

# Lakshmi D

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

 Quick Submit Quick Submit Panimalar Engineering College

### 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





# 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.

3

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.

2

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

6

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.

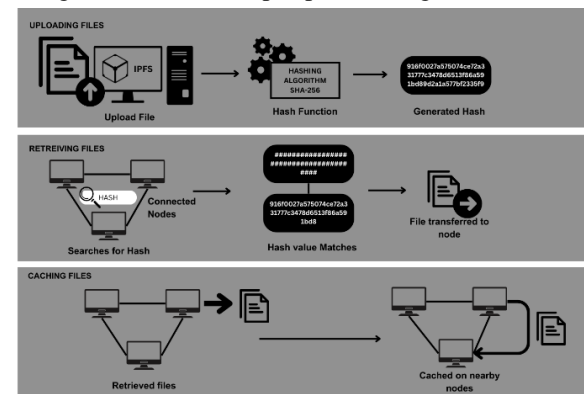


Fig. 1. Diagram For Working IPFS

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  $M$ :

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

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  $H_s$  and the recomputed hash  $H_r$  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.

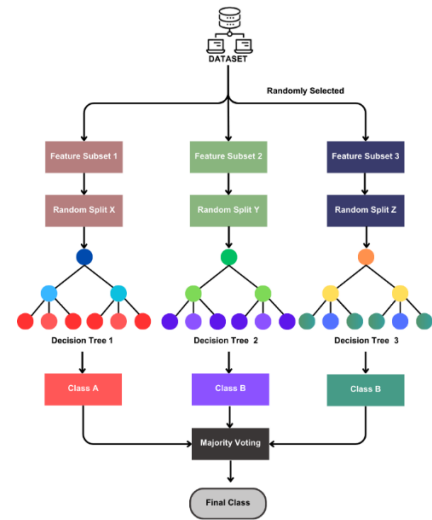


Fig. 3. Working of Extra -Trees Classifier

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

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

Where,  $f_j$  is a randomly selected feature,  $S_j$  is a randomly selected split threshold.

A majority vote over  $N$  trees yields the final prediction:

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

### 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.

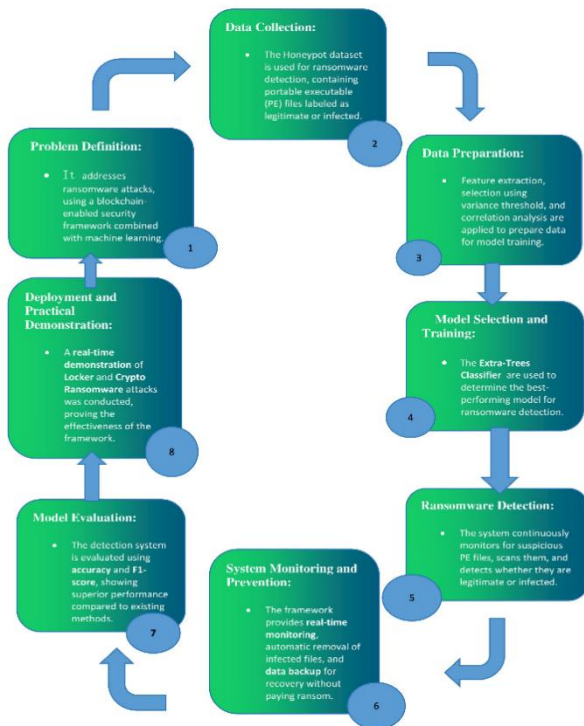


Fig. 2. Machine Learning Process



### 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.

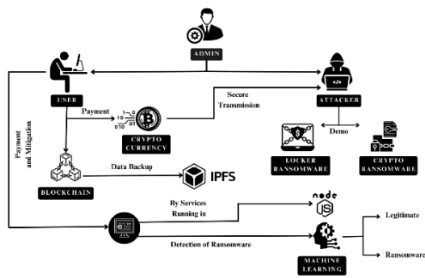


Fig. 4. System Workflow

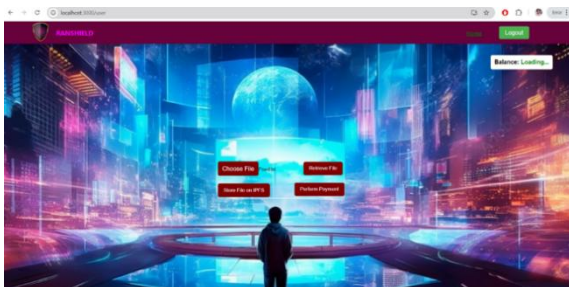


Fig. 5. User Module

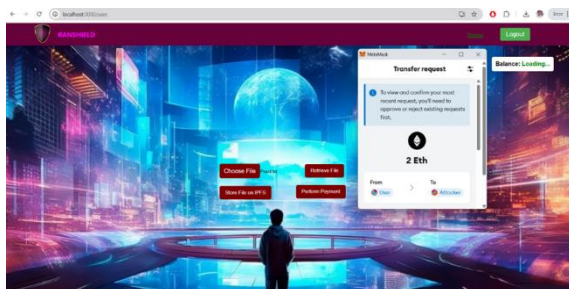


Fig. 6. Smart Contract-Based Payment Module

## 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..

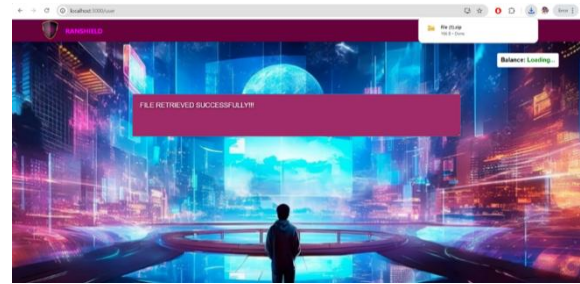


Fig. 7. File Retrieval Using Blockchain Backup



Fig. 8. Secure Payment Using MetaMask

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

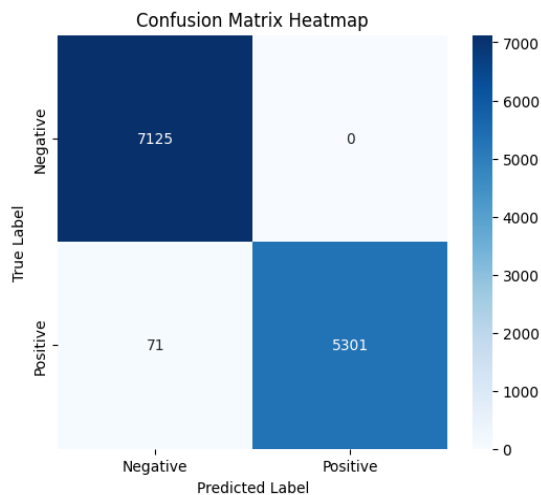


Fig. 9. Confusion Matrix of the Classifier Model

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. 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] 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] J. A. A. Darem, A. A. Alhashmi, T. M. Alkhalidi, 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] J 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.