ISSN 2319 - 5975

Volume 13, No.1, December 2023 – January 2024

International Journal of Networks and Systems

Available Online at http://www.warse.org/IJNS/static/pdf/file/ijns111312024.pdf

https://doi.org/10.30534/ijns/2024/111312024

Safeguarding Networks: The Role of Cryptography

Adithi[1], Amrutha G K[2], Farheen Sadia[3], Keerthi R[4], Prof. Venkatesh[5]

Students, Department of Computer Science and Engineering[1,2,3,4]

Senior Associate Professor, Department of Computer Science and Engineering[5]

[1]Alva's Institute of Engineering and Technology, India, adithimoodbidri@gmail.com

[2]Alva's Institute of Engineering and Technology, India, amruthagk555@gmail.com

[3]Alva's Institute of Engineering and Technology, India, farheensadia16@gmail.com

[4]Alva's Institute of Engineering and Technology, India, keerthiraghunathareddy72@gmail.com

[5]Alva's Institute of Engineering and Technology, India, venkateshbhat@aiet.org.in

Received Date : November 24, 2023 Accepted Date : December 23, 2023 Published Date : January 07, 2024

ABSTRACT

Due to complex network threats, network security faces unprecedented challenges in a rapidly changing environment. These details highlight the importance of cryptography in protecting networks from today's threats. The development of technology has led to the increase in connected devices, the expansion of parking areas and the need for security measures. Honest and confidential information is protected by encryption technology using complex methods and algorithms. The brief reviews state-of-the-art cryptographic techniques and highlights the importance of quantum-resistant mechanisms against the threat of quantum computing. It explores how cryptography can be used together with technologies such as blockchain, artificial intelligence and the Internet of Things, and emphasizes its importance in ensuring the security of these areas. It envisions the development and implementation of post-quantum cryptography, covers concepts such as homomorphic encryption and zero-knowledge proofs, and addresses issues of cryptographic efficiency and creative control. It aims to protect networks from new threats and ensure secure data exchange by meeting the need for strong cryptographic protection in the evolving business environment.

Key words: Cryptography, Quantum computing, Block chain, Internet of things, Artificial intelligence, Encryption

1. INTRODUCTION

Due to the complexity of cyber threats, cyber security has become one of the most important issues in today's rapidly changing environment. The number of stops has increased due to the growth of connected devices and the development of digital ecosystems driven by the Internet of Things (IoT). In addition to providing previously unheard-of connections, this expansion also creates previously unheard-of vulnerabilities, making the network vulnerable to serious cyber-attacks[1].

Cyber-attacks are becoming increasingly complex and create many problems in protecting sensitive information, network infrastructure and networks. information. Criminals are threatening to use a variety of attacks, including ransomware, phishing, malware, and zero-day attacks, and they are always evolving to bypass traditional security measures [28]. The importance of cryptography in network security cannot be overstated. Sensitive data is encrypted to ensure confidentiality and data integrity is maintained to ensure data is not altered during transmission or storage. Additionally, cryptography allows access to security controls and aids in authentication by verifying the identity of communicators.

Due to the development of technology and the increasing number of cybercrimes and cyber-attacks, cryptography plays an important role in improving cyber security. It is important for organizations to understand and use strong encryption techniques and algorithms to reduce risk and protect their digital assets [14].

This article aims to explore the complex world of cybersecurity issues in today's technological world. . Its main purpose is to demonstrate the important role cryptography plays as an important tool in protecting networks against threats. It also highlights the importance of cryptography in protecting the confidentiality, integrity and authenticity of information in a dynamic digital environment.

2. FUNDAMENTALS OF CRYPTOGRAPHY

The study of secure communication, or cryptography, has a long and rich history dating back thousands of years. Its development has resulted from constant changes and modifications to accommodate security changes, starting from old ciphers to modern encryption algorithms.

2.1 Historical evolution

After centuries of development, cryptography has become an advanced field that adapts to the needs of today's technological environment. The historical trajectory includes the transition from traditional encryption methods (such as changing and modifying passwords) to the introduction of modern encryption algorithms and methods that change the approach to security. The development of post-quantum

cryptographic solutions has been influenced not only by historical technologies, but also by the growth of computing power and the emergence of quantum computing.

2.2 Basic Cryptographic concepts

Hashing, Decryption and Encryption Principles Encryption is crucial to modern cryptography. Encryption uses strong encryption algorithms and keys to convert plaintext data into ciphertext to protect data confidentiality during transmission or storage. To convert ciphertext back to plaintext, a reverse process called decryption is required to access the original data. Data integrity and authentication can be verified using hashing, which creates a constant value of the input data and uses it as a digital fingerprint. Today's systems often use advanced cryptographic hashing techniques such as SHA-256 and SHA-3 to ensure data integrity.

3. KEY MANAGEMENT

Effective management of encryption keys is crucial to the security of the database system. Even with strong encryption algorithms, leaking or mishandling keys can render data completely unsecured. The main management process is production, inspection, distribution, transmission, storage, use, disposal, etc. Contains. Key management is an important part of the encryption process that ensures the safe and effective use of encryption keys [23].

Here's a brief explanation of the key steps involved:

- *Key Generation:*

Importance: Correctly generated keys are important for the security of encryption algorithms.

Brief Explanation: Strong random number generation creates unique and unknown keys, making it difficult for attackers to crack encrypted data.

- *Key Distribution:*

Ensure that legitimate parties have access to the necessary keys while preventing organizations from unauthorized access to these keys. Communication or key exchange techniques are often used to share keys among authorized users, thus preventing tampering and misuse during transmission.

- *Key Storage:*

Integrity of encrypted data. Secure storage methods such as hardware security modules or security safes can protect keys from theft, tampering, or accidental loss.

- *Key Revocation:*

Allows removal of relevant or unusable keys to prevent unauthorized access or possible security breaches. Once the key is compromised or no longer needed, the removal mechanism ensures that the key becomes instantly invalid and the system no longer accepts it for cryptographic operations. This helps maintain the overall security of the system.

Proper key management contributes to the overall security of the cryptographic process by protecting sensitive data and ensuring the secure operation of connection security and data protection mechanisms.

4. DIGITAL SIGNATURES

Digital signature is an important general element for identifying messages. In the real world, it is common to use symbols written or written on written notes. They are used to associate the signer with the message. Essentially, computerized tagging is the process of linking individuals/objects to digital data. This guarantee can be personally confirmed by the beneficiary and a third party. A digital signature is a cryptographic value determined by the information known to the signatory and the secret key. In the real world, the journalist must understand that the message is the messenger and should not be ready to deny the source of the message. This prerequisite is exceptionally significant in business applications, since probability of a disagreement regarding traded information is extremely high [24].

4.1 Process involved in Digital Signature

Each participant uses several keys: a public key for encryption/decryption and a separate private key for signing/verification. The private key chosen for signing is called the signing key, and the corresponding public key is called the verification key.

To create a digital signature, the signer processes data through a hash function to create a unique hash value. The signature algorithm then uses the hash value along with the signature key to create a digital signature based on the given hash value. The resulting signature is added to the profile and both are sent to the designated person.

After receiving, the verifier goes into the process of verifying the digital signature and proof key to generate the output value. At the same time, the validator applies the same hash function to the received data to generate the hash value.

During the verification process, the hash value of the received data is compared with the output of the data verification algorithm. This comparison determines the validity of the digital signature. More importantly, because the digital signature is created using the signer's private key and is unique to the signer, there is no way to reject the signature in future transactions.

4.2 Importance of Digital Signature

- *Authentication*

A digital signature identifies the identity of the sender or creator of a digital document or message. The unique signature is associated with a private key to verify that the data comes from the requested source.

- *Data Integrity*

Digital signatures provide a way to ensure that the content of a message or document has not been altered during transmission. Any changes made to the file will not use the signature when checked.

- *Tamper Detection*

Digital signatures help detect unauthorized changes to signature data. If the data is modified, verification of the digital signature will fail, indicating that it may have been tampered with.

- *Secure Communication*

Digital signatures facilitate secure communication on the internet by ensuring that information exchanged between two parties remains confidential, immutable and fact-checked. It is a tool for accuracy and security.

In conclusion, by connecting an individual or organization to digital data through the process of encryption, they provide recipients and third parties with a reliable method of authentication. The process of creating and verifying digital signatures using key pairs and hash functions helps improve their performance. Its main purposes are to ensure authentication, ensure data integrity, investigate security vulnerabilities, and facilitate secure communication on the Internet. Digital signatures, the main source of message authentication, play an important role in resolving disputes in the business world and ensuring trust in information exchange.

5. NETWORK SECURITY PROTOCOLS

In a digital environment, encryption protocols and algorithms are required to ensure secure communication, protect data integrity and facilitate recognition. In today's world of cryptography, various cryptographic protocols and algorithms are important for the security of networks, data protection and digital communication.

5.1 SSL/TLS (Secure Sockets Layer/Transport Layer Security)

The SSL/TLS protocol is crucial to the security of the connection language network as it provides authentication and encryption between the web server and the browser. An alternative to SSL, TLS encrypts data sent over the Internet to prevent manipulation and eavesdropping. The TLS protocol provides a secure connection for many online activities, such as browsing, online transactions, and the exchange of sensitive information. An important security and privacy requirement for online commerce is SSL/TLS. For example, your laptop must authenticate the remote host before uploading credit card information to the Amazon.com website. Protocols such as SSL/TLS can help solve this problem. Additionally, the protocol is often used to protect chat servers (using the XMPP protocol), email servers (using the SMTP, POP, and IMAP protocols), instant messaging (IM), remote security settings (use the SSH server), and some virtual servers. Private network (SSL VPN).[25]

SSL/TLS supports only server or server-client authentication. The client receives server credentials only on server authentication. After verifying the server's certificate, the client generates a key and encrypts it using the server's public key. The encrypted key is sent by the client to the server, the server decrypts it using its own key, and then uses the client-generated key to encrypt the message sent to the client. The client provides the server with its certificate, which is used by the server to authenticate the client, along with the key during server-client session product authentication.

Actually, SSL/TLS is not a rule and it is not a rule. Contract layer. As shown in Figure 1, SSL has four rules divided into two layers. The SSL protocol and the SSL handshake protocol are the two most important of the four protocols that make up SSL. After the server and client authenticate each other, the server sends private information. The SSL password change protocol and the SSL notification protocol (the other two protocols shown in the diagram) are essentially unrelated to the operation of SSL.

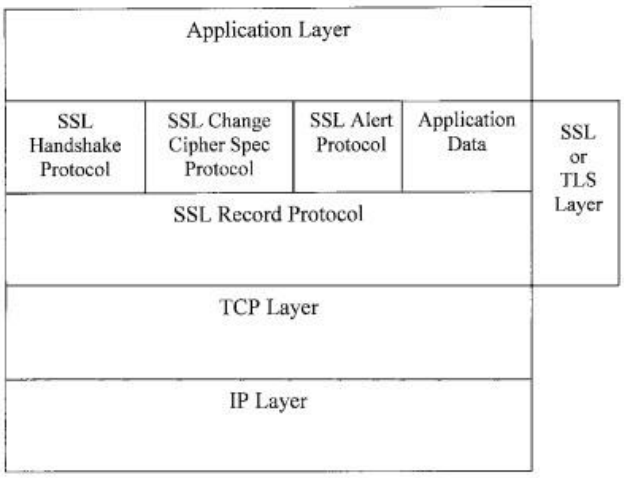

Figure 1: SSL layers [30]

5.2 Pretty Good Privacy (PGP)

PGP is a data encryption and decryption tool created by Phil Zimmermann in 1991. Supports symmetric and asymmetric encryption. Users can use it to generate public and private keys. Since the public key is freely distributed, anyone can encrypt files or messages meant for the key owner. The owner's secret private key is used to sign digital documents to verify their authenticity and decrypt incoming encrypted messages [28].

PGP's primary components are encryption and decryption, which combine:

- *Symmetric and Asymmetric Encryption Techniques*

Asymmetric encryption, like ElGamal or RSA, is used to safely exchange the session key used in symmetric encryption, while symmetric encryption, like the IDEA or AES algorithm, is used to encrypt the message itself.

- *Digital Signatures*

To verify the message's integrity and authenticity, PGP additionally offers the ability to generate digital signatures using the sender's private key. The sender's public key can be used by recipients to validate the signature.

- *Keyrings*

PGP groups public keys into keyrings that hold the public keys of other users as well as the user's own private and public keys [28].

5.3 GNU Privacy Guard (GPG)

An open-source version of the PGP standard with more features and better compatibility is called GPG. GPG adheres to the OpenPGP standard, guaranteeing compatibility with different PGP versions.

Important GPG features include:

- *OpenPGP Compliance*

GPG complies with the OpenPGP standard, which enables users to sign, decrypt, encrypt, and validate files and messages using a generally recognized protocol.

- *Cross-Platform Compatibility*

GPG offers flexibility and user-friendliness as it is compatible with a wide range of email clients and file encryption tools. It is accessible on multiple platforms.

- *Key management*

GPG has extensive key management capabilities that let users create, import, export, and manage key pairs as well as other people's public keys [28].

6. AES, RSA, ECC: Key Cryptographic Algorithms

Key encryption algorithms, RSA (Rivest-Shamir-Adleman), ECC (Elliptic Curve Cryptography) and AES (Advanced Encryption Standard), are widely used to protect digital communications, security and safety of data. is used. information. Various online businesses. Each algorithm has its own advantages and is used in various cryptographic fields.

6.1 AES (Advanced Encryption Standard)

- *Description*

The National Institute of Standards and Technology (NIST) has developed a combination encryption algorithm called AES. Encrypting and decrypting sensitive data is widely used.

- *Strengths*

AES is known for its performance and security. It comes in three different lengths (AES-128, AES-192 and AES-256) providing different levels of security. AES-256 in particular is widely used to protect sensitive data and is considered very secure.

- *Applications*

Use AES to protect data at rest (data storage) and data in transit (transit across the network). Encrypted storage systems, secure messaging apps, VPNs, etc. It is frequently used in many applications [28].

6.2 RSA (Rivest-Shamir-Adleman)

- Key exchange, digital signatures, and encryption are all done with the asymmetric encryption algorithm known as RSA.

- *Strengths*

The security of RSA is based on the generation of complex numbers. Its two keys (private key for decryption and public key for encryption) enable secure communication and verification of digital signatures.

- *Applications*

RSA is widely used in digital signature, email encryption, secure transaction and encryption. Applications include digital certificates, SSL/TLS for secure communications, and email encryption [2].

6.3 ECC (Elliptic Curve Cryptography)

- Asymmetric encryption algorithm ECC uses elliptic curves of finite fields to provide encryption functions.

- *Strengths*

Compared to RSA, ECC provides better security and shorter key; This makes it particularly suitable for limited domains such as mobile devices and the Internet of Things. With its smaller size, it provides security while consuming less power than RSA.

- *Applications*

ECC is used in many different areas such as secure communications, network security (SSL/TLS), cryptocurrencies (e.g. Bitcoin), mobile communications (3G/4G/5G) and IoT devices [28].

7.CRYPTOGRAPHIC ATTACKS AND VULNERABILITIES

Cryptographic attack is a method used by attackers to obtain passwords such as ciphertext and encryption keys. These attacks aim to expose sensitive or decrypted data by exploiting weaknesses in cryptographic techniques, encryption algorithms or key management techniques.

There are two types of password protection: passive and active.

Passive attacks focus on hiding sensitive data by intercepting communications without altering or interfering with the data.

An attack, on the other hand, involves tampering with information or communications as well as unauthorized access that may alter the integrity of the information [10].

7.1 Some encryption attacks and vulnerabilities

- *Brute Force Attack*

In cryptography, a brute force attack will systematically try many passwords or passphrases until one is found. In theory, it could try to decrypt data unless the data is protected in a way that makes them safe. While shorter passwords are faster, longer passwords double the time required for brute force lookups, making the dictionary more vulnerable to longer passwords and keys. Techniques such as hiding

information or increasing the amount of work required for each guess will reduce the effectiveness of brute force attacks, and the strength of an encryption system is often measured by the time required for such an interception [11]. A brute force attack works by trying every combination to find the correct password, and the time required increases exponentially as the password length increases. Although this method has been around for a long time, it is still popular among hackers due to its reliability. Additionally, phishing attacks are another major cyber threat that targets people through spoofed emails to capture login credentials or sensitive information. Spear phishing and whaling are unique types of phishing attacks that target specific individuals using customized email content for maximum fraud [13].

- *Man-in-the-Middle (MitM) attack*

It involves a malicious third-party intercepting and controlling communications between two or more parties without being detected. It compromises the confidentiality of communications, allowing attackers to intercept, modify or read data.

Malware attacks, which also include viruses, spyware and ransomware, pose a serious threat by installing malware on users' computers without permission. These attacks are designed to access other people's networks, disrupt business computers, and steal sensitive information, often targeting business or financial information [12].

- *Side-channel attack*

The concept of side-channel attacks (SCA) and their threats to tamper-resistant products. There are two main types of power analysis: Simple Power Analysis (SPA) and Power Analysis (DPA).

This article divides insider attacks into malicious and malicious attacks and explains how attackers can obtain information by monitoring applications, electricity, and analytics. respectively, it is interference in wafer processing. It also explores specific methods such as Differential Power Analysis (DPA), Simple Power Analysis (SPA), Data Bit Differential Power Analysis (DDPA), Address Bit Differential Power Analysis (ADPA), Zero Value Point Attack (ZPA) and others [15].

- *Key management flaws*

If keys are not properly handled, it can lead to unauthorized access to the information which needed to be protected. This could also lead to a security breach if keys are used by people who have unauthorized access. focusing on its authentication and key management protocols, security concerns, and proposed solutions for vulnerabilities Security goals include ensuring privacy, message authenticity, anti-replay, non-repudiation, access control, and availability. The standard employs a security sublayer at the MAC layer's bottom to safeguard both Base Stations (BS) and Subscriber Stations (SS). This sublayer involves protocols for encrypting packet data and managing key distribution (PKM) [14].

8. EMERGING TRENDS AND TECHNOLOGIES

Parallel computing has brought significant changes to various computer science domains, including cryptography. Cryptographic hash functions (CHFs), as essential tools in cryptography, have gained increased attention for leveraging parallelism to enhance speed, security, and efficiency, especially following the competition for the SHA-3 standard. Hashing techniques have been pivotal in computing since early systems and have gained more importance in the information age. Cryptographic hash functions (CHFs) ensure data authenticity and security, producing fixed-length outputs for arbitrary-length messages.

The significance of cryptography in safeguarding sensitive digital information is very much more it’s evolution from ancient techniques to modern cryptographic algorithms. It emphasizes the importance of encryption in securing data transmission and storage and explores its various applications such as secure communication, cloud computing, and blockchain technology. There are also concerns about emerging threats such as quantum computing and ethical and legal issues surrounding cryptography [16]. Cryptography has been described as an essential part of modern life, tracing its important history in protecting confidential information and its important role in today's digital world. Contributions to cryptography such as Goldwasser and Bellare's book on modern cryptography, the RSA algorithm, the introduction to Bitcoin, Craig Gentry's advances in homomorphic encryption, and efforts towards post-quantum cryptography. This work demonstrates the evolution of cryptography from theory to practical application. Research methods include data collection, theoretical framework research, algorithm evaluation, practical implementation and testing, security evaluation, simulation, modelling, and ethical considerations. He explains how each step leads to understanding the cryptosystem.

The COVID-19 pandemic has disrupted the traditional way of distributing school surveys to participating universities. To solve this challenge, a method using N-out-of-N encryption technology and AES encryption is proposed to secure the test text during transmission. The goal of this approach is to reduce the security risks associated with online distribution, where hackers could steal or alter data. The presented scheme demonstrates a promising way to replace the physical distribution of test papers with secure digital transmission using optical cryptography and encryption techniques.

Integrate blockchain technology, especially Identity-Based Cryptography (IBC), into the financial auditing process to combat fraud. It explores how blockchain, with its decentralized nature and transparency, can revolutionize auditing by providing a secure, tamper-proof record of transactions [17].

9. REAL-WORLD APPLICATIONS

Cryptography has many uses, including finance, healthcare, and government. Encryption technology is used in the financial industry to protect customer information, especially bank information and credit card numbers. Cryptography is used in the healthcare industry to protect patient information, especially test results and medical records. Secret documents

and other confidential information related to national security are protected by the government using cryptography.

Encryption is widely used to protect information sent over the Internet. Confidential information is ensured during online transactions such as online business and e-commerce by using techniques such as End-to-End Communications and Transport Layer Security to encrypt data transmitted between web browsers and servers [18].

Currently, WhatsApp is one of the most used messaging applications. Conversations and calls using the latest version of WhatsApp are encrypted "end-to-end". While the communication is being sent, end-to-end encryption ensures that only the intended recipient receives the communication. WhatsApp ensures that even "itself" cannot read the message and supports very strong messaging. This also means that outsiders or third parties cannot listen to phone calls of intended recipients [19] & [21].

Authentication The SIM card must be authenticated to determine whether it is allowed to access the network. The operator generates a random number and sends it to the mobile device. This random number is passed through the A3 algorithm along with the key. The result of the calculation is sent back to the operator, who compares it with the result of his own calculation [19].

Digital signatures and public key encryption are crucial to ensuring the integrity and validity of financial transactions [18].

10. CHALLENGES AND FUTURE DIRECTIONS

Cryptography has come a long way since the advent of safe online browsing and ATM withdrawals. With strong support from CISOs, businesses are beginning to increasingly embrace encryption. In the past, the expense, user interaction, and deployment issues associated with encryption have been viewed as problematic. Recently, it seems that the cloud has greatly increased the use of cryptocurrency. Businesses and financial services companies use it for general network security, key management, signature authentication, sales invoicing, data protection during transit travel and recreation, and many other purposes. With additional options and the ability to reduce costs, the cloud makes it easier for businesses to manage their encryption processes [20].

- Post-Quantum Cryptography

Modern encryption schemes such as RSA and ECC are endangered by the development of quantum computers, which will soon solve some of the most difficult mathematical problems that underpin them. This problem can be solved by designing and developing encryption methods that prevent attacks by quantum computers. Hash-based, code-based, and lattice-based cryptography are still in the research phase.

- Blockchain and Cryptocurrency

The challenge is to ensure the security and privacy of transactions and the security of user identities on blockchain networks. It can be improved by creating new cryptographic foundations for security and privacy that store smart contracts, improving consensus algorithms, and solving scalability problems in blockchain systems.

- Key Management

Effectively managing encryption keys is a difficult task, especially in large systems and IoT devices. To overcome this problem, significant solutions and safety must be developed, including improving the importance of distribution, storage and removal procedures [22].

REFERENCES

1. Bruce Schneier. **Applied Cryptography: Protocols, Algorithms and Source Code in C**, 20th Anniversary Edition.
2. Raza Imam, Qazi Mohammad Areeb, Abdulrahman Alturki, And Faisal Anwer. **Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status.** IEEE Access, vol. 9, 2021
3. Roza Dastres, Mohsen Soori. R. A. Scholtz. **The Spread Spectrum Concept**, in *Multiple Access*, N. Abramson, Ed. Piscataway, NJ: IEEE Press, 1993, ch. 3, pp. 121-123.
4. G. O. Young. **Synthetic structure of industrial plastics**, in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15-64.
5. S. P. Bingulac. **On the compatibility of adaptive controllers**, in *Proc. 4th Annu. Allerton Conf. Circuits and Systems Theory*, New York, 1994, pp. 8-16.
6. W. D. Doyle. **Magnetization reversal in films with biaxial anisotropy**, in *Proc. 1987 INTERMAG Conf.*, 1987, pp. 2.2-1-2.2-6.
7. J. Williams. **Narrow-band analyzer**, Ph.D. dissertation, Dept. Elect. Eng., Harvard Univ., Cambridge, MA, 1993.
8. N. Kawasaki. **Parametric study of thermal and chemical nonequilibrium nozzle flow**, M.S. thesis, Dept. Electron. Eng., Osaka Univ., Osaka, Japan, 1993.
9. Nadeem Ahmad, M. Kashif Habib. School of Engineering Department of Telecommunication Blekinge Institute of Technology SE - 371 79 Karlskrona Sweden **Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution** Master Thesis Electrical Engineering Thesis No: MEE10:76 Sep 2010
10. J. DiGiacomo, **Active vs Passive Cyber Attacks Explained | Revision Legal,** 2017. [Online]. Available: https://revisionlegal.com/internet-law/cyber-security/active-passive-cyber-attacks-explained/
11. Rajendra P. Pandey, Assistant Professor, College of Computing Sciences and Information Technology, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh, India. **An Explanation on Different Types of Attacks in Modern Cryptography System,** Ijfans International Journal of Food and Nutritional Sciences**,** UGC CARE Listed (Group-I) Journal Volume 11, Iss 1, Jan 2022
12. M. Conti, N. Dragoni, and V. Lesyk, **A Survey of Man in the Middle Attacks,** IEEE Communications Surveys and Tutorials. 2016.

13. G. Sowmya, D. Jamuna, and M. V. Reddy Krishna, **Blocking of Brute Force Attack**, Int. J. Eng. Res. Technol., 2012.
14. Sen Xu, Manton Matthews, Chin-Tser Huang, and Jingshan Huang. **Security Issues in Privacy and Key Management Protocols of 802.16,** Conference: Proceedings of the 44st Annual Southeast Regional Conference, 2006, Melbourne, Florida, USA, March 10-12, 2006
15. Z. Wang, F. Meng, Y. Park, J. K. Eshraghian and W. D. Lu are with the Department of Electrical Engineering and Computer Science, the University of Michigan, Ann Arbor, MI, 48109, USA. **Side-Channel Attack Analysis on In-Memory Computing Architectures**, IEEE Transactions on Emerging Topics in Computing (2023), Corresponding Author: Wei D. Lu.
16. Mr. Sneh Shrimankar1, Mr. John Bright Raj2, Mrs. Abhilasha Maurya, **Emerging Trends In Cryptography And Digital Forensics,** International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 10 Issue: 12 | Dec 2023.
17. Muhammad Zubair, Muhammad Munawar Ahmed, Aqib Ali, Samreen Naeem, and d Sania Anam. **Network Security and Cryptography Challenges and Trends on Recent Technologies**, Journal of Applied and Emerging Sciences Vol (13), Issue (01).
18. **Cryptography-Real World Application**, Netleon Technologies, June 4, 2022.
19. Prashanth Reddy, **Real Life Applications of Cryptography**, Nov 8, 2019.
20. Ryan Smith. **Challenges and Future Trends in Cryptography**, Infosecurity Magazine, Sep 6, 2021.
21. Jayanthi, **Basics of Cryptography: The Practical Application and Use of Cryptography,** Infosec, April 7, 2018.
22. Abderrahmane Nitaj and Tajjeeddine Rachidi. **Applications of Neural Network-Based AI in Cryptography,** MDPI-Publisher of Open Access Journals, August 11, 2023.
23. Shi **Yan "Research on Implementation Method of Key Management Based on Data Encryption Technology",** IOP Conf. Series: Materials Science and Engineering 677 (2019) 042018 doi:10.1088/1757-899X/677/4/042018.
24. https://www.tutorialspoint.com/cryptography/cryptography_digital_signatures.htm
25. Roza Dastres, Mohsen Soori **"Secure Socket Layer (SSL) in the Network and Web Security"** World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering Vol:14, No:10, 2020.
26. Bahnasse, A., Talea, M., Badri, A., Louhab, F. E., & Laafar, S. (2020). **"Smart hybrid SDN approach for MPLS VPN management on digital environment. Telecommunication Systems",** 73(2), 155-169.
27. Lotfi Firdaouss*, Bahnasse Ayoub, Belkadi Manal, Yazidi Ikrame **"Automated VPN configuration using DevOps"**, The second International Workshop of Innovation and Technologies(IWIT 2021) ,Procedia Computer Science 198(2022) 632-637
28. William Stallings, **Cryptography and Network Security: Principles and Practice,** 6th edition
29. Kinjal Raut**, Chaitrali Katkar, A Comprehensive Review of Cryptographic Algorithms,** https://doi.org/10.22214/ijraset.2021.39581
30. Robert J. Boncella, Washburn University, **Secure Sockets Layer (SSL),** Research gate publications, WL040/Bidgolio-Vol I