International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 04 April-2026 | Impact Factor: 3.5

AI Based Early Ransomware Detection System using LLM

K. Dhivya[1], R. Sri Nithya[2], S. Niranchana[3]

[1] Assistant Professor, Department of CSE (Cyber Security), Sri Shakthi Institute of Engineering and Technology, Coimbatore, TamilNadu, India
B.E. Students, Computer Science Engineering (Cyber Security), Sri Shakthi Institute of Engineering and Technology, Coimbatore, TamilNadu, India

Corresponding Author Email: srinithyaramesh431@gmail.com

How to Cite this Article:
Dhivya, K., Nithya, R. S. & Niranchana, S. (2026). AI Based Early Ransomware Detection System using LLM. International Journal of Creative and Open Research in Engineering and Management, 02(04). https://doi.org/10.55041/ijcope.v2i4.474

https://doi.org/10.55041/ijcope.v2i4.357

Abstract—

Ransomware attacks are a problem now. They target people, companies and the government by locking up information and asking for money to get it back. The old ways of keeping things safe often do not catch these attacks until it is too late. So it is very important to catch them as they happen. This project is about making a system that can detect ransomware in time. It uses Artificial Intelligence and Large Language Models to find and stop ransomware.The system watches what is happening on the computer all the time. It looks at things like what filesre being used what programs are running and if anything strange is happening with encryption. The system uses machine learning to tell the difference between bad behavior. It learns from what it has seen. The Large Language Models help the system understand what is going on by looking at patterns and giving more information. This helps the system catch types of ransomware.

The system also has a part that can pretend to be a ransomware attack. This helps us test the system and see how well it works. The goal of the system is to catch the attack act fast and prevent damage. It tells the user what is happening and takes steps to stop it. The system is designed to work and be able to handle real situations.This project shows that using Artificial Intelligence and
advanced language models can be a way to fight ransomware. It gives us a way to defend against these attacks that's smart and acts before they can do harm. The system uses Ransomware Detection to keep us safe, from Ransomware attacks. Ransomware attacks are a deal and the system is designed to detect Ransomware and prevent Ransomware from causing damage.

Keywords— Ransomware Detection, Machine Learning, Behavioral Analysis, Cybersecurity, Real-Time Monitoring, Malware Analysis

I. INTRODUCTION

Ransomware is one of the kinds of cyberattacks that we have seen in the last few years. It has affected people organizations and government institutions over the world. Ransomware is a software that locks your files or systems and asks for money to unlock them. Because we are using systems and storing data more and more the bad effects of ransomware attacks have become worse. This has led to money losses secret information getting out and systems not working properly. The old security systems like antivirus software and firewalls are not good enough to find ransomware attacks, especially the ones that are smart and can avoid being found.

To solve these problems new cybersecurity solutions are using Artificial Intelligence and Machine Learning to find threats before they happen. These technologies can look at a lot of data find patterns and detect strange things as they happen. In this project we made a system that can find ransomware in time using Artificial Intelligence and Large Language Models to make detection better. The system watches what the computer is doing like how filesre changed how programs are working and how encryption is happening to find bad actions before they cause a lot of damage.

We also used Large Language Models to make the system smarter by understanding computer behavior and sending out useful warnings. The project includes an attack environment to test how well the detection system works in a controlled setting. The main goal of this project is to make a system that can find ransomware attacks early is reliable works well and can be used by people. It also shows how important it is to combine Artificial Intelligence with cybersecurity to build defense systems against new threats. Ransomware detection is a part of this project and we want to make sure that our system can detect ransomware attacks as soon, as possible.

II. RANSOMEWARE AND ITS TYPES

Ransomware is a type of malicious software that denies access to all computer systems, networks, or data until payment of a ransom has been made. Ransomware represents a serious cyber threat since it affects both the ability of users to access their data as well as its confidentiality. The majority of the time, once a computer has been infected by ransomware, files that were previously accessible will have either been encrypted (in the case of crypto ransomware), or the user will have had their access to the infected computer denied by an attacker until they paid the ransom demanded by the attacker. Ransomware has evolved from simple "lock-type" attacks to more complex and focused attacks aimed at large organizations, hospitals, and local/federal government agencies. Ransomware is primarily distributed by way of phishing email messages, infected attachments, compromised websites, or exploiting vulnerabilities within the software programs of the system being attacked. Financial losses are only part of what can occur to victims of ransomware; victims also could experience operational losses as a result of losing data, being unable to perform their work, suffering reputational damage, or incurring possible legal penalties.

Ransomware has many different types of classifications depending on how it attacks its victim and the severity of the attack. One of the most prevalent types of ransomware is crypto ransomware, where the data stored on the user's hard drive has been encrypted, and to retrieve the data, the user has to pay the ransom to the attacker for the decryption key. The most problematic aspect of crypto ransomware is that while the user still has access to their computer's operating system, the user cannot access any of the data stored on their computer until they receive the decryption key from the attacker that encrypted their data.

Worldwide ransomware attacks have caused an enormous amount of disruption and also causing numerous incidents that occurred in real-time illustrate that they are an urgent issue to our

economy and society.Two of the most recognized ransomware attack occurrences include WannaCry (2017) and NotPetya (2017). WannaCry spread quickly through 150 countries, took over mass numbers of outdated Microsoft Windows systems, and victimized major hospitals of the UK's National Health Service ("NHS"); causing major disruptions to critical medical services, cancelling appointments, and rendering patient data unusable and placing lives at risk. NotPetya, while initially targeting the country of Ukraine, rapidly spread around the world and impacted multimillion-dollar multinational corporations such as Maersk (the shipping company). NotPetya, in contrast to traditional ransomware, caused permanent data loss leading to billions of dollars in damages. This demonstrates how ransomware can extend beyond just individuals to potentially impact our entire economy through damaging large corporation's operations.Since these incidents, more recent ransomware attacks have been specified and more advanced. Two examples are the Colonial Pipeline attack (2021) in the United States, which disrupted major fuel supplies resulting in panic buying across much of the United States by shutting down a major gas pipeline, and disrupted hospital services for days after the AIIMS Delhi cyberattack (2021) in India halted hospital services and created disruptions for patients

III. METHODOLOGY

The methodology behind the proposed approach to detecting a ransomware attack consists of real-time detection by applying artificial intelligence and behavioral analysis. Firstly, there is constant monitoring of different actions performed by the system, including but not limited to file operations, processes execution, and RAM usage. All the data obtained from the activity are analyzed to determine what the usual behavior pattern of the system looks like. Based on the established behavior, it becomes possible to identify abnormal cases.

Later, the gathered data will be processed and transformed into a form suitable for analysis. The following features have been recognized: changes in files frequency, encryption activities, unusual process traits, and quick file accesses. They are then fed into a machine learning algorithm trained to differentiate between good and bad behaviors. The data stream is analyzed by the algorithm and the behavior is classified as good or bad.

In order to improve detection accuracy, the system uses the LLM feature within itself. This will help the system interpret and analyze the behavioral pattern with intelligent insights based on system logs and activities analysis. By doing so, this helps the system in giving more relevant information and alerts to the user rather than just giving out simple alerts. It increases the ability of the system to detect new or unidentified ransomware.

Further, an artificial attack simulation module is added to the system for testing purposes. The artificial attack simulation module simulates the behavior of ransomware in terms of rapid file encryption and unusual access patterns. The inclusion of an artificial attack simulation module allows testing of the effectiveness of the system in detecting ransomware without causing any harm.

In conclusion, once the ransomware infection is detected within the computer, this results in the notification of the user. The user will be alerted, and some measures may be taken, including the suspension of any activity that may result in harm, denial of access to the file, and isolation of the affected part of the computer system.

IV. RESULTS AND DISCUSSION

This project’s results make it clear: the AI-based ransomware detection system works well at spotting threats early by constantly watching how the system behaves. In testing, we ran the system through both normal use and simulated

ransomware attacks. It did a solid job telling the difference between regular and suspicious activity, using things like how files were accessed, how quickly encryption happened, strange processes running, and odd network activity.The model caught ransomware-like behavior with high accuracy and barely any false alarms, which shows that this behavior-based method is more dependable than the old signature-based methods, especially when facing new or unknown attacks. It didn't just sit back either; it responded quickly, sending alerts before major damage like widespread file encryption could happen. That's real-time detection in action.We also noticed that using machine learning made the system more flexible. It kept learning and adapting to new attack patterns as they came up. Of course, there were a few bumps—like a slight slowdown from the continuous monitoring and the occasional mistake when high-intensity but legitimate processes got flagged. Still, the benefits outweighed these challenges. The bottom line: this system gives stronger, proactive ransomware protection, making it a valuable addition to today's cybersecurity world.

V. CONCLUSION

The above-mentioned approach will enable us to develop a new method of detecting and preventing ransomware attacks. First of all, it means that we should monitor the behavior of the system under the attack. In addition, we will apply different approaches to detect and stop these kinds of attacks. The application of machine learning will improve the effectiveness of the method because we will be able to learn how to detect any malware attack. Nevertheless, there are certain shortcomings associated with this method. On the one hand, our program will use extra processing power and memory space of the user's device. On the other hand, in some cases, it can provide false results because it will be unable to differentiate between harmful software and regular files.

REFERENCES

[1] Almashhadani, A. O., Kaiiali, M., Sezer, S., & O'Kane, P., "A Multi-Classifier Network-Based Crypto Ransomware Detection System," IEEE Transactions on Network and Service Management, 2020.

[2] Homayoun, S., Dehghantanha, A., Ahmadzadeh, M., Hashemi, S., & Khayami, R., "DRTHIS: Deep Ransomware Threat Hunting and Intelligence System," Computers & Security Journal, 2021.

[3] Al-rimy, B. A. S., Maarof, M. A., Shaid, S. Z. M., & Ariffin, A. F., "Ransomware Detection Using Machine Learning: A Comprehensive Review," Journal of Network and Computer Applications, 2022.

[4] Naseer, S., Saleem, Y., Khalid, S., Bashir, M. K., Han, J., Iqbal, M. M., & Han, K., "Enhanced Network Anomaly Detection Based on Deep Neural Networks," IEEE Access, 2023.

[5] Alzahrani, A., & Alghazzawi, D., "AI-Based Ransomware Detection Using Behavioral Analysis," Computers & Security Journal, 2024.

[6] Sharma, T., & Kumar, R., "Real-Time Ransomware Detection Using Machine Learning Techniques," International Journal of Information Security and Privacy, 2025.