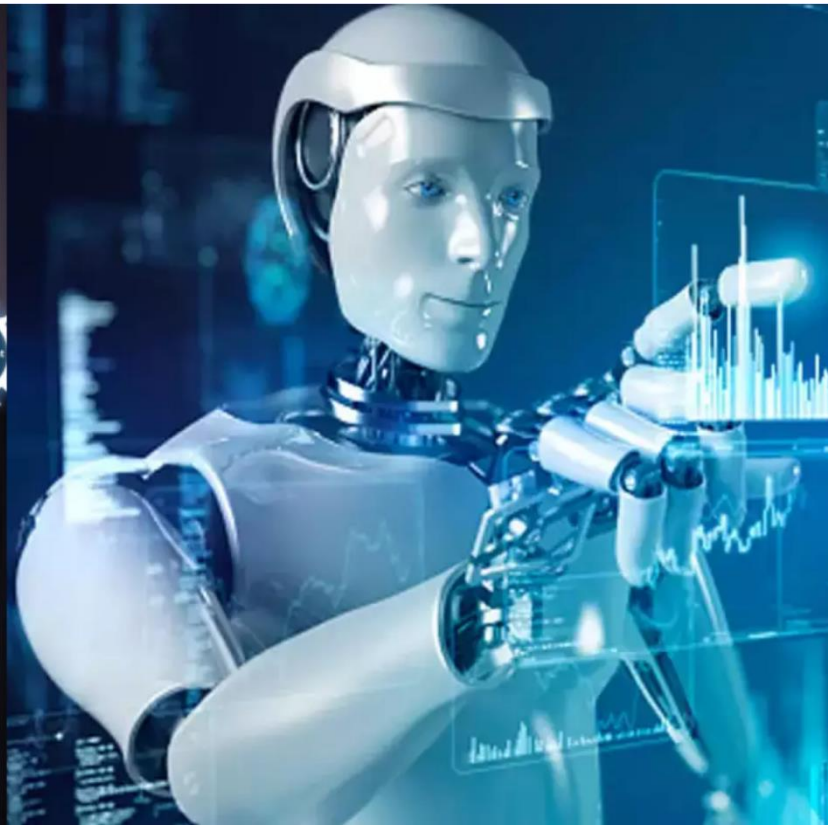
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 5, May 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405213|

Autonomous Defense Framework for Cryptographic Ransomware using BiLSTM and Proactive Data Protection

Mrs. S. Shanmugapriya, G. Thanush Kumar, Mohamed Fazil J, S. Karuppusamy, A. Jeevanatham

Assistant Professor, Department of Computer science engineering, Dhaanish Ahmed Institute of Technology, Coimbatore, India

UG Scholar, Department of Artificial Intelligence and Data Science, Dhaanish Ahmed Institute of Technology, Coimbatore, India

UG Scholar, Department of Artificial Intelligence and Data Science, Dhaanish Ahmed Institute of Technology, Coimbatore, India

UG Scholar, Department of Artificial Intelligence and Data Science, Dhaanish Ahmed Institute of Technology, Coimbatore, India

UG Scholar, Department of Artificial Intelligence and Data Science, Dhaanish Ahmed Institute of Technology, Coimbatore, India

ABSTRACT: Ransomware attacks have become a pervasive cyber threat, targeting organizations of all sizes and causing significant financial and operational disruptions. Ransomware encrypts critical files or locks systems, rendering them inaccessible until a ransom is paid, often with no guarantee of recovery. Despite the availability of numerous ransomware detection tools, emerging ransomware variants continue to outpace traditional defenses, leaving users, businesses, and governments vulnerable. This project addresses the growing threat of cryptographic ransomware by developing an innovative runtime solution that autonomously defends against such attacks. Leveraging a BiLSTM (Bidirectional Long Short-Term Memory) network model, the system identifies and blocks ransomware during its execution by analyzing intricate temporal patterns in its behavior. The BiLSTM model is designed to adapt to evolving attack techniques, ensuring robust and reliable detection. In addition to detection, the project introduces a proactive defense mechanism employing Format Preserving Encryption (FPE) to safeguard data. By camouflaging files as untouchable through excluded extensions and hiding them in obscure directories, the system minimizes the risk of encryption by ransomware. The proposed solution combines advanced detection with proactive data protection strategies, creating a comprehensive defense against cryptographic ransomware. Operating autonomously and without reliance on static or signaturebased methods, this approach enhances resilience against both known and emerging ransomware threats, protecting critical systems and valuable data effectively.

KEYWORDS: **Ransomware, ATTACK Matrix, TF-IDF, Cosine Similarity, Threat Intelligence**

I. INTRODUCTION

Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyber attackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files. Some variants have added additional functionality – such as data theft – to provide further incentive for ransomware victims to pay the ransom. Ransomware has quickly become the most prominent and visible type of malware. Recent ransomware attacks have impacted hospitals' ability to provide crucial services, crippled public services in cities, and caused significant damage to various organizations. The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card, and attackers target individuals, businesses, and organizations of all kinds.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405213|

Impact of ransomware

In 2020, the Snake ransomware attack brought Honda's global operations to a standstill. That same week, Snake, a form of file-encrypting malware, also hit South American energy-distribution company Enel Argentina. In 2019, cybercriminals encrypted files that froze the computer networks of Pemex, Mexico's state-owned gas and oil conglomerate, demanding $5 million to restore service. And in 2017, the WannaCry cryptoworm hit 230,000 computers globally by exploiting a vulnerability in Microsoft Windows. Today, through a mix of outdated technology, "good enough" defense strategies focused solely on perimeters and endpoints, lack of training (and poor security etiquette), and no known "silver bullet" solution, organizations of all sizes are at risk. Especially as cybercriminals are making it their business to encrypt as many computer systems on the corporate network as possible in order to extort a ransom ranging from thousands to millions of dollars. In fact, ransomware attacks were predicted to occur every 11 seconds in 2021 at a global cost of $20 billion.

II. LITERATURE SURVEY

The paper "Similarity Analysis of Ransomware Attacks Based on ATT&CK Matrix" by Zheyu Song, Yonghong Tian, and Junjin Zhang (2023) focuses on analyzing the behavioural patterns of ransomware attacks, an area often overlooked in traditional research. Using the MITRE ATT&CK matrix, the study proposes a method to identify similarities between ransomware incidents by extracting tactics, techniques, and procedures (TTPs) from threat intelligence data. It applies the TF-IDF algorithm to calculate keyword weights in attack descriptions and uses cosine similarity to measure the resemblance between different attacks. This approach provides deeper insights into the technical and tactical behaviours of ransomware groups and suggests countermeasures to improve network security..

The methodology involves collecting reliable ransomware incident data, extracting TTPs, and analyzing similarities based on TF-IDF and cosine similarity within the ATT&CK framework. The results show that ransomware groups often use distinct tactics, which can be accurately detected through this method. Additionally, tools like the D3FEND knowledge graph help in quickly identifying critical attack techniques. The paper also acknowledges limitations, including the scarcity and reliability of threat intelligence and challenges in accurately extracting TTPs. It suggests future enhancements using deep learning and graph neural networks to improve the precision and predictive capabilities of ransomware analysis..

III. METHODOLOGY

- Collect Threat Intelligence.
  Gather detailed information about real ransomware attack incidents from reliable and comprehensive sources.
- Extract Tactics, Techniques, and Procedures (TTPs)

From each incident, extract the attackers' tactics and techniques using the MITRE ATT&CK matrix as a guide.

- Apply TF-IDF Algorithm

Use TF-IDF (Term Frequency–Inverse Document Frequency) to find the important keywords in each attack description and assign weights to them.

- Calculate Cosine Similarity

Compare the ransomware attacks by calculating the cosine similarity between their TF-IDF keyword vectors to measure how similar they are.

- Analyze and Identify Patterns
- Analyze the results to discover patterns in how different ransomware groups operate and find similarities between their attack methods.
- Cross-reference with D3FEND Knowledge Graph

Map detected techniques to defense measures using the D3FEND framework for better protection strategies.

- Propose Countermeasures

Suggest defensive actions based on the critical attack techniques identified, helping organizations strengthen their security.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

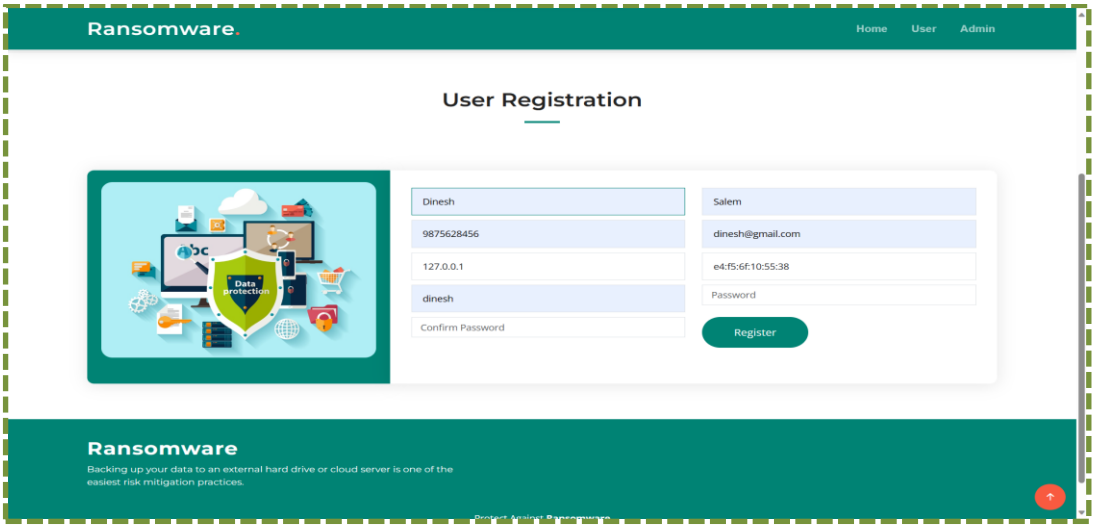
Impact Factor 8.699

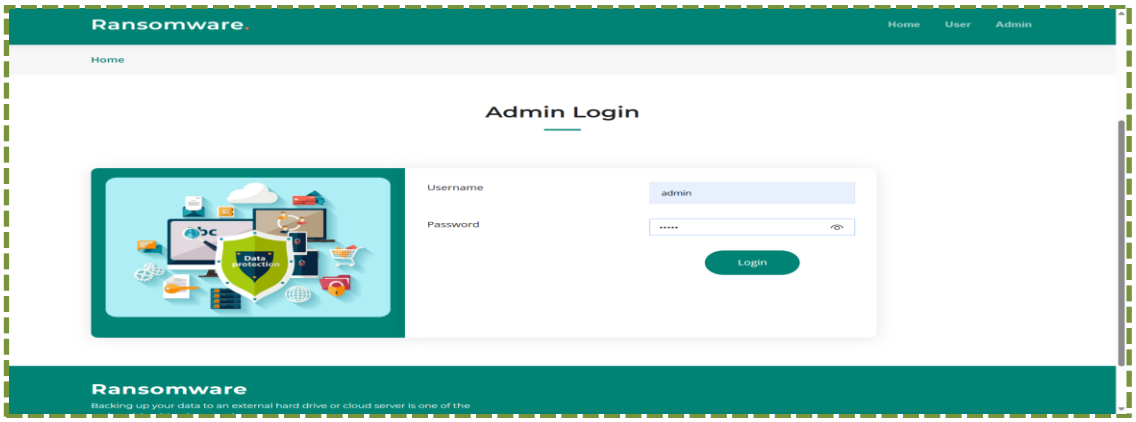
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405213|

IV. EXPERIMENTAL RESULTS





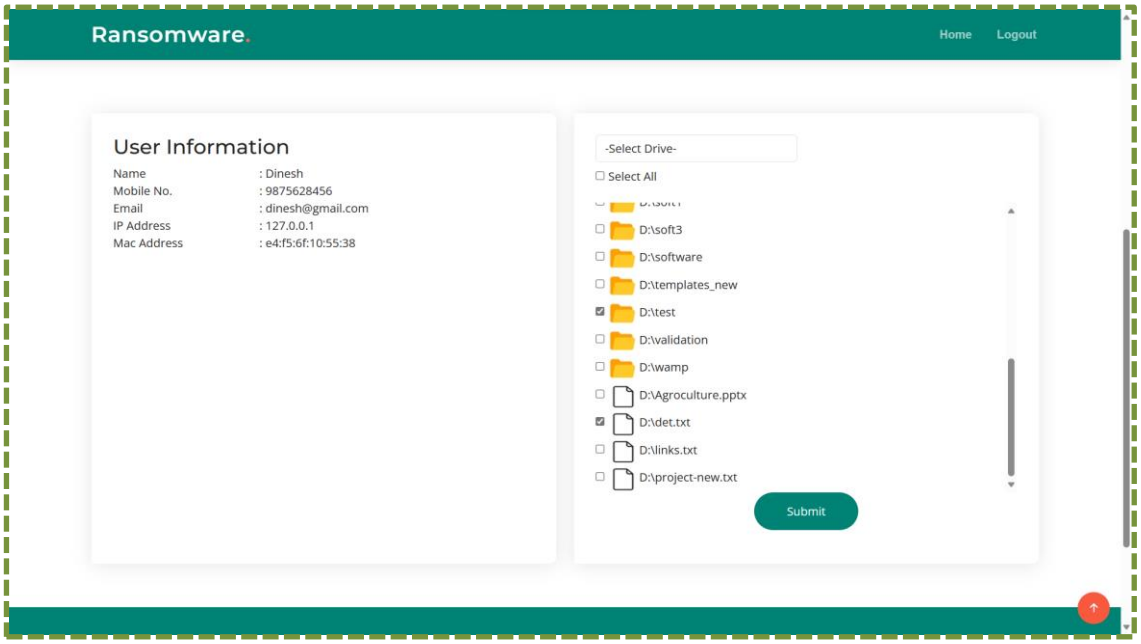
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 5, May 2025

|DOI: 10.15680/IJIRSET.2025.1405213|



V. CONCLUSION

In conclusion, the proactive defensive strategy combining BiLSTM and Proactive Data Protection offers a powerful, adaptive solution against ransomware threats. By merging deep learning detection with cryptographic file concealment, it disrupts ransomware operations at multiple levels. The system's real-time monitoring, user-friendly interface, and customizable settings empower users to tailor protections as needed. It not only secures individuals and organizations but also sets a new benchmark for proactive cybersecurity. Looking ahead, enhancements like advanced threat intelligence and blockchain-based file tracking will further strengthen its resilience, ensuring stronger defenses against the evolving ransomware landscape.

REFERENCES

[1] D. E. García, N. DeCastro-García and A. L. M. Castañeda, "An effectiveness analysis of transfer learning for the concept drift problem in malware detection", Expert Syst. Appl., vol. 212, Feb. 2023.
[2] G. O. Ganfure, C.-F. Wu, Y.-H. Chang and W.-K. Shih, "RTrap: Trapping and containing ransomware with machine learning", IEEE Trans. Inf. Forensics Security, vol. 18, pp. 1433-1448, 2023.
[3] J. Singh, K. Sharma, M. Wazid and A. K. Das, "SINN-RD: Spline interpolation-envisioned neural network-based ransomware detection scheme", Comput. Electr. Eng., vol. 106, Mar. 2023.
[4] D. Hitaj, G. Pagnotta, F. De Gaspari, L. De Carli and L. V. Mancini, "Minerva: A file-based ransomware detector", arXiv:2301.11050, 2023.
[5] F. De Gaspari, D. Hitaj, G. Pagnotta, L. De Carli and L. V. Mancini, "Evading behavioral classifiers: A comprehensive analysis on evading ransomware detection techniques", Neural Comput. Appl., vol. 34, no. 14, pp. 12077-12096, Jul. 2022.
[6] S. H. Kok, A. Abdullah and N. Jhanjhi, "Early detection of crypto-ransomware using pre-encryption detection algorithm", J. King Saud Univ.-Comput. Inf. Sci., vol. 34, no. 5, pp. 1984-1999, May 2022.
[7] M. Amin, B. Shah, A. Sharif, T. Ali, K.-I. Kim and S. Anwar, "Android malware detection through generative adversarial networks", Trans. Emerg. Telecommun. Technol., vol. 33, no. 2, pp. e3675, Feb. 2022.
[8] Rajabi and O. O. Garibay, "TabFairGAN: Fair tabular data generation with generative adversarial networks", Mach. Learn. Knowl. Extraction, vol. 4, no. 2, pp. 488-501, May 2022.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details