# Ransomware Detection Application

Implementation of parts of

**Asynchronous Peer-to-Peer Federated Capability-Based Targeted Ransomware Detection Model for Industrial IoT**

by

**Hemant Kumar**

(Roll No. 20BCS100)

Supervisor:

**Dr. Neelam Dayal**

(Assistant Professor)

Computer Science and Engineering

PDPM IIITDM Jabalpur

Computer Science and Engineering

PDPM Indian Institute of Information Technology, Design and Manufacturing, Jabalpur

(2024)

# Acknowledgement

I would like to express my sincere gratitude to all the people who contributed in some way to the work described in this Project. Primarily I thanks to my respected supervisor, **Dr. Neelam Dayal**, Assistant Professor in Computer Science and Engineering department, during my tenure of **BTP**, she contributed to an enriching college experience by giving me intellectual freedom in my work, providing me inspiration and motivation, engaging me with new ideas, and demanding a high quality of work in all my endeavors. It was a matter of great felicity and privilege for me to work under his auspices. Additionally, I would like to thanks **Dr. Abhishek Verma** (Assistant Professor), I.T Deptt. from the **BabasahEB Bhimrao Ambedkar University, Lucknow** for their interest in my work, for extending their valuable time and support throughout my Project.

I owe special thanks to my Project Partner **Chaitanya Mandi, Roll-no: 20BCS062** for his support and suggestions that kept me motivated to accomplish my research work during my course duration. I would like to thanks my all seniors, of the Computer Science and Engineering Department including the non-teaching staff with whom I got the opportunity to work in a healthy and joyful environment.

Finally, I would like to acknowledge my beloved family members who supported me during my time here. I am really obliged for their constant love and support.

**Hemant Kumar**

# Certificate

This is to certify that the Report entitled, **"Ransomeware Detection Application"**, submitted by **Hemant Kumar, Roll No. 20BCS100** in partial fulfillment of the requirements for the award of **B.Tech Degree in Computer Science and Engineering**, at PDPM Indian Institute of Information Technology, Design and Manufacturing Jabalpur is an authentic work carried out by him under my supervision and guidance.

To the best of my knowledge, the matter embodied in the thesis has not been submitted elsewhere to any other university/institute for the award of any other degree.

**Dr. Neelam Dayal** **2024-02-22**
Assistant Professor
Computer Science and Engineering Discipline,
PDPM Indian Institute of Information Technology, Design and Manufacturing, Jabalpur, M.P, India-482005

# Abstract

**Background:** Ransomware poses a severe threat to the security of digital assets, with a rising frequency of sophisticated attacks targeting individuals and organizations globally. The potential for significant financial and reputational damage underscores the urgent need for robust and proactive countermeasures. Traditional antivirus solutions often fall short in detecting evolving ransomware variants, necessitating the development of advanced detection applications.Kok et al. (2019)

**Aim:** The primary objective of this research is to design, implement, and evaluate a cutting-edge Ransomware Detection Application. Leveraging innovative techniques, including machine learning and behavioral analysis, our application aims to provide real-time detection and mitigation of ransomware threats. By enhancing the resilience of systems against emerging attack vectors, the goal is to fortify the cybersecurity posture of individuals and organizations in the face of evolving ransomware landscape.

**Conclusion:** The developed Ransomware Detection Application showcases promising results in effectively identifying and neutralizing ransomware threats. Through extensive testing and validation, our application demonstrates a high level of accuracy and efficiency in differentiating normal user behavior from malicious activities associated with ransomware attacks. The successful deployment of this solution contributes significantly to the ongoing efforts to secure digital environments against the menace of ransomware.

**Keywords:** Ransomware, Detection Application, Cybersecurity, Machine Learning, Behavioral Analysis, Threat Mitigation, Real-time Protection, Cyber Threats, Digital Security, Antivirus Solutions.

# 1 Introduction

In an era dominated by digital connectivity, the persistent threat of ransomware looms large, posing a formidable challenge to the security of individuals and organizations alike. Ransomware, a malicious software that encrypts or locks files and demands a ransom for their release, has evolved into a sophisticated and dynamic cyber threat. Understanding the nuances of ransomware is pivotal in developing effective countermeasures to safeguard against its pernicious impacts.

Ransomware, at its core, is a form of cyber extortion wherein malicious actors leverage advanced encryption algorithms to restrict access to files or entire systems. The victim, often left with no recourse, is coerced into paying a ransom, typically in cryptocurrency, to obtain the decryption key. This nefarious practice has given rise to various types of ransomware, each exhibiting distinct characteristics and complexities.

*Encrypting Ransomware:* This variant employs robust encryption algorithms, rendering files inaccessible until a ransom is paid. Notable examples include CryptoLocker and WannaCry.

*Locker Ransomware:* Instead of encrypting files, locker ransomware locks users out of their systems, demanding payment for access restoration. Instances like the FBI virus and Winlocker fall into this category.

*Scareware:* While not encrypting files, scareware falsely claims the presence of malware, tricking users into paying for non-existent security solutions.

*Mobile Ransomware:* Targeting mobile devices, this variant demands payment for decrypting files or unlocking the device. Svpeng and Android Defender are prominent examples.

# 2 Methodology

In the fight against ransomware, a comprehensive approach involving various detection techniques is essential. The following sections detail the methodologies employed, each with its strengths and weaknesses.

## 2.1 Static File Analysis

Static file analysis involves examining files for suspicious characteristics without executing them. This can include scrutinizing file headers, code patterns, and file metadata.

Pros:

- Fast and efficient.
- Does not require actual execution.

Cons:

- Limited to known signatures.
- Unable to detect polymorphic or new variants.

## 2.2 Common File Extensions Blacklist

Maintaining a blacklist of common file extensions associated with ransomware can help identify potential threats based on file types.

Pros:

- Targets known ransomware file types.
- Relatively easy to implement.

Cons:

- May generate false positives for legitimate files.
- Ineffective against file-less ransomware.

## 2.3 Honeypot Files / Deception Techniques

Deploying decoy files or using deception techniques can lure ransomware into revealing its presence.

Pros:

- Provides early detection by attracting ransomware.
- Allows for studying ransomware behavior.

Cons:

- Requires careful setup to avoid false positives.
- May not capture all types of ransomware.

## 2.4 Dynamic Monitoring of Mass File Operations

Real-time monitoring of mass file operations, especially encryption-like activities, can signal a ransomware attack.

Pros:

- Detects ransomware during the encryption phase.
- Responsive to active threats.

Cons:

- May generate false alarms during legitimate file operations.
- Reactive in nature.

## 2.5 Measure Changes of Files' Data (Entropy)

Monitoring entropy levels in files helps identify suspicious changes, as ransomware tends to increase entropy during encryption.

Pros:

- Detects alterations in file data.
- Independent of specific ransomware signatures.

Cons:

- Requires baseline entropy data for accurate detection.
- Limited to file modification detection.

Incorporating a combination of these techniques provides a layered defense against ransomware, enhancing the likelihood of early detection and mitigation.

## 3 Results

Result will be disclosed soon, working on it

## 4 Conclusion

Work is going on

Algorithm 1: xyzzy

```
Data: None
Result: Hello, World!
while true do
    Print(”Hello, World!”);
    if Condition then
        DoSomething();
```

# References

Kok, S et al. (2019). “Ransomware, threat and detection techniques: A review”. In: Int. J. Comput. Sci. Netw. Secur 19.2, p. 136.