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, keerthiraghunathreddy72@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