IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 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 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205049 |

Conceal Me: Proactive Defensive Strategy Against Ransomware Threads Using RAN GAN And Hash Conceal

K. Dinesh[1], B. Kamalesh[2], P. Pravinraj[3], S. Elamathi[4]

UG Student, Dept. of CSE., Sir Issac Newton College of Engg. & Technology, Nagapattinam, Tamil Nadu, India[1-3]

Assistant Professor, Dept. of CSE., Sir Issac Newton College of Engg. & Technology, Nagapattinam, Tamil Nadu, India[4]

ABSTRACT: Ransomware is a type of malware that locks a victim's data or device and threatens to keep it locked or worse unless the victim pays a ransom 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 analyzing 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. This project developed a proactive defense strategy against ransomware threats, leveraging Ran GAN for early detection and Hash Conceal for data protection. RanGAN (Ransomware Generative Adversarial Network) employs advanced machine learning techniques to detect ransomware behavior patterns in real-time, while Hash Conceal secures critical data from malicious encryption. Together, these technologies form a robust defense, 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. This proactive approach not only bolsters an organizations resilience to ransomware but also reduces the potential impact on critical data and operations. By leveraging RanGAN for early threat detection and Hash Conceal for data protection, organizations can enhance there be security posture and safeguard against the evolving ransomware threat landscape.

KEYWORDS: Ransomware, security, RAN, GAN, Hash, Defence

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.

II. RELATED WORK

"**Python Crash Course:A Hands-on, Project-based Introduction to Programming**": Eric Matthes.
Year: 2016

Python Crash Course is a fast-paced, thorough introduction to programming with Python that will have you writing programs, solving problems, and making things that work in no time. In the first half of the book, you'll learn about basic programming concepts, such as lists, dictionaries, classes, and loops, and practice writing clean and readable code with exercises for each topic. You'll also learn how to make your programs interactive and how to test your code safely before adding it to a project. In the second half of the book, you'll put your new knowledge into practice with three substantial projects: a Space Invaders-inspired arcade game, data visualizations with Python's super-handy libraries, and a simple web app you can deploy online.

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

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205049 |

III. EXISTING SYSTEM

A. *Existing System:*

In the existing system for ransomware detection and prevention, various traditional methods and machine learning algorithms have been employed to safeguard systems and data. These methods often fall into two categories: signature-based and behaviour-based approaches. Here's 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 in real-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. However, it is pront to generating false positives, which can lead to operational disruptions and alert fatigue.

B. *Disadvantages*

- Limited coverage due to reliance on known signatures.
- High false positive rates in behaviour-based detection.
- Resource-intensive algorithms limit scalability.
- Difficulty in adapting to rapidly evolving ransomware tactics.
- Privacy concerns when analysing user data.
- Complex implementation and management.
- Dependency on historical data for training.
- Lack of active user involvement in prevention.

IV. PROPOSED SYSTEM

A. Proposed System

The proposed system for a proactive defensive strategy against ransomware threats using RanGAN (Ransomware Generative Adversarial Network) and Hash Conceal combines cutting-edge technologies to offer a robust defense against ransomware attacks. Here's an overview of the proposed system. 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 employs dynamic analysis techniques to monitor file and process behaviors in real-time. It continuously assesses whether any deviations from normal behavior patterns are indicative of ransomware activities. This dynamic approach allows for the proactive identification of emerging ransomware threats, reducing the risk of zero-day attacks.

B. Advantages

- Early threat identification, reducing potential damage.
- Minimized false positives for efficient alerts.
- Enhanced data protection and privacy.
- Comprehensive defence strategy against various attack vectors.
- Rigorous testing for reliable threat detection.
- Scalable and easily integrated into existing systems.

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

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205049 |

V. DATA FLOW DIAGRAM

DFD LEVEL 0

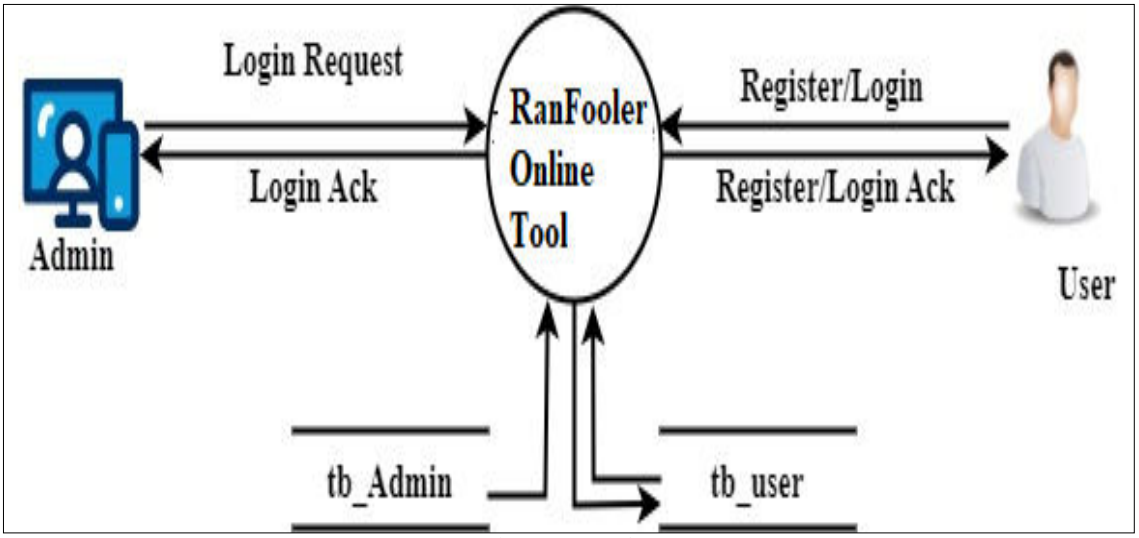

Fig1: DFD Level 0

DFD LEVEL 1

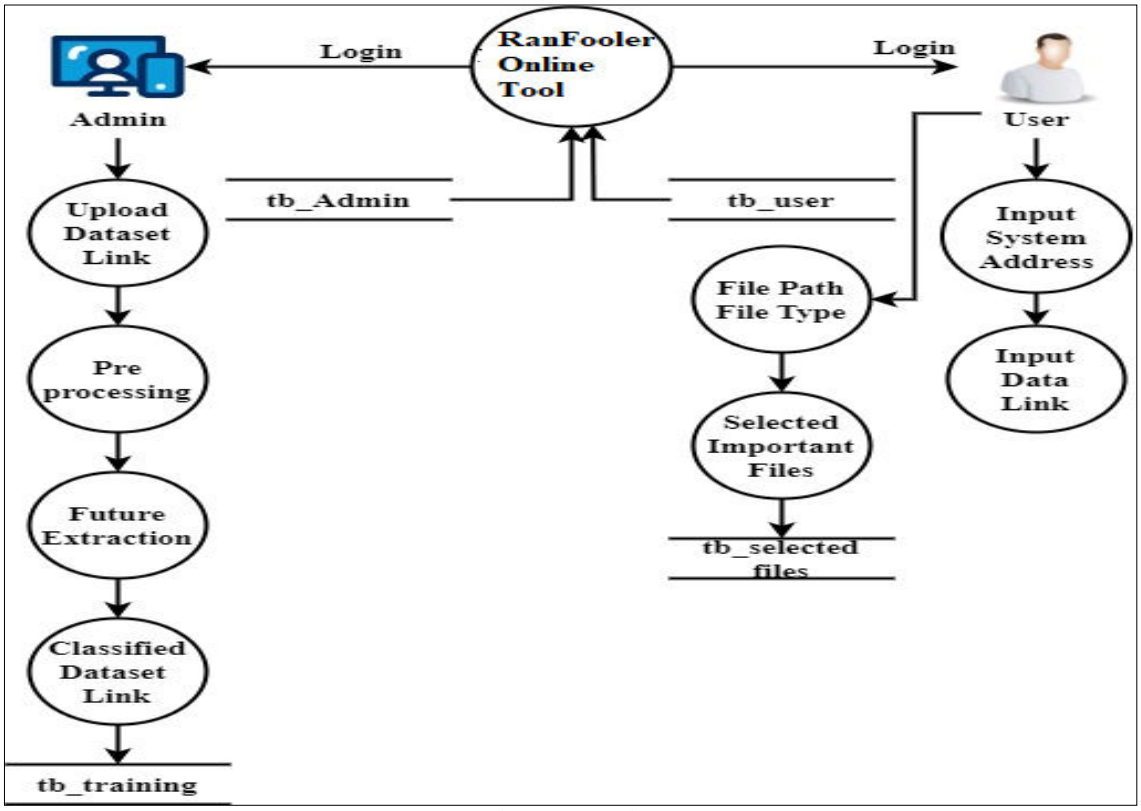

Fig2: DFD Level 1

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

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205049 |

DFD Level -2

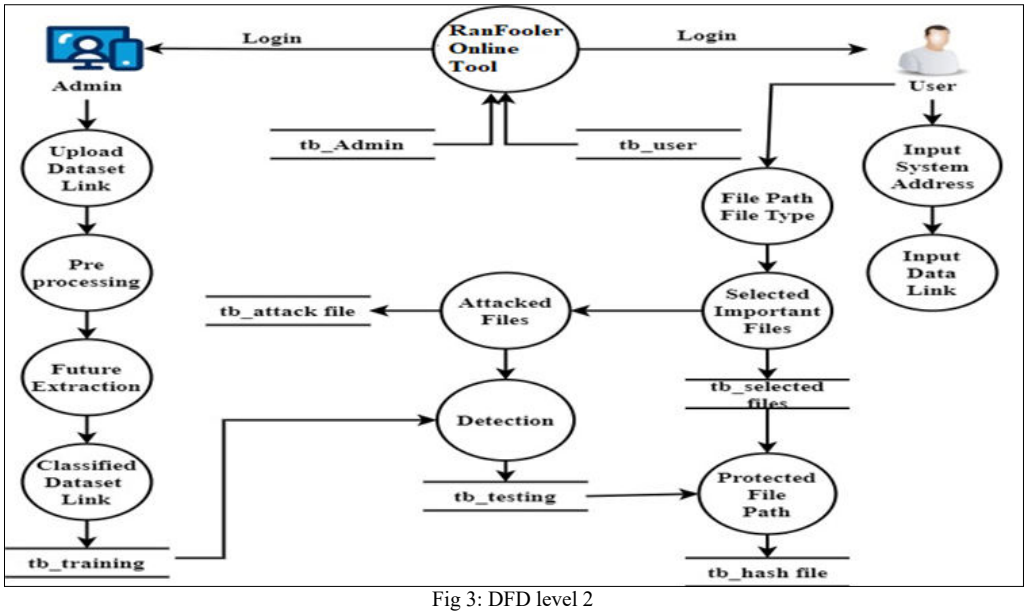

Fig 3: DFD level 2

VI. ALGORITHM

DECISION TREE

A decision tree is non paramatical problematic algorithm. It has a hierarchical, tree structure, which consists of a root node, branches, internal nodes and leaf nodes.

Algorithm 1: RanGAN algorithm

```
def create_generator():
def create_dicriminator():
def binary_cross_entropy_loss(predictions, targets):
def train_gan(generator, discriminator,data_loader, num_epochs, learning_rate):
Generator_optimizer = Adam(generator.parameters(), lr=learning_rate)
discriminator_optimizer = Adam(discriminator.parameters(), lr =learning_rate)
for epoch in range(num_epochs):
for real_data in data loader:
Real_labels = torch.ones(real_data.size(0),1)
fake_lables = torch.zero(real_data.size(0),
real_outputs = discriminator(real_data)
real_loss = binary_cross_entropy_loss(real_outputs, real_labels)
fake_data = generator(generate_noise(real_data.size(0)))
fake_outputs = discriminator(fake_data.detach())
fake_loss = binary_cross_entropy_loss(fake_outputs,fake_labels)
discriminator_loss = real_loss + fake_loss
discriminator_optimizer.zero_grad()
discrcrimmminator_loss.backward()
discriminator_optimizer.step()
updated_fake_outputs = discriminator(fake_data)
generator_loss = binary_cross_entropy_loss(updated_fake_outputs, real_label
generator_optimizer.zero_grad()
generator_loss.backward()
geenerator_optimizer.step()
def generate_noise(batch_size):
return torch.randn(batch_size, latent_dim)
```

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

|| Volume 12, Issue 5, May 2024 ||

| DOI: 10.15680/IJIRCCE.2023.1205049 |

VII. CONCLUSION AND FUTURE WORK

The 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. As we look ahead, the envisioned enhancements, such as advanced threat intelligence integration and blockchain-based file tracking, promise to further elevate the strategy's efficacy.

REFERENCES

1. D. E. García, N. DeCastro-García and A. L. M. Castañeda, "An effectiveness analysis of transfer learning for the concept drift problem in malware detection", Expert Syst. Appl.,vol. 212, Feb.2023.
2. G. O. Ganfure, C.-F. Wu, Y.-H. Chang and W.-K. Shih, "RTrap: Trapping and containing ransomware with machine learning", IEEE Trans. Inf. Forensics Security, vol. 18, pp. 1433-1448,2023.
3. J. Singh, K. Sharma, M. Wazid and A. K. Das, "SINN-RD: Spline interpolation-envisioned neural network-based ransomware detection scheme", Comput. Electr. Eng., vol. 106, Mar. 2023.
4. D. Hitaj, G. Pagnotta, F. De Gaspari, L. De Carli and L. V. Mancini, "Minerva: A file-based ansomware detector", arXiv:2301.11050, 2023.
5. F. De Gaspari, D. Hitaj, G. Pagnotta, L. De Carli and L. V. Mancini, "Evading behavioral classifiers: A comprehensive analysis on evading ransomware detection techniques", Neural Comput. Appl., vol. 34, no. 14, pp. 12077-12096, Jul. 2022.

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