MACHINE LEARNING-DRIVEN SECURITY FRAMEWORK INTEGRATED WITH BLOCKCHAIN FOR RANSOMWARE PREVENTION AND MITIGATION IN THE BANKING SECTOR

A PROJECT REPORT

Submitted by

CHARMINE MARIA THOMAS [REGISTER NO: 211421104043]

GUNASHRI S [REGISTER NO: 211421104082]

JANANI A [REGISTER NO: 211421104101]

in partial fulfilment for the award of the Degree of

BACHELOR OF ENGINEERING

In

COMPUTER SCIENCE AND ENGINEERING

PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)

APRIL 2025

MACHINE LEARNING-DRIVEN SECURITY FRAMEWORK INTEGRATED WITH BLOCKCHAIN FOR RANSOMWARE PREVENTION AND MITIGATION IN THE BANKING SECTOR

A PROJECT REPORT

Submitted by

CHARMINE MARIA THOMAS [REGISTER NO: 211421104043]

GUNASHRI S [REGISTER NO: 211421104082]

JANANI A [REGISTER NO: 211421104101]

in partial fulfilment for the award of the Degree of

BACHELOR OF ENGINEERING

In

COMPUTER SCIENCE AND ENGINEERING

PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)

APRIL 2025

PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)

BONAFIDE CERTIFICATE

Certified that this project report **"MACHINE LEARNING-DRIVEN SECURITY FRAMEWORK INTEGRATED WITH BLOCKCHAIN FOR RANSOMWARE PREVENTION AND MITIGATION IN THE BANKING SECTOR"** is the bonafide work of **CHARMINE MARIA THOMAS [211421104043], GUNASHRI S [211421104082] and JANANI A [211421104101]"** who carried out the project work under my supervision.

Signature of the HOD

Dr.L.JABASHEELA, M.E., Ph.D.,

PROFESSOR AND HEAD OF THE DEPARTMENT,
Department of CSE,
Panimalar Engineering College,
Chennai-600 123.

Signature of the Supervisor

Dr.D.LAKSHMI, M.E., Ph.D.,

ASSOCIATE PROFESSOR,
Department of CSE,
Panimalar Engineering College,
Chennai-600 123.

Certified that the above candidate(s) were examined in the End Semester Project Viva-Voce Examination held on 03.04.2025.

INTERNAL EXAMINER **EXTERNAL EXAMINER**

DECLARATION BY THE STUDENT

We **CHARMINE MARIA THOMAS [211421104043], GUNASHRI S [211421104082] and JANANI A [211421104101]** hereby declare that this project report titled **"Machine Learning-Driven Security Framework Integrated with Blockchain for Ransomware Prevention and Mitigation in the Banking Sector"**, under the guidance of **Dr. D. LAKSHMI, M.E., Ph.D.,** is the original work done by us and we have not plagiarized or submitted to any other degree in any university by us.

CHARMINE MARIA THOMAS

GUNASHRI S

JANANI A

ACKNOWLEDGEMENT

Our profound gratitude is directed towards our esteemed Secretary and Correspondent, **Dr. P. CHINNADURAI, M.A., Ph.D**., for his fervent encouragement. His inspirational support proved instrumental in galvanizing our efforts, contributing significantly to the successful completion of this project

We express our sincere thanks to our directors **Tmt. C.VIJAYARAJESWARI**, **Dr.C.SAKTHI KUMAR, M.E., Ph.D.** and **Dr**. **SARANYASREE SAKTHI KUMAR B.E., M.B.A.,Ph.D.,** for graciously affording us the essential resources and facilities for undertaking of this project.

Our gratitude is also extended to our Principal, **Dr. K. MANI, M.E., Ph.D.,** whose facilitation proved pivotal in the successful completion of this project.

We express our heartfelt thanks to **Dr. L. JABASHEELA, M.E., Ph.D.,** Head of the Department of Computer Science and Engineering, for granting the necessary facilities that contributed to the timely and successful completion of project.

We would like to express our sincere thanks to **Dr. D. LAKSHMI, M.E., Ph.D.** and all the faculty members of the Department of CSE for their unwavering support for the successful completion of the project.

CHARMINE MARIA THOMAS

GUNASHRI S

JANANI A

PROJECT COMPLETION CERTIFICATE

Global Techno Solutions®
Solutions unlimited

01/04/2025

TO WHOMSOEVER IT MAY CONCERN

This is to certifythat the following final year B.E(Computer Science and Engineering) students of Panimalar Engineering College, Chennaihave successfully completed their project work title **"Machine Learning-Driven Security Framework Integrated with Blockchain for Ransomware Prevention and Mitigation in the Banking Sector"** during December, 2024 to March, 2025 in our organization.

Ms. Charmine Maria Thomas	**(Reg. No. 211421104043)**
Ms. Gunashri. S	**(Reg. No. 211421104082)**
Ms. Janani. A	**(Reg. No. 211421104101)**

We wish them all success for their future endeavors.

ForGlobal Techno Solutions

Global Techno Solutions ★ Chennai ★

Loganathan. D
Executive Manager

No.60/4, 11th Avenue, Ashok Nagar, Chennai - 600 083. INDIA.
Tel : +91-44-4203 3422 Email : career@globaltechnosolutions.net Web : www.globaltechnosolutions.net

ABSTRACT

Ransomware attacks are a growing concern in the banking sector, causing financial losses, data breaches, and operational disruptions. This system proposes a Machine Learning-Driven Security Framework (ML-DSF) integrated with blockchain technology to enhance ransomware detection and mitigation. It leverages the Extra-Trees Classifier to analyze patterns in executable files, detecting and preventing ransomware before encryption occurs. Additionally, a private blockchain is employed for secure, immutable data backups, ensuring recovery without the need for ransom payments. The integration of decentralized storage (IPFS) and Ethereum-based smart contracts further strengthens data security and integrity. The framework enables real-time monitoring, automated threat detection, and efficient incident response, reducing the risk of cyberattacks. Experimental results validate the effectiveness of the approach, achieving high accuracy in ransomware classification. By combining advanced machine learning techniques with blockchain's tamper-proof security, this system provides a scalable and proactive defense mechanism. It ensures the resilience of banking environments, safeguarding sensitive financial data and minimizing disruptions caused by ransomware threats.

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ML-DSF	-	Machine Learning-Driven Security Framework
RaaS	-	Ransomware-as-a-Service
MVC	-	Model-view-controller
dApps	-	Decentralized Applications
DeFi	-	Decentralized Finance
IPFS	-	Interplanetary File System
PE	-	Portable Executable
SHA-256	-	Secure Hash Algorithm-256
ETH	-	Ether
API	-	Application Programming Interface
P2P	-	Peer-to-Peer
CID	-	Content Identifiers
DOM	-	Document Object Model

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

CHAPTER 1
INTRODUCTION

Ransomware attacks have become a major cybersecurity threat, particularly in the banking sector, where financial institutions handle sensitive data and large-scale transactions. A ransomware attack involves malicious software encrypting an organization's critical files, demanding ransom payments to restore access. This can cause severe financial losses, data breaches, and operational disruptions. The banking sector is a prime target due to its reliance on digital systems, making it vulnerable to Ransomware-as-a-Service (RaaS) and double extortion tactics, where attackers threaten to leak stolen data even after receiving payment.

Recent ransomware incidents highlight the growing threat. In 2023, a major financial institution faced a crippling attack, disrupting online transactions and exposing customer data. Similarly, the Clop ransomware group targeted global banks, demanding millions in cryptocurrency. These incidents emphasize the need for proactive security solutions beyond traditional antivirus programs.

Our Machine Learning-Driven Security Framework (ML-DSF) integrates blockchain technology with machine learning for real-time ransomware detection and mitigation. The system employs the Extra-Trees Classifier to analyze executable files, detecting threats before encryption occurs. A private blockchain ensures tamper-proof backups, reducing reliance on ransom payments.

Our system leverages advanced technologies to enhance banking cybersecurity, integrating decentralized storage, blockchain security, and machine learning-based threat detection. IPFS (InterPlanetary File System) ensures secure, decentralized file storage, reducing the risk of data loss or unauthorized access. Blockchain and Ethereum provide immutable transaction records, ensuring transparency and

security in financial operations. Smart contracts, deployed using Ganache and MetaMask, automate secure transactions, reducing vulnerabilities in banking systems.

To combat ransomware threats, our framework utilizes the Honeypot Dataset, which collects real-world ransomware samples. These datasets train a machine learning model to detect and prevent potential cyber threats before they cause damage.

1.1. OVERVIEW

The Machine Learning-Driven Security Framework (ML-DSF) integrated with Blockchain enhances ransomware prevention in banking. It detects ransomware in real-time using Extra-Trees Classifier and ensures tamper-proof backups via IPFS and Ganache blockchain. Smart contracts enable secure transactions, preventing ransom payments. The system provides real-time monitoring, secure file recovery, and attack simulation for improved cybersecurity. By combining machine learning and blockchain, it offers proactive threat mitigation, data integrity, and resilience, making it a scalable and robust cybersecurity solution.

1.2. PROBLEM DEFINITION

The banking sector is highly vulnerable to ransomware attacks, which lead to financial losses, operational disruptions, and data breaches. Traditional security solutions fail to detect advanced threats like Ransomware-as-a-Service (RaaS) and double extortion tactics. Cybercriminals exploit phishing, unpatched vulnerabilities, and weak security policies to infiltrate systems. Existing backup mechanisms are centralized and prone to tampering, increasing reliance on ransom payments. Hence, a robust, intelligent, and decentralized solution is required to ensure real-time threat detection, secure data storage, and reliable recovery without ransom payments.

CHAPTER 2
LITERATURE REVIEW

CHAPTER 2
LITERATURE REVIEW

"BSFR-SH: Blockchain-Enabled Security Framework Against Ransomware Attacks for Smart Healthcare" – **M. Wazid, A. Kumar Das, S. Shetty** [1]. This study proposes BSFR-SH, a blockchain-driven security model designed to detect and mitigate ransomware attacks targeting smart healthcare systems. The framework ensures secure and tamper-proof data storage by leveraging blockchain's immutability and decentralization, reducing the risk of data loss or unauthorized modifications. It also employs machine learning algorithms to analyze ransomware behavior, enabling proactive threat detection. **Advantage:** Provides enhanced data security, prevents unauthorized access, and improves ransomware detection accuracy through real-time blockchain integration. **Disadvantage:** The high cost of integrating blockchain with existing healthcare infrastructures makes implementation complex, especially for legacy systems.

"AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking" – **Suri Babu Nuthalapati** [2]. This paper introduces an AI-driven cybersecurity solution for digital banking that focuses on fraud detection and loan prediction. It employs machine learning models such as Random Forest and Support Vector Machines (SVM), achieving 92% accuracy in loan approvals and 90% in fraud detection. The system continuously trains on real-time transaction data, enhancing security through adaptive learning. **Advantage:** Improves fraud detection by identifying suspicious transactions with high accuracy, thereby reducing financial losses in digital banking. **Disadvantage:** The reliability of AI-based fraud detection

depends on the quality of training data, which, if biased or incomplete, may lead to incorrect classifications and increased false positives.

"A Systematic Literature Review on Blockchain-Based Cybersecurity Models for Ransomware Mitigation" – **Ade Ilham Fajri, Mohammad Isa Irawan** [3]. This research systematically reviews blockchain-based models aimed at mitigating ransomware threats. It examines decentralization, smart contracts, and immutable ledgers to assess their effectiveness in cybersecurity. The study compares existing blockchain models, highlighting their strengths and potential integration challenges. Future research directions are suggested to optimize blockchain security frameworks. **Advantage:** Provides an extensive evaluation of blockchain solutions for cybersecurity, offering insights into best practices and future trends. **Disadvantage:** Lacks experimental validation, as the study relies solely on a literature review without empirical testing in real-world cybersecurity environments.

"A Bayesian Attack-Network Modeling Approach to Mitigating Malware-Based Banking Cyberattacks" – **Aaron Zimba** [4]. This study introduces a Bayesian Attack Network model to assess and mitigate banking cyber threats, particularly malware such as the GameOver Zeus virus. It utilizes conditional probability assignments and dynamic adaptation techniques to predict vulnerabilities within banking systems. The research demonstrates how probability density curves can be used to evaluate exploitability and financial risks. **Advantage:** Provides structured probabilistic modeling, allowing financial institutions to visualize attack paths and take preventive security measures. **Disadvantage:** The model's accuracy is dependent on CVSS (Common Vulnerability Scoring System) scores, which may

not always reflect emerging real-time threats, potentially leading to underestimation of risks.

"SFMR-SH: Secure Framework for Mitigating Ransomware Attacks in Smart Healthcare Using Blockchain Technology" – **J. Alenizi, I. Alrashdi** [5]. This paper introduces SFMR-SH, a blockchain- and IoT-integrated framework for mitigating ransomware attacks in healthcare. It utilizes machine learning algorithms such as KNN, SVM, Random Forest, and Gradient Boosting, achieving a high accuracy of 99.33%. Blockchain ensures secure and immutable storage of patient data, while IoT devices facilitate real-time monitoring. **Advantage:** Enhances cybersecurity in healthcare by enabling real-time threat detection, secure data logging, and improved response mechanisms. **Disadvantage:** The system demands high computational resources, making implementation difficult for institutions with limited technical infrastructure and expertise.

"Evolution, Mitigation, and Prevention of Ransomware" – **I.A. Chesti, M. Humayun, N. U. Sama, N. Jhanjhi** [6]. This study explores the evolution of ransomware from its early forms in the 1980s to the modern era of cryptocurrency-driven ransom payments. It examines various ransomware attack techniques, including phishing, trojans, and double extortion. The paper also reviews mitigation strategies such as email security protocols, trusted download mechanisms, and proactive system updates. **Advantage:** Provides practical and widely applicable preventive measures to safeguard organizations and individuals from ransomware threats. **Disadvantage:** The study primarily focuses on preventative measures rather

than recovery mechanisms, leaving a gap in addressing post-attack mitigation strategies.

"Cyber Threats Classifications and Countermeasures in Banking and Financial Sector" – **A.A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi, S. A. Ebad** [7]. This paper categorizes various cyber threats faced by the banking sector, ranking them based on severity and financial impact. It examines advanced threat detection techniques, regulatory measures, and machine learning-based anomaly detection models. The study emphasizes the need for continuous adaptation to evolving cyber threats. **Advantage:** Strengthens cybersecurity in financial institutions by systematically classifying threats and recommending targeted mitigation strategies. **Disadvantage:** The rapid evolution of cyber threats makes it challenging to maintain up-to-date defense mechanisms, requiring continuous research and investment.

"Machine Learning Algorithms and Frameworks in Ransomware Detection" – **D. Smith, S. Khorsandroo, K. Roy** [8]. This research investigates various machine learning techniques for ransomware detection, including Decision Trees, Random Forest, Long Short-Term Memory (LSTM), and Naïve Bayes. It analyzes attack methods used by prominent ransomware strains such as Ransom32 and RAA. **Advantage:** Provides a detailed comparison of different ML models, offering insights into their strengths and weaknesses in ransomware detection. **Disadvantage:** Some ML models exhibit high false positive rates, which can lead to unnecessary system disruptions and inefficiencies in real-world cybersecurity applications.

"Ransomware Prevention and Mitigation Strategies" – Sandeep Reddy Gudimetla [9]. This study analyzes 24 ransomware prevention approaches, including behavior-based detection, API call monitoring, and network traffic analysis. It also evaluates case studies such as the infamous WannaCry ransomware attack, highlighting its impact on organizations. **Advantage:** Offers a comprehensive guide to security policies, access controls, and user awareness strategies to mitigate ransomware risks effectively. **Disadvantage:** The constant monitoring and deep packet inspection required for behavior-based detection can introduce latency and impact system performance.

"Avoiding Future Digital Extortion Through Robust Protection Against Ransomware Threats Using Deep Learning-Based Adaptive Approaches" – S. Sharmeen, Y. A. Ahmed, S. Huda, B. Ş. Koçer, M. M. Hassan [10]. This study proposes an adaptive deep learning-based ransomware detection model that combines unsupervised feature extraction with supervised classification. It applies real ransomware samples in a dynamic environment to train and validate its effectiveness. **Advantage:** Achieves high detection accuracy (95%) by utilizing deep learning models that adapt to evolving ransomware patterns. **Disadvantage:** The computational cost of running deep learning models in real time is significant, requiring high-end hardware and advanced processing capabilities.

The management of ransomware attack repercussions is the main objective of the current model. By employing blockchain technology to provide safe backups of medical data, it offers a recovery-focused strategy. Even in the case of an attack, the data is protected because these backups are kept on a Peer-to-Peer Cloud Server network. To ensure the blockchain's dependability when adding new blocks, nodes use Practical Byzantine Fault Tolerance (pBFT) to come to a consensus.

CHAPTER 3
THEORETICAL BACKGROUND

CHAPTER 3
THEORETICAL BACKGROUND

3.1. IMPLEMENTATION ENVIRONMENT

The implementation of the proposed machine learning and block chain integrated ransomware prevention and mitigation system requires a robust and well-configured environment which involves a combination of hardware and software resources essential to handle the functioning of the application and optimize its performance.

3.1.1. HARDWARE ENVIRONMENT

Processor: The system was equipped with an Intel Core i3 processor or higher to ensure smooth performance.

RAM: A minimum of 6 GB of RAM was used to handle multiple processes effectively.

Hard Disk: The system had at least 250 GB of storage capacity to store project files and databases.

3.1.2. SOFTWARE ENVIRONMENT

Operating System:

Windows 10 or higher was used to provide a stable and secure environment.

Development Environment:

Visual Studio Code was used as the primary IDE for developing and managing code.

Backend Environment:

Node.js was used to run the server-side logic and manage dependencies.

Frontend Framework:

React was utilized to build the front end framework of our system.

React.js:

React.js is an open-source JavaScript library, that is utilized for building interactive user interfaces.React's primary role in an application is to handle the view layer of that application just like the V in a model-view-controller (MVC) pattern by providing the best and most efficient rendering execution.

Ganache:

Ganache is a personal Ethereum blockchain used for developing, testing and deploying smart contracts. It is a part of truffle suite and allows developers to run a local blockchain that mimics the Ethereum network. .

MetaMask :

MetaMask is a cryptocurrency wallet and browser which is used in this project to store, manage, and interact with Ethereum-based assets.MetaMask is one of the most popular tools in the decentralized finance (**DeFi**) ecosystem.

3.1.3. TECHNOLOGIES UTILIZED

IPFS :

IPFS is a peer-to-peer distributed storage system for files. The cloud storage services work based centralized servers, while IPFS uses a network of nodes that are distributed to store and retrieve files.

Blockchain :

Blockchain is a decentralized and distributed technology that ensures secure and tamper-proof data storage.Blockchain Ganache is used in conjunction with IPFS (InterPlanetary File System) to create a secure and resilient backup system that prevents ransom payments and ensures data recovery.

Python :

Python is a widely used, general-purpose, high-level programming language that emphasizes code readability which has clean and concise syntax allows programmers to express concepts with fewer lines of code, making it an ideal choice

for rapid development. In this project, Python was used to develop a scanning feature aimed at preventing ransomware attacks.

3.2. SYSTEM ARCHITECTURE

The system is a Ransomware Detection and Prevention Framework that integrates machine learning, IPFS for decentralized file storage, and blockchain technology (Ganache) to ensure data security and immutability. The application uses React.js for the frontend, Node.js for backend processing, and a smart contract deployed on the Ethereum network to manage IPFS hashes and transactions securely.

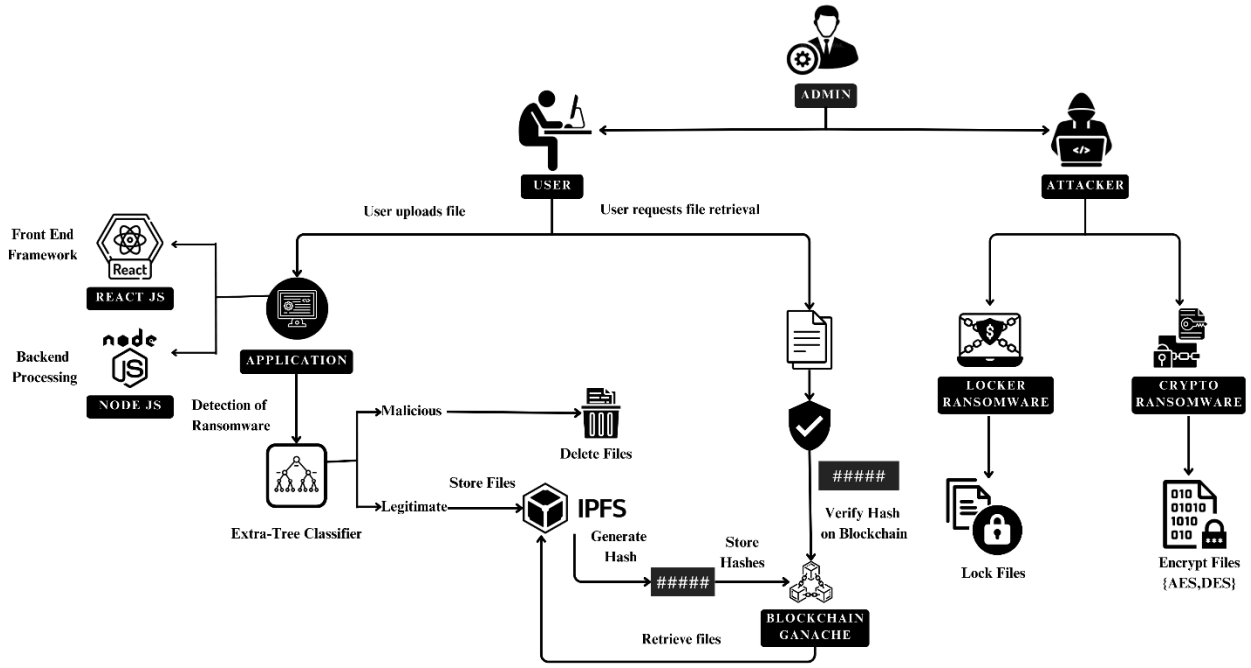


Fig 3.1 Architecture Diagram

3.2.1. HIGH-LEVEL ARCHITECTURE OVERVIEW

The system follows a multi-layered architecture comprising:

Frontend Layer: It is developed using React.js, a powerful JavaScript library known for creating dynamic, responsive, and component-based user interfaces. This layer is responsible for enabling user interaction with the system

Backend Layer: It is built using Node.js, a lightweight and efficient JavaScript runtime that excels at handling asynchronous operations. This layer is responsible for managing API requests, interacting with smart contracts deployed on the Ethereum blockchain, and communicating with IPFS (InterPlanetary File System) to ensure secure backup and file retrieval.

Smart Contract Layer: The Smart Contract Layer is a critical component of the Ransomware Detection and Prevention Framework, responsible for managing the secure storage of IPFS hashes, validating file integrity, and handling transactions on the Ethereum blockchain. Smart contracts, written in Solidity, provide a tamper-proof mechanism to ensure that backup hashes generated by IPFS are securely stored and verified during file retrieval.

IPFS Layer: IPFS splits and distributes files across a peer-to-peer (P2P) network, ensuring redundancy and resilience, making it highly effective in safeguarding clean backups against ransomware attacks.

Blockchain Layer: leverages Ganache, a local Ethereum blockchain simulator, to securely store IPFS file hashes and manage smart contract interactions. This layer ensures data immutability and enables seamless verification of file integrity, protecting against unauthorized alterations.

3.2.2. TECHNOLOGY STACK

- Frontend: React.js
- Backend: Node.js, Express
- Smart Contracts: Solidity, deployed on Ganache

- IPFS Protocol: File storage and hash generation
- Ethereum Blockchain: Ganache for hash verification and immutability

3.2.3. WORKFLOW DIAGRAM

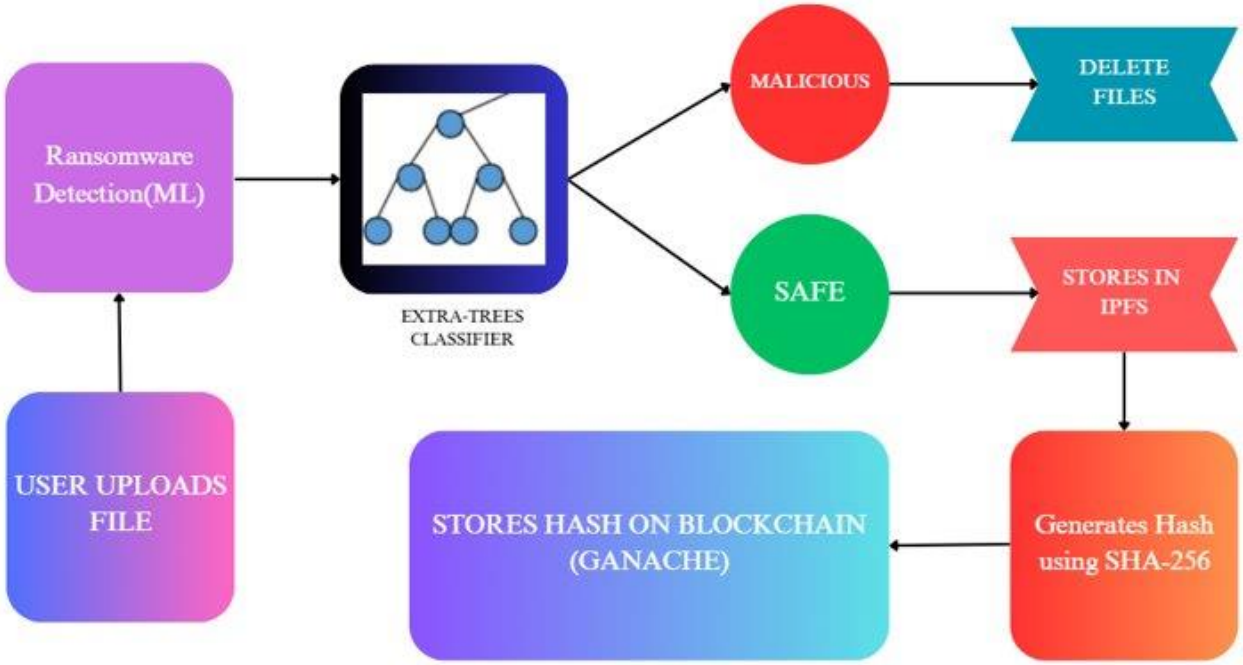


Fig 3.2 Prevention of Ransomware

- User Uploads File: The file is uploaded to the system for ransomware detection.
- Ransomware Detection Using ML: The Extra-Trees Classifier model analyzes the file to determine if it is malicious or safe.

- Malicious Files: These are automatically deleted to prevent system compromise.
- Safe Files: These files are stored in IPFS after generating a secure hash using SHA-256.
- Hash Storage on Blockchain: The generated hash is stored on the blockchain using Ganache to ensure data integrity and immutability.

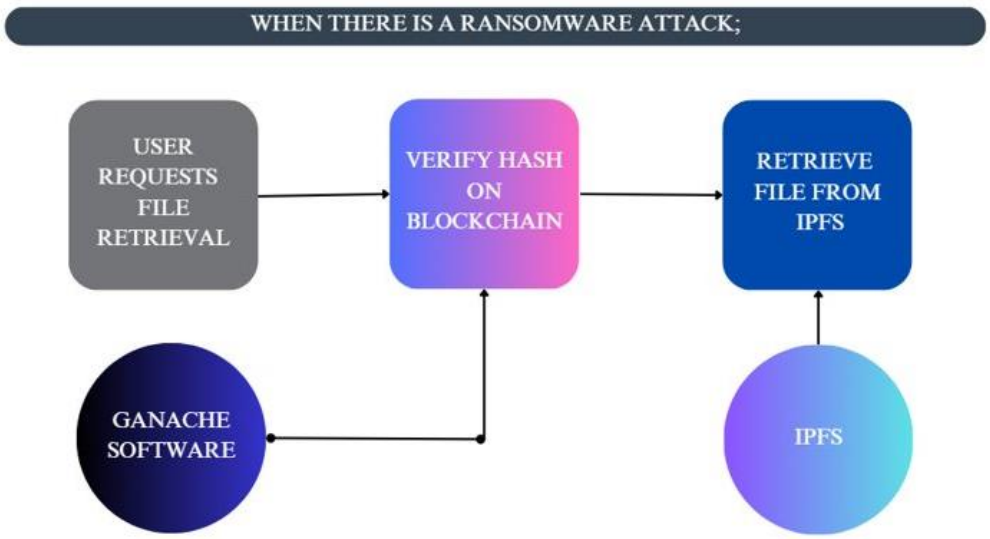


Fig 3.3 Aftermath of Ransomware Incident

- User Requests File Retrieval: The user initiates a request to restore the file.
- Verify Hash on Blockchain: The system verifies the file's hash stored on the blockchain using Ganache to ensure the integrity of the requested file.
- Retrieve File from IPFS: Upon successful verification, the file is retrieved from IPFS and restored to the system.

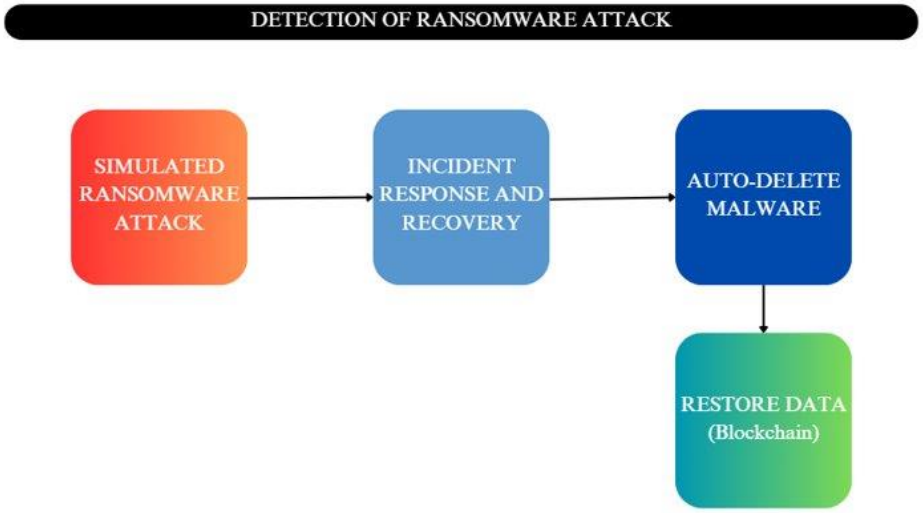


Fig 3.4 Detection of Ransomware

- Simulated Ransomware Attack: The system simulates an attack scenario to identify vulnerabilities and test response efficiency.
- Incident Response and Recovery: The system triggers an incident response to mitigate the impact and ensure data safety.
- Auto-Delete Malware: Detected malware is automatically deleted to prevent further damage.
- Restore Data Using Blockchain: Data integrity is maintained by restoring original files using blockchain-backed storage.

3.3. PROPOSED SYSTEM

The system integrates machine learning algorithms to analyze data patterns, particularly in executable files, enabling real-time ransomware detection. To ensure secure data protection, it leverages a private blockchain to store backups, providing a tamper-proof recovery solution without requiring ransom payments. Alongside detection, the system incorporates prevention mechanisms that automatically isolate suspicious files, preventing the spread of ransomware. Continuous real-time

monitoring tracks system activities, identifying and mitigating potential threats in banking systems before any damage occurs.

3.3.1. DATASET DESCRIPTION

Ransomware detection dataset contains features extracted from Windows Portable Executable (PE) files, including both benign and malicious samples. The dataset is designed for malware detection and analysis research, containing various static features extracted from PE file headers and structures.

The dataset consists of PE file characteristics extracted from a collection of Windows executables and DLL files. Each entry represents a unique file with various attributes extracted from its PE header and structure. The dataset includes both benign software samples and known malware samples (identified by VirusShare hashes).

Objective:

The primary objective of using this dataset is to build a machine learning model to detect ransomware attacks by analyzing static features extracted from PE files. The goal is to distinguish between benign and malicious files effectively, enabling improved security and threat prevention.

Use Cases :

- Malware Detection
- PE File Analysis
- Machine Learning for Security
- Static Analysis Research

Column Descriptions :

Table 3.1 Dataset Feature Description

Column Name	Description
FileName	Name or identifier of the PE file
md5Hash	MD5 hash of the file for unique identification
Machine	Target machine architecture identifier
DebugSize	Size of debug information
DebugRVA	Relative Virtual Address of debug information
MajorImageVersion	Major version number of the image
MajorOSVersion	Major version number of required operating system
ExportRVA	Relative Virtual Address of export table
ExportSize	Size of export table
IatVRA	Relative Virtual Address of Import Address Table
MajorLinkerVersion	Major version number of linker
MinorLinkerVersion	Minor version number of linker
NumberOfSections	Number of sections in the PE file
SizeOfStackReserve	Size of stack to reserve
DllCharacteristics	DLL characteristics flags
ResourceSize	Size of resource section
BitcoinAddresses	Number of potential Bitcoin addresses found
Benign	Binary label (1 for benign, 0 for malicious)

Context and Sources :

- The dataset includes samples from legitimate Windows system files and applications
- Malicious samples are identified by VirusShare hashes
- Features are extracted from PE file headers and structures using static analysis
- The dataset used for this project was obtained from the MLRD Machine Learning Ransomware Detection repository hosted by SecuryCore on GitHub

File Information :

- data_file.csv: Main dataset file containing PE file features
- Format: CSV (Comma-Separated Values)
- Size: 62,000+ samples approximately

3.3.2. MODULE DESIGN

The system is designed with a modular approach to ensure scalability, efficiency, and seamless integration. The modules are – User Module, Attacker Module, Detection of ransomware using Machine learning.

Data Flow Diagram

A Data Flow Diagram (DFD) visually represents how data moves through a system, illustrating processes, data stores, external entities, and data flows. It helps in understanding system functionality, identifying data inputs/outputs, and improving process efficiency. DFDs are structured in levels, with Level 0 providing a high-level overview and Level 1 and beyond detailing specific processes.

0 – Level DFD

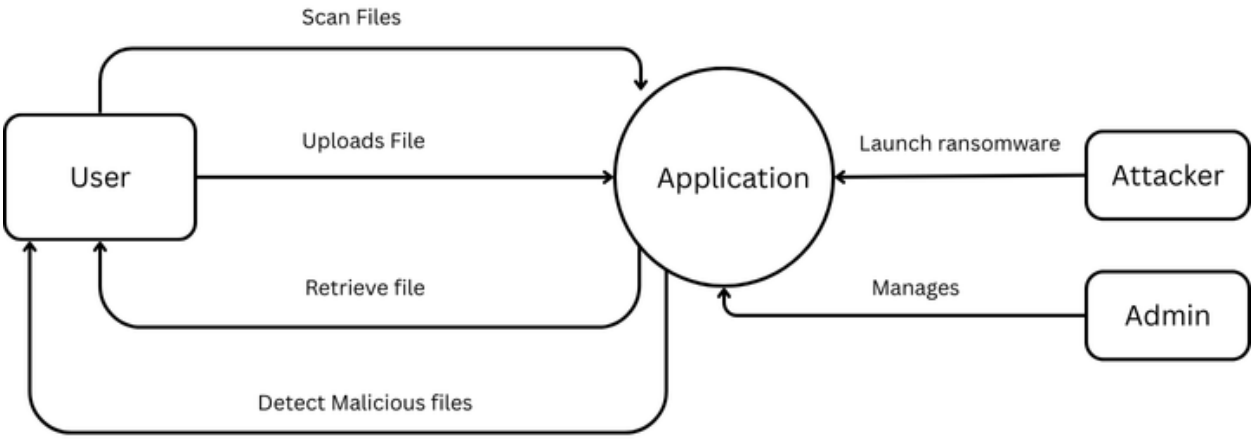


Fig 3.5 Zero Level DFD

First Level DFD

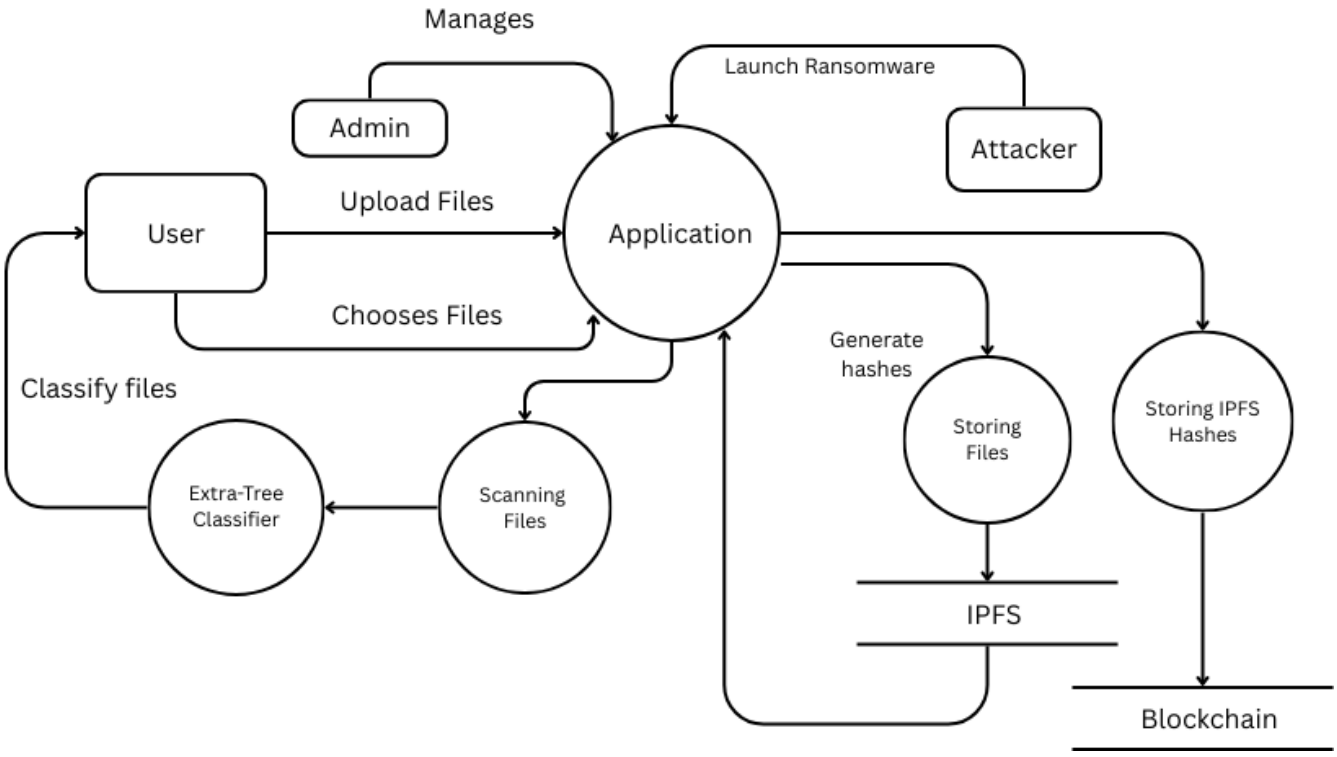


Fig 3.6 First Level DFD

Second Level DFD

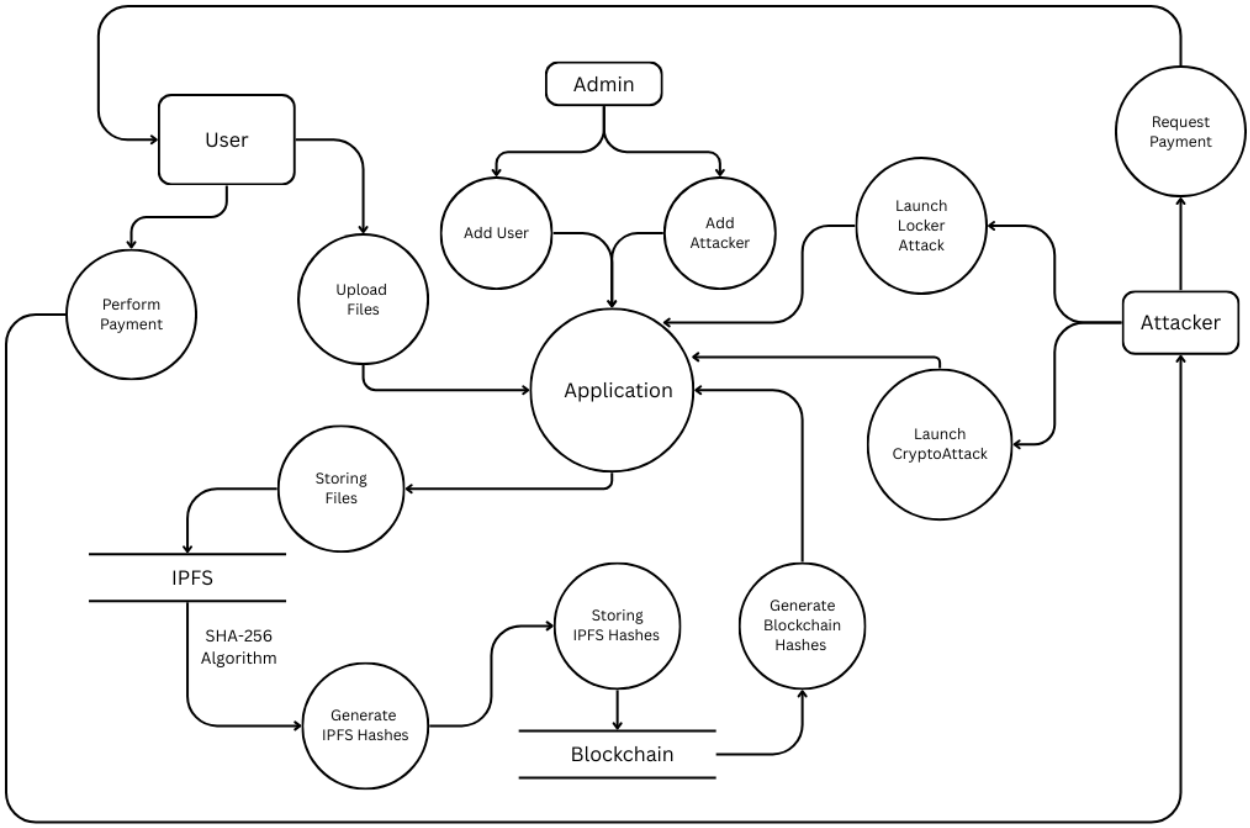


Fig 3.7 Second Level DFD

The Data Flow Diagrams (DFDs) illustrate the ransomware detection and prevention system. The Zero-Level DFD (Fig 3.5) provides a high-level overview of user interactions, file uploads, scanning, and ransomware attacks. The First-Level DFD (Fig 3.6) expands on file classification, scanning, and secure storage using IPFS and Blockchain. The Second-Level DFD (Fig 3.7) details advanced processes like SHA-256 hashing, attacker actions, and user payments, showcasing how the system ensures data security and mitigates ransomware threats.

Use Case Diagram

A Use Case Diagram visually shows how a system interacts with external entities, known as actors (such as users or other systems). It highlights the system's use cases, which are the functionalities or actions the system performs in response to an actor's request, and defines the system boundary, indicating the scope of the system.

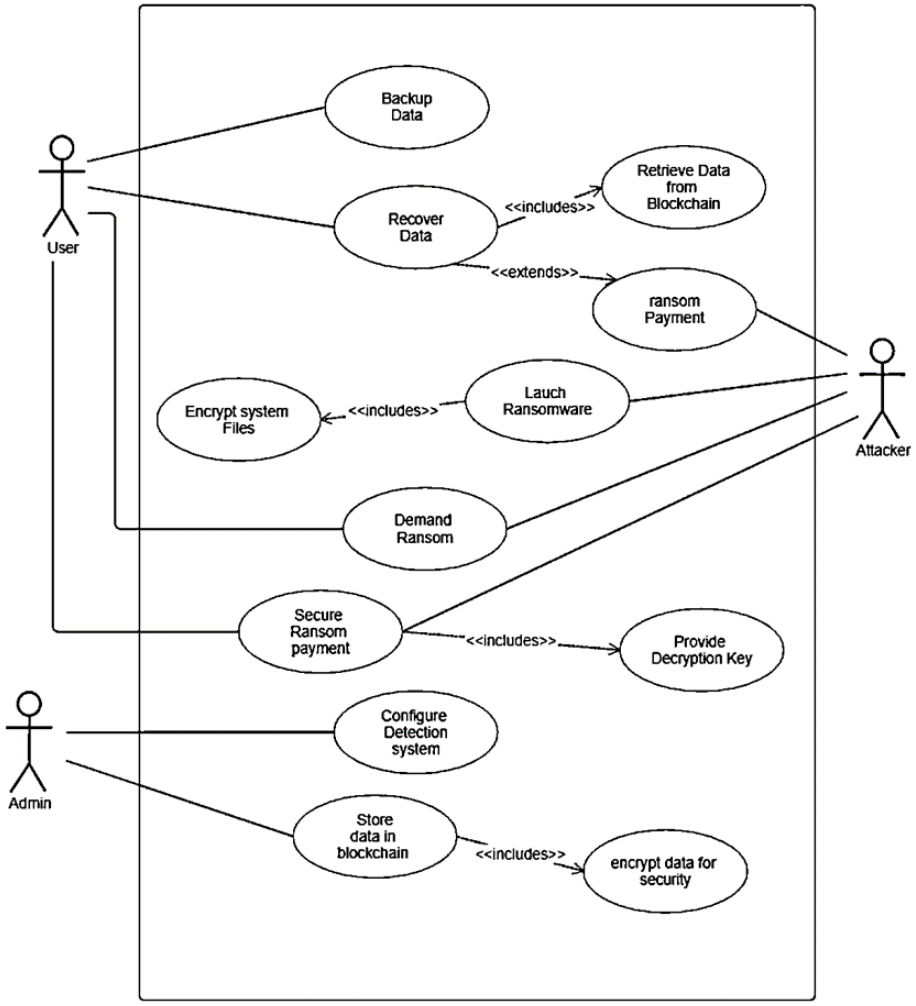


Fig 3.8 Use Case Diagram

Activity Diagram

An Activity Diagram visually represents the flow of activities in a system, showing the sequence of actions, decision points, and parallel processes. It includes start and end nodes to indicate the beginning and completion of the process and helps in understanding system workflows and behavior.

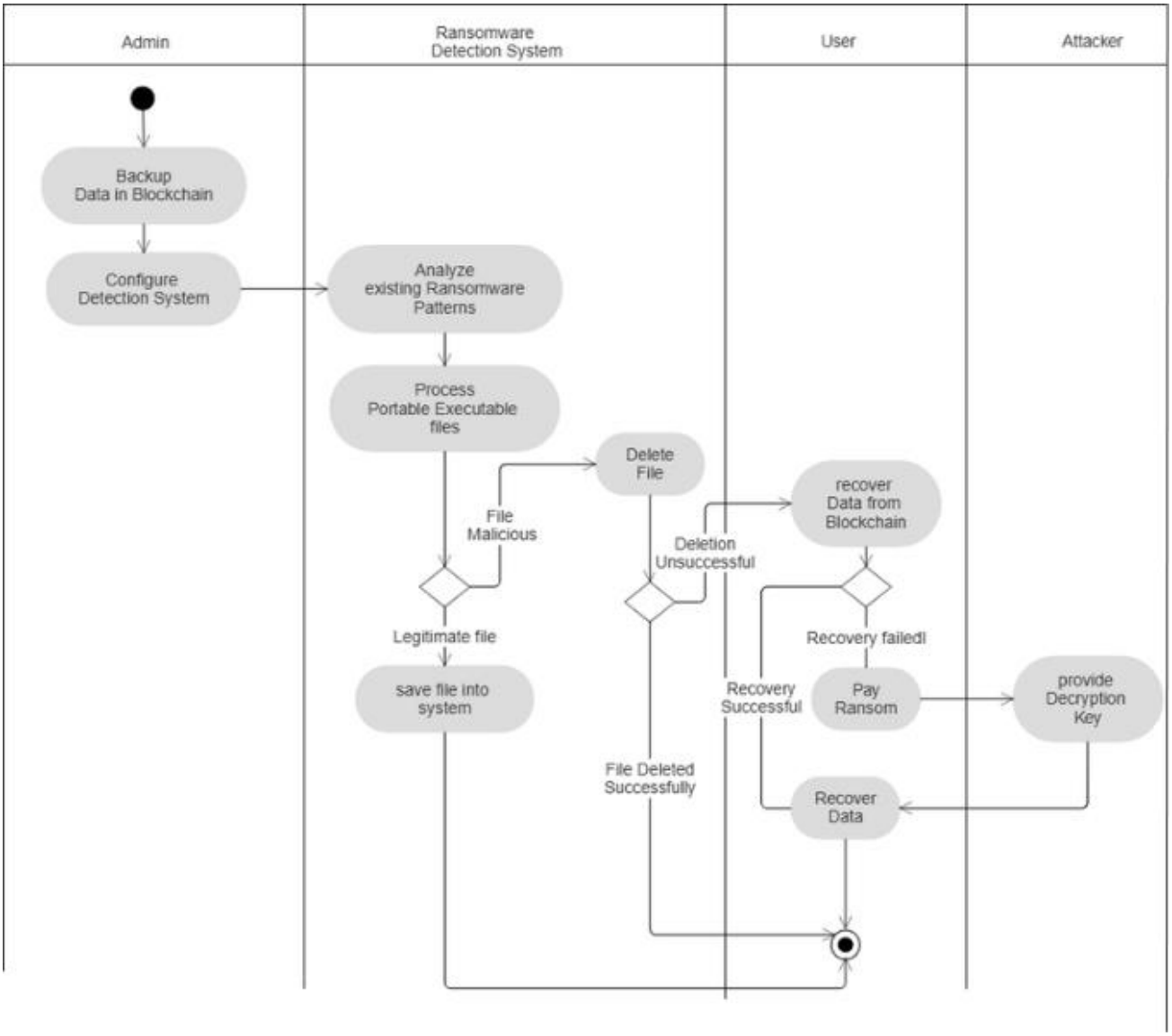


Fig 3.9 Activity Diagram

Sequence Diagram

A Sequence Diagram visually represents the interaction between objects in a system over time. It shows how messages are exchanged between objects to carry out a specific task, with lifelines representing the objects and arrows indicating the flow of communication. Sequence diagrams help in understanding the sequence of interactions and identifying system behavior. They also show the order of method calls and the time taken for each interaction. Sequence diagrams are useful for designing, analyzing, and documenting system processes effectively.

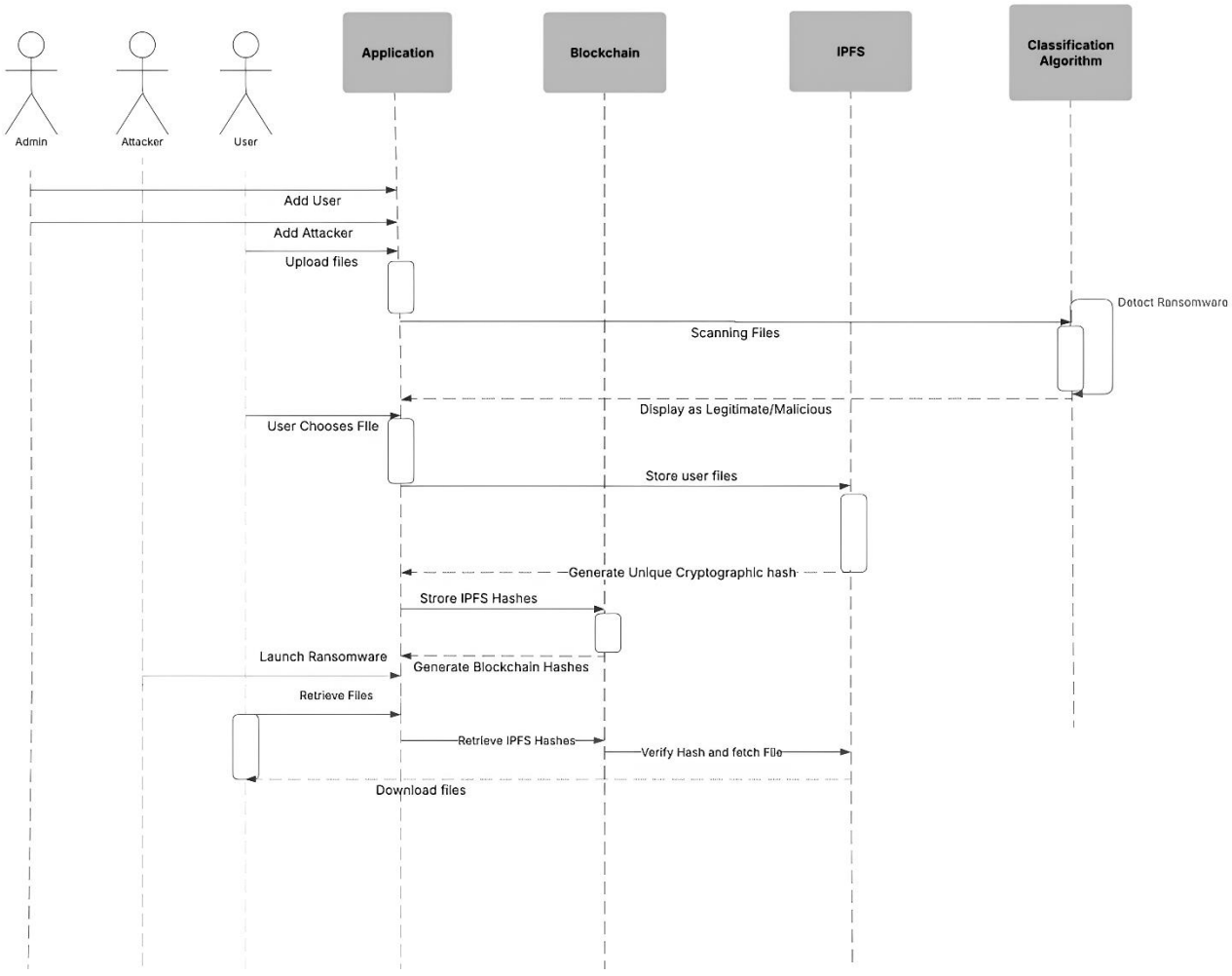


Fig 3.10 Sequence Diagram

Class Diagram

A Class Diagram is a UML diagram that illustrates the structure of a system by depicting its classes, attributes, methods, and relationships between classes. It visually represents how different classes interact and collaborate to perform system functions. Each class is shown as a rectangle with three sections: the class name, attributes, and methods. Relationships such as association, inheritance, and composition show how classes are linked and influence one another. Class diagrams help in designing object-oriented systems and serve as a blueprint for implementation. Key Elements of a Class Diagram:

- Classes: Represent entities with attributes and methods.
- Attributes: Define the properties or characteristics of a class.
- Methods: Specify the operations or functions performed by the class.
- Relationships: Illustrate connections between classes.

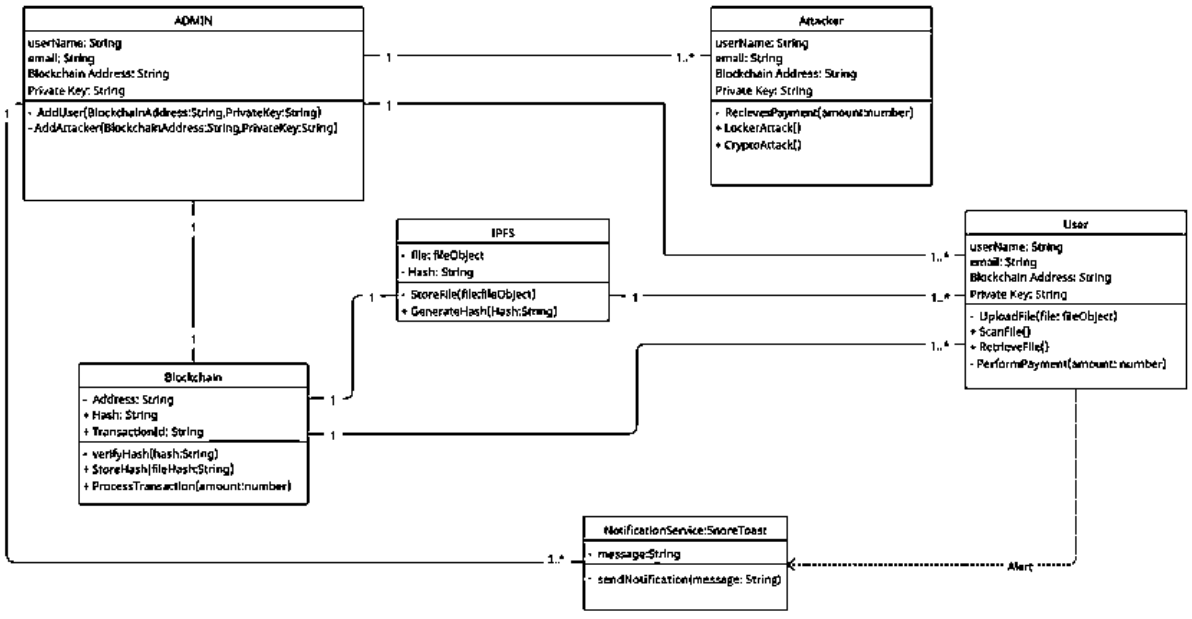


Fig 3.11 Class Diagram

CHAPTER 4
SYSTEM IMPLEMENTATION

CHAPTER 4
SYSTEM IMPLEMENTATION

4.1. ALGORITHMS

This system leverages blockchain (Ganache), decentralized storage (IPFS), and AI-driven detection to protect users from ransomware attacks. It is built using React.js (frontend) and Node.js & Java (backend).

4.1.1. IPFS (Inter planetary file system)

- IPFS is a peer-to-peer distributed storage system for files. The cloud storage services work based centralized servers, while IPFS uses a network of nodes that are distributed to store and retrieve files.

- IPFS also replaces the location-based addressing with content-based addressing in which each file is assigned with a unique cryptographic hash (CID) generated using SHA-256.

- To safeguard files from ransomware, we securely back them up using the IPFS system, which generates a unique hash code for each file, and is stored in blockchain.

- IPFS enables faster and more efficient file retrieval by leveraging a distributed network, reducing reliance on a single central server and improving availability.

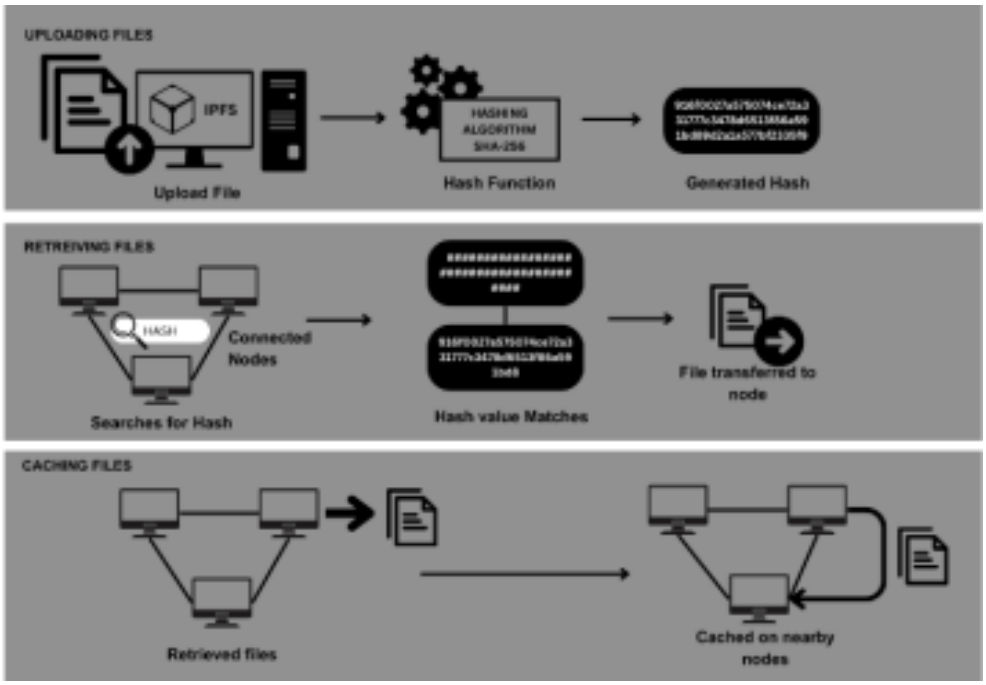


Fig 4.1 Working of IPFS

4.1.2. SHA-256 ALORITHM

SHA-256 (Secure Hash Algorithm 256-bit) is a cryptographic hash function used to ensure file integrity. In this system, SHA-256 plays a crucial role in verifying whether a file has been altered due to a ransomware attack.

$$H(M) = SHA\text{-}256(M)$$

Where M is the file data, H(M) is the 256-bit hash. Any alteration in M will result in a completely different hash

$$H_s \neq H_r \Rightarrow \text{Data has been tampered with.}$$

4.1.3. EXTRA-TREES CLASSIFIER

- The Extra-Trees Classifier is an ensemble learning algorithm that is used to detect ransomware by classifying PE files as legitimate or malicious.

- Unlike Random Forests, Extra-Trees use the entire dataset without bootstrapping and select splits randomly, reducing overfitting.
- The Extra-Trees algorithm selects a random feature and split value at each node.
- Given a dataset D = {X, Y}, where X is the input feature set and Y is the class label set, the split function at node t is:

$$f(X) = \begin{cases} \text{Left Subtree}, & X[f_j] \leq s_j \\ \text{Right Subtree}, & X[f_j] > s_j \end{cases}$$

where:

- f j is a randomly selected feature,
- s j is a randomly selected split threshold

The final classification prediction is determined by majority voting from N trees in the ensemble:

$$\hat{Y} = \text{mode}\{h_1(X), h_2(X), ..., h_N(X)\}$$

4.1.4. WORKING OF EXTRA-TREES CLASSIFIER

- **Feature Extraction**: Important properties of PE files (header characteristics, entropy, section data, etc.) are extracted.
- **Random Feature Selection**: Instead of computing the best split, Extra-Trees randomly selects features and thresholds.
- **Decision Tree Construction**: Multiple decision trees are built independently.
- **Majority Voting**: The final classification is made based on the majority vote across all trees.

- **Faster Training:** Because Extra-Trees uses random feature splits and thresholds, it reduces computation time and speeds up the training process compared to traditional decision trees.
- **High Variance Reduction:** By using multiple randomized trees and combining their results, Extra-Trees significantly reduces variance and overfitting.
- **Robustness to Noise:** The randomization in feature selection makes the model more robust to noisy or irrelevant features in the dataset.

Fig 4.2 Working of Extra -Trees Classifier

4.1.5. BLOCKCHAIN

Blockchain is a decentralized and distributed digital ledger that records transactions across multiple computers in a secure and transparent way. Each record in the blockchain is called a block, and these blocks are linked together in a chain, forming a continuous record of data. Once information is recorded in a block, it cannot be easily altered or deleted, making the system highly secure and trustworthy. Blockchain works without a central authority and uses cryptographic techniques to ensure that data is safe from tampering. It is widely used in cryptocurrencies like Bitcoin and Ethereum, but its applications also extend to industries such as finance, healthcare, supply chain, and voting systems, where secure and transparent data management is required.

4.1.6. GANACHE SOFTWARE

Ganache is a personal Ethereum blockchain that helps developers build, test, and deploy smart contracts in a local environment. As part of the **Truffle Suite**, it allows developers to simulate blockchain behavior without using the real Ethereum network. Ganache provides pre-funded test accounts with test Ether for easy contract deployment and transactions. It also shows detailed logs, events, and gas usage, helping developers debug and improve their smart contracts. With its easy-to-use GUI or CLI, developers can track transactions, blocks, and events in real time.

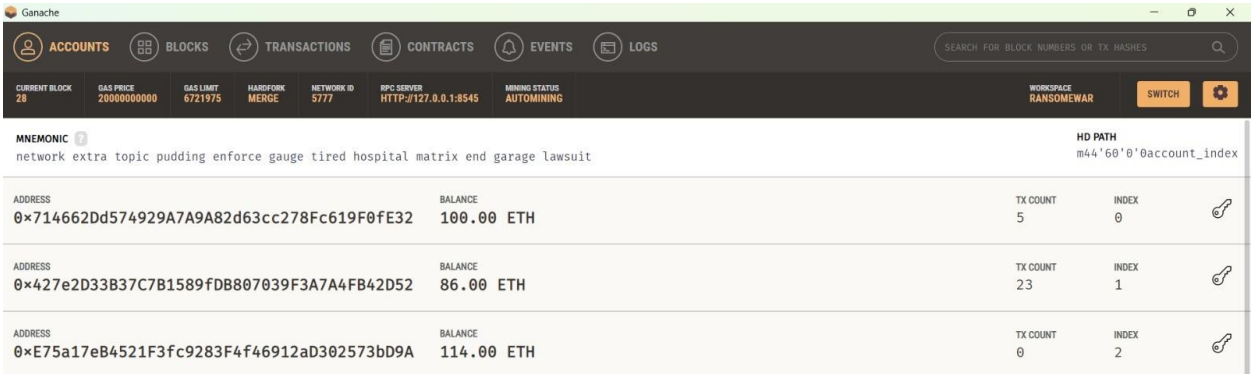


Fig 4.3 Ganache Software

- **Accounts**: Shows a list of test accounts with their addresses and balances.
- **Blocks**: The current section, showing recently mined blocks.
- **Transactions**: Displays all transactions with details like sender, receiver, gas used, and status.
- **Contracts**: Lists the deployed smart contracts with addresses and details.
- **Events**: Shows events triggered by contracts during transactions.
- **Logs**: Displays all activities and errors for debugging purposes.

4.1.7. SMART CONTRACT

A **smart contract** is a self-executing program stored on a blockchain that automatically runs when certain conditions are met. It helps in making agreements between parties without the need for intermediaries. Smart contracts are written in coding languages like **Solidity** and are mostly used on blockchain platforms like **Ethereum**. They ensure secure, transparent, and tamper-proof transactions, commonly used for tasks like transferring funds, managing digital assets, or automating agreements.

4.1.8. WORKING OF SMART CONTRACT

- **Compile the Contract:**

  The code is compiled into bytecode so that it can be understood by the **Ethereum Virtual Machine (EVM)**.
- **Deploy to Blockchain:**

  The compiled contract is deployed onto the blockchain using a wallet or development tools like Remix or Truffle.

- **Get Contract Address:**
  After deployment, the blockchain assigns a unique address to the smart contract.
- **Interact with the Contract:**
  Users or applications send transactions to the contract address to trigger its functions.
- **Execution by EVM:**
  The EVM executes the contract, checking conditions and performing actions automatically.
- **Record on Blockchain:**
  The result (like sending funds or changing data) is permanently recorded on the blockchain

4.1.9. ETHEREUM STORAGE SLOT:

An **Ethereum storage slot** is a fixed 32-byte space in the blockchain where smart contract data is stored permanently. Each state variable in a smart contract is stored in these slots, starting from slot 0 and moving sequentially for simple variables. Complex structures like arrays and mappings use calculated storage slots. Understanding storage slots is important for managing gas costs, optimizing smart contracts, and ensuring security, especially when upgrading contracts or reading data directly from the blockchain.

4.2. MODULES

The system integrates multiple security layers, including machine learning-based detection, blockchain-backed storage, and secure payment handling to combat ransomware effectively. Each module plays a crucial role in ensuring data integrity,

early threat detection, and controlled recovery, minimizing potential damage from cyber threats. By combining real-time monitoring, decentralized storage, and AI-driven classification, the system provides a comprehensive approach to ransomware prevention and mitigation.

4.2.1. USER MODULE

- The user will log in to their account to back up their files on the blockchain, ensuring they can retrieve their data if a ransomware attack occurs.
- They can scan their files to check for any infection.
- If the data is damaged beyond recovery after an attack, the user can securely pay the ransom through the blockchain to the attacker, ensuring safe and transparent transactions.
- This system provides an added layer of security by allowing easy access to backups and offering a secure method to handle ransom payments, minimizing potential damage from ransomware attacks.

Choose file: the file is selected from the system

Store the IPFS: the file is stored in IPFS

Retrieve files: after storing, the file can also be retrieved

4.2.2. ATTACKER MODULE

- The attacker can demonstrate Locker Ransomware and Crypto Ransomware through their login.
- After executing the ransomware attack, the attacker receives the ransom payment from the victim in exchange for restoring access to their encrypted data.

- This setup highlights how ransomware attacks can compromise data access, while also showing the attacker’s ability to demand payment for restoring control over the victim's files.
- Locker ransomware attack: It locks the entire system preventing the user from accessing it until ransom is paid.
- Crypto ransomware attack: It encrypts the victim’s files and demands ransom for the decryption key to restore data access.

4.2.3. DETECTION OF RANSOMWARE USING MACHINE LEARNING MODULE

- Portable Executable (PE) files in Windows systems are integral to system-level operations and are frequently exploited during ransomware attacks.
- Attackers may target PE files directly or utilize them as vectors to deliver ransomware.
- The module employs a machine learning classification model trained using a honeypot dataset.
- The honeypot dataset acts as a decoy, offering ransomware and malware samples to enhance the model's training process.
- The model classifies PE files into two categories: legitimate or malicious (ransomware-containing).
- Malicious PE files identified by the model are automatically removed to prevent potential harm to the user’s system.

- The model extracts important features from PE files such as header information, section characteristics, imported DLLs, and file entropy values to improve classification accuracy.

- The module is designed to continuously update its model by incorporating newly detected ransomware samples, making it more robust against evolving ransomware threats.

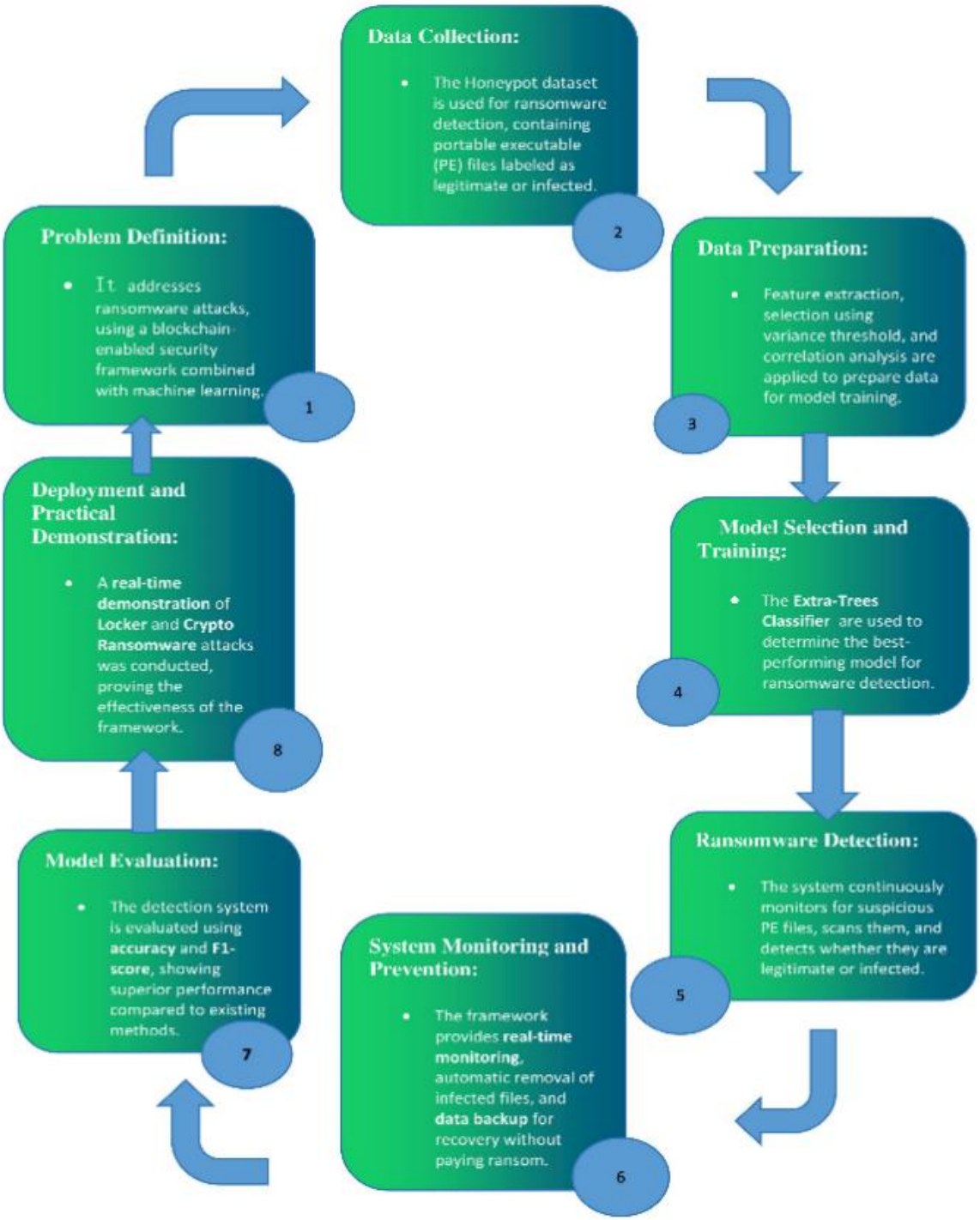


Fig 4.4 Lifecycle of Ransomware Detection

CHAPTER 5
RESULTS AND DISCUSSION

CHAPTER 5
RESULTS AND DISCUSSION

5.1. PERFORMANCE PARAMETERS

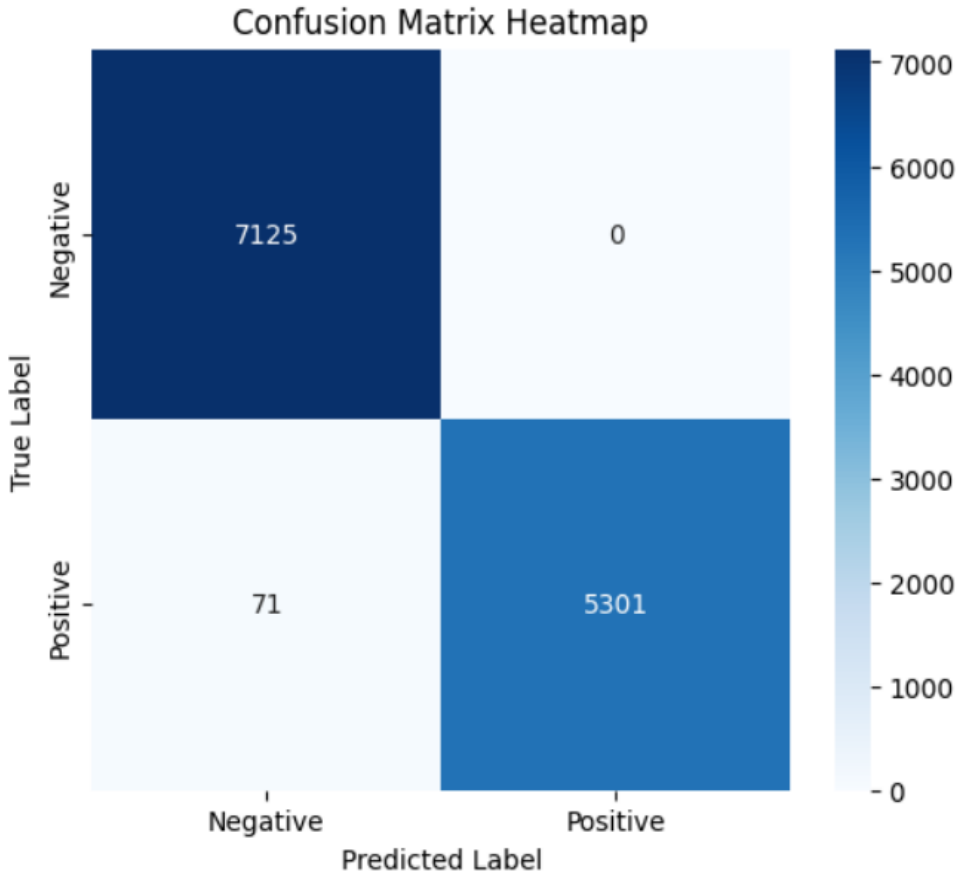


Fig 5.1 Confusion Matrix of the model

With a remarkable 99.43% accuracy and an F1-score of 0.99, the Extra-Trees Classifier showed its exceptional ability to accurately and consistently distinguish between malicious and legitimate data. By leveraging machine learning, the model provides a robust security layer that significantly guarantees proactive defense against upcoming cyberthreats.

5.2. RESULTS & DISCUSSION

Our application provides a seamless and secure experience for users, beginning with real-time system monitoring and ransomware detection. Users can upload files for scanning, and the system analyzes them using the Extra-Trees Classifier to detect potential threats. If ransomware is detected, it is automatically removed, and users are alerted. Additionally, the system stores critical files in blockchain-based backup, ensuring tamper-proof recovery in case of an attack. In extreme cases, secure transactions via MetaMask enable safe ransom payments. By combining machine learning and blockchain, our system provides enhanced cybersecurity, data integrity, and ransomware resilience for users.

To evaluate the effectiveness of our ransomware detection model, we examine its performance using a confusion matrix. This visualization provides data on categorization accuracy together with false positive and false negative rates. By improving overall threat identification, reducing errors, and fine-tuning the detection algorithm, this method strengthens our system's resistance to changing ransomware attacks. To improve accuracy, we additionally update the model on a regular basis. To guarantee adaptive security, we use fresh datasets and patterns. In the financial industry, the combination of blockchain technology and machine learning offers a scalable, intelligent, and future-proof security against cyberattacks.

We evaluate the effectiveness of our ransomware detection technology by analyzing its performance using an error matrix. This visualization provides data on categorization accuracy together with false positive and false negative rates.

CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1. CONCLUSION

The Machine Learning-Driven Security Framework (ML-DSF) integrated with Blockchain provides a robust and scalable solution for preventing and mitigating ransomware attacks in the banking sector. By utilizing Extra-Trees Classifier, the framework ensures real-time threat detection, reducing operational disruptions and financial losses. The incorporation of private blockchain technology guarantees tamper-proof data storage, secure file recovery, and protection against data manipulation, effectively eliminating the need for ransom payments. The combination of machine learning-based threat identification, decentralized authentication, and immutable backups enhances cybersecurity resilience. The results indicate that the proposed system significantly improves incident response capabilities and safeguards critical financial data against evolving ransomware threats.

6.2 FUTURE ENHANCEMENTS

Future enhancements to the ML-DSF framework can focus on real-time adaptive learning to detect emerging ransomware variants dynamically. Scalability optimizations will ensure seamless deployment in large-scale banking systems. Integrating multi-model fusion techniques like LSTM and CNN can improve detection accuracy. SIEM (Security Information and Event Management) system integration can enhance automated threat response. Quantum-resistant cryptography can strengthen blockchain security against future threats. Additionally, expanding this framework to healthcare, government, and IoT infrastructures can provide broader protection against ransomware. These improvements will make ML-DSF more resilient, adaptive, and effective against evolving cyber threats.

APPENDICES

APPENDICES

A1. SDG GOALS

SDG 8 – Decent Work and Economic Growth

Ransomware attacks cause financial losses and disrupt operations. This project mitigates threats, ensuring business continuity in banking. By securing financial infrastructure, it supports economic stability. It reduces cybercrime-related disruptions and enhances trust in digital transactions.

SDG 9 – Industry, Innovation, and Infrastructure

This project enhances banking cybersecurity using machine learning and blockchain. It ensures ransomware detection and secure data recovery. By promoting resilient financial systems, it mitigates cyber threats. It fosters secure, tamper-proof, and innovative banking operations.

SDG 16 – Peace, Justice, and Strong Institutions

By preventing ransomware, this system ensures data integrity and security. It reduces cybercrime, promoting transparency in financial operations. Blockchain secures data, while machine learning detects threats proactively. This strengthens financial institutions, fostering trust and stability.

A2. SOURCE CODE

Routes.tsx

```
import { useDispatch, useSelector } from "react-redux";

import { RootState } from "../store/reducers";

import { Route, Routes as ParentRoutes, Outlet, useNavigate } from "react-router-dom";

import React from "react";

import { UserRole } from "../repository/interfaces";

import ErrorPage from "../error-page";

import Admin from "../components/Admin/Admin";

import User from "../components/User/User";

import PrivateRoute from "../middlewares/private-route";

import { setLoginStatus } from "../store/actions/action";

import Navigation from "../components/Navigation/Navigation";

import Hacker from "../components/Hacker/Hacker";

import Scanner from "../components/Scanner/Scanner";

import Home from "../components/Home/Home";


const Routes = () => {
```

```
  const { isUserLoggedIn, userDetails } = useSelector(
    (state: RootState) => state.generalReducer
  );
  const dispatch = useDispatch();
  const user = localStorage.getItem("LOGGEDIN_USER");
  if (user && !isUserLoggedIn) {
    dispatch(setLoginStatus({ status: true }));
  }

  const navigate = useNavigate();
  return (
    <>
    <ParentRoutes>
<Route path="/*" element={<> <Home />
            <Outlet /> {/* Renders child routes */}
        </>} />
        <Route path="/navigation" element={ <Navigation />} />
        <Route path="/admin" element={ <Admin />} />
        <Route path="/user" element={ <User />} />
```

```
    <Route path="/hacker" element={ <Hacker  />} />
  {/* <Route path="/all-products" element={<AllProducts />} />
   <Route path="/product/:productid" element={<ProductDetails />} />   */}
    <Route path="*/*" element={<ErrorPage />} />
{userDetails.role === UserRole.Admin && (
<Route
  path="/admin"
    element=
 {
    <>
      <Route
        index
        element={
          <PrivateRoute>
          </PrivateRoute>
        }
       />
    </>
  }
```

```
      />
    )}
      </ParentRoutes>
      </>
    );
  };
  export default Routes;
```

index.tsx

```
import React from 'react';
import ReactDOM from 'react-dom/client';

import { BrowserRouter as Router, Route, Routes } from "react-router-dom";
import { Provider } from "react-redux";
import configureStore from './store/configureStore';
import './index.css';
import App from './App';

const store = configureStore();
```

```
const root = ReactDOM.createRoot(document.getElementById("root")as
HTMLElement);


root.render(
<React.StrictMode>
   <Provider store={store}>
     <Router>
       <Routes>
         <Route path="*" element={<App />} />
       </Routes>
     </Router>
   </Provider>
 </React.StrictMode>,);
```

App.tsx

```
import React from 'react';
import './App.css';
import Navbar from './components/Navbar/Navbar';
import Navigation from './components/Navigation/Navigation';
import Admin from './components/Admin/Admin';
```

```
import User from './components/User/User';
import Hacker from './components/Hacker/Hacker';
import Scanner from './components/Scanner/Scanner';
import Routes from './Routes/routes';
function App() {
  return (
    <>      <Navbar />
      {/* <Navigation />
      <Admin />
      <User />
      <Hacker />*/}


      <Routes />
    </>
  );
}
export default App;
```

ransomeware.py

```
from flask import Flask, request, jsonify
```

```
from flask_cors import CORS
import pefile
import joblib
import numpy as np
from sklearn.preprocessing import MinMaxScaler
import pandas as pd
import pickle
scaler = MinMaxScaler()
X_train=pd.read_csv('./training.csv')
scaler.fit(X_train)


app = Flask(__name__)
CORS(app)


file = None
model = joblib.load('./knn')
def extract_features_from_file(file_data):
    try:
        # Call a function to extract features directly from the file data
```

```
        extracted_features = extract_features(file_data)
        # Print or use the extracted features as needed
        for key, value in extracted_features.items():
            print(f'{key}: {value}')
        return {"message": "File processed successfully", "features":
extracted_features}
    except Exception as e:
        return {"error": str(e)}, 500
@app.route('/receiveFile', methods=['POST'])
def receive_file():
    try:
        # Check if the POST request has the file part
        if 'file' not in request.files:
            return jsonify({"error": "No file provided"}), 400

        global file
       file = request.files['file']

        # Call a function to extract features directly from the file data
```

```
        response = extract_features_from_file(file.read())


        # Return a response to the React app
        return jsonify(response)


    except Exception as e:
        return jsonify({"error": str(e)}), 500
def extract_features(file_data):
    pe = pefile.PE(data=file_data)
    if pe:
        characteristics = pe.FILE_HEADER.Characteristics
        major_linker_version = pe.OPTIONAL_HEADER.MajorLinkerVersion
        size_of_code = pe.OPTIONAL_HEADER.SizeOfCode
        size_of_initialized_data = pe.OPTIONAL_HEADER.SizeOfInitializedData
        image_base = pe.OPTIONAL_HEADER.ImageBase
        major_os_version =
pe.OPTIONAL_HEADER.MajorOperatingSystemVersion
        minor_os_version =
pe.OPTIONAL_HEADER.MinorOperatingSystemVersion
        major_image_version = pe.OPTIONAL_HEADER.MajorImageVersion
```

```
check_sum = pe.OPTIONAL_HEADER.CheckSum

    dll_characteristics = pe.OPTIONAL_HEADER.DllCharacteristics

    sections_nb = len(pe.sections)

    sections_mean_entropy = sum(section.get_entropy() for section in
pe.sections) / len(pe.sections)

    sections_max_entropy = max(section.get_entropy() for section in pe.sections)

    imports_nb_dll = len(pe.DIRECTORY_ENTRY_IMPORT)

    imports_nb_ordinal = sum(len(x.imports) for x in
pe.DIRECTORY_ENTRY_IMPORT)

    resources_nb = len(pe.DIRECTORY_ENTRY_RESOURCE.entries)

    ResourcesMeanEntropy= 3.904

    ResourcesMinEntropy= 2.49

    ResourcesMeanSize= 4794.61

    load_configuration_size =
pe.OPTIONAL_HEADER.DATA_DIRECTORY[pefile.DIRECTORY_ENTRY['I
MAGE_DIRECTORY_ENTRY_LOAD_CONFIG']].Size

    VersionInformationSize= 14.108

    arr = np.array([[characteristics, major_linker_version, size_of_code,
size_of_initialized_data, image_base, major_os_version, minor_os_version,
major_image_version, check_sum, dll_characteristics, sections_nb,
sections_mean_entropy, sections_max_entropy, imports_nb_dll,
```

```
imports_nb_ordinal, resources_nb, ResourcesMeanEntropy,
ResourcesMinEntropy, ResourcesMeanSize, load_configuration_size,
VersionInformationSize]])
        print(arr)
        loaded_min_values = np.load('original_min_values.npy')
        loaded_max_values = np.load('original_max_values.npy')

# Set the parameters of the existing scaler
scaler.set_params(feature_range=(loaded_min_values, loaded_max_values))

# Use reshape to convert the 1D array to a 2D array
        X_new_scaled = scaler.transform(arr)

# Make prediction
        output = model.predict(X_new_scaled)
        print(output.tolist())

        return ({"status":output.tolist()})  # Convert NumPy array to a list
 if __name__ == '__main__':
    app.run(host='127.0.0.1', port=5006, debug=True)
```

A3. SCREENSHOTS

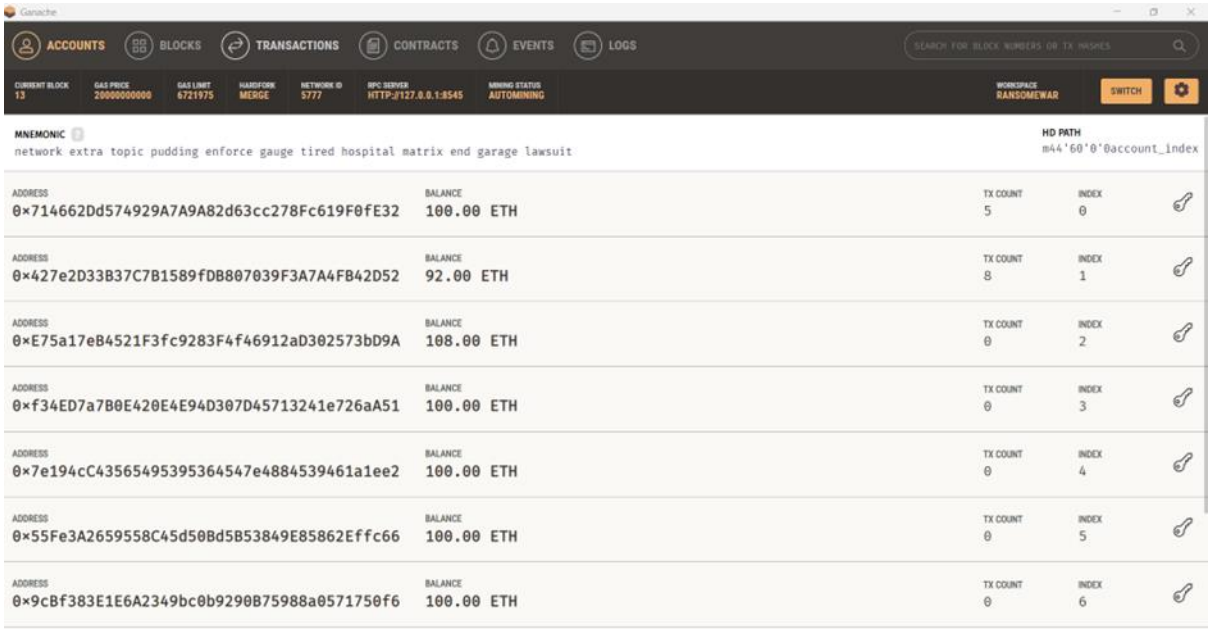


Fig A.3.1 Ganache Software Interface- Accounts

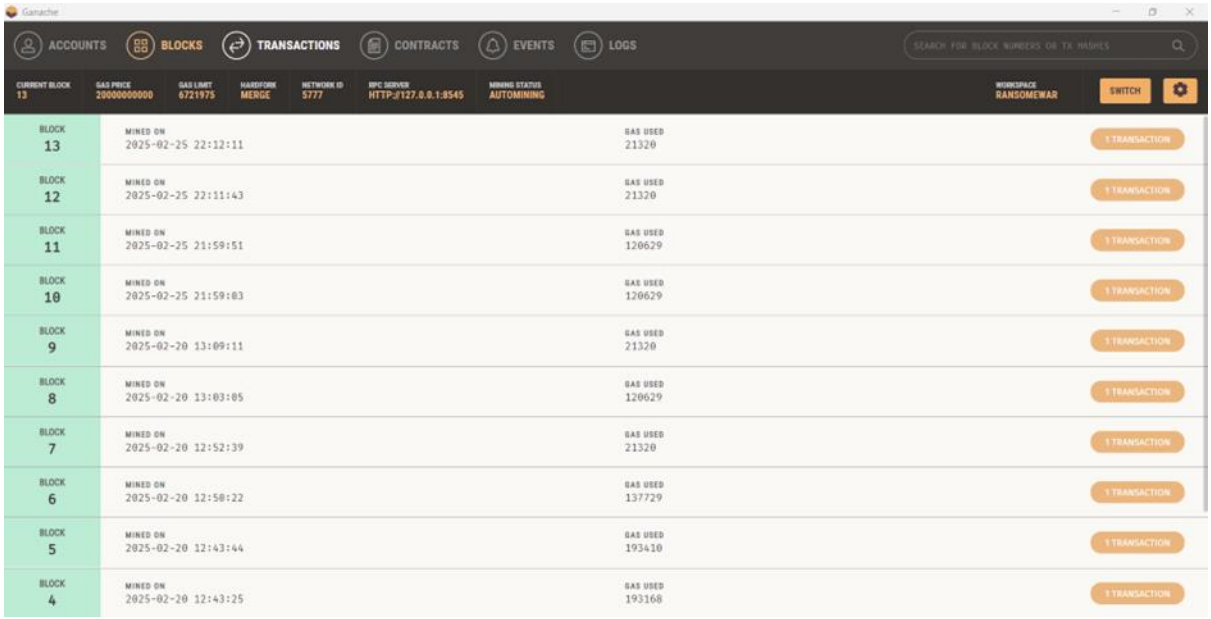


Fig A.3.2 Ganache Software Interface- Blocks

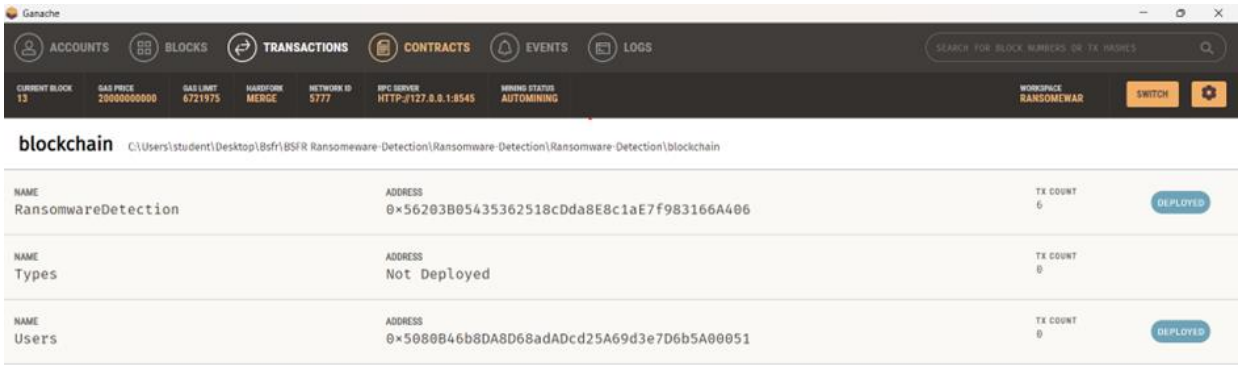


Fig A.3.3 Ganache Software Interface- Contracts

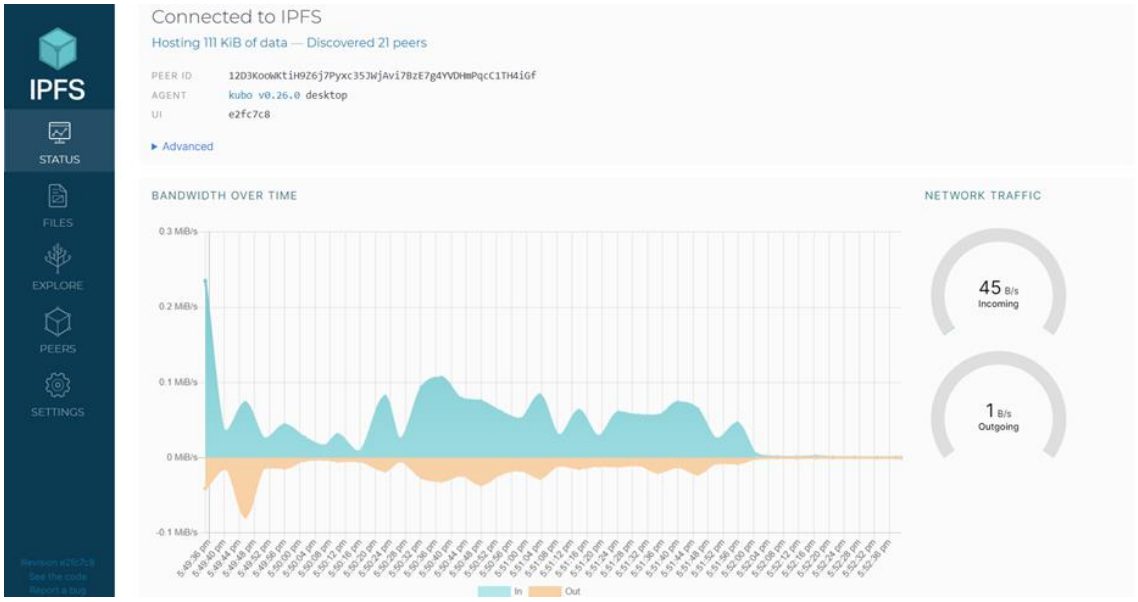


Fig A.3.4 IPFS Initialization

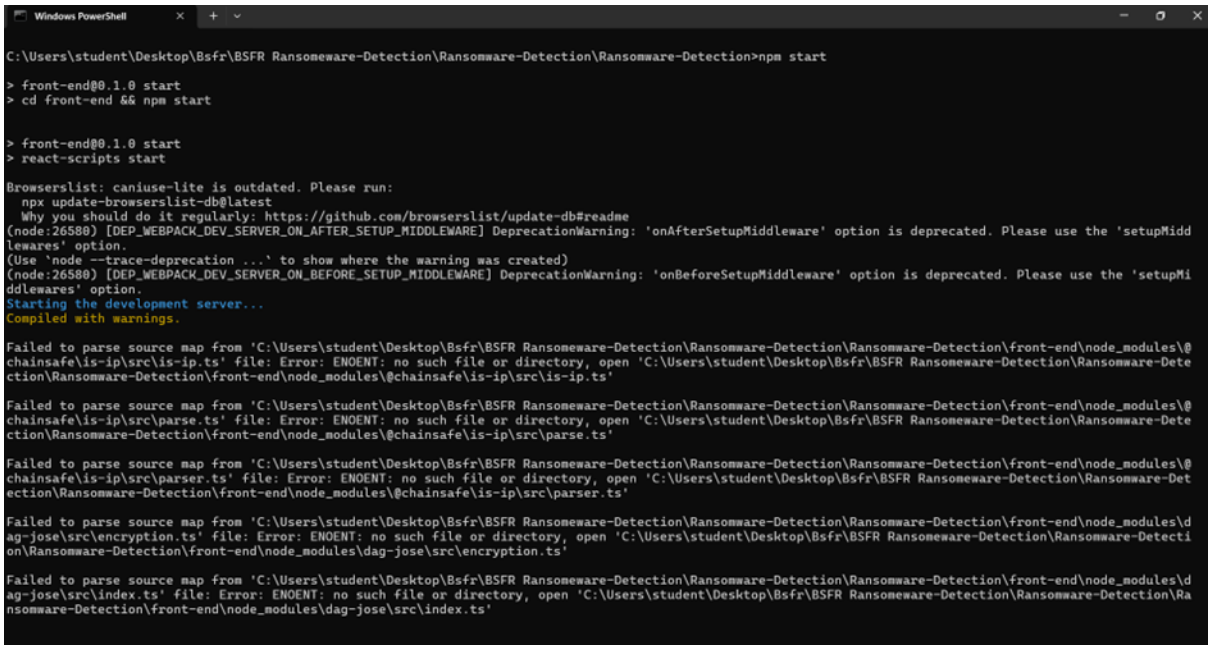


Fig A.3.5 Running npm start Command

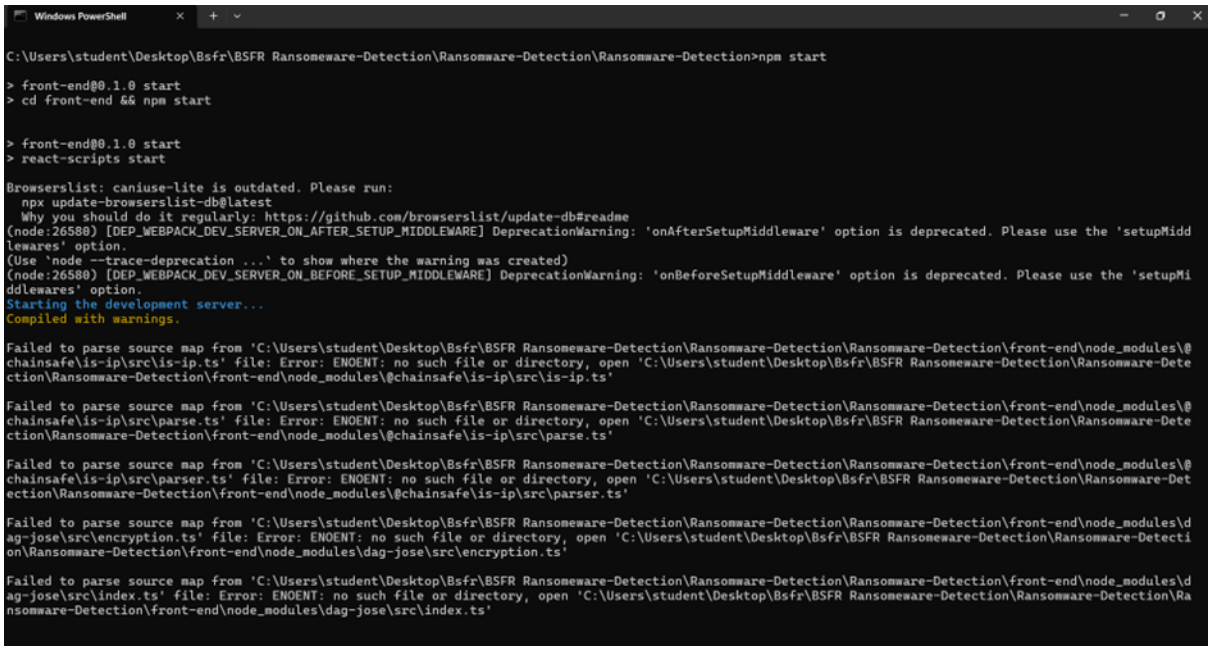


Fig A.3.6 Executing npm run start-node-scripts

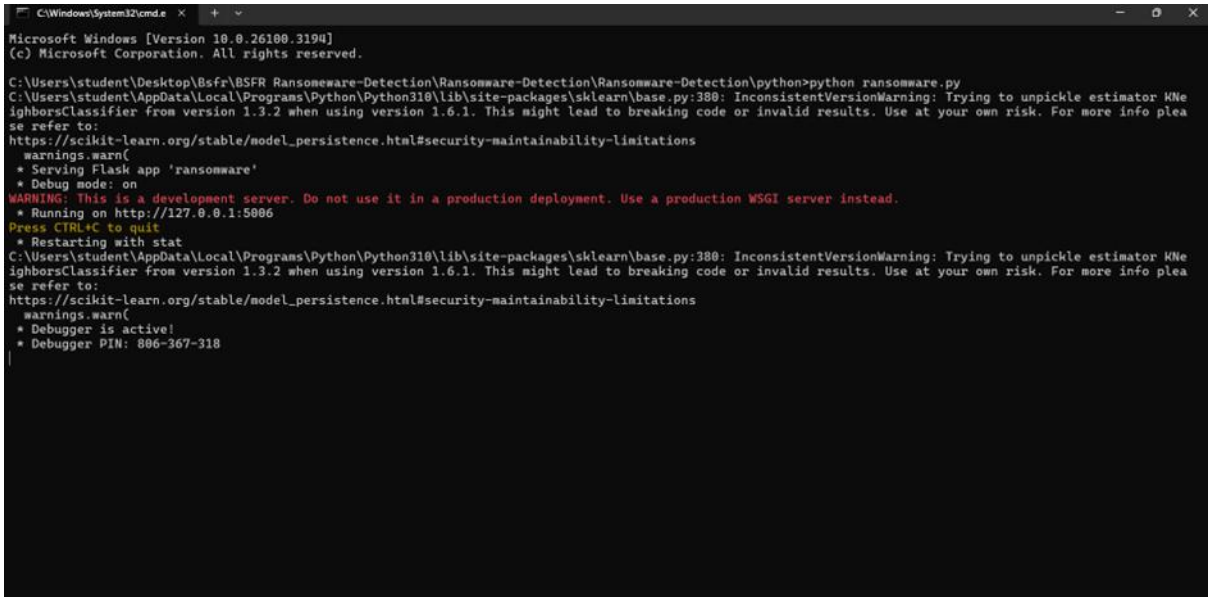


Fig A.3.7 Running Python ransomware.py Script

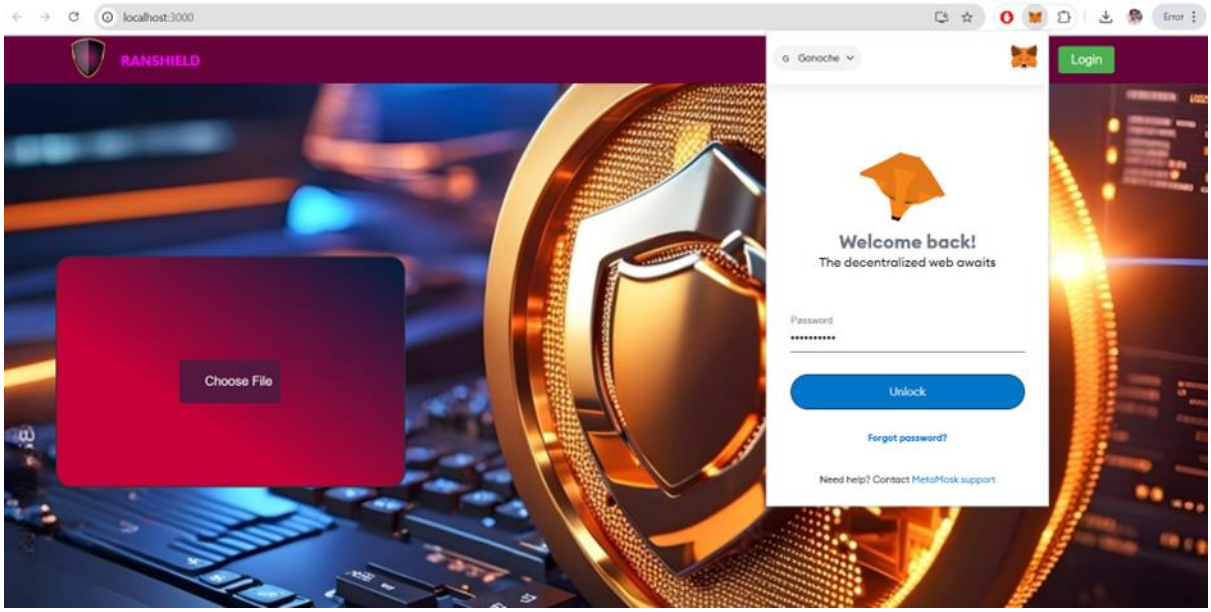


Fig A.3.8 Metamask Extension Setup

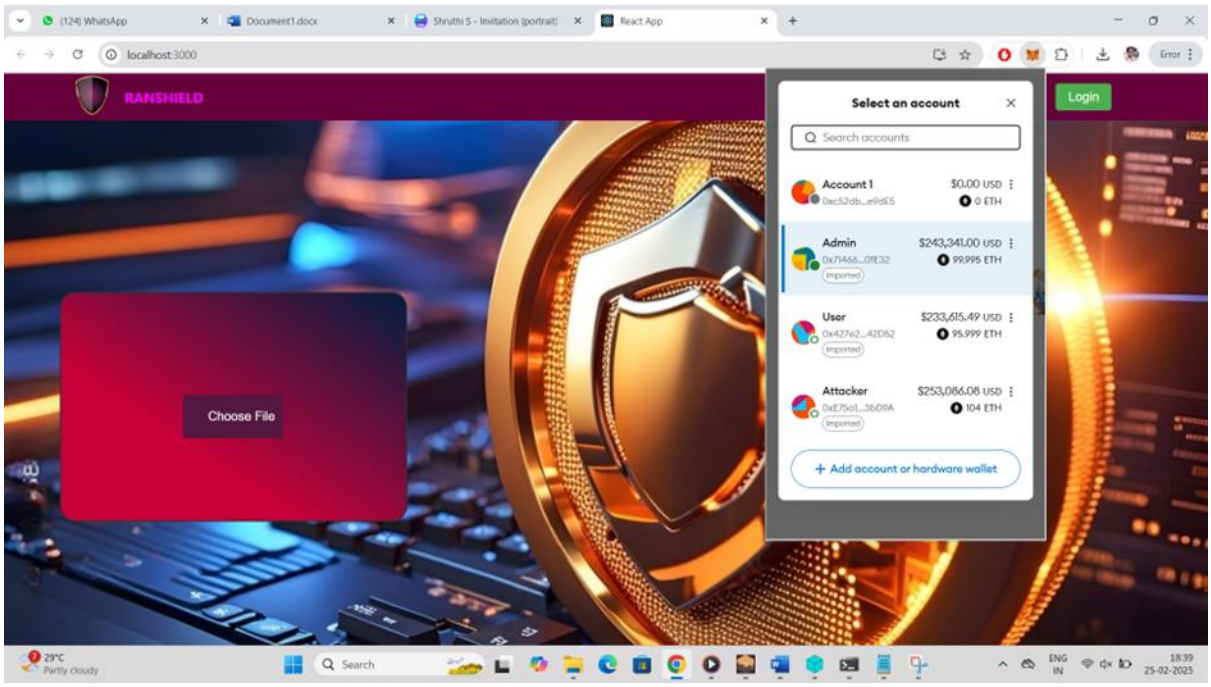


Fig A.3.9 MetaMask-Account Selection

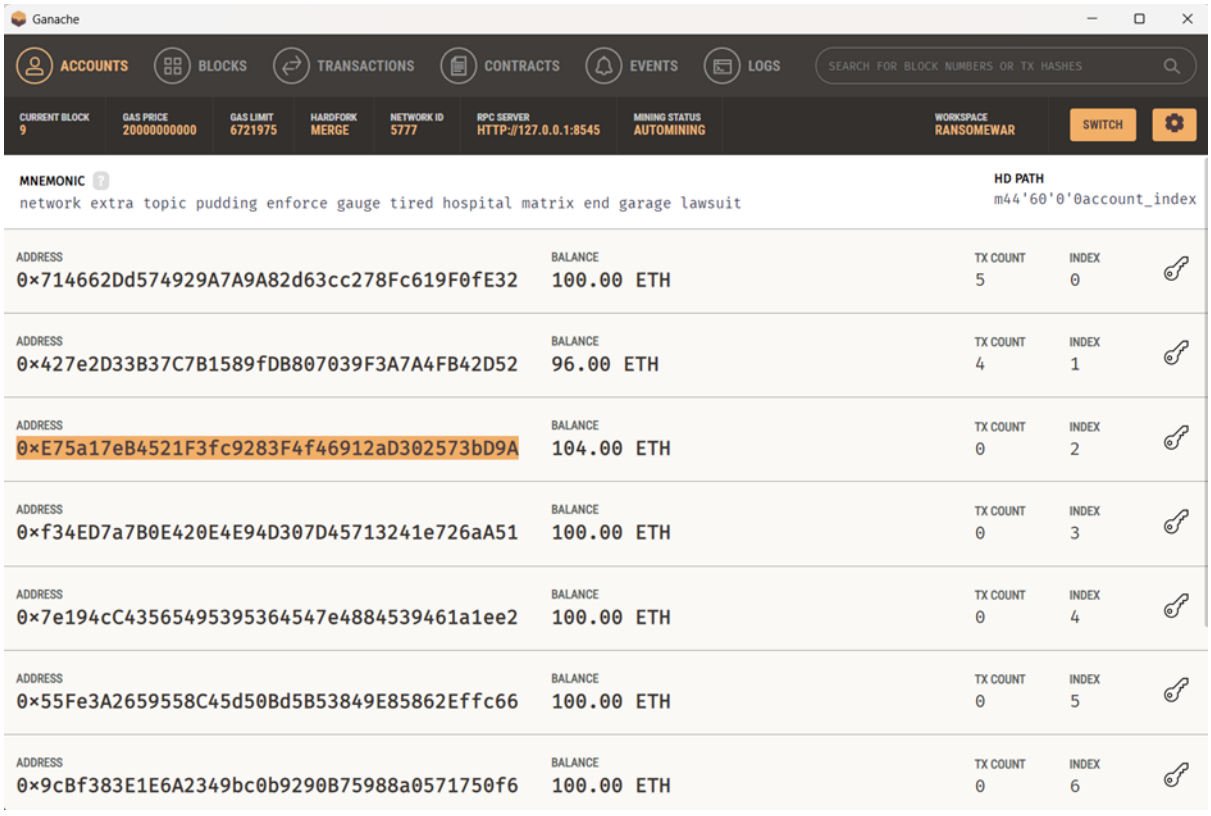


Fig A.3.10 Copying Attacker Address from Ganache

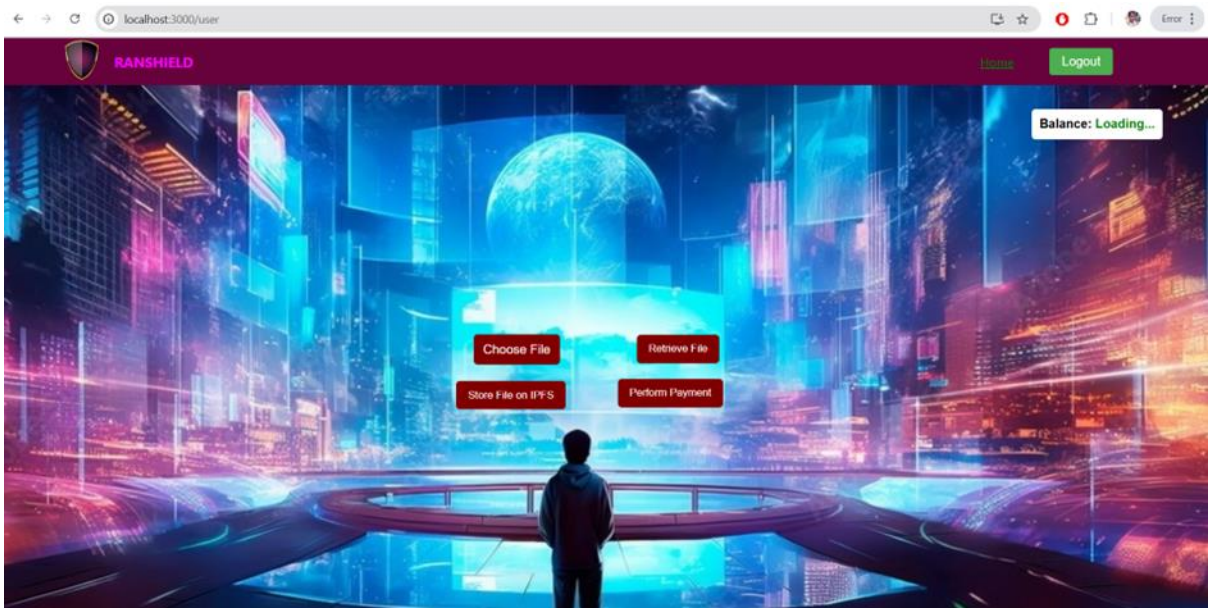


Fig A.3.11 User Login

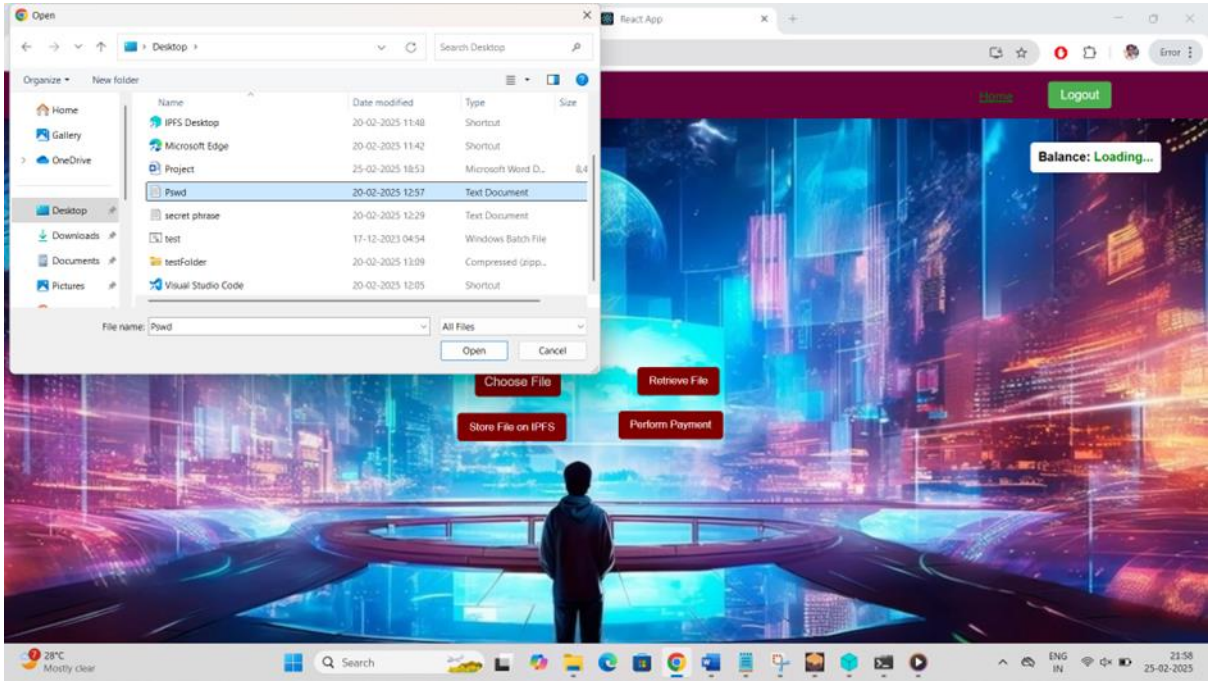


Fig A.3.12 User Login- Choose File

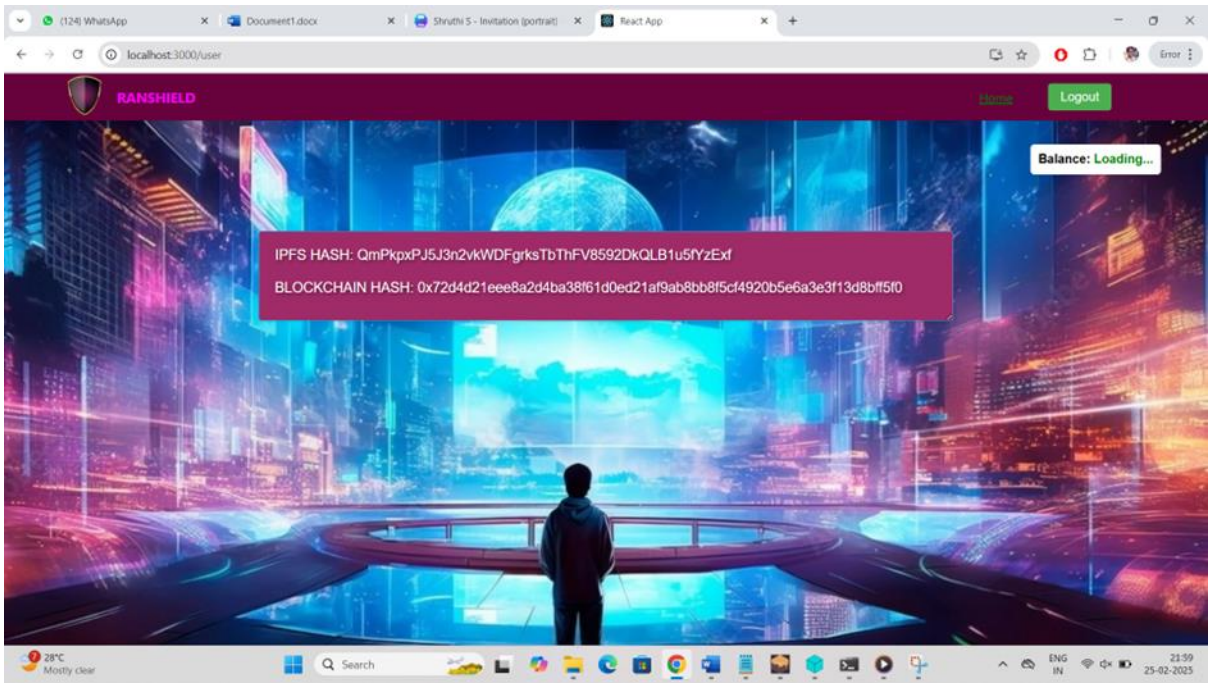


Fig A.3.13 User Login- Store File on IPFS

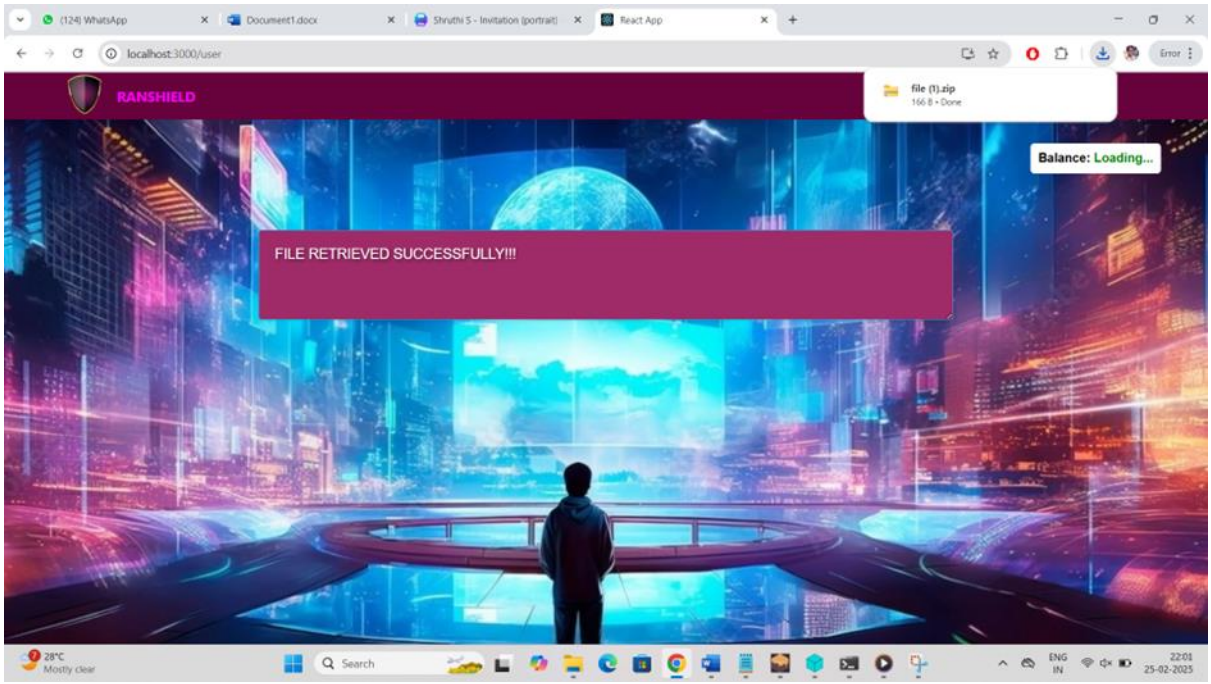


Fig A.3.14 User Login- Retrieve File

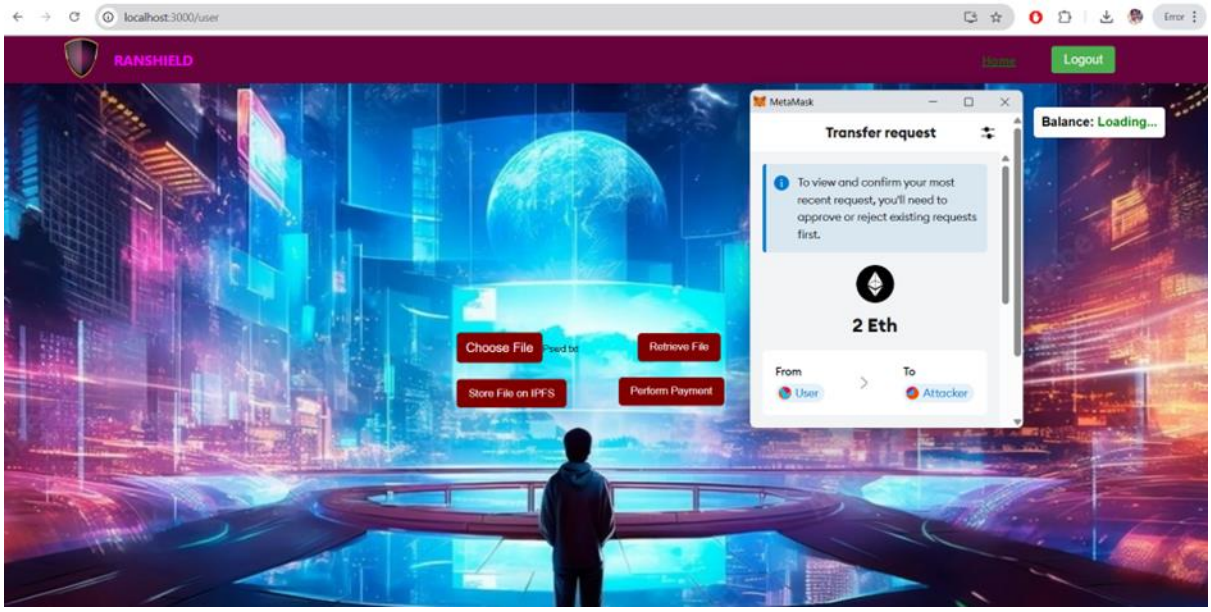


Fig A.3.15 User Login- Perform Payment

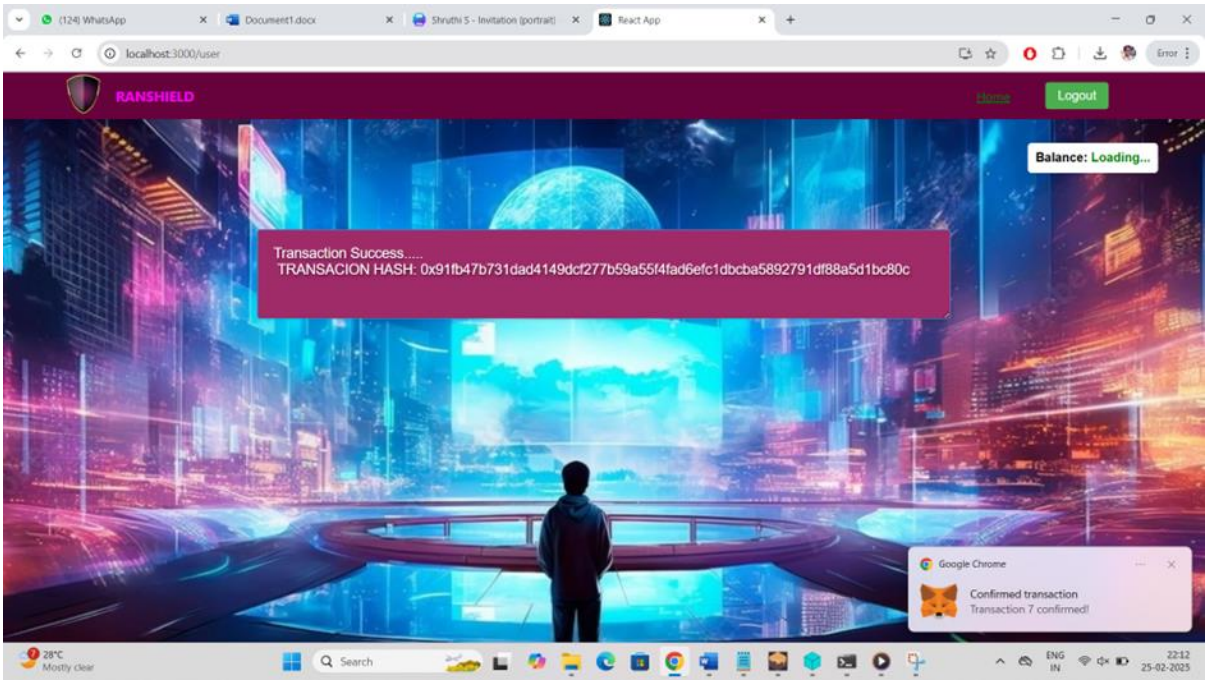


Fig A.3.16 Snore Toast Notification- Confirmed Transaction

Fig A.3.17 Attacker Login

Fig A.3.18 Crypto Attack- Encrypt Data

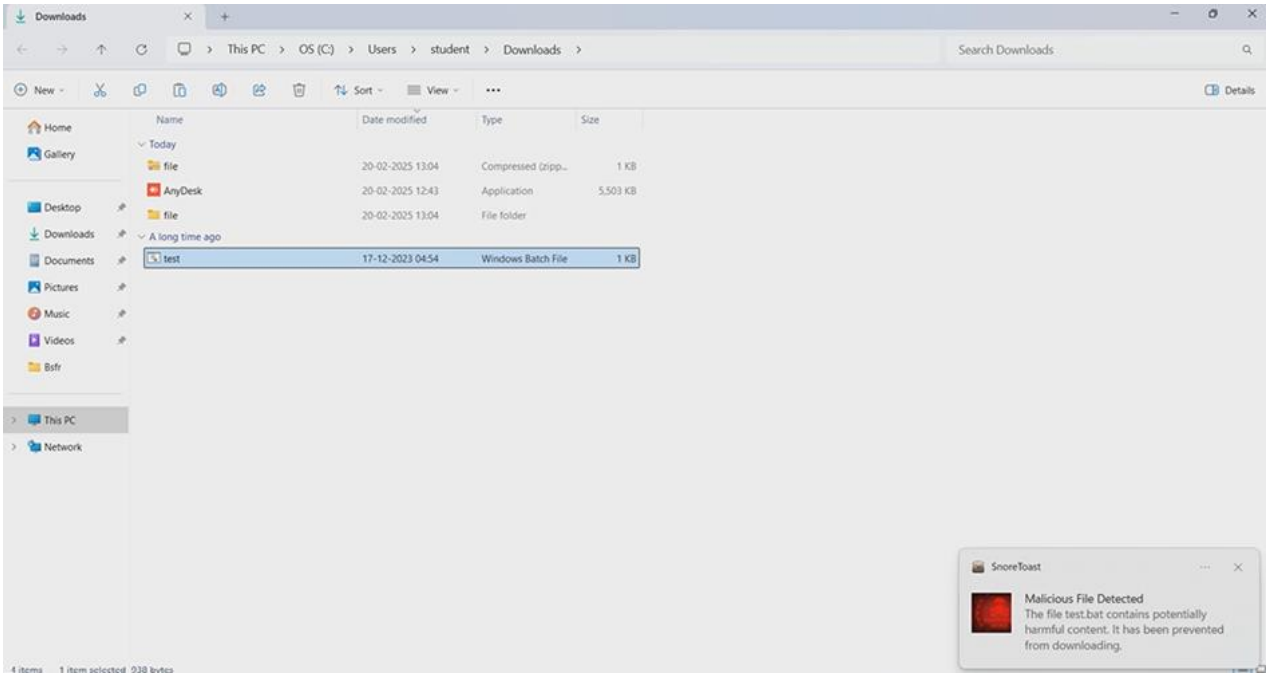


Fig A.3.19 Detection of Malicious Files

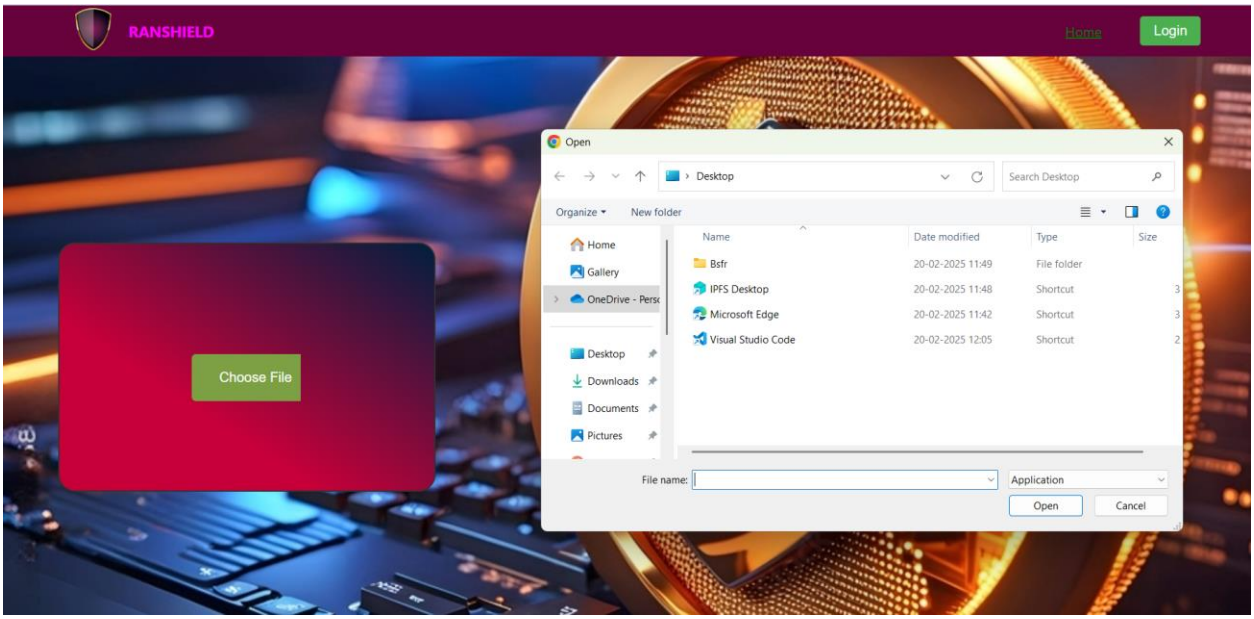


Fig A.3.20 Selecting a File for Security Check

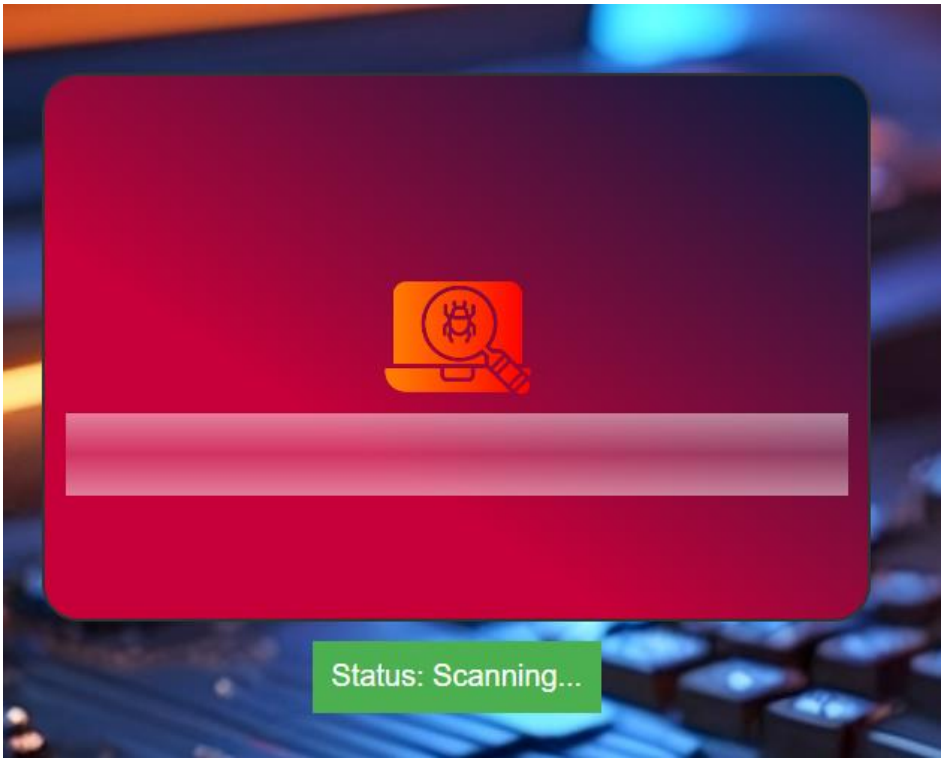


Fig A.3.21 System Scan in Progress

Fig A.3.22 Scan Complete – Status Verified as Legitimate

A4. PLAGIARISM REPORT

The plagiarism report reflects a strong commitment to originality, with only a 5% similarity detected. Most matches come from credible sources, indicating well-researched content. No integrity flags were found, demonstrating a responsible approach to academic writing. With minor improvements in citations, the document showcases a high standard of authenticity and credibility.

Document Details

Submission ID
trn:oid:::1:3186721117

Submission Date
Mar 18, 2025, 11:13 AM GMT+5:30

Download Date
Mar 18, 2025, 11:14 AM GMT+5:30

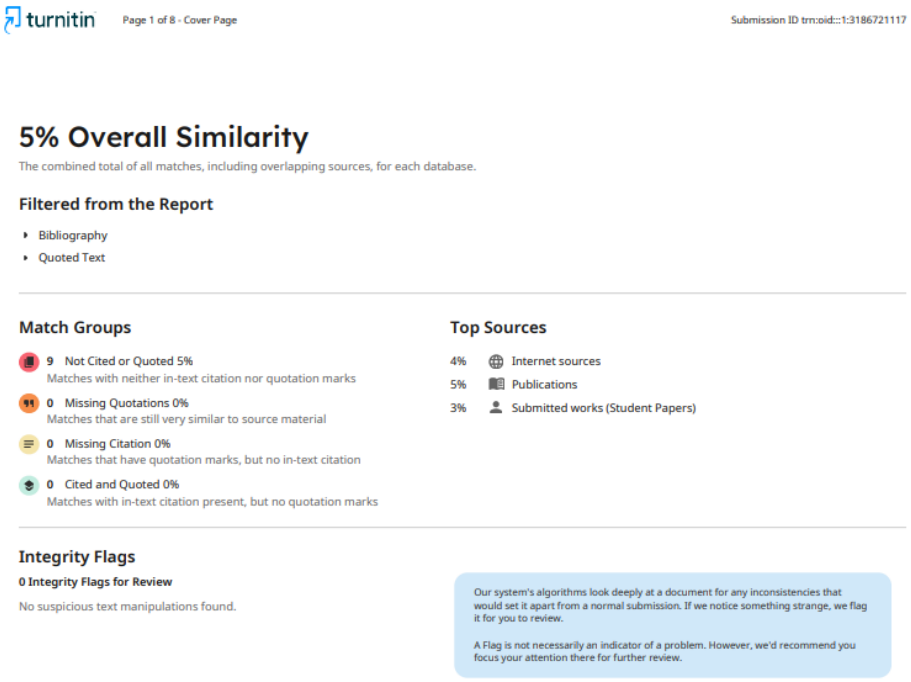
File Name
Paper_final1.0.pdf

File Size
597.5 KB

5 Pages

2,948 Words

17,970 Characters



turnitin Page 1 of 8 - Cover Page Submission ID trn:oid:::1:3186721117

5% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text

Match Groups

9 Not Cited or Quoted 5%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

4% Internet sources
5% Publications
3% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- 9 Not Cited or Quoted 5%
  Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
  Matches that are still very similar to source material
- 0 Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

4% Internet sources
5% Publications
3% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
ijritcc.org		1%
2	Internet	
researchoutput.csu.edu.au		<1%
3	Internet	
lup.lub.lu.se		<1%
4	Student papers	
Panimalar Engineering College		<1%
5	Internet	
www.researchgate.net		<1%
6	Publication	
H.L. Gururaj, Francesco Flammini, S. Srividhya, M.L. Chayadevi, Sheba Selvam. "Co...		<1%
7	Publication	
Nadeem Ahmed, Fayaz Hassan, Khursheed Aurangzeb, Arif Hussain Magsi, Musae...		<1%

Machine Learning-Driven Security Framework Integrated with Blockchain for Ransomware Prevention and Mitigation in the Banking Sector

Charmine Maria Thomas
B. E Department of Computer Science and Engineering
Panimalar Engineering College
Chennai, India
charminethomas12@gmail.com

Janani A
B. E Department of Computer Science and Engineering
Panimalar Engineering College
Chennai, India
janu.401anand@gmail.com

Lakshmi D
Associate Professor
Panimalar Engineering College
Chennai, India
dlakshmicse105@gmail.com

Gunashri S
B. E Department of Computer Science and Engineering
Panimalar Engineering College
Chennai, India
gunashri2003@gmail.com

***Abstract*—Ransomware attacks, which can cause operational disruptions and financial losses, are particularly common in the banking industry. A Blockchain-integrated ML-DSF (Machine Learning- Driven Security Framework) is suggested as a countermeasure to these dangers. For real-time ransomware detection, the system analyses data patterns in executable files using machine learning methods. The technology reduces the chance of ransomware execution by spotting dangerous patterns early. The system incorporates a private blockchain to store backups and provide safe, tamper-proof data retrieval without the need for ransom payments. Payments can be paid securely, even if the ransom is less than the value of the file, and user credentials are kept anonymous to stop hackers from using them for further thefts. Blockchain and machine learning together improve threat detection, speed up IR(Incident Response), and guarantee operational resilience. This all-inclusive solution protects vital financial information and offers banking environments a strong, safe, and scalable defence against ransomware.**

Keywords*—ML-DSF** (*Machine Learning- Driven Security Framework*), **IR** (*Incident Response*), ***Ransomware Detection, Private Blockchain

I. Introduction

The banking industry is at menace from ransomware since it can cause financial losses and service outages. Phishing, unpatched vulnerabilities, and inadequate security are all targets for cybercriminals. Risks are increased by sophisticated strategies like RaaS and double extortion. Due to the shortcomings of traditional security, blockchain backups and machine learning detection are crucial (1)(3)(9).

A. Ransomware in the Banking Sector

Ransomware poses a threat to banking through losses, service interruptions, and data exposures. Cybercriminals take advantage of weaknesses like phishing, which are made worse by RaaS and double extortion. Machine learning and blockchain backups guarantee real-time security and detection.

B. Blockchain and Machine Learning

Blockchain makes backups unchangeable, and SHA-256 detects unwanted alterations. To improve real-time cybersecurity and secure recovery, machine learning (Extra-Trees Classifier) examines PE files to identify ransomware pre-encryption.

C. Ganache and MetaMask

Blockchain backups and safe smart contract testing are made possible by Ganache. Secure ransom payments are guaranteed by MetaMask, which also handles transactions. When combined, they improve productivity, security, and transparency against ransomware.

II. Related Works

An overview of further similar schemes in the area is given in this section.

M. Wazid, A. Kumar Das and S. Shetty [1]A blockchain-based platform called BSFR-SH is suggested by the study as a ransomware defence tool for smart healthcare. Tamper-proof security is guaranteed by its transparency and immutability. BSFR-SH improves threat detection by outperforming current techniques in terms of accuracy and F1-score.

Suri babu Nuthalapati[2]In order to detect fraud and predict loans in digital banking, this study use machine learning. While Random Forest gets 92% accuracy for loans, SVM detects fraud with 90% accuracy. Future studies will examine scalability and blockchain integration as ways to improve security through adaptive learning.

Ade Ilham Fajri, Mohammad Isa Irawan[3]For ransomware mitigation, this SLR investigates blockchain-based cybersecurity with an emphasis on security, transparency, and issues including scalability. It evaluates important paradigms and emphasises how blockchain can lead to better security and interoperability.

Aaron Zimba[4]A Bayesian Attack Network model is presented in this paper to analyse cyber intrusions in GameOver Zeus. It strengthens financial cybersecurity by enhancing attack modelling and evaluating exploitability concerns through the use of phishing and CVEs.

I. A. Chesti, M. Humayun, N. U. Sama and N. Jhanjhi[6]This article examines ransomware's evolution,

financial effects, and concerns, including cryptocurrency payments and ambiguous file recovery. It examines defence strategies, recovery methods, and the need for advanced cybersecurity to fend off new threats.

A.A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi and S. A. Ebad[7]This study helps with risk management by classifying cyberthreats in banking according to their level of severity. It looks at countermeasures, changing hazards, and protections. In order to safeguard resources, confidence, and financial stability, cybersecurity must be strengthened.

Sandeep Reddy Gudimetla [9] This study examines 24 ransomware prevention solutions, emphasising user awareness, security policies, backups, and detection methods. It highlights the necessity of preventative security measures by classifying ransomware kinds and analysing actual incidents like WannaCry.

S. Sharmeen, Y. A. Ahmed, S. Huda, B. Ş. Koçer and M. M. Hassan[10]This study emphasises the changing threat of ransomware and its detection difficulties. It suggests a semi-supervised deep learning approach that combines supervised classification and unsupervised learning to find hidden patterns. Real ransomware data is used to test the framework.

A. Role of Machine Learning in Detection

Machine learning models, including Random Forest, SVM, Decision Tree, and LSTM, that are trained on labelled datasets are used to detect ransomware. Detecting banking fraud is made easier by the excellent accuracy of SVM and Random Forest. [3].

B. Bayesian Attack Networks (BANs) for Threat Prediction

In order to estimate cyber threats, Bayesian Attack Networks (BANs) use CVSS scores to map vulnerabilities and attack probability. Conditional Probability Tables help with proactive defence and improve cybersecurity by forecasting the spread of attacks.[5].

C. Application in Banking Sector and General Cybersecurity Measures

Banking transaction monitoring, credit risk modelling, and fraud detection are all aided by machine learning. To safeguard private information from online attacks, organisations use firewalls, routers, and frequent vulnerability assessments.[21][25]

D. Disadvantages

The current approach does not stop attacks; it controls the results. pBFT creates latency, inadequate cryptographic verification restricts security, and peer-to-peer storage poses centralisation threats. Issues with feature selection and overfitting plague conventional models such as Random Forest and SVM.

III. PROPOSED MACHINE LEARNING-DRIVEN SECURITY FRAMEWORK INTEGRATED WITH BLOCKCHAIN FOR RANSOMWARE PREVENTION AND MITIGATION IN THE BANKING SECTOR

The Ransomware Detection and Mitigation System safeguards users from ransomware attacks using blockchain (Ganache), decentralized storage (IPFS), and smart contract-based security. The front end, built with React.js, ensures a responsive UI, while Java and Node.js handle backend threat detection. The system includes three key roles: Admin, User, and Attacker.

Front End:A JavaScript library called React.js is freely accessible and intended for creating interactive user interfaces. It allows for effective DOM updates for dynamic web apps by organising programs into reusable components.

In this system, React is used to build an intuitive interface for:

- File scanning and ransomware detection
- Blockchain-based file backup and recovery
- Real-time monitoring, interactive alerts, and data visualization

A. Secure File Backup Using Ipfs And Blockchain

Users can securely store their files on IPFS (InterPlanetary File System), ensuring data integrity and resistance to tampering.

- IPFS hashes are stored on the Ganache blockchain, preventing unauthorized alterations.
- In case of a ransomware attack, users can retrieve original files from IPFS by verifying hashes on the blockchain.

IPFS Working: The InterPlanetary File System (IPFS) is a redistributed, peer-to-peer storehouse network. Unlike traditional cloud storage that relies on centralized servers, IPFS distributes files across nodes. It replaces location-based addressing with content-based addressing, assigning each file a unique cryptographic hash (CID) using SHA-256 for tamper-proof storage.

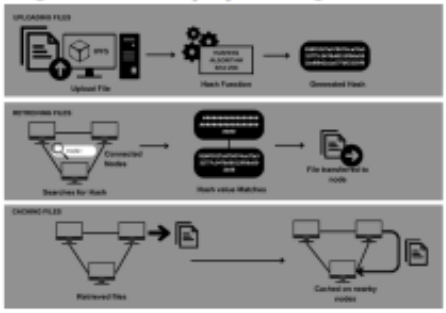


Fig. 1. Diagram For Working IPFS

A cryptographic hash from the SHA-2 family, SHA-256 gives a 256-bit hash for any input, ensuring data integrity and tamper-proof storage. It produces a unique fingerprint H(M) for input M:

$$H(M) = SHA\text{-}256(M) \quad (1)$$

Where M is the file data, H(M) is the 256-bit hash. Any alteration in M will result in a completely different hash, which

$$H_s \neq H_r \Rightarrow \text{Data has been tampered with.}$$

helps detect changes or ensure authenticity. For data integrity verification, if the stored hash Hs and the recomputed hash Hr do not match, then the data has been tampered. (2)

B. Ransomware Detection System

The system features a ransomware scanning capability, enabling users to assess files for potential threats before storing or retrieving them. A honeypot-based dataset trains the ransomware detection model using real-world ransomware samples.A decoy system attracts ransomware, collecting malware samples for analysis. For efficiency, the extracted features are subsequently input into the Extra-Trees Classifier.

Machine Learning Model : Extra-Trees Classifier: It is an ensemble learning algorithm which improves decision trees by randomizing feature selection and split points. Unlike Random Forests, Extra-Trees use the entire dataset without bootstrapping and select splits randomly, reducing overfitting.

Fig. 2. Machine Learning Process

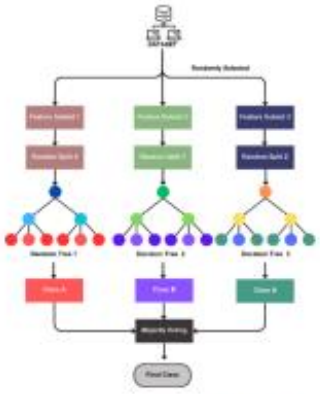


Fig. 3. Working of Extra -Trees Classifier

At each node, a random feature fj and random split S_j are chosen:

$$f(X) = \begin{cases} \text{Left Subtree}, & X[f_j] \le s_j \\ \text{Right Subtree}, & X[f_j] > s_j \end{cases} \quad (3)$$

Where, fj is a randomly selected feature, Sj is a randomly selected split threshold.

A majority vote over N trees yields the final prediction:

$$\hat{Y} = \text{mode}\{h_1(X), h_2(X), ..., h_N(X)\} \quad (4)$$

C. Blockchain and Ganache

Blockchain is a digital ledger that securely records transactions across nodes. It is decentralized, unchangeable, and ensures data integrity, security, and transparency. File hashes from IPFS are stored on Ganache, a personal Ethereum blockchain. Smart contracts are developed, tested, and deployed locally in Ganache before release on the main Ethereum network.

Ganache hosts a private Ethereum blockchain on your PC, enabling smart contract testing without an internet connection. It provides pre-funded accounts with test ETH to simulate transactions. When launched, Ganache generates ten accounts with preloaded ETH for testing dApps, transactions, and smart contracts without real money.

D. Simulated Ransomware Attack

The Attacker Module mimics ransomware attacks to evaluate the effectiveness of blockchain-based mitigation. Real-world attack scenarios test the system's resistance to unauthorized access and data breaches. The two main attack types simulated are:

- Locker Ransomware: Modifies login credentials to block user access until a ransom is paid. Unlike crypto ransomware, it doesn't encrypt files.
- Crypto Ransomware: Encrypts user data, making it unreadable without a decryption key. Attackers demand cryptocurrency and threaten permanent data loss if unpaid.

E. *Metamask*

MetaMask, a blockchain gateway and cryptocurrency wallet, enables secure transactions, storage, and seamless interaction with dApps. It enables users to manage digital assets across several blockchains and is accessible as a browser extension and mobile app. Including encryption and authentication tools, MetaMask ensures private key safety and full user control. In blockchain-based transactions, MetaMask secures money transfers, data verification, and financial operations. It enhances cybersecurity by verifying file authenticity in ransomware mitigation. If blockchain verification fails to recover data, MetaMask serves as a backup for ransom payments.

IV. SYSTEM IMPLEMENTATION

The user system integrates a machine learning model to classify portable executable (PE) files into legitimate or ransomware files, ensuring real-time threat detection.Upon detecting ransomware, the system automatically deletes the malicious files to prevent further damage and ensure data security. A backup kept on the blockchain allows the user to safely restore their data in the event of a ransomware attack, guaranteeing reliability and protection. Blockchain's decentralized and impermeable structure ensures the security of the data that has been backed up, eliminating the necessity for cryptocurrency payments in order to recover the data.

Fig. 4. System Workflow

Fig. 5. User Module

Fig. 6. Smart Contract-Based Payment Module

V. RESULTS AND DISCUSSION

Our application provides a seamless and secure experience for users, beginning with real-time system monitoring and ransomware detection. Users can upload files for scanning, and the system analyzes them using the Extra-Trees Classifier to detect potential threats. If ransomware is detected, it is automatically removed, and users are alerted. Additionally, the system stores critical files in blockchain-based backup, ensuring tamper-proof recovery in case of an attack. In extreme cases, secure transactions via MetaMask enable safe ransom payments. By combining machine learning and blockchain, our system provides enhanced cybersecurity, data integrity, and ransomware resilience for users.

To evaluate the effectiveness of our ransomware detection model, we examine its performance using a confusion matrix. This visualization provides data on categorization accuracy together with false positive and false negative rates. By improving overall threat identification, reducing errors, and fine-tuning the detection algorithm, this method strengthens our system's resistance to changing ransomware attacks. In order to improve accuracy, we additionally update the model on a regular basis. To guarantee adaptive security, we use fresh datasets and patterns. In the financial industry, the combination of blockchain technology and machine learning offers a scalable, intelligent, and future-proof security against cyberattacks..

Fig. 7. File Retrieval Using Blockchain Backup

Fig. 8. Secure Payment Using MetaMask

We evaluate the effectiveness of our ransomware detection technology by analysing its performance using a error matrix. This visualization provides data on categorization accuracy together with false positive and false negative rates.

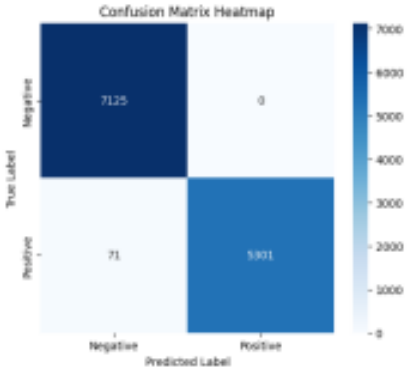


Fig. 9. Confusion Matrix of the Classifier Model

With a remarkable 99.43% accuracy and an F1-score of 0.99, the Extra-Trees Classifier showed its exceptional ability to accurately and consistently distinguish between malicious and legitimate data. By leveraging machine learning, the model provides a robust security layer that significantly guarantees proactive defence against upcoming cyberthreats.

VI. CONCLUSION

In summary, the proposed Machine Learning-Driven Security Framework (ML-DSF) in conjunction with Blockchain provides a dependable and scalable approach to preventing and reducing ransomware in the banking sector. The architecture employs machine learning algorithms for real-time ransomware detection and a private blockchain for safe, tamper-proof data storage, improving cybersecurity resilience while lowering operational disruptions and financial losses. Secure transactions, immutable backup storage, and proactive threat detection work together to guarantee data integrity and do away with the need for ransom payments. This multi-layered strategy offers a state-of-the-art, future-proof defence against changing ransomware threats while also greatly enhancing incident response capabilities and safeguarding sensitive financial data.

REFERENCES

[1] M. Wazid, A. Kumar Das and S. Shetty, "BSFR-SH: Blockchain-Enabled Security Framework Against Ransomware Attacks for Smart Healthcare," in IEEE Transactions on Consumer Electronics, vol. 69, no. 1, pp. 18-28

[2] Suri babu Nuthalapati. (2023). AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking. Educational Administration: Theory and Practice, 29(1), 357–368.

[3] A.I. Fajri, M. I. Irawan and F. Maharanto, "A Systematic Literature Review on Blockchain-based Cybersecurity Models for Ransomware Mitigation," 2024 IEEE International Symposium on Consumer Technology (ISCT), Kuta, Bali, Indonesia, 2024, pp. 799-804

[4] Aaron Zimba, "A Bayesian Attack-Network Modeling Approach to Mitigating Malware-Based Banking Cyberattacks", International Journal of Computer Network and Information Security(IJCNIS), Vol.14, No.1, pp.25-39, 2022

[5] Alenizi , J. and Alrashdi, I. (2023) "SFMR-SH: Secure Framework for Mitigating Ransomware Attacks in Smart Healthcare Using Blockchain Technology", Sustainable Machine Intelligence Journal, 2, pp. (4):1–19.

[6] I. A. Chesti, M. Humayun, N. U. Sama and N. Jhanjhi, "Evolution, Mitigation, and Prevention of Ransomware," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2020, pp. 1-6.

[7]] A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi and S. A. Ebad, "Cyber Threats Classifications and Countermeasures in Banking and Financial Sector," in IEEE Access, vol. 11, pp. 125138-125158, 2023.

[8] D. Smith, S. Khorsandroo and K. Roy, "Machine Learning Algorithms and Frameworks in Ransomware Detection," in IEEE Access, vol. 10, pp. 117597-117610, 2022.

[9] Sandeep Reddy Gudimetla. (2022). Ransomware Prevention and Mitigation Strategies. International Journal on Recent and Innovation Trends in Computing and Communication, 10(12), 12–20.

[10] S. Sharmeen, Y. A. Ahmed, S. Huda, B. Ş. Koçer and M. M. Hassan, "Avoiding Future Digital Extortion Through Robust Protection Against Ransomware Threats Using Deep Learning Based Adaptive Approaches," in IEEE Access, vol. 8, pp. 24522-24534, 2020.

[11] Nkongolo, M. and Tokmak, M., 2024. Ransomware detection using stacked autoencoder for feature selection. arXiv preprint arXiv:2402.11342.

[12] Nkongolo Wa Nkongolo, M., 2024. RFSA: A Ransomware Feature Selection Algorithm for Multivariate Analysis of Malware Behavior in Cryptocurrency. International Journal of Computing and Digital Systems, 15(1), pp.893-927.

[13] Arugo, P., Venter, H. and Nkongolo, M.W., 2024. Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset. arXiv preprint arXiv:2404.12855

[14]] Huan, N.T.Y. and Zukarnain, Z.A., 2024. A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications. IEEE Access.

[15] S. I. Bae, G. B. Lee, and E. G. Im, "Ransomware detection using machine learning algorithms," Concurrency Comput., Pract. Exper., Jun. 2019, Art. no. e5422.

[16] F. Malecki, "Best practices for preventing and recovering from a ransomware attack," Comput. Fraud Secur., vol. 2019, no. 3, pp. 8–10, Mar. 2019

[17] K. Lee, S.-Y. Lee, and K. Yim, "Machine learning based file entropy analysis for ransomware detection in backup systems," IEEE Access, vol. 7, pp. 110205–110215, 2019.

[18] G. Hull, H. John, and B. Arief, "Ransomware deployment methods and analysis: Views from a predictive model and human responses," Crime Sci., vol. 8, no. 1, p. 1, 2019.

[19] S. Poudyal, K. P. Subedi, and D. Dasgupta, "A framework for analyzing ransomware using machine learning," in Proc. IEEE Symp. Ser. Comput. Intell. (SSCI), Nov. 2018, pp. 1692–1699

[20] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, "Ransomware, threat and detection techniques: A review," Int. J. Comput. Sci. Netw. Secur., vol. 19, no. 2, pp. 136–146, Feb. 2019.

[21] D. Ghelani, T. K. Hua, and S. K. R. Koduru, "Cyber security threats, vulnerabilities, and security solutions models in banking," Authorea, Sep. 2022

[22] L. Freedman. (2020). Ransomware Attacks Predicted to Occur Every 11 Seconds in 202 With a Cost of $20 Billion. Accessed: Jan. 11, 2021.

[23] A. Q. Stanikzai and M. A. Shah, "Evaluation of cyber security threats in banking systems," in Proc. IEEE Symp. Ser. Comput. Intell. (SSCI), Dec. 2021, pp. 1–4.

[24] M. Best, L. Krumov, and I. Bacivarov, "Cyber security in banking sector," Int. J. Inf. Secur. Cybercrime, vol. 8, no. 2, pp. 39–52, Dec. 2019

[25] M. Leo, S. Sharma, and K. Maddulety, "Machine learning in banking risk management: A literature review," Risks, vol. 7, no. 1, p. 29, Mar. 2019.

A.5. PAPER PUBLICATION

Conference: 8th INTERNATIONAL CONFERENCE on INTELLIGENT COMPUTING

Paper Id: 962

Title: Machine Learning-Driven Security Framework Integrated with Blockchain for Ransomware Prevention and Mitigation in the Banking Sector

Reviewer Comments:

Blockchain-integrated ML-DSF offers a strong, scalable defense by combining machine learning for real-time ransomware detection with tamper-proof blockchain-based data backups, enhancing security and operational resilience.

PANIMALAR ENGINEERING COLLEGE

JAISAKTHI EDUCATIONAL TRUST
An Autonomous Institution & Affiliated to Anna University,
Approved by AICTE, New Delhi, Accredited by National Board of Accreditation(NBA)
Bangalore Trunk Road, Poonamallee, Chennai-600123

BEST PAPER

PECTEAM 2K25

This is to certify that Dr./Mr./Ms. JANANI. A from
PANIMALAR ENGINEERING COLLEGE has received BEST PAPER AWARD
entitled MACHINE LEARNING - DRIVEN SECURITY FRAMEWORK
INTEGRATED WITH BLOCKCHAIN FOR RANSOMWARE
in the 8th International Conference on Intelligent Computing (IConIC) held on
21 st & 22 nd March, 2025.

HEAD OF DEPARTMENT
CONVENER
Dr.S.MALATHI,M.E.,Ph.D.,
CO - PATRON
Dr.K.MANI, M.E.,Ph.D.,

IEEE MADRAS SECTION
IEEE COMPUTER SOCIETY

PANIMALAR ENGINEERING COLLEGE

JAISAKTHI EDUCATIONAL TRUST
An Autonomous Institution & Affiliated to Anna University,
Approved by AICTE, New Delhi, Accredited by National Board of Accreditation(NBA)
Bangalore Trunk Road, Poonamallee, Chennai-600123

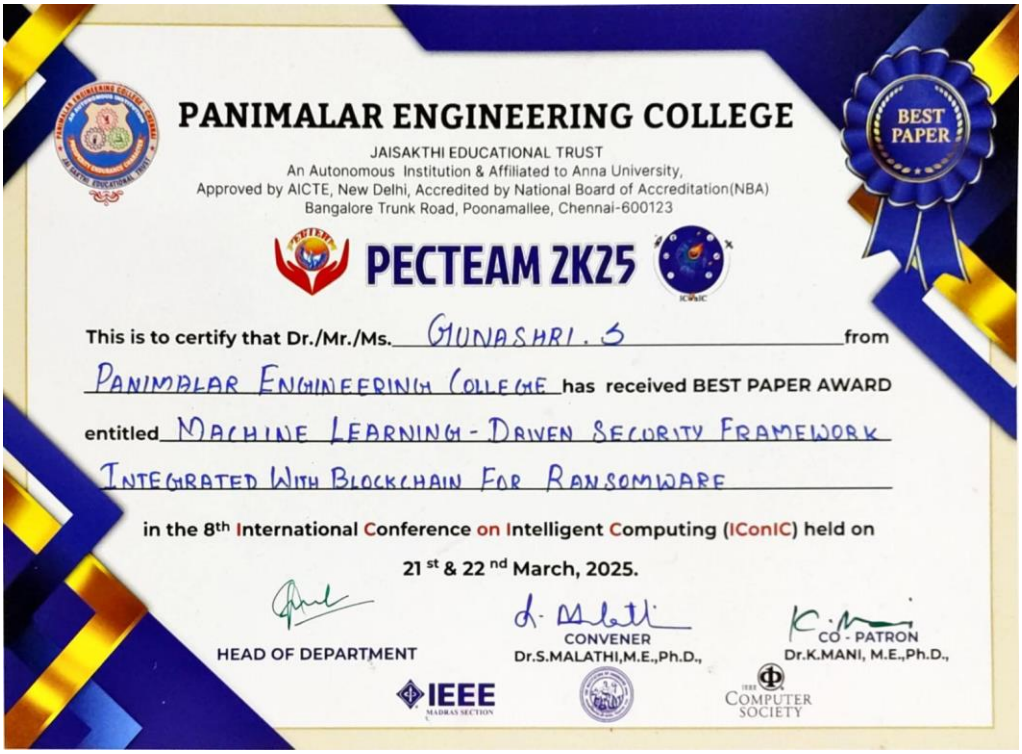
BEST PAPER

PECTEAM 2K25

This is to certify that Dr./Mr./Ms. CHARMINE MARIA THOMAS from
PANIMALAR ENGINEERING COLLEGE has received BEST PAPER AWARD
entitled MACHINE LEARNING - DRIVEN SECURITY FRAMEWORK
INTEGRATED WITH BLOCKCHAIN FOR RANSOMWARE
in the 8th International Conference on Intelligent Computing (IConIC) held on
21 st & 22 nd March, 2025.

HEAD OF DEPARTMENT
CONVENER
Dr.S.MALATHI,M.E.,Ph.D.,
CO - PATRON
Dr.K.MANI, M.E.,Ph.D.,

IEEE MADRAS SECTION
IEEE COMPUTER SOCIETY



PANIMALAR ENGINEERING COLLEGE

JAISAKTHI EDUCATIONAL TRUST
An Autonomous Institution & Affiliated to Anna University,
Approved by AICTE, New Delhi, Accredited by National Board of Accreditation(NBA)
Bangalore Trunk Road, Poonamallee, Chennai-600123

BEST PAPER

PECTEAM 2K25

This is to certify that Dr./Mr./Ms. GUNASHRI. S from
PANIMALAR ENGINEERING COLLEGE has received BEST PAPER AWARD
entitled MACHINE LEARNING-DRIVEN SECURITY FRAMEWORK
INTEGRATED WITH BLOCKCHAIN FOR RANSOMWARE
in the 8th International Conference on Intelligent Computing (IConIC) held on
21 st & 22 nd March, 2025.

HEAD OF DEPARTMENT
CONVENER
Dr.S.MALATHI,M.E.,Ph.D.,
CO - PATRON
Dr.K.MANI, M.E.,Ph.D.,

IEEE MADRAS SECTION
IEEE COMPUTER SOCIETY

REFERENCES

REFERENCES

[1] M. Wazid, A. Kumar Das and S. Shetty, **"BSFR-SH: Blockchain-Enabled Security Framework Against Ransomware Attacks for Smart Healthcare,"** in IEEE Transactions on Consumer Electronics, vol. 69, no. 1, pp. 18-28

[2] Suri babu Nuthalapati. (2023). **"AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking."** Educational Administration: Theory and Practice, 29(1), 357–368.

[3] A.I. Fajri, M. I. Irawan and F. Mahananto, **"A Systematic Literature Review on Blockchain-based Cybersecurity Models for Ransomware Mitigation,"** 2024 IEEE International Symposium on Consumer Technology (ISCT), Kuta, Bali, Indonesia, 2024, pp. 799-804

[4] Aaron Zimba, **"A Bayesian Attack-Network Modeling Approach to Mitigating Malware-Based Banking Cyberattacks,"** International Journal of Computer Network and Information Security (IJCNIS), Vol.14, No.1, pp.25-39, 2022

[5] Alenizi , J. and Alrashdi, I. (2023) **"SFMR-SH: Secure Framework for Mitigating Ransomware Attacks in Smart Healthcare Using Blockchain Technology,"** Sustainable Machine Intelligence Journal, 2, pp. (4):1–19.

[6] A. Chesti, M. Humayun, N. U. Sama and N. Jhanjhi, **"Evolution, Mitigation, and Prevention of Ransomware,"** 2020 2nd International Conference

on Computer and Information Sciences (ICCIS), Sakaka, Saudi Arabia, 2020, pp. 1-6.

[7] A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi and S. A. Ebad, **"Cyber Threats Classifications and Countermeasures in Banking and Financial Sector,"** in IEEE Access, vol. 11, pp. 125138-125158, 2023.

[8] D. Smith, S. Khorsandroo and K. Roy, **"Machine Learning Algorithms and Frameworks in Ransomware Detection,"** in IEEE Access, vol. 10, pp. 117597-117610, 2022.

[9] Sandeep Reddy Gudimetla. (2022). **"Ransomware Prevention and Mitigation Strategies."** International Journal on Recent and Innovation Trends in Computing and Communication, 10(12), 12–20.

[10] S. Sharmeen, Y. A. Ahmed, S. Huda, B. Ş. Koçer and M. M. Hassan, **"Avoiding Future Digital Extortion Through Robust Protection Against Ransomware Threats Using Deep Learning Based Adaptive Approaches,"** in IEEE Access, vol. 8, pp. 24522-24534, 2020.

[11] Nkongolo, M. and Tokmak, M. (2024). **"Ransomware detection using stacked autoencoder for feature selection."** arXiv preprint arXiv:2402.11342.

[12] Nkongolo Wa Nkongolo, M. (2024). **"RFSA: A Ransomware Feature Selection Algorithm for Multivariate Analysis of Malware Behavior in Cryptocurrency."** International Journal of Computing and Digital Systems, 15(1), pp.893-927.

[13] Azugo, P., Venter, H. and Nkongolo, M.W. (2024). **"Ransomware Detection and Classification Using Random Forest: A Case Study with the UGRansome2024 Dataset."** arXiv preprint arXiv:2404.12855.

[14] Huan, N.T.Y. and Zukarnain, Z.A. (2024). **"A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications."** IEEE Access.

[15] S. I. Bae, G. B. Lee, and E. G. Im, **"Ransomware detection using machine learning algorithms,"** Concurrency Comput., Pract. Exper., Jun. 2019, Art. no. e5422.

[16] F. Malecki, **"Best practices for preventing and recovering from a ransomware attack,"** Comput. Fraud Secur., vol. 2019, no. 3, pp. 8–10, Mar. 2019.

[17] K. Lee, S.-Y. Lee, and K. Yim, **"Machine learning based file entropy analysis for ransomware detection in backup systems,"** IEEE Access, vol. 7, pp. 110205–110215, 2019.

[18] G. Hull, H. John, and B. Arief, **"Ransomware deployment methods and analysis: Views from a predictive model and human responses,"** Crime Sci., vol. 8, no. 1, p. 1, 2019.

[19] S. Poudyal, K. P. Subedi, and D. Dasgupta, **"A framework for analyzing ransomware using machine learning,"** in Proc. IEEE Symp. Ser. Comput. Intell. (SSCI), Nov. 2018, pp. 1692–1699.

[20] S. H. Kok, A. Abdullah, N. Z. Jhanjhi, and M. Supramaniam, **"Ransomware, threat and detection techniques: A review,"** Int. J. Comput. Sci. Netw. Secur., vol. 19, no. 2, pp. 136–146, Feb. 2019.

[21] D. Ghelani, T. K. Hua, and S. K. R. Koduru, **"Cyber security threats, vulnerabilities, and security solutions models in banking,"** Authorea, Sep. 2022.

[22] L. Freedman. (2020). **"Ransomware Attacks Predicted to Occur Every 11 Seconds in 2021 With a Cost of $20 Billion."** Accessed: Jan. 11, 2021.

[23] Q. Stanikzai and M. A. Shah, **"Evaluation of cyber security threats in banking systems,"** in Proc. IEEE Symp. Ser. Comput. Intell. (SSCI), Dec. 2021, pp. 1–4.

[24] M. Best, L. Krumov, and I. Bacivarov, **"Cyber security in banking sector,"** Int. J. Inf. Secur. Cybercrime, vol. 8, no. 2, pp. 39–52, Dec. 2019.

[25] M. Leo, S. Sharma, and K. Maddulety, **"Machine learning in banking risk management: A literature review,"** Risks, vol. 7, no. 1, p. 29, Mar. 2019.

[26] M. A. Kazi, S. Woodhead, and D. Gan, **"An investigation to detect banking malware network communication traffic using machine learning techniques,"** J. Cybersecurity Privacy, vol. 3, no. 1, pp. 1–23, Dec. 2022.

[27] Segun, B. I. Ujioghosa, S. O. Ojewande, F. O. Sweetwilliams, S. N. John, and A. A. Atayero, **"Ransomware: Current trend, challenges, and research directions,"** in Proc. World Congr. Eng. Comput. Sci., 2017, pp. 169–174.

[28] O. Mbaabu. (Dec. 11, 2020). **"Introduction to Random Forest in Machine Learning."** Accessed: Jan. 22, 2021.

[29] D. Sgandurra, L. Munoz-Gonzalez, R. Mohsen, and E. C. Lupu, **"Automated dynamic analysis of ransomware: Benefits, limitations and use for detection,"** 2016, arXiv:1609.03020.

[30] O. Delgado-Mohatar, J. M. Sierra-Camara, and E. Anguiano, **"Blockchain-based semi-autonomous ransomware,"** Future Gener. Comput. Syst., vol. 112, pp. 589–603, Nov. 2020.