyber Security for Beginners, Publisher: Lambert Publication, ISBN: 978-620-6-76822-7, 2023.
11. Wasyihun Sema Admass, Yirga Yayeh Munaye, Cyber security: State of the art, challenges and future directions, Cyber Security and Applications, 2024,1-9, https://doi.org/10.1016/j.csa.2023.100031.
12. Yuchong Liu, Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, Elsevier, Energy Reports, 2021, 7, 8176-8186, https://doi.org/10.1016/j.egyr.2021.08.126 .