PANIMALAR
ENGINEERING COLLEGE
An Autonomous Institution
Affiliated to Anna University, Chennai
(JAISAKTHI EDUCATIONAL TRUST)

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

SDG 9
SDG 16

BATCH NO: A7

PROJECT GUIDE: DR.D. LAKSHMI, ASSOCIATE PROFESSOR

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

CHARMINE MARIA THOMAS 211421104043
GUNASHRI S 211421104082
JANANI A 211421104101

SDG GOALS

Cybersecurity can help safeguard critical Banking Industry

Cybersecurity can help fight cybercrime, which can threaten the safety of community

OBJECTIVE

- The Machine Learning-Driven Security Framework uses blockchain’s secure and unchangeable nature along with machine learning’s ability to detect unusual patterns to fight ransomware attacks.
- Designed for the banking sector, it helps detect threats, reduce risks, and prevent future attacks.
- By combining real-time threat detection with secure record-keeping, it ensures strong data protection, transparency, and reliability for financial transactions and sensitive information.

BASE PAPER

Title: Blockchain-Enabled Security Framework Against Ransomware Attacks for Smart Healthcare (BSFR-SH)

Authors: Mohammad Wazid, Ashok Kumar Das, Sachin Shetty

Transaction: IEEE Transactions on Consumer Electronics

Volume: 69

Published Date: February 2023

ABSTRACT

Ransomware attacks pose a significant risk, causing financial losses and operational disruptions. This system introduces a Machine Learning-Driven Security Framework integrated with Blockchain to tackle ransomware threats in the banking sector. The framework employs the machine learning algorithm Extra-Trees Classifier to analyze the data patterns in executable files and detect malicious files to prevent ransomware attacks. When a ransomware incident occurs the proposed approach utilizes blockchain to securely backup data ensuring immutable data recovery without ransom payments. This integrated system provides a comprehensive solution for safeguarding banking environments from ransomware attack.

LITERATURE SURVEY

S.NO	YEAR	AUTHOR DETAILS	JOURNAL DETAILS	APPROACH	OUTCOME
1.	2023	BSFR-SH: Blockchain-Enabled Security Framework Against Ransomware Attacks for Smart Healthcare M. Wazid, A. Kumar Das and S. Shetty	IEEE Transactions on consumer Electronics,Vol.69,No. 1,February 2023	BSFR-SH uses blockchain and machine learning to detect ransomware, log activities securely, and trigger automated responses via smart contracts. It isolates affected nodes to enhance security. Accuracy:98%	Advantage: Blockchain ensures secure, tamper-proof data handling. Disadvantage: Integration with legacy systems is costly.
2.	2023	AI-Enhanced Detection and Mitigation of Cybersecurity Threats in Digital Banking. Suri babu Nuthalapati.	Researchgate 2023 Educational Administration: Theory and Practice	The approach uses AI models like Random Forest for loan prediction and SVM for fraud detection, achieving 92% and 90% precision, respectively.	Advantage: AI boosts accuracy, reducing risks. Disadvantage: Flawed data can cause errors.

S.NO	YEAR	AUTHOR DETAILS	JOURNAL DETAILS	APPROACH	OUTCOME
3.	2024	A Systematic Literature Review on Blockchain-based Cybersecurity Models for Ransomware Mitigation Ade Ilham Fajri, Mohammad Isa Irawan	IEEE International Symposium on Consumer Technology (ISCT),pp. 799-804,2024	Systematic literature review (SLR) using PRISMA guidelines to analyze blockchain-based ransomware mitigation models.	Advantage: Analysing models for ransomware mitigation. Disadvantage: Relies solely on existing literature
4.	2022	A Bayesian Attack-Network Modeling Approach to Mitigating Malware-Based Banking Cyberattacks Aaron Zimba	International Journal of Computer Network and Information Security(IJCNIS) Vol.14, No.1, 2022	Modelling Approach that uses Conditional Probability Assignments,Dynamic Adaptation,Probability Density Curves,Graph Structure achieving (Accuracy:83%)	Advantage: The model assess multiple attack paths based on quantifiable metrics. Disadvantage: The accuracy is limited by CVSS scores, which may not reflect real-time emerging threats.

S.NO	YEAR	AUTHOR DETAILS	JOURNAL DETAILS	APPROACH	OUTCOME
5.	2023	SFMR-SH:Secure Framework for Mitigating Ransomware Attacks in Smart Healthcare Using Blockchain Technology Jamal Alenizi,Ibrahim Alrashdi	Sustainable Machine Intelligence Journal, 2,pp.(4):1-19.	Internet of Things,Machine Learning algorithms(KNN,SVM ,Random Forest,Gradient Boosting,and XGB)Accuracy(99.33 %)	Advantage: Ensures strong ransomware detection in healthcare Disadvantage: Needs high resources,expertise and complexity
6.	2020	Evolution, Mitigation, and Prevention of Ransomware Ikra Afzal Chesti,Najm Us Sama,etal.	(IEEE)2nd International Conference on Computer and Information Sciences (ICCIS)	This research suggests on following these mechanisms: System Update Management,Trusted Download Protocols,Email Security Measures for protection against ransomware.	Advantage: The research provides protocols and methods that can be used by all the users with ease. Disadvantage: proposed methods prevent ransomware in the surface level,high probabilities for ransomware attack.

S.NO	YEAR	AUTHOR DETAILS	JOURNAL DETAILS	APPROACH	OUTCOME
7.	2023	Cyber Threats Classifications and Countermeasures in Banking and Financial Sector Sultan M.Alanazi,Asma A.Alhashmi	IEEE Access (Volume: 11) 23 October 2023	Random Forest classifies threats by severity, while SVM and KNN detect anomalies in network traffic.(Accuracy: 85% to 95%)	Advantage: Enhances data protection and trust. Disadvantage: Hard to keep up with evolving threats.
8.	2022	Machine Learning Algorithms and Frameworks in Ransomware Detection Daryle Smith , Sajad Khorsandroo	IEEE Access, vol. 10, pp. 117597-117610, 2022	Machine Learning Algorithms(Support Vector Machines (SVM) K-Nearest Neighbors (KNN) Neural Networks) (Accuracy: 97.6%)	Advantage: Detailed review of ML algorithms for detection. Disadvantage: No solutions for slow detection or evasive tactics.

S.NO	YEAR	AUTHOR DETAILS	JOURNAL DETAILS	APPROACH	OUTCOME
9.	2022	Ransomware Prevention and Mitigation Strategies Sandeep Reddy Gudimetla	Journal of Innovative Technologies Vol.5(2022)	Behavior-Based Detection,Traffic Based Detection,API Call Monitoring	Advantage: detailed insights into system behavior by tracking API calls, revealing malicious activities. Disadvantage: Continuous monitoring causes latency and affects system performance.
10.	2020	Avoiding Future Digital Extortion Through Robust Protection Against Ransomware Threats Using Deep Learning Based Adaptive Approaches Shamsul Huda,Shaila Sharmeen	IEEE Access(Volume: 8) 30 January 2020	It uses dynamic analysis to monitor ransomware and applies deep learning models for unsupervised and supervised detection. (Accuracy: 85%)	Advantage: Achieves 95% accuracy in ransomware detection. Disadvantage: High computational complexity

SUMMARY OF LITERATURE SURVEY

The survey reveals limitations in ransomware mitigation techniques. Machine learning models rely heavily on datasets and lack interpretability. Blockchain solutions ensure security but struggle with scalability and integration. Bayesian modeling, though useful for probabilistic assessments, has low accuracy (53%) and high complexity. Random Forest, while effective, can be computationally expensive and prone to overfitting. Deep learning offers high accuracy but demands extensive computational resources. Systematic reviews provide insights but lack real-world validation, highlighting the need for adaptive, scalable, and cost-effective security frameworks.

PROBLEM STATEMENT

- Existing solutions often rely on traditional antivirus or multi-algorithm machine learning, lacking real-time accuracy and adaptability to evolving ransomware threats.
- Additionally, insecure backup mechanisms leave data exposed, increasing dependence on ransom payments.
- Our proposed system addresses these limitations by using, Extra-Trees Classifier algorithm for real-time detection and a private blockchain for immutable data storage.
- The framework prevents ransomware spread and ensures robust, secure protection for the banking sector.

EXISTING SYSTEM

- The existing systems for ransomware management primarily focus on addressing the detection of ransomware attacks.
- They emphasize detecting ransomware once it has already infiltrated a system and subsequently recovering encrypted or lost data.
- Typically, existing solutions involve signature-based or behavior-based detection methods that recognize malicious activity post-infection.
- These solutions often require user intervention, such as restoring from backups or resetting the system, which can lead to downtime and loss of sensitive data.

LIMITATIONS

- The existing systems for ransomware management focus primarily on reactive measures, addressing attacks only after they have occurred.
- These systems are limited to detecting ransomware and recovering data, often neglecting preventive mechanisms to stop attacks beforehand.
- They rely heavily on user intervention for recovery, such as restoring backups or resetting devices, leading to potential downtime and data loss if proper backups are unavailable.
- Real-time monitoring is either absent or insufficient, making systems vulnerable to stealthy ransomware that can execute attacks undetected over time.

PROPOSED SYSTEM

- The existing system detects ransomware post-infection requiring manual recovery.
- Our proposed system integrates Machine Learning and Blockchain, enabling proactive detection, automated mitigation, and secure, tamper-proof data recovery without ransom payments.
- Advantages:

Continuous Monitoring: Real-time tracking of system activities to identify abnormal behavior and detect ransomware early.

Automatic File Removal: Suspicious files are automatically deleted, preventing ransomware from spreading across the system.

Proactive Threat Mitigation: Unlike traditional systems, it focuses on early detection and prevention, minimizing damage before it occurs.

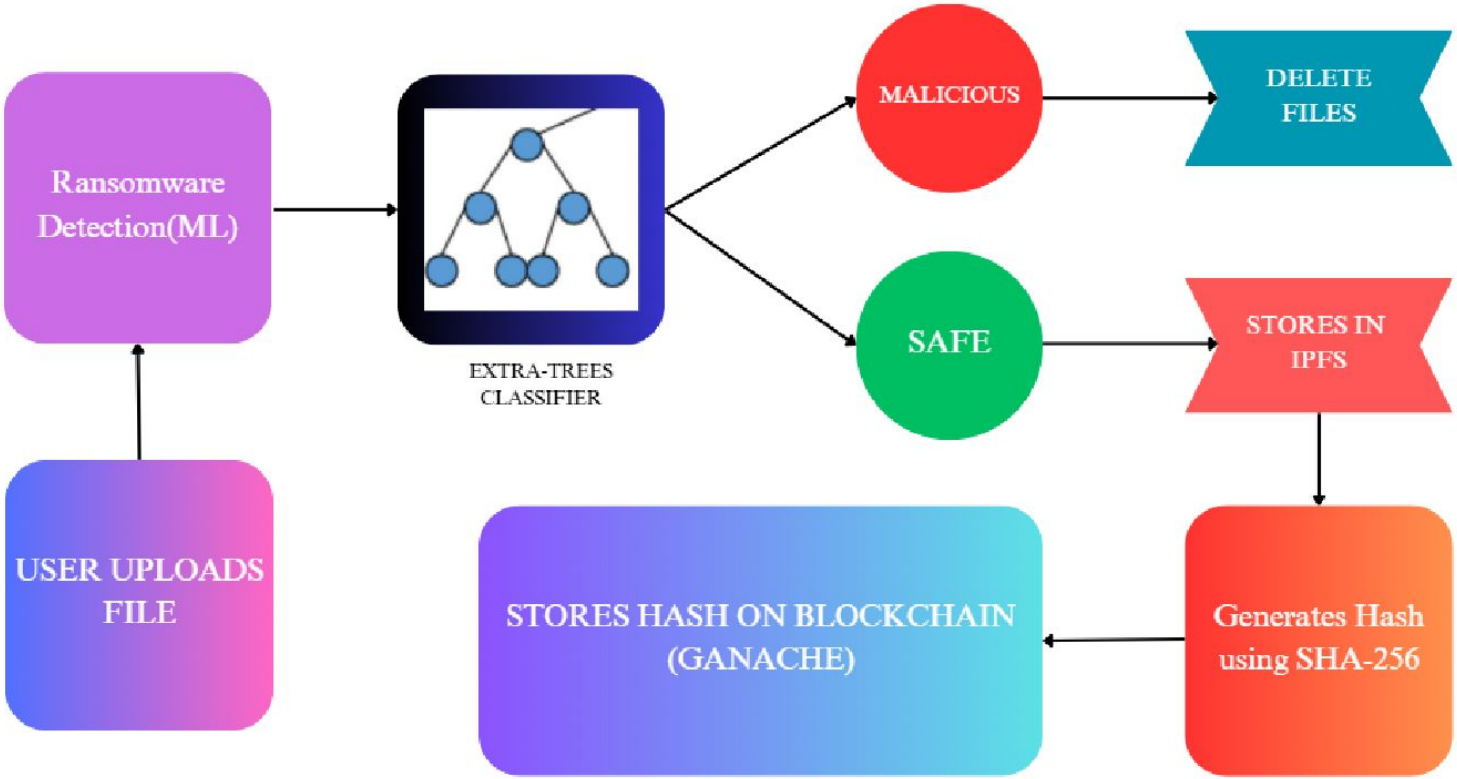
Efficient Data Recovery: Data can be recovered quickly and securely without the need for ransom payments.

Elimination of Ransom Payments: The system removes the need to pay ransom to cybercriminals.In unavoidable scenarios where ransom payment is required ,the payment is done securely through blockchain.

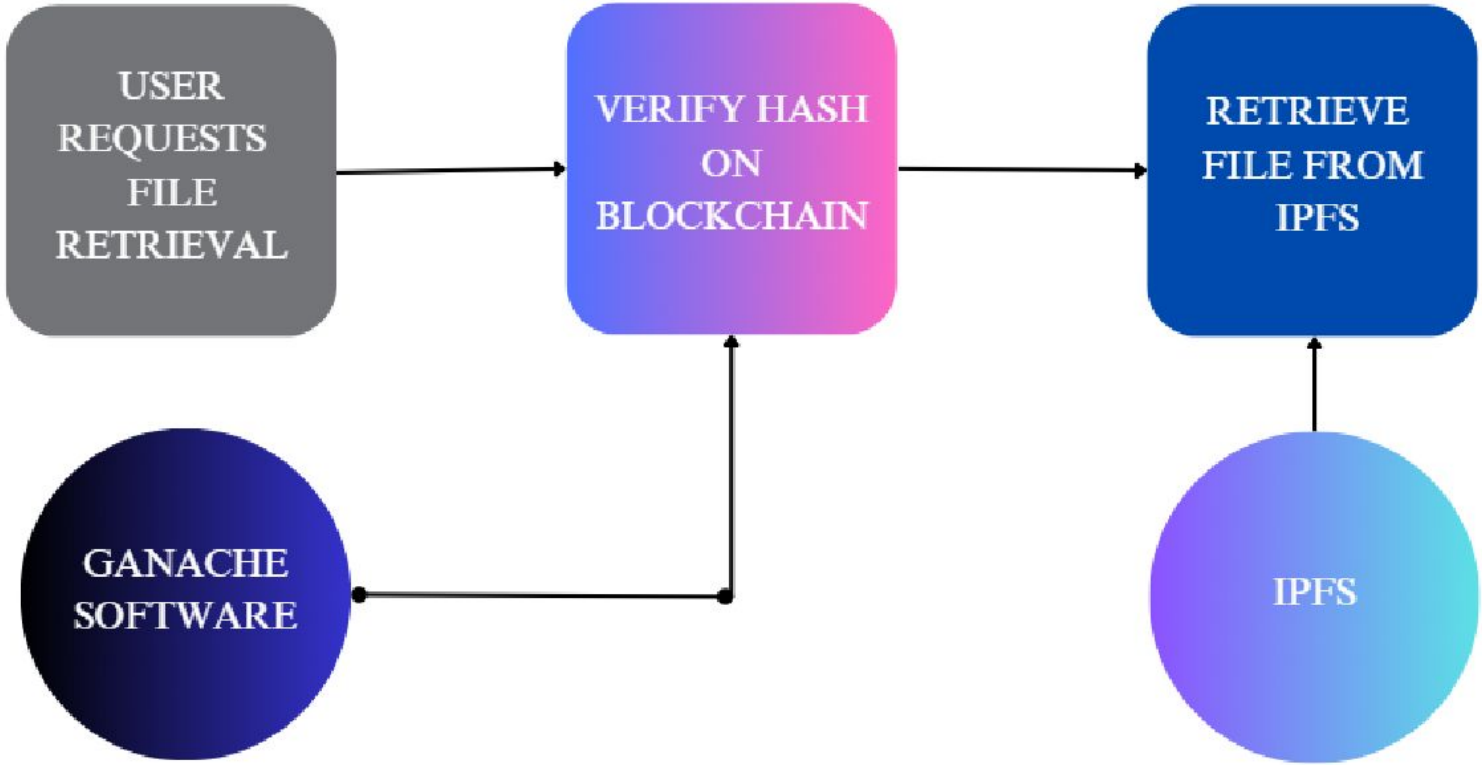
Enhanced Protection: A multi-layered approach ensures robust security and minimal disruption to financial operations.

Blockchain for Data Backup: User data is securely stored using blockchain, ensuring tamper-proof backups.

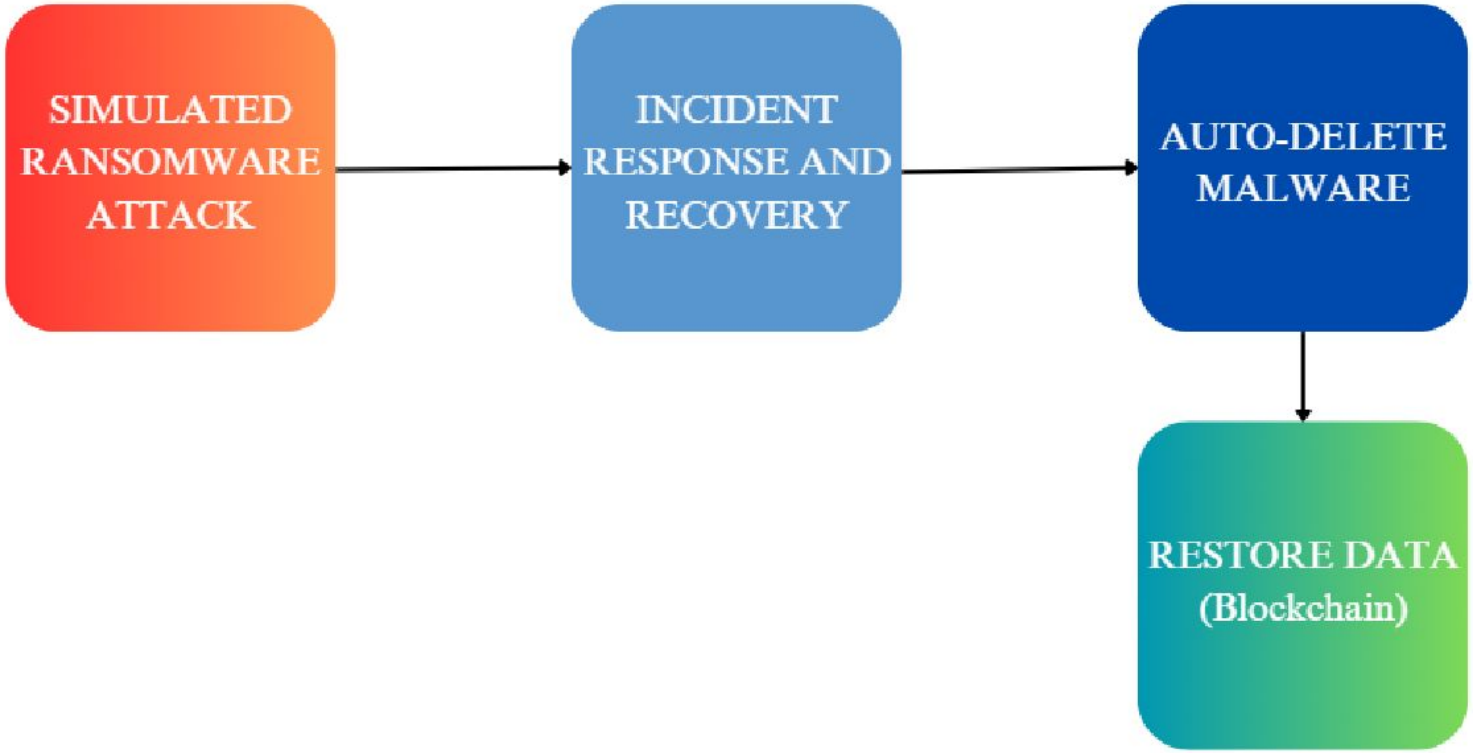
Workflow of the System



WHEN THERE IS A RANSOMWARE ATTACK;



DETECTION OF RANSOMWARE ATTACK



METHODOLOGY :

The Integration of Machine Learning and Blockchain provides a robust protection mechanism.

- Introduction to ransomware Attacks
- Machine Learning Framework
- IPFS file storage
- Blockchain for Data Integrity and Recovery
- Metamask and Blockchain Interaction

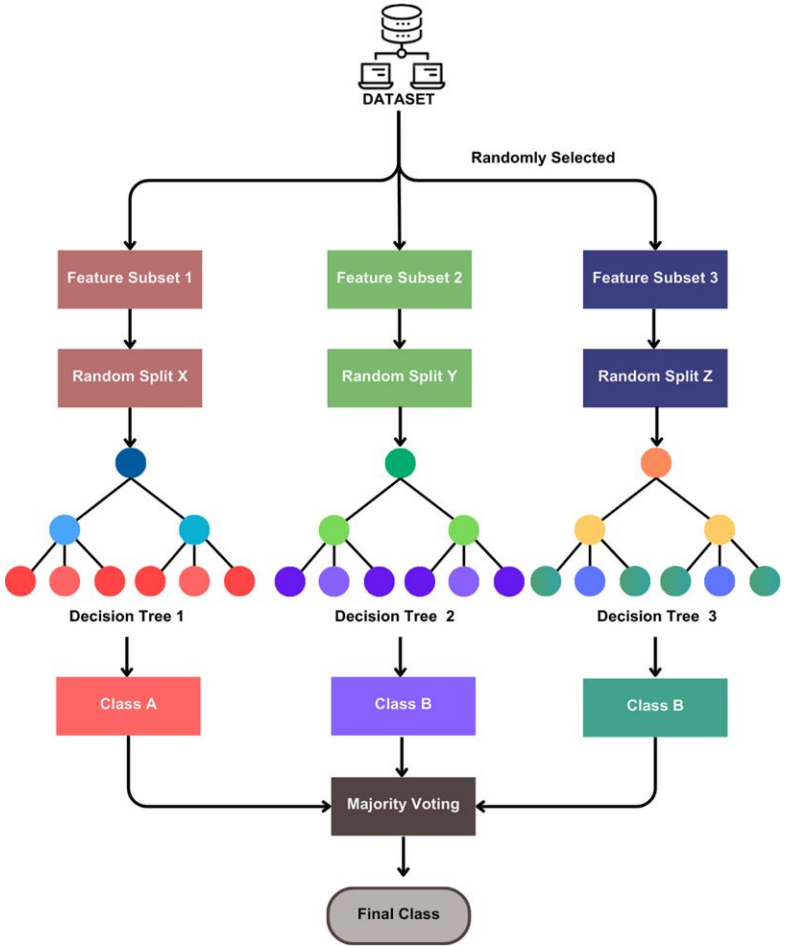
INTRODUCTION TO RANSOMWARE ATTACKS

- Ransomware targets Portable Executable system files by encrypting their content or corrupting the file making it inaccessible for operating system to execute file.
- Some ransomware variants inject malicious code into PE files which spreads the infection across a network leading to widespread file encryption and system compromise.
- To prevent this scenario, our system proposes a machine learning approach.

MACHINE LEARNING FRAMEWORK

- The Extra-trees classifier is an ensemble learning algorithm that is used here to classify the PE files as legitimate and malicious files.

- The algorithm divides the dataset into multiple feature subsets.



- Extra-Trees uses random splits at each node instead of selecting best possible split.
- This randomness introduces diversity among the trees, making the model less prone to overfitting.
- These random splits are further used to create decision trees, where each decision tree makes a prediction.
- The model provides the final result by aggregating the results of the trees through majority voting.

- 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:

- ➢ fj is a randomly selected feature,
- ➢ sj is a randomly selected split threshold

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

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

IPFS file storage(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.

BLOCKCHAIN FOR DATA INTEGRITY AND RECOVERY

- Blockchain is a decentralized and distributed technology that ensures secure and tamper-proof data storage.
- Here we use Blockchain Ganache, which is a personal Ethereum blockchain used for developing, testing and deploying smart contracts.
- Ganache is used here to store the IPFS hashes, further blockchain ensures data integrity using hashing mechanism and therefore provides hash code.

METAMASK AND BLOCKCHAIN INTERACTION

- MetaMask is a browser extension which is used in this project to store, manage, and interact with the Ethereum network.
- It serves as bridge between traditional web browsers and the Ethereum blockchain we use allowing to access the ganache and application.

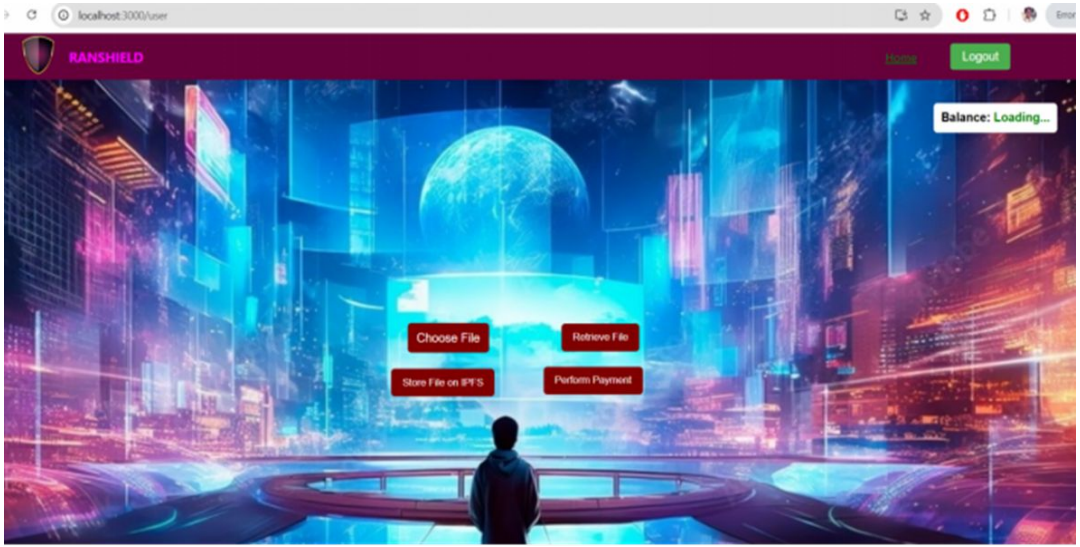
MODULES

- USER MODULE
- ATTACKER MODULE
- DETECTION OF RANSOMWARE USING MACHINE LEARNING

USER

- The user will log in to their account to backup 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 for IPFS: the file is stored in IPFS
- Retrieve files: after storing ,the file can also be retrieved
- Perform payment: the payment is being made



ATTACKER

- 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.

DETECTION OF RANSOMWARE USING MACHINE LEARNING

- 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.

SOFTWARE REQUIREMENT

Operating System:

- Windows 10 or Above

Programming Languages:

- Node.js
- React
- Python

Development Tools:

- Visual Studio Code (IDE for code editing)

Frontend Framework:

- React (for building the user interface)

Backend and Blockchain Development:

- Node.js (for backend development and server-side logic)

Blockchain Tools:

- Ganache (local Ethereum blockchain for testing smart contracts)
- MetaMask (browser extension for managing Ethereum accounts and interacting with the blockchain)

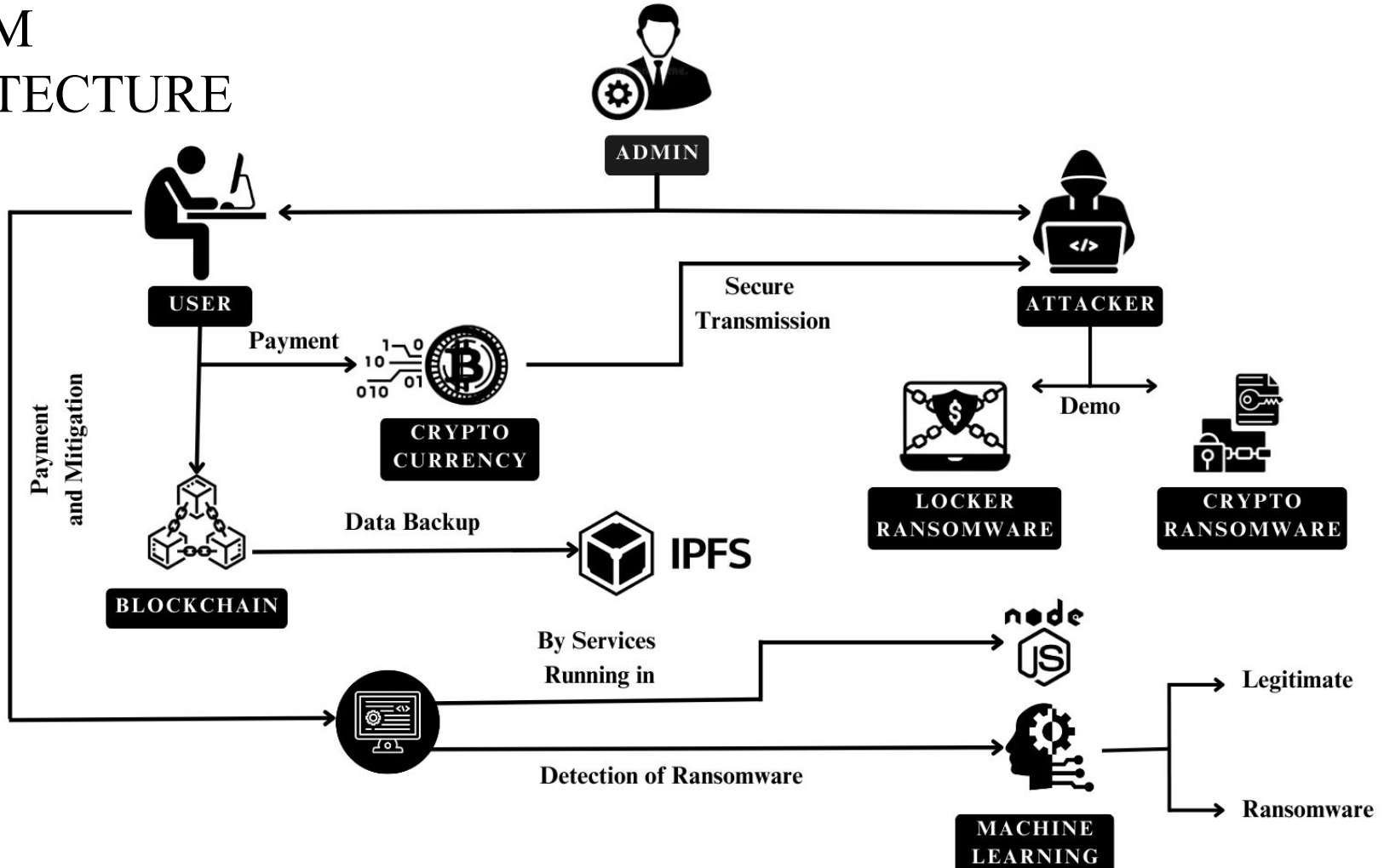
HARDWARE REQUIREMENT

Hard Disk : 250GB and Above

RAM : 6GB and Above

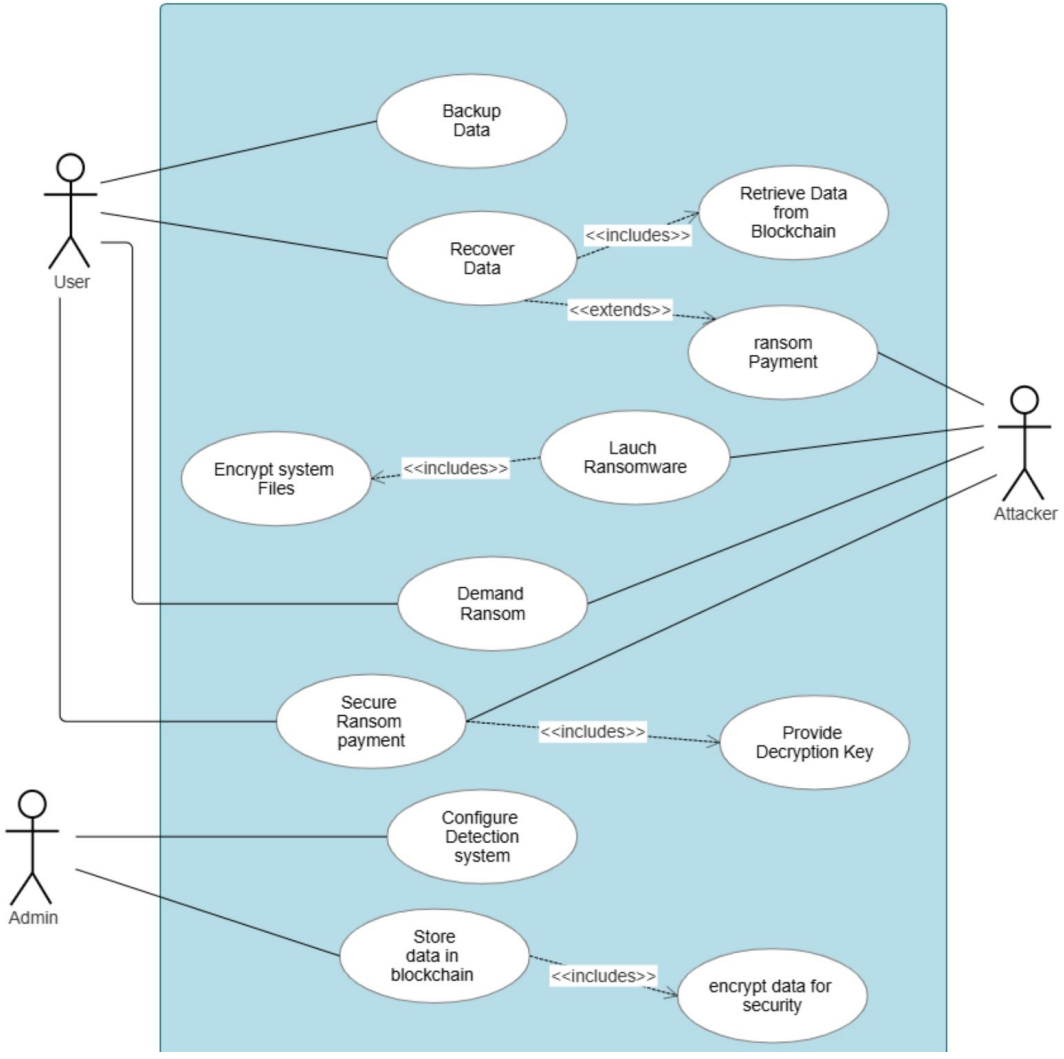
Processor : i3 and Above

SYSTEM ARCHITECTURE

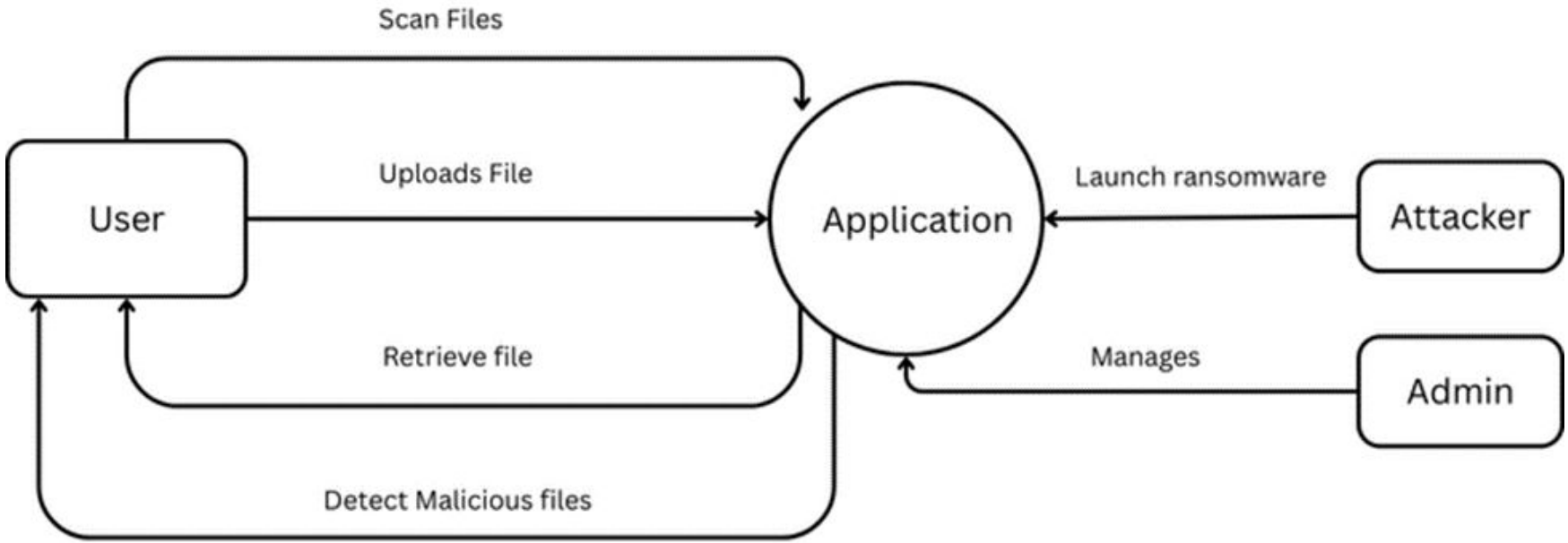


- The user system integrates a machine learning model to classify portable executable (PE) files into legitimate or ransomware files, ensuring real-time threat detection.
- Upon detecting ransomware, the system automatically deletes the malicious files to prevent further damage and ensure data security.
- In case of a ransomware attack, the user can securely recover their data from a backup stored on the blockchain, ensuring data integrity and security.
- Blockchain’s decentralized and tamper-proof architecture ensures that the backed-up data remains secure, eliminating the need for cryptocurrency payments for recovery.

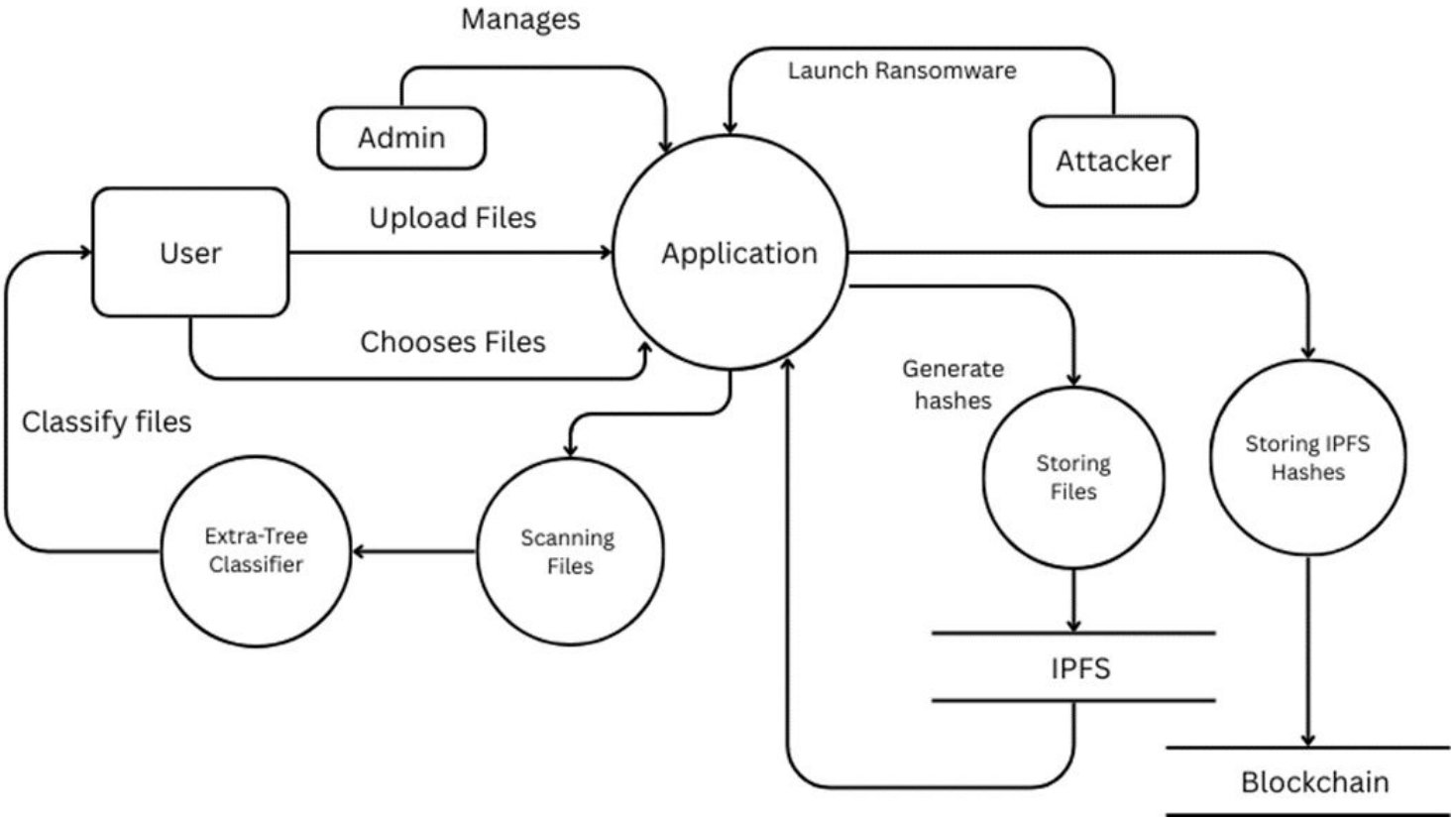
USE CASE DIAGRAM



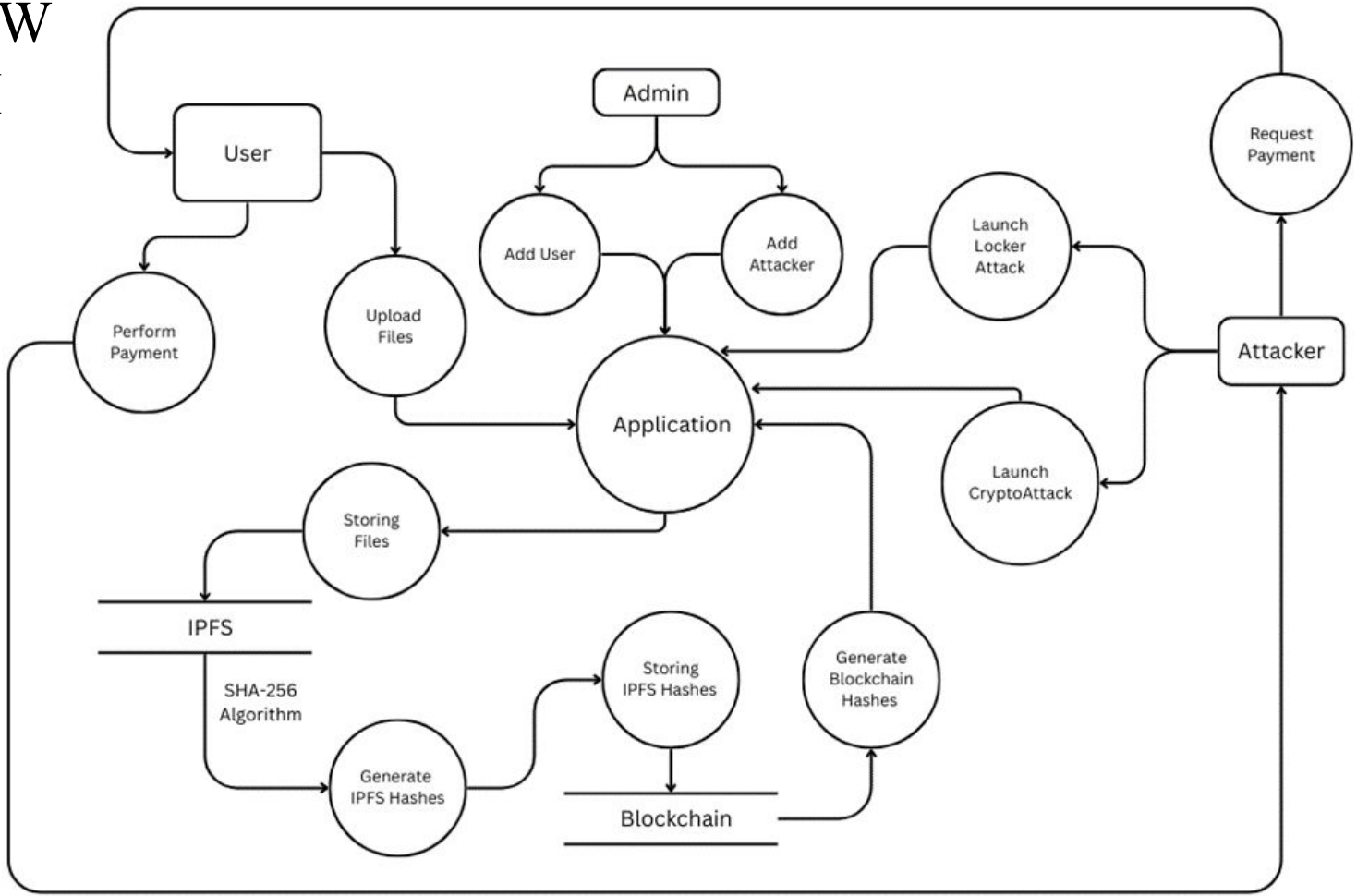
DATA FLOW DIAGRAM
LEVEL - 0



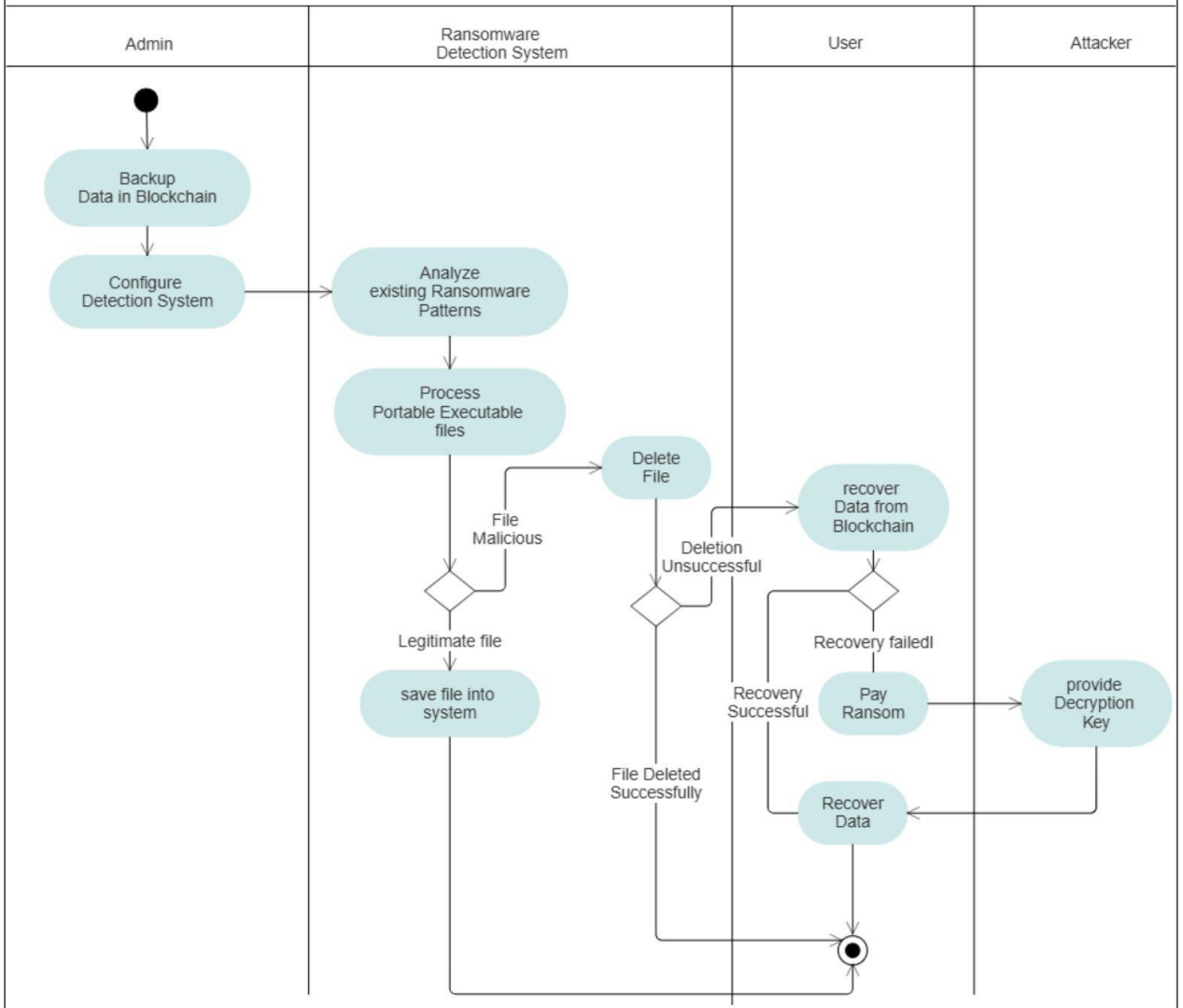
DATA FLOW DIAGRAM
LEVEL - 1



DATA FLOW DIAGRAM LEVEL - 2



ACTIVITY DIAGRAM



SYSTEM IMPLEMENTATION

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).

Secure File Backup with IPFS & Blockchain

- Files stored on IPFS with unique SHA-256 hashes to prevent tampering.
- Ganache blockchain stores hashes for integrity verification.
- Users can recover original files from IPFS in case of an attack.

SHA-256

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.

The input message MMM is padded to ensure its length is a multiple of 512 bits.Formula for total length after padding:

$$(L+1+K) \bmod 512 \equiv 448$$

- L = Original message length in bits
- K = Number of bits added as padding
- The message is padded with a single "1" bit followed by K "0" bits.

The padded message is divided into 512-bit chunks.

Each block is further split into 16 words of 32 bits each.

Message Expansion (Creating 64 Words)

Each 512-bit block is expanded into 64 words using:

$$W_{t} = \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16}$$

Where:

$$\sigma_0(x)=ROTR^{7}(x) \oplus ROTR^{18}(x) \oplus (x>>3)$$

$$\sigma_1(x)=ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus (x>>10)$$

For each of the 64 iterations (t=0 to 63), the following updates are applied:

$$T1 = H + \Sigma 1(E) + Ch(E,F,G) + Kt + Wt$$

$$T2 = \Sigma_0(A) + Maj(A,B,C)$$

where:

- $\Sigma_0(x) = ROTR^2(x) \oplus ROTR^{13}(x) \oplus ROTR^{22}(x)$
- $\Sigma_1(x) = ROTR^6(x) \oplus ROTR^{11}(x) \oplus ROTR^{25}(x)$
- $Ch(x,y,z) = (x \wedge y) \oplus (\neg x \wedge z)$ (Choose function)
- $Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$ (Majority function)
- Kt represents 64 fixed round constants, derived from the fractional parts of the cube roots of the first 64 prime numbers.

Updating Hash Values

After each iteration, the working variables are updated:

$$H=G, \quad G=F, \quad F=E, \quad E=D+T1$$

$$D=C, \quad C=B, \quad B=A, \quad A=T1+T2$$

Final Hash Computation

After processing all blocks, the final hash value is:

$$Hi=Hi+Ai$$

The output is a 256-bit hash, represented as a 64-character hexadecimal string.

RANSOMWARE DETECTION SYSTEM

- The system features ransomware scanning to detect threats before file storage or retrieval.
- A honeypot-based dataset, trained on real ransomware samples, captures authentic attack behaviors to improve accuracy.
- A decoy system attracts and collects malware for analysis.
- Extracted features are processed using the Extra-Trees Classifier, enhancing machine learning training.

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:

- fj is a randomly selected feature,
- sj is a randomly selected split threshold

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

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

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.

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.

- Secure transactions and proactive threat detection work together to guarantee data integrity and do away with ransom payments.

- This multi-layered strategy offers a future-proof defence against ransomware threats while safeguarding sensitive financial data.

REFERENCES

[1] 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

[2] 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.

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

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

[5] 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.

[6] 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

[7] 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.

[8] 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.

[9] 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.

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

[11]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.

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

[13] 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.

[14] 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.

[15] 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

[16] 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

[17] 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.

[18] D. Ghelani, T. K. Hua, and S. K. R. Koduru, ‘‘Cyber security threats, vulnerabilities, and security solutions models in banking,’’ Authorea, Sep. 2022

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

[20] 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.

[21] 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

[22] 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.

[23] 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.

[24] I. 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.

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

[26] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, ‘‘Automated dynamic analysis of ransomware: Benefits, limitations and use for detection,’’ 2016, arXiv:1609.03020

[27] O. Delgado-Mohatar, J. M. Sierra-Cámara, and E. Anguiano, ‘‘Blockchainbased semi-autonomous ransomware,’’ Future Gener. Comput. Syst., vol. 112, pp. 589–603, Nov. 2020.


THANK YOU