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 un-

locking the device. Svpeng and Android Defender are prominent examples.

2 Methodology

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetuer a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetuer. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui. Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetuer odio sem sed wisi.

Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris. Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.

3 Results

Result will be disclosed soon, working on it

4 Conclusion

Etiam pede massa, dapibus vitae, rhoncus in, placerat posuere, odio. Vestibulum luctus commodo lacus. Morbi lacus dui, tempor sed, euismod eget, condimentum at, tortor. Phasellus aliquet odio ac lacus tempor faucibus. Praesent sed sem. Praesent iaculis. Cras rhoncus tellus sed justo ullamcorper sagittis. Donec quis orci. Sed ut tortor quis tellus euismod tincidunt. Suspendisse congue nisl eu elit. Aliquam tortor diam, tempus id, tristique eget, sodales vel, nulla. Praesent tellus mi, condimentum sed, viverra at, consectetuer quis, lectus. In auctor vehicula orci. Sed pede sapien, euismod in, suscipit in, pharetra placerat, metus. Vivamus commodo dui non odio. Donec et felis.

Etiam suscipit aliquam arcu. Aliquam sit amet est ac purus bibendum congue. Sed in eros. Morbi non orci. Pellentesque mattis lacinia elit. Fusce molestie velit in ligula. Nullam et orci vitae nibh vulputate auctor. Aliquam eget purus. Nulla auctor wisi sed ipsum. Morbi

porttitor tellus ac enim. Fusce ornare. Proin ipsum enim, tincidunt in, ornare venenatis, molestie a, augue. Donec vel pede in lacus sagittis porta. Sed hendrerit ipsum quis nisl. Suspendisse quis massa ac nibh pretium cursus. Sed sodales. Nam eu neque quis pede dignissim ornare. Maecenas eu purus ac urna tincidunt congue.

References

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