ISSN: 2349-6002

AI-Driven Self-Healing and Energy-Efficient Software Defined Data Center Network for Ransomware Defense

Mr. P. Ganesh[1], Anbarasi M[2], Jayalakshmi L[3], Pavithira P[4]
[1]*HOD/AD, Department Computer Science and Engineering, Surya Group of institutions, Anna University*
[2,3,4]*Department Computer Science and Engineering, Surya Group of institutions, Anna University*
doi.org/10.64643/IJIRTV12I11-201014-459

***Abstract*—Ransomware attacks are one of the most serious cybersecurity threats affecting modern software-defined data center networks. These attacks encrypt critical data and demand ransom payments, leading to severe financial loss, operational downtime, and compromised data integrity. Traditional security mechanisms such as signature-based detection or rule-based monitoring struggle to detect new or evolving ransomware variants, especially zero-day attacks. This project proposes an AI-driven self-healing ransomware defense framework designed specifically for Software Defined Data Center Networks (SDDCN). The system uses deep learning techniques, particularly a GRU-based model (RanNet), to analyze system call sequences and detect suspicious behaviors associated with ransomware attacks in real time. Once ransomware activity is detected, the system immediately activates a self-healing mechanism. This mechanism encrypts important files using AES-CTR encryption with dynamic key rotation and securely uploads the encrypted files to cloud storage. This ensures that even if local files are compromised, a secure backup remains available for recovery. Additionally, the system deploys decoy honey files that attract ransomware processes away from real data. Any interaction with these decoy files triggers alerts and containment actions. By combining AI detection, encrypted backup, and deception techniques, the system significantly improves resilience and ensures data protection in modern data center environments.**

***Index Terms*—AI Security, Ransomware Detection, Self-Healing Systems, GRU Deep Learning, Software Defined Data Center Network, Honey files, Cloud Backup, Cybersecurity.**

I. INTRODUCTION

The rapid growth of digital infrastructure and cloud computing has increased the importance of protecting data center networks from cyber threats. One of the most dangerous threats today is ransomware, which encrypts important files and demands payment to restore access. In modern Software Defined Data Center Networks (SDDCN), ransomware attacks can disrupt large numbers of services, leading to data loss, downtime, and financial damage. Traditional security systems often fail to detect new or evolving ransomware attacks, especially zero-day threats, which makes advanced security mechanisms necessary.

This project proposes an AI-Driven Self-Healing and Energy-Efficient Software Defined Data Center Network to detect and defend against ransomware attacks. The system uses Artificial Intelligence and Deep Learning techniques to analyze system behaviors and detect malicious activities. A GRU (Gated Recurrent Unit) based deep learning model called RanNet is used to analyze system call sequences and behavioral patterns. This allows the system to detect ransomware activity in real time, even if the attack is new or previously unknown.

Several technologies are used to build this system. The project is developed using Python programming language, which provides strong support for machine learning and system monitoring. Deep learning libraries such as TensorFlow or PyTorch are used to train the GRU-based detection model, while NumPy, Pandas, and Scikit-learn help with data preprocessing and analysis. A Flask web framework is used to create a web dashboard where administrators can monitor system activity, view alerts, and manage security operations. The system also uses MySQL database to store user data, logs, and detection results.

To improve security and recovery, the system integrates AES encryption for data protection, cloud backup storage, and honeyfile (decoy file) deployment. When ransomware activity is detected,

important files are encrypted and automatically backed up to the cloud to prevent data loss. Honeyfiles act as traps that attract ransomware processes and help detect attacks early. By combining AI-based detection, automated backup, encryption, and deception techniques, the proposed system provides a reliable and intelligent solution for protecting modern data center networks from ransomware attacks.

A. Problem Statement

Ransomware attacks have rapidly increased in recent years and have become one of the most damaging forms of cybercrime. These attacks encrypt important files and demand ransom payments in exchange for decryption keys. Organizations operating large-scale data centers are particularly vulnerable because a single ransomware attack can disrupt multiple services simultaneously.

Traditional ransomware detection systems rely mainly on signature-based or rule-based techniques. While these approaches can detect known malware, they fail to identify new or modified ransomware variants. As cyber attackers continuously develop sophisticated techniques, these traditional methods struggle to provide adequate protection.

Furthermore, many systems lack real-time recovery mechanisms. Even if ransomware is detected, organizations may still suffer data loss and downtime due to the absence of automated recovery systems. This highlights the need for an intelligent system that not only detects ransomware but also protects and restores data automatically.

Therefore, this project aims to develop an AI-driven self-healing ransomware defense system capable of detecting both known and unknown ransomware attacks while ensuring secure backup and rapid recovery of critical data.

B. Objectives

The main objective of this project is to design and implement an AI-based ransomware detection and prevention system for Software Defined Data Center Networks. The system aims to enhance security, improve detection accuracy, and minimize data loss caused by ransomware attacks.

One important objective is to develop a deep learning model using GRU architecture (RanNet) capable of analyzing system call sequences and identifying abnormal behaviors. This allows the system to detect ransomware attacks even if the malware has never been seen before.

Another objective is to create a self-healing data protection mechanism that automatically encrypts and backs up important files to the cloud when suspicious activity is detected. This ensures data integrity and enables quick recovery after an attack.

Finally, the system aims to integrate deception techniques such as honeyfiles, real-time alerts, and automated response mechanisms to stop ransomware activity before it spreads across the network.

II. RELATED WORK

Several researchers have proposed different techniques to detect and prevent ransomware attacks in modern computing environments. Traditional approaches mainly rely on signature-based detection methods, where malware is identified by comparing file signatures with known ransomware databases. While effective against known threats, these methods fail to detect new or modified ransomware variants.

Recent research has explored machine learning and deep learning techniques for ransomware detection. Studies have shown that analyzing system behavior, such as file access patterns, process activities, and system call sequences, can help detect ransomware more effectively than traditional methods. Behavioral analysis allows systems to identify malicious actions even if the malware has never been seen before.

Other research has focused on entropy-based detection methods, which measure changes in file randomness during encryption. Since ransomware encrypts files rapidly, entropy analysis can detect suspicious encryption activities early.

However, entropy detection alone may not always provide accurate results.

To overcome these limitations, modern systems combine multiple techniques such as AI-based detection, cloud backup mechanisms, and deception strategies like honeyfiles. These integrated approaches improve detection accuracy, reduce false positives, and provide stronger protection against evolving ransomware threats.

ISSN: 2349-6002

III. SYSTEM ANALYSIS

A. Existing System

The existing ransomware detection systems rely mainly on traditional security mechanisms such as signature-based detection, heuristic analysis, rule-based monitoring, and sandboxing techniques. Signature-based systems identify ransomware by comparing files against a database of known malware signatures.

Heuristic analysis attempts to detect suspicious activities such as rapid file encryption or abnormal file access patterns. While this approach can detect unknown threats, it often produces false alarms because legitimate applications may also perform similar operations.

Rule-based monitoring systems use predefined rules to detect abnormal system behavior. For example, they may detect unusual file renaming patterns or sudden changes in file extensions. However, these rules are limited to known attack scenarios and cannot adapt to new threats.

Sandboxing techniques execute suspicious programs in isolated environments to observe their behavior safely. Although this provides deeper analysis, sandboxing requires high computational resources and may be bypassed by advanced ransomware that detects virtual environments.

B. Drawbacks

Existing ransomware detection systems suffer from several limitations that reduce their effectiveness in modern cyber environments. One major drawback is the inability to detect zero-day ransomware attacks that use new or modified encryption techniques.

Another limitation is the heavy reliance on signature databases and predefined rules. These methods require continuous updates and fail when attackers introduce new malware variants that do not match existing signatures.

Traditional systems also lack real-time response mechanisms. Even if ransomware is detected, the system may not be able to protect files immediately, leading to significant data loss and operational downtime.

Additionally, many machine learning models used in earlier research have limited accuracy and poor generalization capabilities. This results in false positives or missed detections, which reduces trust in automated ransomware defense systems.

C. Proposed System

The proposed system introduces a multi-layered AI-driven ransomware defense framework designed for software-defined data center networks. The system uses a deep learning model called RanNet, which is based on the GRU (Gated Recurrent Unit) architecture.

The RanNet model analyzes system call sequences, file access behavior, and process activity patterns to detect ransomware attacks in real time. Unlike traditional methods, this approach does not rely on predefined signatures and can detect unknown ransomware variants.

When suspicious activity is detected, the system activates an autonomous data protection mechanism. Important files are encrypted using AES-CTR encryption with dynamic key rotation and uploaded to secure cloud storage for backup.

Additionally, the system deploys decoy honeyfiles that act as traps for ransomware processes. Any interaction with these decoy files triggers alerts and activates containment procedures, preventing further damage.

D. Advantages

The proposed system offers several advantages over traditional ransomware detection methods. First, it improves detection accuracy by using AI-based behavioral analysis, which allows the system to identify both known and unknown ransomware threats.

Another advantage is the self-healing capability, which automatically protects and backs up important files when an attack is detected. This ensures that critical data remains safe even if ransomware attempts to encrypt local files.

The use of encrypted cloud backup further enhances data security. Even if attackers compromise the local system, encrypted backups stored in the cloud can be used to restore the system quickly.

Finally, the integration of deception techniques such as honeyfiles helps detect ransomware at an early stage. This reduces the spread of the attack and minimizes operational downtime.

ISSN: 2349-6002

IV. SYSTEM DESIGN

A. System Architecture

The system architecture consists of several interconnected modules designed to detect, prevent, and recover from ransomware attacks. The architecture includes the RanDetector web interface, RanNet deep learning model, ransomware detection engine, data protection module, and cloud backup system.

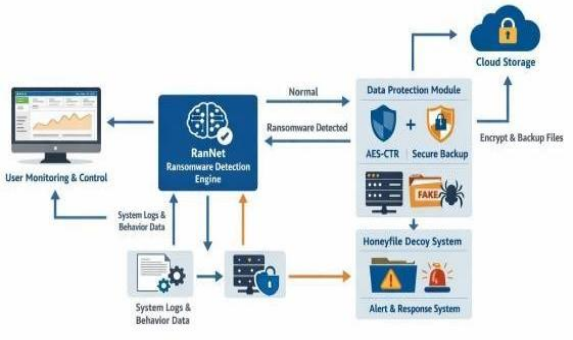

Figure 1: System Architecture

B. Module Description

The system consists of several modules that work together to provide comprehensive ransomware protection.

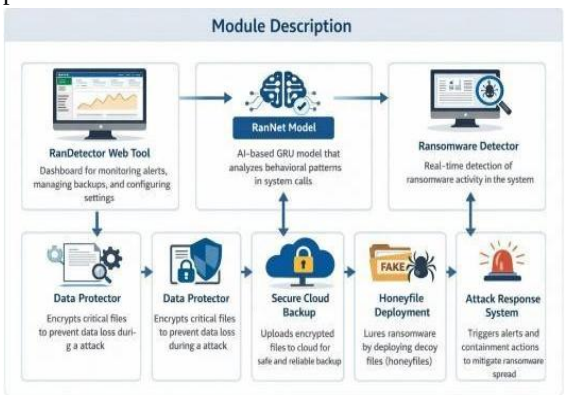

Figure 2: Module Description

C. Data Flow Diagram

The data flow diagram illustrates how information moves through the ransomware detection system. Initially, system activities such as file access, process execution, and system calls are collected by the monitoring component.

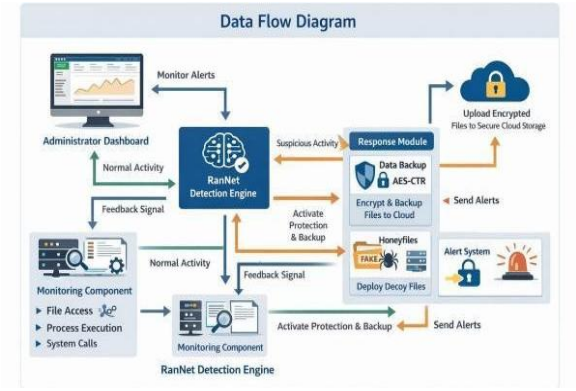

Figure 3: Data Flow Diagram

D. Database Design

The system database is designed to store important information related to users, system activities, detection results, and backup records. A MySQL database is used to maintain structured data and support efficient queries.

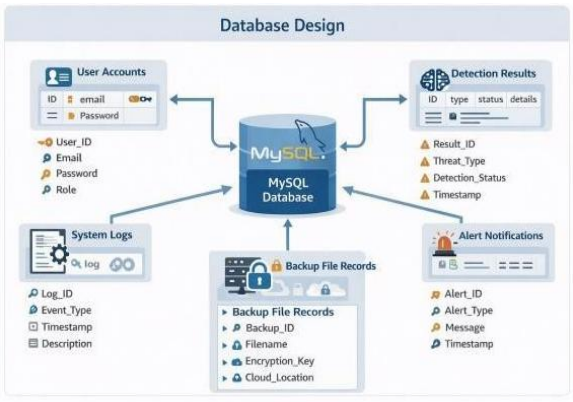

Figure 4: Database Design

V. IMPLEMENTATION

A. Hardware Requirements

The hardware requirements for the proposed system include a processor such as Intel i5 or AMD Ryzen 5, which provides sufficient computing power for running the ransomware detection system.

The system requires at least 8 GB of RAM, although 16 GB is recommended for training deep learning models. Adequate memory ensures smooth execution of machine learning algorithms and system monitoring tasks.

A 256 GB SSD storage device is recommended for faster data processing and storage of system logs, backup files, and datasets. SSD storage improves system performance and reduces data access delays.

For faster model training, an optional NVIDIA GPU with CUDA support can be used. Additionally, a stable internet connection is required for cloud backup and remote monitoring.

B. Software Requirements

The software environment for this project includes Windows operating system as the primary platform for development and deployment.

The system is developed using Python programming language, which provides extensive libraries for machine learning and system monitoring. Python frameworks simplify implementation and integration of different system components.

Machine learning libraries such as NumPy, Pandas, Scikit-learn, and TensorFlow/PyTorch are used for training and deploying the RanNet deep learning model.

A Flask web framework is used to develop the user dashboard, while MySQL is used for database management. Bootstrap may also be used to design the graphical user interface.

C. Implementation

The implementation of the proposed ransomware detection system involves integrating machine learning, system monitoring, and cloud backup technologies. The first step is collecting behavioral data such as system call sequences and file access patterns.

Next, the RanNet deep learning model is trained using GRU architecture to learn the difference between normal system behavior and ransomware activity. The trained model is then integrated into the detection module.

A monitoring system continuously collects system events and sends them to the detection engine for classification. If ransomware behavior is detected, the system triggers encryption and backup procedures.

Finally, the system deploys honeyfiles and generates alerts through the web dashboard, enabling administrators to monitor attacks and respond quickly.

D. Algorithm

The proposed system begins by continuously monitoring system activities, including system call sequences, file access patterns, and process execution behaviors. These activities are collected by a monitoring component and converted into structured behavioral data. The collected data is then preprocessed using Python-based data processing libraries such as NumPy and Pandas to remove noise and prepare the data for analysis. After preprocessing, the behavioral data is sent to the RanNet deep learning model, which is built using a GRU (Gated Recurrent Unit) architecture with frameworks such as TensorFlow or PyTorch. The model analyzes sequential patterns in system behavior and classifies them as either normal system activity or potential ransomware behavior.

If the RanNet model detects ransomware activity, the system immediately activates a security response mechanism. Critical files are protected by encrypting them using AES-CTR encryption, ensuring that sensitive data cannot be compromised. The encrypted files are then uploaded to secure cloud storage to maintain backup copies and enable recovery if local files are affected. At the same time, honeyfiles (decoy files) are deployed to mislead attackers and detect malicious file interactions. The system also generates real-time alerts through the monitoring dashboard, allowing administrators to respond quickly and contain the threat. This automated process ensures continuous monitoring, early ransomware detection, and rapid protection of critical data within the network system.

VI. RESULT ANALYSIS

The proposed ransomware detection system was evaluated using behavioral datasets containing both normal system activities and ransomware attack patterns. The RanNet model demonstrated high detection accuracy due to its ability to analyze sequential behavioral patterns.

Experimental results show that the system can detect ransomware attacks before large-scale file encryption occurs, allowing preventive actions to be taken. This significantly reduces potential data loss.

The integration of encrypted cloud backup ensures that critical files remain safe even if ransomware successfully encrypts local data. The self-healing mechanism allows the system to recover quickly without requiring ransom payments. Overall, the results indicate that combining AI-based detection, encrypted backup, and deception techniques provides a robust defense against ransomware attacks in modern data center environments.

VII. CONCLUSION

Ransomware attacks continue to pose a significant threat to modern computing systems, especially in large-scale data center environments. Traditional detection methods are often unable to detect new ransomware variants, leading to severe data loss and operational disruptions.

This project presents an AI-driven self-healing ransomware defense framework that combines deep learning detection, encrypted cloud backup, and deception strategies. The GRU-based RanNet model effectively analyzes system behaviors to detect ransomware attacks in real time.

The integration of honeyfiles and automated backup mechanisms ensures that critical data remains protected even during an attack. These features significantly reduce system downtime and improve recovery speed.

In conclusion, the proposed system provides a powerful and intelligent cybersecurity solution capable of protecting modern data center networks from evolving ransomware threats.

REFERENCES

[1] J. Choi *et al.*, "A defense mechanism against attacks on files by hiding files," *Journal of Korea Society of Industrial Information Systems*, 2022.

[2] J. Yuste and S. Pastrana, "Avaddon ransomware: An in-depth analysis and decryption of infected systems," *Computers & Security*, 2021.

[3] S. Homayoun *et al.*, "Know abnormal, find evil: Frequent pattern mining for ransomware threat hunting," *IEEE Trans. Emerging Topics in Computing*, 2020.

[4] K. Lee *et al.*, "Machine learning-based file entropy analysis for ransomware detection in backup systems," *IEEE Access*, 2019.

[5] Zhou *et al.*, "Hardware performance counters can detect malware: Myth or fact?" in *Proc. AsiaCCS*, 2018.

[6] Alraizza and A. Algarni, "Ransomware detection using machine learning: A survey," *Big Data and Cognitive Computing*, 2023.

[7] Chew *et al.*, "Real-time system call-based ransomware detection," *International Journal of Information Security*, 2024.

[8] M. Rele *et al.*, "Exploring ransomware detection based on artificial intelligence and machine learning," *Procedia Computer Science*, 2025.

[9] T. McIntosh *et al.*, "The inadequacy of entropy-based ransomware detection," *Information Security Journal*, 2019.

[10] K. Lee *et al.*, "Effective ransomware detection using entropy estimation for cloud services," *Sensors*, 2023.

[11] Kritika *et al.*, "A comprehensive literature review on ransomware detection using deep learning," *Computer Networks*, 2024.

[12] S. Kiyol *et al.*, "Ransomware detection using LSTM networks and file entropy analysis," *Cybersecurity Journal*, 2022.

[13] L. Harishni, "Real-time ransomware detection and response system using behavioural monitoring," *SSRN Research Paper*, 2025.

[14] Casino *et al.*, "Ransomware detection through classification of high-entropy files," *Cybersecurity Journal*, 2025.

[15] M. Gazzan *et al.*, "RWArmor: Early detection of cryptographic ransomware using dynamic analysis," *International Journal of Information Security*, 2023.

[16] Alzahrani *et al.*, "Randroid: Structural similarity approach for detecting ransomware applications," in *Proc. IEEE Int. Conf. Electro/Information Technology*, 2018.

[17] Y. Wan *et al.*, "Feature selection-based ransomware detection using machine learning," in *Proc. Int. Conf. Computer and Communication Systems*, 2018.

[18] U. Adamu and I. Awan, "Ransomware prediction using supervised learning algorithms," in *Proc. Future Internet of Things and Cloud Conf.*, 2019.

[19] Noorbehbahani *et al.*, "Analysis of machine learning techniques for ransomware detection," in *Proc. Information Security and Cryptology Conf.*, 2019.

[20] Cheng *et al.*, "A systematic review of ransomware detection techniques," *Journal of Computer Science and Technology*, 2021.

[21] M. Masum *et al.*, "Ransomware classification and detection with machine learning algorithms," in *Proc. IEEE Computing and Communication Workshop and Conf.*, 2022.

[22] J. Bang *et al.*, "Entropy sharing in ransomware: Bypassing detection techniques," *Cybersecurity Research Journal*, 2024.

ISSN: 2349-6002

[23] P. Idliman *et al.*, "Entropy-synchronized neural hashing for unsupervised ransomware detection," arXiv, 2025.
[24] V. Iskorohodov *et al.*, "Hierarchical entropic diffusion for ransomware detection," arXiv, 2025.
[25] Starchenko *et al.*, "Decentralized entropy-driven ransomware detection using neural graph embeddings," arXiv, 2025.