IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Network Security Using Tripleshield & Blockchain

1st Rohit Gupta
Artificial Intelligence and Data Science
University of Mumbai
Thane, India

2nd Sahil Mhatre
Artificial Intelligence and Data Science
University of Mumbai
Thane, India

3rd Sakshi Naik
Artificial Intelligence and Data Science
University of Mumbai
Thane, India

4th Aaditya Singh
Artificial Intelligence and Data Science
University of Mumbai
Thane, India

5th Megha Gupta
Artificial Intelligence and Data Science
University of Mumbai
Thane, India

***Abstract*—**We propose a network-level system using hybrid cryptography and blockchain techniques to fortify digital transmissions. Existing proposals for network security are often expensive subscriptions using third-party software or use a single algorithm and a hash-key system for security. This makes the system share the vulnerabilities of used algorithm along with giving the matter of security in someone else's hand. Additionally, any hardware solution available in the market is a USB that acts as an intermediary, or a bulky hardware extension that connects to the router. Introducing an intermediary reduces the speed of transmissions that can prove detrimental in some cases while also raising questions for practicality of the excess equipment. Our approach makes it so a single router is capable of securing all transmissions. TripleShield combines the strengths of a triple-layer encryption, secure key exchange and blockchain. Through a custom PCB that replaces the router, we look to both- fortify the transmissions along with maintaining an audit trail for everything. By using multi-layered encryptions and pen-testing we aim to make cracking the network a formidable nightmare for any adversaries.

Keywords--Cybersecurity; Hybrid cryptography; Hardware systems; Network security; Secure key exchange; Digital signatures; Immutability; Audit trails

I. INTRODUCTION

The demand for strong security and privacy solutions is stronger than ever in an era characterized by digital innovation and interconnection. Introduce yourself to TripleShield, a cutting-edge security platform that combines several cutting-edge technologies to protect your digital environment.

TripleShield is a comprehensive protector meant to safeguard your communications, identity, and data—it's not just a security system. TripleShield gives you the assurance to securely traverse the digital environment by combining the strength of three security pillars: secure key exchange, asymmetric and symmetric cryptography, and blockchain technology. In our increasingly interconnected world, the "Triple Shield" aims to mitigate the growing susceptibility of digital assets and communication to cyber threats. It seeks to offer a complete solution to protect information and encourage confidence in online transactions. Making the "TripleShield" a trifecta of –

Triple-Layer Encryption: TripleShield employs a sophisticated triple-layer encryption approach, combining RSA encryption and Twofish encryption algorithms to ensure robust protection against unauthorized access and data breaches. This multi-layered encryption strategy enhances data security by adding multiple barriers for potential attackers to breach.

Secure Key Exchange: Facilitated by the Diffie-Hellman key exchange protocol, TripleShield ensures secure and efficient key exchange between parties involved in data communication. This mechanism enables seamless and tamper-proof key negotiation, enhancing the overall security of data transfers.

Blockchain Integration: TripleShield integrates blockchain technology to create a transparent and immutable ledger of security related events. By recording user authentication, data transfers, and key exchange information on the blockchain, TripleShield provides a comprehensive audit trail, ensuring accountability and facilitating forensic analysis in the event of security incidents.

The project uses a combination of cutting-edge technologies, such as secure key exchange methods, symmetric and asymmetric cryptography, and blockchain technology, to accomplish this. By using blockchain technology, data transactions are made transparent and unchangeable by producing audit trails and records that are impenetrable by tampering. Algorithms for symmetric cryptography are used to efficiently encrypt and decrypt data, improving data security without sacrificing speed. Strong data protection and confidentiality are guaranteed by asymmetric cryptography, more especially by the RSA encryption technique. To strengthen data encryption, the project also uses Twofish encryption.

II. LITERATURE SURVEY

The paper on data governance [1] outlines a solution for security and privacy challenges in traditional cloud storage. It utilizes blockchain and attribute-based encryption to prevent privacy breaches and enable efficient data sharing. The approach includes a decentralized storage system (IPFS) and a smart contract for access control. An improved CP-ABE scheme supports fine-grained access control and multi-authority with privacy preservation. The proposal is backed by a systematic security analysis and outperforms related works in performance and security. In summary, it provides a robust, privacy-focused data governance framework based on blockchain technology and enhanced CP-ABE with policy hiding.

The paper [2] presents a comprehensive study on the impact of DDoS attacks in cloud computing and the need for robust defense mechanisms. We review existing DDoS prevention methods, both past and state-of-the-art, and propose future work to develop more efficient defenses. Our analysis covers various prevention techniques, including machine learning, artificial intelligence, blockchain, and genetic algorithms, emphasizing their effectiveness. Using real-world NIDS, we assess the performance of these methods, offering valuable insights into their capabilities compared to existing approaches.

The paper discussing attack detection and automation [3] conducts a comprehensive analysis of intelligent techniques for network attack detection. It addresses the pressing need for advanced defenses against a rising number of threats. The study reviews machine learning and deep learning algorithms, with Random Forest and Support Vector Machine being popular choices. It also identifies challenges in using intelligent techniques and offers research recommendations. The work emphasizes the importance of ML and DL methods, highlights prevalent algorithms like Random Forest and Support Vector Machine, but also points out unresolved challenges in accurately identifying attack types. This review provides valuable insights for further research and practical network security applications.

The paper on mobile attacks [4] focuses on cyber-attacks against in-vehicle networks, uncovering vulnerabilities and proposing security measures. It reviews past cyber-attacks and stresses the importance of vehicle network security. The study offers insights into future threats and aims to educate readers on this topic while emphasizing the need for vigilance and the application of standard security practices, including collaborating with ethical hackers to identify and address vulnerabilities proactively.

The document by S. Vishnu Kumar [5] provides a comprehensive overview of network security, including its research background, significance, methods, and theories. It addresses the core aspects of network security, analyzes computer network security challenges, and proposes protective measures. The emphasis lies in enhancing network administrators' awareness and fostering a sound security concept to safeguard campus networks against potential attacks.

The paper on MANETs [6] focuses on addressing the threat of Wormhole attacks in Mobile Ad hoc Networks (MANETs), which exploit vulnerabilities in routing protocols. Wormhole attacks involve creating tunnels between malicious nodes to redirect and manipulate network traffic. The Dynamic Source Routing (DSR) protocol, a prominent MANET routing protocol, is examined in this study. The authors simulate the formation of Wormhole tunnels within DSR using the NS3 simulator. By analyzing the behavior of DSR under Wormhole attacks, this research aims to enhance understanding of the attack's impact on DSR and provide insights for future security measures in MANETs.

The paper by Ravi Kishore Kodali and Bysani Kirti, [7] delves into the realm of Internet of Things (IoT) networks, which are revolutionizing various aspects of our daily lives by enabling seamless communication between devices and sensors. IoT networks typically comprise a diverse array of embedded sensors, processors, and communication hardware. Given the complexity and cost associated with experimental setups, simulation tools are essential for understanding the performance of designed networks in real-time scenarios. By utilizing the ns-3 simulation tool, which allows for the creation of virtual networks through scripting in C++ and Python on a single computer researchers can simulate IoT networks by defining virtual nodes and configuring them with various components such as internet stacks and applications using Helper classes.

This research paper by Maleh Yassine [8] seeks to enhance comprehension of blockchain's applicability in bolstering cybersecurity and privacy. It explores fundamental concepts, architectural frameworks, and associated challenges, providing insights into the integration of blockchain across various domains such as IoT and healthcare systems. Additionally, it investigates blockchain's role in securing payment systems and facilitating digital forensics. Through case studies and analyses, the paper elucidates practical implementations and potential future use cases of blockchain technology in cybersecurity. It addresses inherent threats, vulnerabilities, and security considerations pertinent to blockchain adoption.

The paper by C. H. Ng. [9] explores the topic on building a custom router and supporting IC. The router described in this paper is part of a complete CAD system which aims at hierarchical designs of customized VLSI MOS circuits. It routes global signals as symbolic interconnect and is guaranteed to complete all routing in one pass. The router is fully automatic as well as highly interactive. It employs the novel idea of buoyancy and produces wires with a natural bus structure. The router is fully operational, and has been used in routing a number of real-world integrated circuits.

III. MATERIALS AND METHODS

3.1. Feasibility Analysis: Feasibility analysis is mentionedin project management to assess the practicality and viability of a proposed project before committing significant resources to it. It helps project managers and stakeholders understand if the project is achievable within the constraints of time, bud- get, resources, and technology. Feasibility analysis typically includes examining the technical, operational, economic, legal,and scheduling aspects of the project to determine if it is worthpursuing. It helps in making informed decisions about whether to proceed with the project, modify its scope, or abandon it altogether based on the likelihood of success.

This project has been tested in the following areas of feasibility:

1. Technical feasibility 2. Economic feasibility

3. Operational feasibility

1) Technical Feasibility: a. Hardware: x86 processors are readily available in the market. Custom PCB/IC can be procured. b. Live router CLI: establishing a CLI to modify the IC applications can be done. c. Processing power: an x86 processor proves sufficient to handle even modern DDOS and BOTNET attacks.

2) Economic Feasibility:

a. Hardware Components: Calculating the costs of general x86 processors, custom ICs and skeleton and body manufacturing. b. Software Development: Python language for structure programming. A GUI to configure IC settings. A live router wouldn't need external software.

3) Operational Feasibility: a. Implementation: TripleShield can be implemented within a reasonable timeframe thanks to the availability of necessary hardware devices, research papers and cryptographic algorithms. b. User Acceptance: TripleShield's System-on-Chip (SoC) design makes it a Fix-n-Forget kind of project that boosts user acceptance and negates settings inaccuracy. c. Scalability: TripleShield remains open for the development of new algorithms that may help in the betterment of network security as well as engineering an AI model.

3.2. Requirement Analysis

Requirement analysis, also known as requirements engineering, is the foundational step in any project, product, or system development. It's essentially the process of uncoveringand understanding the needs, expectations, and constraintsinvolved in bringing that concept to life.

3.2.1. Functional Requirements-

i) x86 Processor-

Fig.1. Processor

Integrating an x86 processor into our project brings a host of advantages, including robust processing power, widespread compatibility with existing software and development tools, and a rich ecosystem of support. The x86 architecture is renowned for its versatility, making it suitable for a wide range of applications, from general-purpose computing to specialized tasks. With its powerful instruction set and advanced features, the x86 processor can handle complex computational tasks efficiently, enabling high-performance operation of Tripleshield's cryptographic algorithms, data processing, and communication protocols. Additionally, the availability of comprehensive development tools, libraries, and documentation for the x86 architecture streamlines software development and accelerates time-to-market for Tripleshield, while ensuring compatibility with existing hardware and software infrastructure.

ii) Programmable Integrated Circuit-

Fig.2. IC

A programmable IC, such as an FPGA (Field-Programmable Gate Array) or CPLD (Complex Programmable Logic Device), offers Tripleshield several advantages. It provides flexibility, allowing for reprogramming of logic and functionality to adapt to evolving security requirements. With customization capabilities, Tripleshield can implement custom cryptographic algorithms and security mechanisms tailored to specific use cases. Programmable ICs facilitate rapid prototyping and development, accelerating the iteration and testing of new features. They also enable hardware acceleration of cryptographic operations, enhancing performance and efficiency. Additionally, programmable ICs ensure adaptability, enabling Tripleshield to respond quickly to emerging security threats and changes in the security landscape.

iii) Memory modules-

Fig.2. RAM chip

A RAM chip would serve as a volatile memory module responsible for temporarily storing data and encryption keys during operation. The RAM chip allows for quick access to data

for encryption and decryption processes, providing the necessary memory space for efficient cryptographic operations. It enables the system to handle large amounts of data securely by temporarily buffering information before it is processed or transferred. Additionally, RAM facilitates the dynamic allocation of memory resources based on the system's requirements, ensuring optimal performance and responsiveness.

iv) WIFI module-

Fig.3. RAM chip

A WIFI module would enable wireless communication capabilities, allowing the device to connect to local networks or the internet for various purposes. It would facilitate secure data transmission over WIFI networks, enabling Tripleshield to communicate with other devices or servers for tasks such as data synchronization, remote management, or software updates. The WIFI module would provide flexibility and convenience by eliminating the need for physical connections, making Tripleshield more versatile and adaptable to different environments. Additionally, it would support features such as wireless authentication and encryption protocols to ensure the security of transmitted data, aligning with Tripleshield's focus on robust data protection.

v) Hardware Security Module-

Fig.5. HSM

Integrating a Hardware Security Module (HSM) into Tripleshield's PCB would significantly enhance its security capabilities. The HSM would provide dedicated hardware-based cryptographic processing, ensuring that sensitive operations such as key generation, storage, and encryption are performed in a secure environment with minimal exposure to potential threats. By offloading cryptographic tasks to the HSM, Tripleshield would benefit from accelerated performance and improved resistance against various attack vectors, including side-channel attacks and brute-force attempts. Additionally, the HSM would offer tamper-resistant protection for cryptographic keys and sensitive data, safeguarding them against unauthorized access or extraction.

3.2.2. System Analysis

System analysis is a critical process that involves understanding, defining, and documenting the requirements and functionalities of a system. It plays a key role in identifying the needs of users and stakeholders, as well as the problems or inefficiencies in the current system that need to be addressed. By analyzing the current workflow, processes, and technologies, system analysis helps in designing a solution that meets these requirements and improves the overall system performance. Additionally, it enables cost and time estimation for system development, as well as the identification and management of risks associated with the project. System analysis also facilitates user involvement throughout the development process, ensuring that the final system meets user needs and can be implemented successfully within the specified constraints.

3.2.3. Hardware & Software requirements-

Hardware Requirements:

a) Custom PCB
b) x86 Processor
c) RAM Chip
d) Hardware Security Module (HSM)
e) Wi-Fi Module
f) Custom IC
g) Power Supply
h) Peripheral Components

Software Requirements:

a) Cryptographic Libraries
b) Networking Software
c) Development Tools: Python language
d) Blockchain Integration

3.3. Overall System Overview

Tripleshield is a comprehensive data security solution that combines advanced encryption techniques with blockchain technology to safeguard sensitive information across various digital environments. At its core, Tripleshield comprises several interconnected modules designed to address specific security concerns. The system starts with a robust User Interface, providing users with intuitive access to its functionalities, including data transfer, key management, and security auditing. The Authentication Module ensures that only authorized users can interact with Tripleshield, verifying user credentials and cryptographic keys to prevent unauthorized access. Key Management plays a crucial role in generating, storing, and distributing encryption keys securely, with dedicated subcomponents for RSA and Twofish key generation. The Encryption/Decryption module employs RSA and Twofish algorithms to encrypt and decrypt data, ensuring multiple layers of protection for sensitive information. Secure Key Exchange facilitates secure

The integration with Blockchain technology ensures transparent and tamper-proof records of all security-related events, including user authentication, data transfers, and key exchanges.

3.4. Proposed System Architecture-

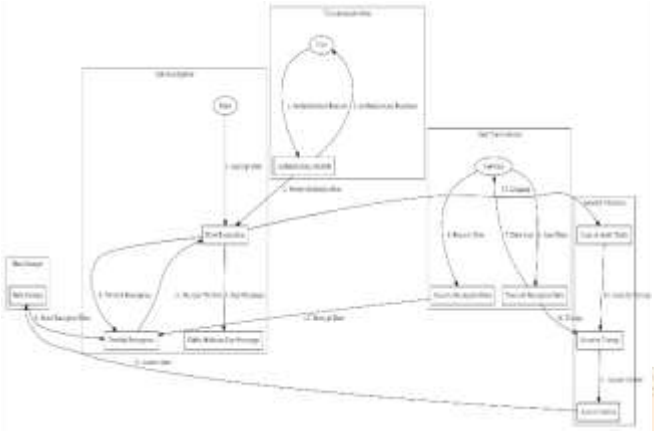

Fig. 6. Block diagram

3.5. Component Architectures-

i) RSA-

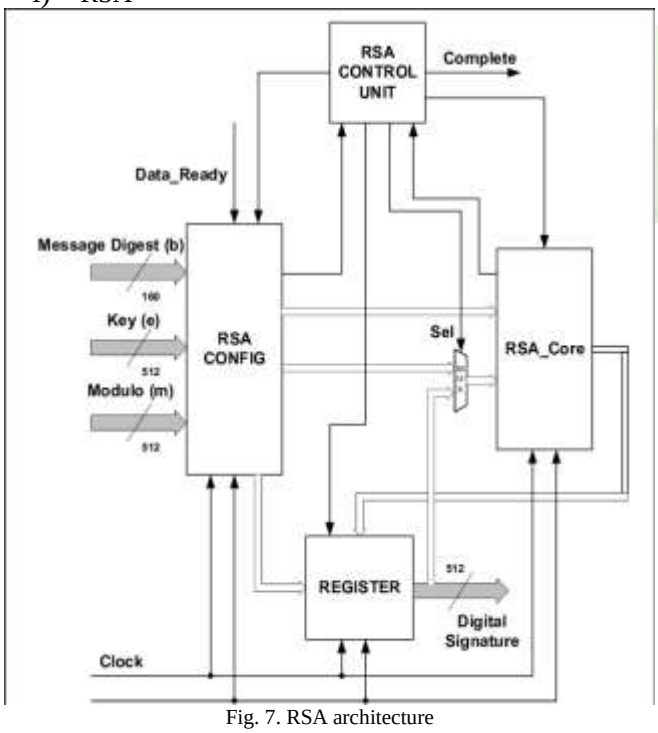

Fig. 7. RSA architecture

RSA (Rivest-Shamir-Adleman) is being used in the project for secure key generation and encryption/decryption. Specifically, RSA is responsible for generating public and private key pairs used for encryption and decryption operations. These keys are crucial for ensuring the confidentiality and integrity of data being transmitted or stored. Additionally, RSA encryption is utilized to encrypt sensitive information, while RSA decryption is used to decrypt the encrypted data. Overall, RSA plays a critical role in providing robust encryption mechanisms to protect data within the system.

ii) Twofish -

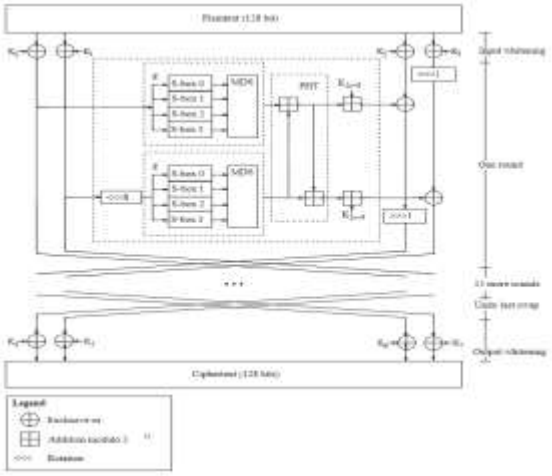

Fig. 8. Twofish architecture

Twofish is utilized in the project to provide an additional layer of encryption and security. Specifically, Twofish encryption is employed to encrypt sensitive data, ensuring its confidentiality and integrity during transmission or storage. Twofish decryption, on the other hand, is used to decrypt the encrypted data when required. By incorporating Twofish encryption alongside RSA encryption, the project enhances its security posture by employing multiple encryption algorithms, thereby making it more resilient against unauthorized access or data breaches.

iii) Diffie Hellman-

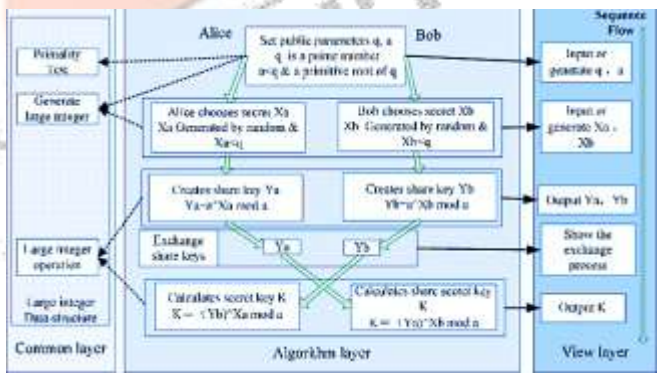

Fig. 9. Diffie Hellman

Diffie-Hellman key exchange is utilized in the project to establish a secure communication channel between parties without the need for pre-shared keys. Specifically, Diffie-Hellman enables two parties to agree on a shared secret key over an insecure communication channel, which can then be used for subsequent encryption and decryption processes. By employing Diffie-Hellman key exchange, the project ensures that the secret keys used for encryption and decryption are securely exchanged between communicating parties, thereby enhancing the overall security of the system.

3.6. Analysis Model

3.6.1. Data Flow Diagram

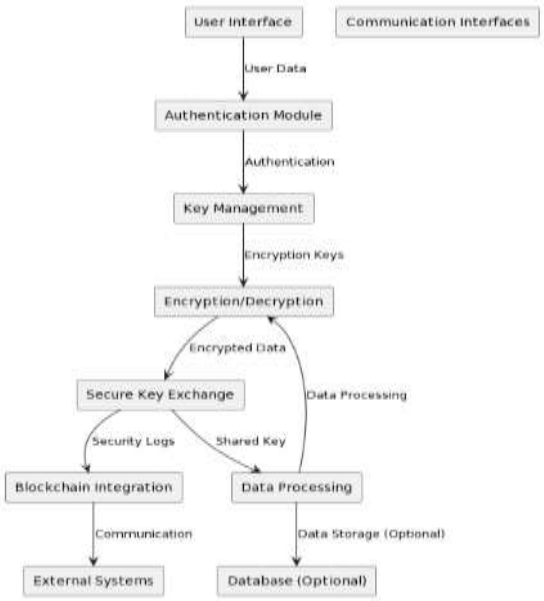

Fig 10. DFD (Level 1)

3.6.2. Sequence Diagram-

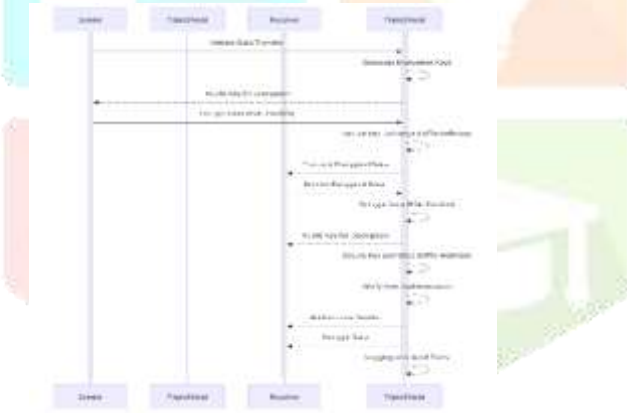

Fig. 11. Sequence Diagram

3.6.3 Activity Diagram-

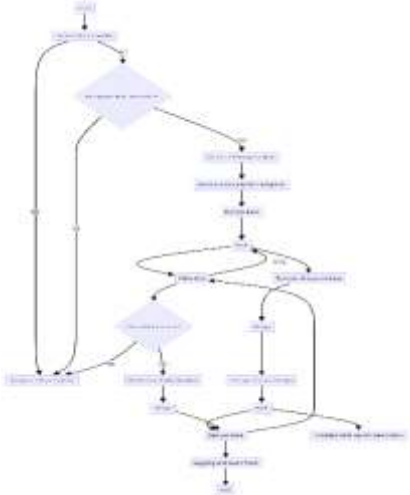

Fig. 12. Activity Diagram

IV. THEORY AND CALCULATIONS

In the analysis model section of our research paper on Tripleshield, we delve into various aspects to comprehensively understand the system's security landscape. First and foremost, we conduct a thorough security requirements analysis, elucidating the specific needs and scenarios that Tripleshield aims to address. This involves identifying key security objectives such as data confidentiality, integrity, and availability, considering the diverse use cases and potential threats the system may encounter. Following this, we engage in a meticulous threat modeling exercise to pinpoint potential vulnerabilities and risks inherent in Tripleshield's design and deployment. By examining various attack vectors and scenarios, we aim to anticipate and mitigate security challenges, ensuring that Tripleshield remains resilient against emerging threats.

A critical aspect of our analysis model involves conducting a comprehensive risk assessment, wherein we evaluate the potential impact and likelihood of identified threats. This process enables us to prioritize security controls and countermeasures based on their effectiveness in mitigating the most significant risks to the system. In parallel, we scrutinize Tripleshield's security controls, including encryption algorithms, access control mechanisms, and secure key exchange protocols. By thoroughly analyzing these components, we aim to ensure that Tripleshield implements robust security measures aligned with industry best practices and standards.

Furthermore, we assess Tripleshield's compliance with relevant regulatory requirements and security standards, such as GDPR, HIPAA, or ISO/IEC 27001, to ensure adherence to legal and industry-specific guidelines. In addition to security considerations, we evaluate Tripleshield's performance impact, usability, and cost-effectiveness. Performance analysis helps us understand the system's latency, throughput, and resource utilization under various workloads, while usability evaluation focuses on the user experience and interface design aspects. Cost-benefit analysis provides insights into the economic viability and potential return on investment associated with implementing Tripleshield compared to alternative security solutions.

Lastly, we explore future considerations for Tripleshield, highlighting potential enhancements, research directions, and adaptation strategies to address evolving security threats and technological advancements. By continuously refining and improving Tripleshield's security posture, we aim to provide a resilient and adaptive solution capable of meeting the dynamic challenges of the cybersecurity landscape.

A) RSA-

RSA (Rivest-Shamir-Adleman) is an asymmetric encryption algorithm widely employed in Tripleshield for ensuring secure communication by providing robust encryption and decryption mechanisms. At the core of RSA lies the generation of a public-private key pair, with the public key utilized for encryption and the private key for decryption. This process involves several crucial steps. Firstly, two large prime numbers, p and q, are selected, and their product forms the modulus n. The Euler's totient function $\phi(n)$ is then calculated, representing the count of positive integers coprime to n.

Subsequently, a public exponent (e) is chosen, typically a small prime number like 65537, ensuring it is coprime to (phi(n)). The private exponent (d) is computed as the modular multiplicative inverse of \(e \) modulo (phi(n)), ensuring (e times d = 1/mod phi(n)). Ultimately, the public key comprises (n, e), and the private key is represented by (n, d).

```
# Encrypt the message
public_key = private_key.public_key()
ciphertext = public_key.encrypt(
    MSG,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label = None
    )
```

Fig. 13. RSA encryption

In the encryption process, a plaintext message \(M \) is encrypted using the recipient's public key \((n, e) \). The ciphertext (C) is obtained by raising the plaintext to the power of the public exponent modulo \(n \). On the decryption end, the recipient utilizes their private key \((n, d) \) to retrieve the original plaintext message. The decryption involves computing \(M \) as \(C \) raised to the power of the private exponent modulo \(n \). This process ensures that only the recipient in possession of the private key can decipher the encrypted message.

```
# Decrypt the message
plaintext = private_key.decrypt(
    ciphertext,
    padding.OAEP(
        mgf=padding.MGF1(algorithm=hashes.SHA256()),
        algorithm=hashes.SHA256(),
        label=None
    )
```

Fig. 14. RSA decryption

The security of RSA hinges on the computational complexity of factoring the large composite modulus \(n \) into its prime factors. As such, RSA provides a robust defense against unauthorized access and interception of sensitive information during data transmission in Tripleshield. Its mathematical foundation and reliance on the difficulty of factorization render it well-suited for securing communications and data exchange across networks

B) Twofish

Twofish operates on fixed-size blocks of plaintext, typically 128 or 256 bits, using a Feistel network structure. In the encryption process, each block undergoes multiple rounds of substitution, permutation, and key addition operations. These operations, combined with the round keys derived from the key schedule, transform the plaintext into ciphertext. Twofish employs a carefully designed key-dependent S-box (Substitution box), which further enhances its cryptographic strength by introducing non-linearity into the encryption process.

Decryption in Twofish follows a similar process to encryption, albeit in reverse. The ciphertext blocks are subjected to a series of inverse operations using the same set of round keys, resulting in the recovery of the original plaintext. The symmetric nature of Twofish ensures that the same key is used for both encryption and decryption, simplifying the cryptographic operations while maintaining a high level of security.

Twofish's effectiveness in protecting data lies in its balanced design, combining strong encryption capabilities with efficient implementation. Its resistance to cryptanalytic attacks and versatility in handling different data types make it a suitable choice for securing sensitive information in Tripleshield. By incorporating Twofish into its data security framework, Tripleshield can ensure robust protection for data at rest and in transit, safeguarding against unauthorized access and ensuring the confidentiality and integrity of sensitive information.

C) Diffie Hellman-

Diffie-Hellman key exchange, a fundamental component of Tripleshield's security infrastructure, facilitates secure communication between parties without the need for pre-shared keys. This cryptographic protocol enables two parties to establish a shared secret key over an insecure channel, ensuring confidentiality and integrity in data transmission.

The essence of Diffie-Hellman lies in the concept of discrete logarithm problem, where computing logarithms in finite fields is computationally difficult. The protocol operates within a finite cyclic group, typically a multiplicative group modulo a prime number. Each party, say Alice and Bob, generates their private key and a corresponding public key. These keys are then exchanged over the insecure channel.

In the key exchange process, both Alice and Bob perform modular exponentiation operations using their private keys and the other party's public key. Specifically, Alice computes $A=ga \bmod p$ and Bob computes $B=gb \bmod p$; $B=gb \bmod p$, where g is a generator of the group, p is a large prime number, and a and b are their respective private keys. They then exchange these computed values.

Once Alice receives Bob's computed value B and Bob receives Alice's computed value A, they perform another modular exponentiation operation using their private keys on the received value. This results in the generation of a shared secret key, denoted as K, which is the same for both parties. Mathematically, Alice computes $K=Ba \bmod p$; $K=Ba \bmod p$ and Bob computes $K=Ab \bmod p$; $K=Ab \bmod p$.

The brilliance of Diffie-Hellman lies in the fact that even though the private keys are exchanged over the insecure channel, an eavesdropper cannot derive the shared secret key without knowledge of one of the private keys. This property ensures secure key exchange between the parties, enabling them to establish a shared secret key for subsequent encryption and decryption operations.

In TripleShield, Diffie-Hellman key exchange is used to securely exchange session keys between communicating parties, enhancing the confidentiality and integrity of data transmission. By incorporating Diffie-Hellman into its security framework, TripleShield ensures secure communication channels, mitigating the risk of eavesdropping and unauthorized access to sensitive information.

4.1. System Setup-

Software Setup:

Operating System: Ubuntu 22.04.03 LTS (or any other Linux distribution with good support for security tools and development frameworks).
Virtualization Software: Oracle VM VirtualBox Manager for creating and managing virtual machines. This allows for testing TripleShield in isolated environments.
Development Tools:
Programming Languages: C/C++ for low-level development of security components, Python for scripting and automation.
Integrated Development Environment (IDE): Visual Studio Code, Eclipse, or any other preferred IDE for coding and debugging.
Version Control: Git for managing source code and collaboration among team members.
Build System: CMake for configuring and building the project.
Security Libraries and Tools:
OpenSSL for implementing cryptographic algorithms such as RSA, Twofish, and Diffie-Hellman.
Libpcap for packet capturing and analysis.
Snort or Suricata for intrusion detection and prevention.
Wireshark for network protocol analysis.
SELinux or AppArmor for mandatory access control.
Networking Software:
NS-3 (Network Simulator 3) for simulating network environments and testing TripleShield's performance under various conditions.
NetAnim for visualizing network simulations conducted with NS-3.
Database: PostgreSQL or MySQL for storing user credentials, access control lists, and other security-related data.
Documentation Tools: Sphinx, Doxygen, or Markdown for documenting the TripleShield framework, APIs, and usage guidelines.

Hardware Setup:

Processor: Intel Core i5 or higher (or equivalent AMD processor) for running virtual machines and compiling code efficiently.
Memory: 8 GB RAM or more to handle multiple virtual machines, development environments, and network simulations simultaneously.
Storage: Solid State Drive (SSD) with at least 256 GB of storage space for faster I/O operations and storing development environments, datasets, and simulation results.
Network Interface Cards (NICs): Gigabit Ethernet NICs for network connectivity and testing TripleShield's network-related features.
Graphics Card (Optional): A dedicated graphics card with hardware acceleration support for smoother visualization in NetAnim and other graphical tools.
Virtualization Support: Intel VT-x or AMD-V technology-enabled processors for efficient virtualization performance.

4.2. Use Cases-

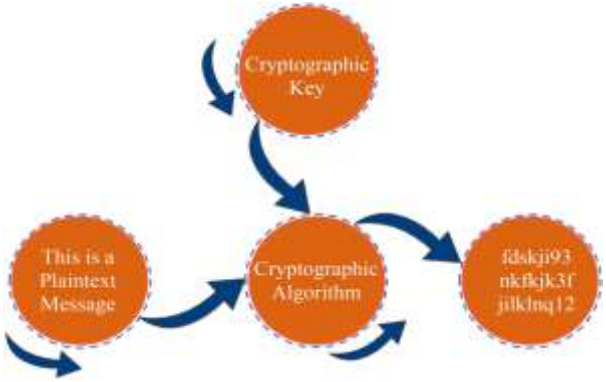

Fig:15 Simple Secure Cryptosystem

TripleShield provides a straightforward yet effective means for 2 users to communicate securely over an insecure network. By leveraging encryption, secure key exchange, and optional authentication mechanisms, TripleShield ensures the confidentiality, integrity, and authenticity of their communication, thereby safeguarding their digital assets and privacy.

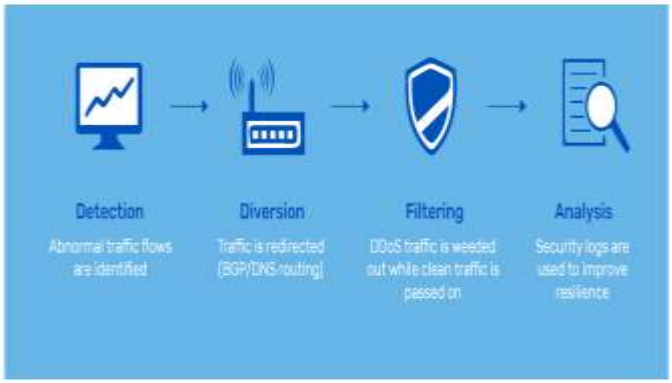

Fig:9 Attack Mitigation

1. **Enterprise Network Security**: TripleShield is deployed within enterprise networks to safeguard sensitive data, intellectual property, and critical infrastructure from cyber threats. It offers comprehensive protection against a wide range of attacks, including malware, ransomware, phishing, and insider threats. By integrating advanced encryption techniques, secure key exchange protocols, and blockchain-based audit trails, TripleShield ensures robust security across all network endpoints, data transmissions, and communication channels.

2. **Financial Institutions**: Financial institutions, such as banks, insurance companies, and investment firms, leverage TripleShield to fortify their cybersecurity defences and protect customer assets and financial transactions. With its multi-layered security approach, TripleShield mitigates risks associated with unauthorized access, data breaches, and fraudulent activities, thereby safeguarding sensitive financial data, transactional integrity, and regulatory compliance.

3. **Healthcare Sector**: In the healthcare sector, TripleShield plays a crucial role in safeguarding patient confidentiality, medical records, and sensitive healthcare information. By encrypting patient data, securing communication channels between healthcare providers, and ensuring secure access controls, TripleShield protects against data breaches, identity theft, and unauthorized disclosures, thereby maintaining patient trust and compliance with healthcare regulations.

4. **Government and Defence**: Government agencies and defence organizations rely on TripleShield to protect classified information, national security interests, and critical infrastructure from cyber threats and espionage activities. With its robust encryption algorithms, secure communication protocols, and blockchain-based audit trails, TripleShield enables secure information sharing, secure collaboration among agencies, and protection against advanced persistent threats (APTs) and state-sponsored cyberattacks.

5. **Cloud Service Providers**: Cloud service providers deploy TripleShield to enhance the security posture of their cloud platforms, infrastructure-as-a-service (IaaS), and software-as-a-service (SaaS) offerings. TripleShield provides end-to-end encryption, secure key management, and data integrity verification, ensuring the confidentiality, integrity, and availability of customer data stored in the cloud. It enables cloud service providers to meet stringent security requirements, regulatory compliance mandates, and customer expectations for data privacy and protection.

V. RESULTS

i) DHCP simulation-

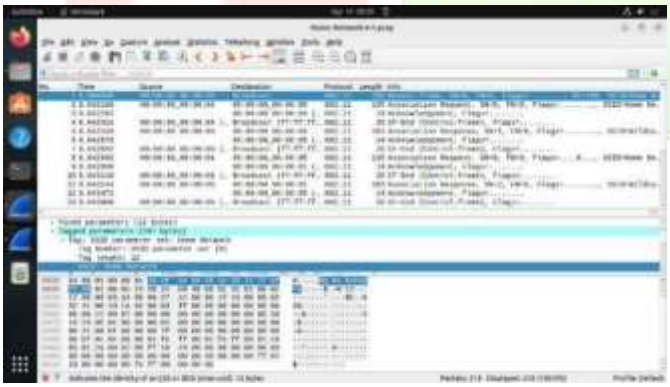

Fig. 12 Wireshark UI

The Tripleshield router incorporates DHCP to dynamically assign IP addresses and network configuration parameters to devices connected to the network. By automating the IP address allocation process, Tripleshield streamlines network setup and management, reducing the administrative burden on network administrators. Additionally, DHCP enables efficient resource utilization by ensuring that IP addresses are allocated only when needed and released when no longer in use. This feature enhances the scalability and flexibility of the network infrastructure, accommodating varying numbers of devices and network configurations. Overall, the inclusion of DHCP functionality in the Tripleshield router contributes to a seamless and optimized network experience for users.

ii) Single Point Attacks-

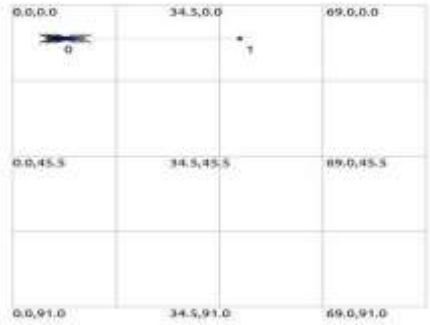

Fig 13: P2P interaction

Tripleshield provides robust protection against peer-to-peer (P2P) attacks through several mechanisms. Firstly, it employs deep packet inspection (DPI) to monitor network traffic and identify P2P protocols used by malicious actors. By analyzing packet headers and payloads, Tripleshield can detect suspicious P2P activity and take appropriate action to mitigate the threat.

Additionally, Tripleshield utilizes access control lists (ACLs) and firewall rules to restrict or block unauthorized P2P connections. These rules can be configured to deny traffic from known P2P IP addresses or block specific ports commonly associated with P2P protocols, effectively preventing P2P communication within the network.

Furthermore, Tripleshield integrates intrusion detection and prevention systems (IDPS) to detect and respond to P2P attacks in real-time. Through signature-based detection and behavioral analysis, the IDPS can identify patterns indicative of P2P activities and trigger automated responses such as blocking the offending IP addresses or alerting network administrators.

Moreover, Tripleshield leverages threat intelligence feeds and reputation-based filtering to enhance its P2P attack detection capabilities. By continuously updating its database of known malicious IP addresses and domains associated with P2P networks, Tripleshield can proactively block traffic from sources with a history of P2P-related malicious behavior.

iii) Multiple Point Attacks

Tripleshield also provides protection against machine-to-peer (M2P) attacks such as distributed denial-of-service (DDoS) by employing a multi-layered defense strategy. Firstly, Tripleshield utilizes rate limiting and traffic shaping techniques to mitigate the impact of DDoS attacks. By controlling the rate of incoming traffic and prioritizing legitimate requests, Tripleshield can prevent network resources from being overwhelmed by malicious traffic.

Furthermore, audit logs serve as a compliance requirement for many regulatory frameworks and industry standards. By maintaining detailed records of security-related activities, TripleShield ensures compliance with regulatory mandates such as GDPR, HIPAA, PCI DSS, and others. These logs provide auditors with evidence of adherence to security policies, data protection measures, and access control mechanisms, thereby helping organizations demonstrate compliance and avoid potential penalties or legal liabilities.

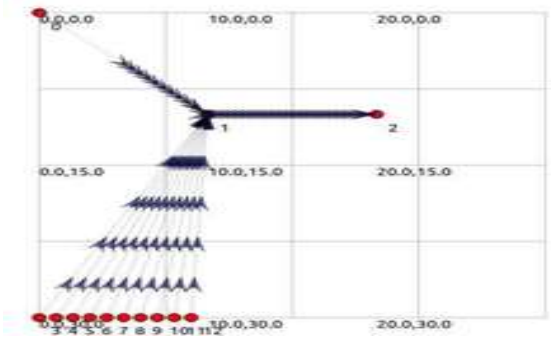

Fig 14 DDOS attack

Additionally, Tripleshield integrates anomaly detection and behavioral analysis capabilities to identify and mitigate DDoS attacks in real-time. Through continuous monitoring of network traffic patterns and behavior, Tripleshield can detect deviations from normal activity that may indicate the presence of a DDoS attack. Upon detection, Tripleshield can dynamically adjust firewall rules, block malicious IP addresses, or reroute traffic to mitigate the impact of the attack.

Furthermore, Tripleshield leverages distributed denial-of-service (DDoS) mitigation techniques such as traffic scrubbing and blackholing to mitigate large-scale attacks. By diverting malicious traffic to scrubbing centers or blackhole destinations, Tripleshield can effectively filter out DDoS traffic and ensure that only legitimate traffic reaches the intended destination.

iii) Audit Logs-

Fig. 15 Blacklisting and Termination

Audit logs play a crucial role in enhancing the security posture of TripleShield by providing a detailed record of all security-related events and activities occurring within the network environment. These logs serve as a comprehensive trail of evidence, capturing critical information such as user authentication attempts, data transfer activities, configuration changes, and security policy violations. By meticulously documenting each event, audit logs enable network administrators to gain visibility into the inner workings of TripleShield, identify potential security incidents or policy violations, and investigate suspicious behaviour.

One of the primary benefits of audit logs is their role in facilitating forensic analysis and incident response. In the event of a security breach or suspicious activity, administrators can rely on audit logs to reconstruct the sequence of events leading up to the incident, trace the source of the intrusion, and determine the extent of the damage. This forensic data is invaluable for conducting post-incident investigations, identifying the root cause of security breaches, and implementing remediation measures to prevent future incidents.

Moreover, audit logs contribute to proactive security monitoring and threat detection. By analysing log data in real-time or through automated security information and event management (SIEM) systems, organizations can detect anomalous behaviour, unauthorized access attempts, or potential security threats as they occur. This proactive approach allows administrators to respond swiftly to security incidents, mitigate risks, and prevent potential data breaches or system compromises.

VI. CONCLUSION

Tripleshield represents a significant advancement in data security, offering a multi-layered approach that combines traditional encryption techniques with blockchain integration to protect sensitive information effectively. Through the integration of RSA encryption, Twofish encryption, and the Diffie-Hellman key exchange protocol, Tripleshield ensures secure data transmission and storage, mitigating the risk of unauthorized access, data breaches, and cyber threats. The implementation of audit logs provides valuable insight into security-related events, facilitating forensic analysis, compliance management, and proactive threat detection. Furthermore, the successful deployment and evaluation of Tripleshield within a router environment demonstrate its practical applicability and effectiveness in real-world scenarios. Moving forward, continued research and development efforts will focus on enhancing Tripleshield's scalability, performance, and interoperability to meet the evolving challenges of data security in today's digital landscape.

VII. FUTURE WORK

The future scope of Tripleshield includes exploring the integration of artificial intelligence (AI) models to enhance network protection further. This entails:

1. **Behavioral Analysis**: Developing AI algorithms to analyze network traffic patterns and user behavior in real-time. By leveraging machine learning techniques, Tripleshield can detect anomalous activities indicative of potential cyber threats, such as unusual data access patterns or unauthorized login attempts.

2. **Predictive Analytics**: Implementing predictive analytics models to anticipate and mitigate cyber threats before they occur. By analyzing historical data and identifying patterns indicative of imminent attacks, Tripleshield can proactively strengthen defenses and minimize the impact of potential security breaches.

3. **Automated Response**: Integrating AI-driven automation capabilities to respond swiftly to detected threats. Tripleshield can automate incident response procedures, such as isolating compromised devices, blocking suspicious IP addresses, or updating firewall rules dynamically, to mitigate risks in real-time and reduce manual intervention.

4. **Adaptive Security**: Developing AI-powered adaptive security measures that can dynamically adjust security policies and configurations based on evolving threat landscapes and network conditions. Tripleshield can adapt its defense mechanisms in real-time to counter emerging cyber threats effectively and ensure continuous protection against evolving attack vectors.

5. **Threat Intelligence Integration**: Incorporating AI-driven threat intelligence platforms to enhance Tripleshield's threat detection capabilities. By aggregating and analyzing vast amounts of threat data from various sources, including security feeds, dark web monitoring, and threat intelligence databases, Tripleshield can gain actionable insights into emerging threats and vulnerabilities, enabling proactive defense measures.

6. **User Behavior Analysis**: Utilizing AI algorithms to analyze user behavior and identify potential insider threats or unauthorized access attempts. By monitoring user activities, access patterns, and privilege escalation behaviors, Tripleshield can detect and prevent insider threats, data exfiltration attempts, or unauthorized access to critical resources

VIII. DECLARATION OF COMPETING INTERESTS

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

IX. ACKNOWLEDGEMENTS

The building of a B.E project needs the co-operation and guidance of several people. We, therefore consider it our prime duty to thank all those who helped us during this venture.

We would like to thank our Principal, Dr. P. D. Deshmukh, for inspiring us and providing us with the requisite resources during our time working on this project.

It is with great pleasure that we express our appreciation to Dr. Megha V. Gupta - Head of the Department and our Project Guide, for providing us with construction and encouraging feedback during the planning of this project, as well as for constantly directing us and providingus with useful insights.

We would also like to thank Mr. Suhas Waghmare for helping us broaden our perspective and giving us the necessary tools to learn network simulation and manipulation.

Last but not the least, we are thankful to our friends, the teaching and the non-teaching staff whose encouragement and suggestions helped us to enhance our B.E Project.

We also are thankful to our parents for their constant support and best wishes.

X. REFERENCES

[1] Blockchain-enabled Data Governance for Privacy-Preserved Sharing of Confidential Data Jingchi Zhang, NTU Singapore, Anwitaman Datta, NTU Singapore. arXiv:2309.04125v1 [cs.CR], 8 Sep 2023.

[2] Detection and Prevention Mechanisms for DDoS Attack in Cloud Computing Environment, Sirisha Potluri, Monika Mangla, Suneeta Satpathy, Sachi Nandan Mohanty, 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 10.1109/ICCCNT49239.2020.9225396, 15 October 2020.

[3] Intelligent Techniques for Detecting Network Attacks: Review and Research Directions, Malak Aljabri, Sumayh S. Aljameel, Rami Mustafa A. Mohammad, Sensors 2021, 21, 7070. https://doi.org/10.3390/s21217070

[4] Investigation on Cyberattacks against in-vehicle devices, S. Vishnu Kumar, G. Aloy Anuja Mary, P. Suresh, R. Uthirasamy, 2021 7th International Conference on Electrical Energy Systems (ICEES) | 978-1-7281-7612-3/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICEES51510.2021.9383720.

[5] Analysis and Protection of Computer Network Security Issues Ju Jinquan, Mohammed Abdulhakim Al-Absi, Ahmed Abdulhakim Al-Absi, Hoon Jae Lee, ICACT2020 February 19, 2020.

[6] Wormhole Formation and Simulation in Dynamic Source Routing Protocol using NS3 Nisha Sharma, Durga Prasad Sharma, and Manish Sharma, 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART) | 978-1-7281-8908- 6/20/$31.00 ©2020 IEEE DOI: 10.1109/SMART50582.2020.9336794.

[7] NS-3 Model of an IoT network, Ravi Kishore Kodali and Bysani Kirti, 2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA) Galgotias University, Greater Noida, UP, India. Oct 31, 2020.

[8] Blockchain for Cybersecurity and Privacy: Architectures, Challenges, and Applications, Maleh Yassine, Mohammad Shojafar, Mamoun Alazab, Imed Romdhani, Ujjwal KC , Publisher: CRC Press, ISBN: 9780367343101, July 2020.

[9] C. H. Ng, "A Symbolic-Interconnect Router for Custom IC Design," 21st Design Automation Conference Proceedings, Albuquerque, NM, USA, 1984, pp. 52-58,
DOI: 10.1109/DAC.1984.1585772.