iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.71684

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Autonomous Defense Frameworkfor Cryptographic Ransomware Using BiLSTM and Proactive Data Protection

Angelin Rosy M[1], Janani R[2]
[1]*Assistant Professor,* [2]*MCA, Department of Master of Computer Applications, Er.Perumal Manimekalai College of Engineering, Hosur,*

Abstract: ***Ransomware has become a dominant and destructive threat in the cybersecurity landscape, targeting organizations across various industries and severely disrupting operations by encrypting data or locking users out of their systems. Victims are often forced to pay a ransom in hopes of restoring access, yet recovery is not always guaranteed. While many ransomware detection tools are available, they frequently fall short when confronted with new, rapidly evolving variants, putting businesses, individuals, and governments at considerable risk.This project introduces an innovative runtime defense mechanism tailored to combat cryptographic ransomware. It utilizes a Bidirectional Long Short-Term Memory (BiLSTM) neural network model capable of detecting and halting ransomware attacks during execution. By observing the time-based behavioral patterns of processes, the BiLSTM system can effectively recognize malicious activity. Its flexibility makes it well-suited to adapt to novel forms of ransomware.In addition to real-time detection, the solution incorporates a forward-looking data protection strategy using Format Preserving Encryption (FPE). This technique obscures sensitive files by altering their extensions to those typically bypassed by ransomware and storing them in concealed directories, thereby reducing the likelihood of compromise.By merging intelligent behavioral analysis with strategic data concealment, this system provides a comprehensive and autonomous shield against both known and emerging ransomware threats. Unlike conventional methods that depend on predefined signatures, this approach offers enhanced security and resilience for mission-critical systems and data.***

Keywords: Encrypted Malware Attack ,Dual-Directional Long-Term Memory Neural Network,Malware Activity Identification ,Hash Concealer

I. INTRODUCTION

Ransomware, a distinct category of harmful software, has rapidly become a significant concern in the field of cybersecurity. Given the evolving nature of these threats, adopting a proactive defense strategy is essential to outpace attackers who constantly adapt their methods. Generative Adversarial Networks (GANs), a type of advanced machine learning model, have demonstrated impressive capabilities across numerous applications. In the realm of ransomware mitigation, RanGAN is specifically designed to comprehend and generate artificial ransomware variants, which aids in developing more robust and adaptive security solutions. Additionally, Hash Conceal offers a novel protective measure by shielding vital data using cryptographic hashing, making it more resistant to unauthorized access or encryption attempts.

II. PROPOSED WORK

The proposed solution, a proactive Anti-Agent Against Ransomware Attacks, combines the strengths of "RanGAN" and "Hash Conceal" to establish a strong, multi-layered security framework.

A. Integration of RanGAN Technology:

RanGAN leverages cutting-edge machine learning algorithms to continuously observe both system and network behavior, enabling it to detect and learn ransomware activity patterns as they occur in real time.

B. Deployment of Hash Conceal:

Hash Conceal utilizes sophisticated cryptographic techniques to protect critical files, effectively making them unreachable to ransomware processes and preventing unauthorized encryption.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

III. MODULES

A. RanFooler Web Tool

To emulate a real-world environment, a three-layer web infrastructure was designed, comprising web servers, application servers, and a centralized database server.

At the entry point, a load balancer is responsible for managing and routing incoming client requests to the appropriate web servers to ensure optimal performance and availability.

RanFooler serves as a protective tool, safeguarding users' systems from ransomware infections and various other online security threats.

A comprehensive ransomware analysis report will present a detailed list of all compromised files, along with potential indicators or causes that led to their detection

B. End UserDevice Configuration:

1) Admin

Administrators begin their tasks by securely accessing the End User Interface, ensuring that only authorized users can interact with system-level controls.

They proceed to upload datasets, which are essential for training the RanGAN model. The interface is designed to be intuitive, allowing seamless uploading of various data types that reflect ransomware traits.

Next, administrators set up the training parameters, including the selection of features, adjustment of hyperparameters, and specification of the training time.

Once training is complete, the trained RanGAN model is deployed to the RanFooler Web Application, embedding it into the live system for real-time threat monitoring and response.

2) User

Users begin the setup process by creating an account on the RanFooler web platform, submitting essential information such as their username, email address, and password.

Once logged in, users register their devices by entering the MAC ID, which serves as a unique identifier for each individual device.

Users can then decide whether to protect all files or specify particular files they wish to shield from ransomware threats.

After making their selections and completing the setup, users receive a comprehensive overview summarizing their configuration settings.

C. Ransomware Classification: Build and Train

1) Dataset Loading

The dataset comprises Byte and ASM files, which represent the assembly-level code of ransomware samples. These files include crucial details about function invocations and memory usage.

2) Data Preprocessing

To prepare the data for model development, only the Byte files were selected, excluding the ASM files. These Byte files were then converted into readable text format to facilitate feature extraction and further analysis in Python.

3) Feature Extraction

To represent the ransomware samples based on their opcode sequences, a shallow deep learning technique—Word2Vec—was employed. Since the length of each Byte file varies due to differing amounts of code, this variation in file size can serve as a distinctive feature to help identify and classify ransomware types.

4) Ransomware Model Development and Training

The model training phase utilizes advanced neural architectures like Bidirectional Long Short-Term Memory (BiLSTM) and Gated Recurrent Units (GRU). These models are trained on a selected portion of the dataset, enabling them to effectively learn and differentiate between harmless and ransomware-infected files. This classification capability forms the core of the next stage within the RanGAN framework.

D. Attacker Model:

1) Ransomware Code or Executable Injection

This phase focuses on delivering ransomware payloads to the target system. The malicious shellcode is retrieved from a remote server, typically after the user accesses a compromised landing page.

This is achieved by:

Embedding scripts or iframe elements on the landing page, where the src attribute links to the malicious distribution server.

Redirecting the browser using various techniques, such as HTTP 302 redirects or JavaScript-based redirection methods.

The payloads delivered are usually heavily obfuscated, making them harder to analyze and enabling them to evade traditional, signature-based detection tools.

E. Ransomware Prediction:

1) Ransomware Detection Scans

RanFooler provides two distinct scanning options to uncover ransomware infections:

The Antivirus Scan targets known ransomware and other harmful programs that may already exist on the system.

The Preventive Scan is geared toward identifying new or unfamiliar ransomware strains by analyzing their unknown attributes and behavior patterns.

2) Real-Time Ransomware Forecasting with RanGAN

In the RanGAN framework, a generator module plays a central role in synthesizing ransomware-like data. It combines random input (noise) with actual ransomware samples from the dataset to create hybrid instances. These generated samples help enhance the detection system's ability to spot ransomware activity, even in real time.

3) Preventing Ransomware Execution

RanFooler employs a dynamic detection engine capable of processing incoming ransomware code. It can uncover and eliminate hidden malicious binaries before they execute.

If integrated with a capable antivirus component that can accurately detect diverse ransomware types, this system becomes a highly effective defense mechanism.

4) Ransomware Blocking and Elimination

RanFooler includes real-time blocking tools that proactively stop the installation or launch of ransomware and potentially harmful applications.

It is equipped to clean the system of various modern threats such as adware, browser hijackers, worms, trojans, scamware, viruses, and other ransomware variants—ensuring a safer computing environment.

5) System Configuration and Integration

RanFooler works in the background to apply user-defined settings to its backend system. It links selected files and configurations with the unique MAC ID of the user's machine.

These settings are applied in real time, allowing the system to adapt instantly to user preferences and protection rules.

6) Ongoing System Surveillance

RanGAN maintains a constant watch over configured systems to detect any suspicious changes or signs of ransomware behavior.

Automated alerts and notifications are sent to users to keep them updated about the integrity and safety of their protected data.

F. Hash Concealer:

1) Hash-Based Concealment for File Security

To defend important files against ransomware threats, the system implements a Hash Conceal strategy. This method securely stores files in a protected, non-visible layer, while placing linked reference files in the user-accessible area. These references act as gateways, allowing users to open the hidden files without directly exposing them.

2) File Mapping and Hash Tables

For efficient recovery and management of secured data, the system uses a mapping table that records the relationship between each file's original location and its secure, hidden counterpart. Additionally, a hash table may be utilized to maintain the integrity and tracking of file access points.

3) Redirector for Secure File Access

To ensure smooth and secure file access, a linker mechanism is integrated. When a user opens a reference file, the linker seamlessly redirects the request to the corresponding protected file stored in the concealed layer, ensuring both usability and security are preserved.

IV. RESULTS

The developed autonomous defense system showed effective capabilities in identifying and countering cryptographic ransomware threats. By incorporating Bidirectional Long Short-Term Memory (BiLSTM) networks, the framework was able to recognize patterns in the sequence of operations typically associated with ransomware, enabling precise differentiation between harmful and safe files.

Performance Metrics:

1) Superior Detection Accuracy: The BiLSTM-driven model achieved a commendable accuracy rate in recognizing ransomware samples, including those not previously encountered during training.
2) Minimal False Positives: Leveraging sequential pattern analysis helped reduce incorrect threat flags, maintaining system functionality without unnecessary disruptions.
3) Live Threat Prediction: Utilizing synthetic data created by the RanGAN generator, the system was able to anticipate ransomware activities as they occurred, offering timely protective responses.
4) Advanced File Safeguarding: The combined use of Hash Concealment and a Linker module effectively hid essential user files from ransomware, while still allowing normal access through controlled links.
5) Resource-Efficient Operation: The system maintained continuous surveillance with automated notifications, responding rapidly to potential threats without overloading system resources or requiring user action.

V. CONCLUSION

This autonomous security framework delivers a smart and forward-looking solution to address the growing threat of cryptographic ransomware. Utilizing BiLSTM neural models, the system learns and identifies the sequential behavior of ransomware, allowing it to recognize both known and novel attacks with high precision. The use of synthetic ransomware instances, generated through RanGAN, further improves the system's adaptability to new and evolving threats in real time.

In addition, the integration of Hash Conceal methods and a Linker-driven file access mechanism adds a strong layer of data protection. By concealing v[illegible]es in a hidden environment while still allowing user interaction via linked access points, the system effectively prevents unauthorized encryption. The framework's built-in real-time monitoring and automatic notifications enhance its ability to respond promptly to any suspicious activity.

Overall, the framework offers a reliable and adaptive defense against ransomware, combining accurate threat detection with proactive data safeguarding to protect systems in an increasingly hostile cybersecurity landscape.

VI. ACKNOWLEDGMENT

The authors confirm that there are no acknowledgments or external contributions to declare for this study.

REFERENCES

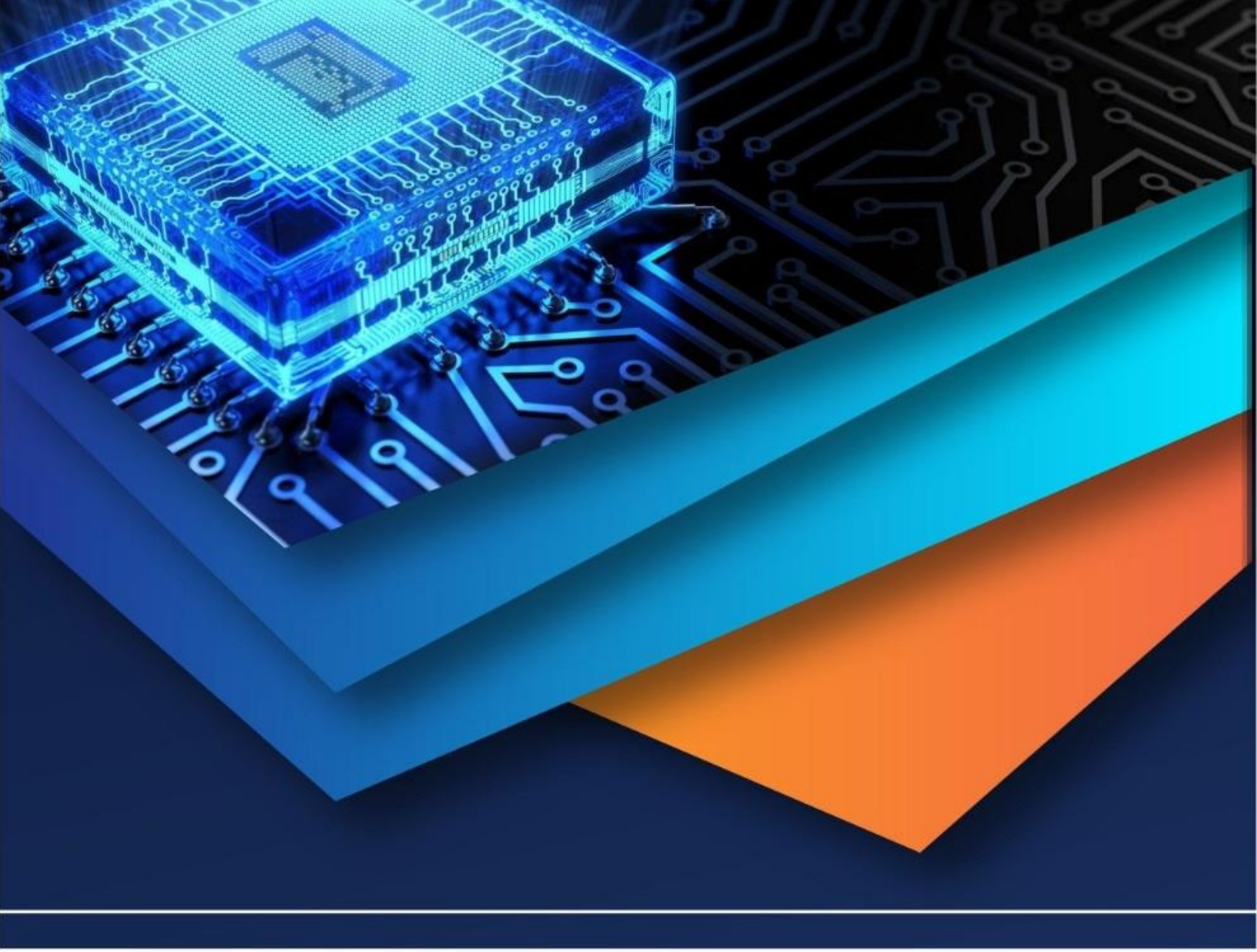
[1] J. Choi, J. Lee, G. Lee, J. Yu, and A. Park introduced a method for protecting files from malicious attacks by concealing them within hidden directories. Their work, published in the Journal of the Korea Society of Industrial Information Systems (Vol. 27, No. 2, 2022), details a strategy for safeguarding files from unauthorized modifications or encryption. [DOI: 10.9723/jksiis.2022.27.2.001]

[2] J. Yuste and S. Pastrana provided a comprehensive investigation into the Avaddon ransomware, exploring its behavior, impact, and potential methods for decrypting infected systems. This research appeared in Computers & Security (Vol. 109, October 2021) under article number 102388. [DOI: 10.1016/j.cose.2021.102388]

[3] S. Homayoun et al. proposed a pattern-mining approach to identify ransomware threats by recognizing abnormal system behavior. Their study, titled "Know abnormal, find evil", was published in IEEE Transactions on Emerging Topics in Computing (Vol. 8, No. 2, April 2020, pp. 341–351).

[4] K. Lee, S. Lee, and K. Yim explored a machine learning-based method to detect ransomware by analyzing file entropy in backup environments. Their findings were shared in IEEE Access (Vol. 7, 2019, pp. 110205–110215), emphasizing the importance of backup integrity in ransomware resilience.

[5] B. Zhou and colleagues examined the potential of using hardware performance counters for malware detection, questioning whether this technique is a reliable indicator or just a misconception. This research was presented at the Asia Conference on Computer and Communications Security in May 2018 (pp. 457–468).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY