IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204060 |

Ransomware Detection and Protection

Harini Priya[1], Aarthi. K[2], Mrs. Priskilla Angel Rani J[3]

Student, Dept. of CSE., Francis Xavier Engineering college, Tirunelveli, Tamil Nadu, India[1 2]

Assistant Professor, Dept. of CSE., Francis Xavier Engineering college, Tirunelveli, Tamil Nadu, India[3]

ABSTRACT: Ransomware is a type of malware that locks avictim's data or device and threatens to keep it locked—or worse—unless the victim pays a ransomware to the attacker. Ransomware often evades antivirus tools, encrypts files, and renders the target computer and its data unusable. The current approaches to detect such ransomware include monitoring processes, system calls, and file activities on the target system and analysing the data collected. Monitoring multiple processes has a very high overhead; newer ransomware may interfere with the monitoring and corrupt the collected data. To address this concern, this project adopted an open design approach to enhance the robustness of the proposed method. The proposed method detect ransomware and protects critical files from existing ransomware by applying a hiding strategy that poses a challenge to attackers in finding the target files. This project developed a proactive defence strategy against ransomware threats, leveraging " RanGAN & quot ; for early detection and "Hash Conceal& quot; for data protection. RanGAN (Ransomware Generative Adversarial Network) employs advanced machine learning techniques to detect ransomware behaviour patterns in real-time, while Hash Conceal secures critical data from malicious encryption. Together, these technologies form a robust defence, ensuring rapid threat identification and minimizing data loss. This strategy aims to fortify cybersecurity against the evolving ransomware landscape, providing a resilient shield for critical assets.

I. INTRODUCTION

Ransomware is a malware designed to deny a user or organization access to files on their computer. By encrypting these files and demanding a ransom payment for the decryption key, cyber attackers place organizations in a position where paying the ransom is the easiest and cheapest way to regain access to their files.Some variants have added additional functionality such as data theft – to provide further incentive for ransomware victims to pay the ransom. Ransomware has quickly become the most prominent and visible type of malware. Recent ransomware attacks have impacted hospitals' ability to provide crucial services, crippled public services in cities, and caused significant damage to various organizations The earliest variants of ransomware were developed in the late 1980s, and payment was to be sent via snail mail. Today, ransomware authors order that payment be sent via cryptocurrency or credit card, and attackers target individuals, businesses, and organizations of all kinds. In 2020, the Snake ransomware attack brought Honda's global operations to a standstill. That same week, Snake, a form of file-encrypting malware, also hit South American energy- distribution company Enel Argentina. In 2019, cybercriminals encrypted files that froze the computer networks of Pemex, Mexico's state- owned gas and oil conglomerate, demanding $5 million to restore service.And in 2017, the WannaCry crypto worm hit 230,000 computers globally by exploiting a vulnerability in Microsoft Windows. Today, through a mix of outdated technology, "good enough" defense strategies focused solely on perimeters and endpoints, lack of training (and poor security etiquette), and no known "silver bullet" solution, organizations of all sizes are at risk. Especially as cybercriminals are making it their business to encrypt as many computer systems on the corporate network as possible in order to extort a ransom ranging from thousands to millions of dollars. In fact, ransomware attacks were predicted to occur every 11 seconds in 2021 at a global cost of $20 billion.

II. RELATED WORK

1.Scareware: Scareware, as it turns out, is not that scary. It includes rogue security software and tech suppohfjrt scams. You might receive a pop-up message claiming that malware was discovered and the only way to get rid of it is to pay up. If you do nothing, you'll likely continue to be bombarded with pop-ups, but your files are essentially safe. A legitimate cybersecurity software program would not solicit customers in this way. If you don't already have this company's software on your computer, then they would not be monitoring you for ransomware infection. If you do have security software, you wouldn't need to pay to have the infection removed —you've already paid for the software to do that very job.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204060 |

2. Screen lockers: Upgrade to terror alert orange for these guys. When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full- size window will appear, often accompanied by an official-looking FBI or US Department of Justice seal saying illegal activity has been detected on your computer and you must pay a fine. However, the FBI would not freeze you out of your computer or demand payment for illegal activity. If they suspected you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.

III. PROPOSED SYSTEM

The proposed system for a proactive defensive strategy against ransomware threats using RanGAN (Ransomware Generative AdversarialNetwork) and Hash Conceal combines cutting-edge technologies to offer a robust defense gainst ransomware attacks.An overview of the proposed system: RanGAN-Based Ransomware Detection The system incorporates RanGAN, a deep learning model specifically designed to identify ransomware patterns and behaviors. RanGAN is trained on a diverse range of ransomware samples, enabling it to recognize both known and emerging threats. It leverages generative adversarial networks to enhance its ability to detect ransomware variants, even those without known signatures.The system establishes a comprehensive proactive defence strategy that combines the strengths of RanGAN, dynamic analysis, and Hash Conceal. This strategy goes beyond traditional, reactive approaches and aims to prevent ransomware attacks before they can cause harm. By identifying and mitigating ransomware threats at an early stage, the system significantly reduces the impact on data and operations.To enhance data protection and privacy, the system integrates Hash Conceal technology. Files and data are hashed, adding an extra layer of security that prevents unauthorized access and ensures data integrity. Hash Conceal helps safeguard sensitive information and provides assurance that data remains intact and unaltered.

IV. EXISTINGSYSTEM

In the existing system for ransomware detection and prevention, various traditional method and machine learning algorithms have been employed to safeguard systems and data. An overview of the existing system and the machine learning algorithms used: Signature-Based Detection Signature-based methods, a fundamental component of traditional antivirus solutions, rely on the identification of known ransomware signatures. When a file or process matches a known signature, it is flagged as ransomware. While this approach is effective in detecting well- established ransomware strains, it falls short when it comes to newer or zero-day ransomware variants that lack known signatures. Behaviour-Based Detection In behaviour-based detection, the system monitors the behaviour of files and processes ireal- time. Any deviation from established behaviour patterns, especially those indicative of ransomware-like actions (e.g., mass file encryption), triggers an alert. Behaviour-based detection is versatile and can identify previously unknown ransomware. Anomaly Detection Anomaly detection algorithms, including Isolation Forest and One-Class Support Vector Machines (SVM), are used to identify outliers in data that deviate from expected patterns. They are particularly useful in capturing ransomware activities that exhibit irregular behavi or or data patterns.

V. SIGNIFICANCE OF PROJECT

This project prioritizes data security and confidentiality, ensuring the integrity of sensitive information, which is crucial in an era of increasing privacy concerns. The practical implications of this project are profound. It significantly reduces the risk of data loss and financial harm associated with ransomware attacks. By doing so, it minimizes operational disruptions, leading to better business continuity and productivity. Moreover, the project contributes to an overall improvement in the cybersecurity posture of organizations and individuals by offering a comprehensive and adaptive defence strategy. Empowering users through training and awareness is another dimension of this project's significance

It not only provides a technological solution but also encourages individuals and organizations to actively engage in their cybersecurity efforts, reducing vulnerabilities and strengthening the human factor in security. The adaptability and scalability of the strategy ensure that it can be seamlessly integrated into various environments and existing security infrastructures. It is designed to evolve over time, thereby providing long-term sustainability in the face of rapidly changing ransomware tactics and threats. Furthermore, this project has a broader economic and social impact. By reducing the financial impact and potential data breaches caused by ransomware, it contributes to the economic and social well-being of organizations and society as a whole. Overall, the project's proactive defence strategy represents a significant step towards a more resilient and secure digital landscape.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204060 |

VI. SYSTEM ARCHITECTURE

In a real-world scenario, a three-tiered web architecture is developed, including web servers, application servers, ana database server. This cloud-based online tool, built with Python and Flask Framework, scans registered devices for security threats, especially Ransomware. It offers a comprehensive report on system security, helping protect users' devices from variousweb threats. Admins securely log in to the End User Interface to access administrative functionalities, managing diverse datasets, configuring model training, deploying the RanGAN model to the RanFooler Web App, and overseeing user accounts to ensure a secure user environment. Users initiate the configuration process by registering with the RanFooler web application. After logging in, they configure their systems by providing the MAC ID for unique identification. Users can flexibly choose files for protection from ransomware attacks, review and confirm their configurations, and access a personalized control panel for system overviews and security-related alerts. In this module, Ransomware detection approaches are developed using DL algorithms like BiLSTM and GRU. Byte files and Asm files are loaded and pre-processed for feature extraction. Shallow deep learning-based feature extraction methods are employed, including word2vec, for effective model training. The attacker model focuses on downloading and installing Ransomware on victim machines using techniques like social engineering and drive-by downloads. Shellcode is fetched from distribution sites, and obfuscated ransomware code is used to exploit vulnerabilities. RanFooler offers online scan for known and unknown Ransomware threats, providing real-time threat detection. It utilizes a one-click scan feature and is regularly updated to stay ahead of evolving threats.

Software testing is the evaluation of how software acts when faced with a variety of tasks or circumstances. For the best results, the software testing process would start as early as possible in the development process and continue until the product launches. Software testing is an intensive process that requires repetition and strong attention to detail from the developer team and the software testers. As new technology emerges, software testing changes and grows to meet the demands of the testing.

VII. SOFTWARE TESTING PROCESS

There is a four-step process for testing software. This plan stays the same whether an individual or team of testers works on the project and repeats every time the team performs a new test. Here's the software testing process:

1. Planning: Every test starts with a plan. The tester gathers the information, like what tests to perform, what bugs to look for and the desired test results, and creates a plan with a set of priorities and tasks.
2. Preparing: Testing requires the correct setting. The tester researches the product features and previous test cases and gathers the tools needed for the particular test set.
3. Executing: The tester runs the tests on the software and records the results. The tester notes which test cases succeeded or failed and how the results compare to the ideal result for the particular task.
4. Reporting: The tester compiles the results for that test into a report and delivers it to project leaders. Documenting the results is important so that the team can fix problems that arose or bugs that appeared.

VIII. SYSTEM DESCRIPTION

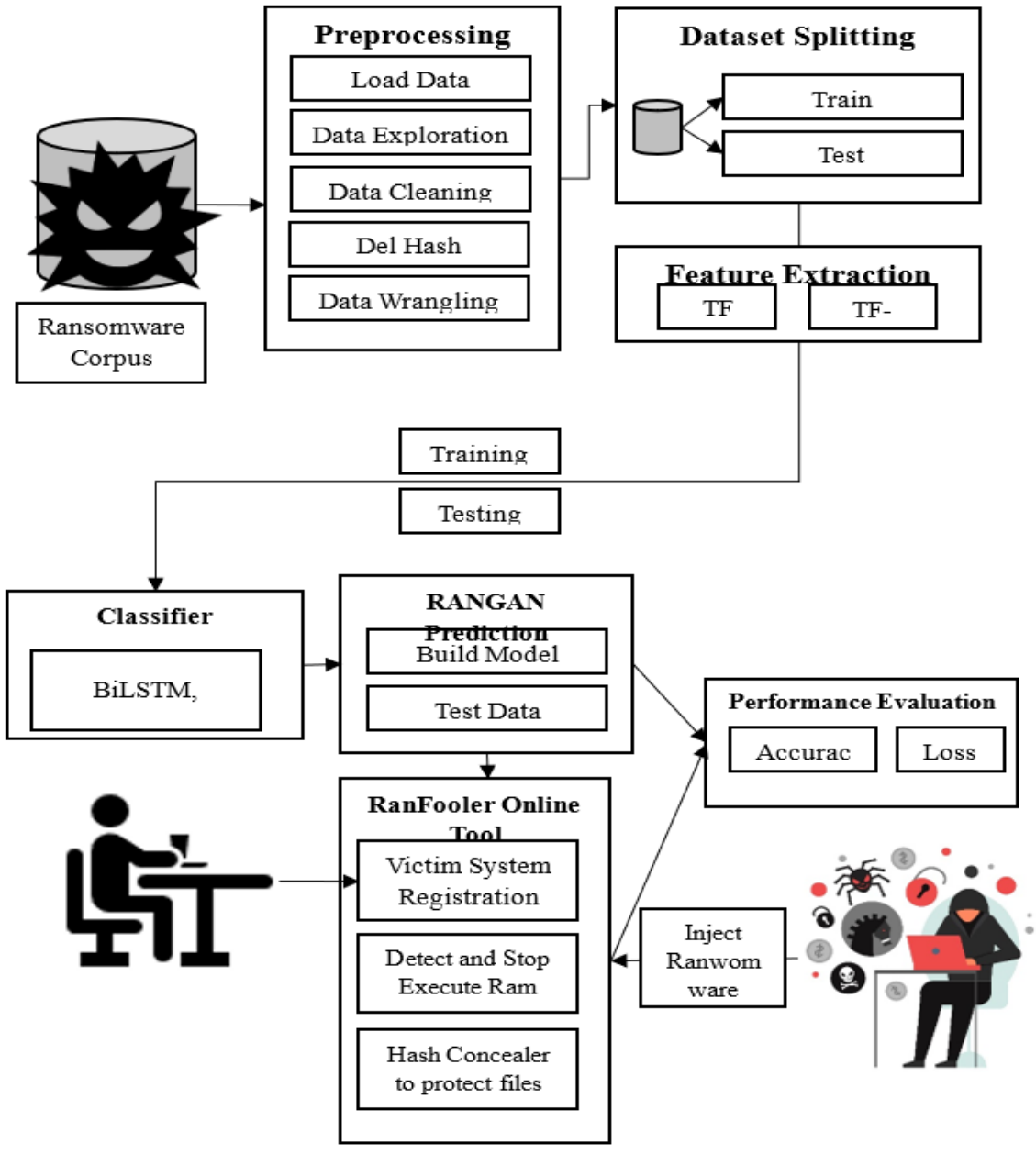
In a real-world scenario, a three-tiered web architecture is developed, including web servers, application servers, and a database server. This cloud-based online tool, built with Python and Flask Framework, scans registered devices for security threats, especially Ransomware. It offers a comprehensive report on system security, helping protect users' devices from various web threats. Admins securely log in to the End User Interface to access administrative functionalities, managing diverse datasets, configuring model training, deploying the RanGAN model to the RanFooler Web App, and overseeing user accounts to ensure a secure user environment. Users initiate the configuration process by registering with the RanFooler web application. After logging in, they configure their systems by providing the MAC ID for unique identification. Users can flexibly choose files for protection from ransomware attacks, review and confirm their configurations, and access a personalized control panel for system overviews and security-related alerts. In this module, Ransomware detection approaches are developed using DL algorithms like BiLSTM and GRU. Byte files and Asm files are loaded and pre-processed for feature extraction. Shallow deep learning-based feature extraction methods are employed, including word2vec, for effective model training. The attacker model focuses on downloading and installing Ransomware on victim machines using techniques like social engineering and drive-by downloads. Shellcode is fetched from distribution sites, and obfuscated ransomware code is used to exploit vulnerabilities.In a real-world scenario, a three-tiered web architecture is developed, including web servers, application servers, and a database server. This cloud-based online tool, built with Python and Flask Framework, scans registered devices for security threats, especially Ransomware. It offers a comprehensive report on system security, helping protect users' devices

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204060 |

from various web threats. Admins securely log in to the End User Interface to access administrative functionalities, managing diverse datasets, configuring model training, deploying the RanGAN model to the RanFooler Web App, and overseeing user accounts to ensure a secure user environment. Users initiate the configuration process by registering with the RanFooler web application. After logging in, they configure their systems by providing the MAC ID for unique identification. Users can flexibly choose files for protection from ransomware attacks, review and confirm their configurations, and access a personalized control panel for system overviews and security-related alerts. In this module, Ransomware detection approaches are developed using DL algorithms like BiLSTM and GRU. Byte files and Asm files are loaded and pre-processed for feature extraction. Shallow deep learning-based feature extraction methods are employed, including word2vec, for effective model training. The attacker model focuses on downloading and installing Ransomware on victim machines using techniques like social engineering and drive-by downloads. Shellcode is fetched from distribution sites, and obfuscated ransomware code is used to exploit vulnerabilities



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1204060 |

IX. CONCULSION AND FUTURE WORK

In conclusion, the proactive defensive strategy against ransomware threats, incorporating RanGAN and Hash Conceal, stands as a groundbreaking solution in the realm of cybersecurity. This innovative approach not only effectively tackles current ransomware challenges but also lays a robust foundation for adaptive defense against future threats. The amalgamation of RanGAN's generative capabilities and Hash Conceal's cryptographic file concealment creates a multi-layered defense mechanism, disrupting ransomware operations at multiple levels. This strategy's adaptability to the evolving tactics of ransomware, combined with user-friendly interfaces and real-time monitoring, positions it as a dynamic and forward-thinking security solution. Moreover, the inclusion of a user configuration interface empowers end-users to customize the system according to their specific needs, fostering a collaborative approach to ransomware defense. In terms of industry impact, this proactive defense strategy not only safeguards individual users and organizations but also sets a precedent for a proactive and collaborative approach in the broader landscape of cybersecurity. Continuous improvement loops, user education initiatives, and cross-platform compatibility are pivotal elements for maintaining the strategy's relevance and resilience in the face of evolving threats. As a call to action, embracing and advancing such proactive strategies becomes imperative.Looking ahead, the proactive defensive strategy against ransomware, incorporating RanGAN and Hash Conceal, envisions key enhancements for heightened resilience. To future-proof against quantum threats, the integration of quantum-resistant cryptography is paramount, ensuring the enduring security of data. Additionally, the adoption of blockchain for decentralized file tracking aims to establish an immutable ledger, enhancing traceability and file integrity across the system. These strategic advancements collectively fortify the system's adaptability to emerging threats, positioning it as a robust defense against the
evolving challenges presented by ransomware.

REFERENCES

1.Python Crash Course" by Eric Matthes: A beginner-friendly guide covering fundamental Python programming with hands-on projects.

2."Flask Web Development" by Miguel Grinberg: Comprehensive guide for building web applications using Flask, covering basics to advanced topics.

3."Python for Data Analysis" by Wes McKinney: Essential resource for learning data manipulation and analysis using Pandas.

4."Introduction to Machine Learning with Python" by Andreas C. Müller, Sarah Guido: Practical introduction to machine learning with hands-on examples using Scikit-learn.

5."Python Plotting with Matplotlib" by Benjamin Root: A guide to creating visualizations using Matplotlib, covering basics to advanced plotting techniques.

6."Learning PHP, MySQL & JavaScript" by Robin Nixon: Integrates PHP, MySQL, and JavaScript for web development using Wampserver.

7."Bootstrap 4 Quick Start" by Jacob Lett: Quick and practical guide for learning Bootstrap 4 to build responsive web applications.

8."Flask Web Development with Python Tutorial" by Lewis Clarke: Practical Flask web development guide suitable for beginners.

9."Learning MySQL" by Robin Nixon: Comprehensive guide covering MySQL from installation to advanced query optimization.

"10.Django for Beginners" by William S. Vincent: A guide to Django for Python web development beginners, though not explicitly covering Flask.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details