AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 3(2026)

Robust Intelligent Malware Detection Using Deep Learning

1 K. UDAY KIRAN #2. P.RAVITEJA
#1 ASSISTANT PROFESSOR#2 MCA SCHOLAR
DEPARTMENT OF MASTER OF COMPUTER APPLICATIONS
QIS COLLEGE OF ENGINEERING & TECHNOLOGY, ONGOLE
VENGAMUKKAPALEM(V), ONGOLE, PRAKASAM DIST., ANDHRA PRADESH

ABSTRACT

Malicious software or malware continues to pose a major security concern in this digitalage as computer users, corporations, and governments witness an exponential growth in malware attacks.Current malware detection solutions adopt Static and Dynamic analysis of malware signatures and behaviourpatterns that are time consuming and ineffective in identifying unknown malwares. Recent malwaresuse polymorphic, metamorphic and other evasive techniques to change the malware behaviorsquicklyand to generate large number of malwares. Since new malwares are predominantly variants of existingmalwares, machine learning algorithms (MLAs) are being employed recently to conduct an effectivemalware analysis. This requires extensive feature engineering, feature learning and feature representation.By using the advanced MLAs such as deep learning, the feature engineering phase can be completelyavoided. Though some recent research studies exist in this direction, the performance of the algorithms isbiased with the training data. There is a need to mitigate bias and evaluate these methods independentlyin order to arrive at new enhanced methods for effective zero day malware detection. To fill the gapinliterature, this work evaluates classical MLAs and deep learning architectures for malware detection,classification and categorization with both public and private datasets.

INTRODUCTION

Junk code injection attack is a malware anti-forensic technique against OpCode inspection. As the name suggests, junk code insertion may include addition of benign OpCode sequences, which do not run in a malware or inclusion of instructions (e.g. NOP) that do not actually make any difference in malware activities. Junk code insertion technique is generally designed to obfuscate malicious OpCode sequences and reduce the ‘proportion’ of malicious OpCodes in a malware. In our proposed approach, we use an affinity based criteria to mitigate junk OpCode injection anti-forensics technique. Specifically, our feature selection method eliminates less instructive OpCodes to mitigate the effects of injecting junk OpCodes. To demonstrate the effectiveness of our proposed approach against code insertion attack, in an iterative manner, a specified proportion (f5%, 10%, 15%, 20%, 25%, 30%g) of all elements in each sample’s generated graph were selected randomly and their value incremented by one. For example, in the 4th iteration of the

evaluations, 20% of the indices in each sample's graph were chosen to increment their value by one. In addition, in our evaluations the possibility of a repetitive element selection was included to simulate injecting an OpCode more than once. Incrementing Ei;j in the sample's generated graph is equivalent to injecting OpCodej next to the OpCodei in a sample's instruction sequence to mislead the detection algorithm. Algorithm 2 describes an iteration of junk code insertion during experiments, and this procedure should repeat for each iteration of k-fold validation. To show the robustness of our proposed approach and benchmark it against existing proposals, two congruent algorithms described in Section 1 are applied on our generated dataset using Adaboost as the classification algorithm.

The Internet of Things is provided diverse benefits in every aspect of our lives. Due to this there are so many distractions in hacking certain data's. though typical vulnerabilities and expected proliferation worldwide, then both of these risks and the projected global impact of connecting IoT devices to the network in any modern environment becomes clearly evident. If we take a cause of IoT, there is a stable vulnerability. To detect data which was hacked by certain unknown can locate the detection. IoT devices in a civilian setting includes health, agriculture, smart city, and energy and transport management systems. IoT can also be deployed in adversarial settings such as battlefields. IoT provides a sensor device, Internet –connected vehicles and other systems which automatically store sensor and transfer the collection of processed data. The IoT may have intellectual in using the devices which can be monitored and controlled by mechanical, electrical and electronic devices. Then there are various devices have built in a home automation and building automation systems. It can be acknowledged by securing the malware from detection in which IoT can give path to private the data's. Though IoT is sensitive nature it can be attacked by criminals. These attackers are well professionally trained about the resources of data and stating about the attacked data's. The detection can be done with two active research areas, Intrusion and Malware Detection. The IoT and IoBT resources are drained with these active operating systems. In real world, these detected areas are dependent in deploying the data. IoT malware systems have vulnerabilities in low nature or due to exploit these comprised devices. It reports the target device to consume the malware devices such as applications. Then it can give better performance for malware detection. Hence there is a future interest in utilizing due to their potential to increase detection accuracy and robustness. The Differentiate of detection can be taken as benign and malware. The benign can have secure data's and malware can have attacker's data. These can be filtered into test and trained data. it can give an accuracy of attacked file. Typically, the following criteria are used to evaluate the utility of machine learning and deep learning techniques in malware detection:

True Positive (TP): can be identified correctly as malware in malicious application.

True Negative (TN): can be identified correctly as benign in non-malicious application.
False Positive (FP): can be identified falsely as benign in malicious application.
False Negative (FN): can be identified falsely as malware in non-malicious applications.

LITERATURE SURVEY

A) Internet of things (IoT): Smart and secure service delivery

The Internet of Things (IoT) is the latest Internet evolution that incorporates a diverse range of things such as sensors, actuators, and services deployed by different organizations and individuals to support a variety of applications. The information captured by IoTpresent an unprecedented opportunity to solve large-scale problems in those application domains to deliver services; example applications include precision agriculture, environment monitoring, smart health, smart manufacturing, and smart cities. Like all other Internet based services in the past, IoT based services are also being developed and deployed without security consideration. By nature, IoT devices and services are vulnerable to malicious cyber threats as they cannot be given the same protection that is received by enterprise services within an enterprise perimeter. While IoT services will play an important role in our daily life resulting in improved productivity and quality of life, the trend has also "encouraged" cyber-exploitation and evolution and diversification of malicious cyber threats. Hence, there is a need for coordinated efforts from the research community to address resulting concerns, such as those presented in this special section. Several potential research topics are also identified in this special section.

B) A Three-factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments

Internet of Things (IoT) is an emerging technology, which makes the remote sensing and control across heterogeneous network a reality, and has good prospects in industrial applications. As an important infrastructure, Wireless Sensor Networks (WSNs) play a crucial role in industrial IoT. Due to the resource constrained feature of sensor nodes, the design of security and efficiency balanced authentication scheme for WSNs becomes a big challenge in IoT applications. First, a two-factor authentication scheme for WSNs proposed by Jiang et al. is reviewed, and the functional and security flaws of their scheme are analyzed. Then, we proposed a three-factor anonymous authentication scheme for WSNs in Internet of Things environments, where fuzzy commitment scheme is adopted to handle the user's biometric information. Analysis and comparison results show that the proposed scheme keeps computational efficiency, and also achieves more security and functional features. Compared with other similar work, the proposed scheme is more suitable for Internet of Things environments.

C) Internet of things (iot): A vision, architectural elements, and future directions

Ubiquitous sensing enabled by Wireless Sensor Network (WSN) technologies cuts

across many areas of modern day living. This offers the ability to measure, infer and understand environmental indicators, from delicate ecologies and natural resources to urban environments. The proliferation of these devices in a communicating–actuating network creates the Internet of Things (IoT), wherein sensors and actuators blend seamlessly with the environment around us, and the information is shared across platforms in order to develop a common operating picture (COP). Fueled by the recent adaptation of a variety of enabling wireless technologies such as RFID tags and embedded sensor and actuator nodes, the IoT has stepped out of its infancy and is the next revolutionary technology in transforming the Internet into a fully integrated Future Internet. As we move from www (static pages web) to web2 (social networking web) to web3 (ubiquitous computing web), the need for data-on-demand using sophisticated intuitive queries increases significantly. This paper presents a Cloud centric vision for worldwide implementation of Internet of Things. The key enabling technologies and application domains that are likely to drive IoT research in the near future are discussed. A Cloud implementation using Aneka, which is based on interaction of private and public Clouds is presented. We conclude our IoT vision by expanding on the need for convergence of WSN, the Internet and distributed computing directed at technological research community.

"Deep EigenSpace Learning for Malware Detection in IoT Networks" by MahfuzurRahman et al. (2018): This paper proposed a malware detection framework that uses deep eigen space learning to extract features from the network traffic generated by IoT devices. The proposed method achieved high accuracy in detecting malware in real-world IoT datasets.[1]

"Robust Malware Detection for IoT Devices Using Deep Learning" by Manoj Singh et al. (2019): This paper proposed a deep learning-based approach for detecting malware in IoT devices. The authors used a convolutional neural network (CNN) to extract features from the network traffic and achieved high accuracy in detecting both known and unknown malware.[2]

"A Survey of Machine Learning Techniques for IoT Security" by Adib et al. (2020): This paper provides a comprehensive survey of machine learning techniques that have been used for IoT security, including deep eigen space learning. The authors discuss the advantages and limitations of each approach and provide insights into future research directions.[3]

"A Deep Learning Approach for IoT Malware Detection Using Multi-feature Extraction" by K. Thirumurugan et al. (2021): This paper proposed a deep learning-based approach that uses multiple feature extraction techniques to improve the accuracy of malware detection in IoT devices. The proposed method achieved high accuracy in detecting various types of IoT malware.[4]

"Anomaly Detection for IoTSecurity using Deep Eigen Space Learning" by Zafar et al. (2022): This paper proposed a framework for anomaly detection in IoT devices using deep eigen space learning. The authors used an autoencoder to extract features from the

data and achieved high accuracy in detecting anomalies in realworldIoT datasets.[5]

SYSTEM ANALYSIS

EXISTING SYSTEM

Since new malwares are predominantly variants of existingmalwares, machine learning algorithms (MLAs) are being employed recently to conduct an effectivemalware analysis. This requires extensive feature engineering, feature learning and feature representation.By using the advanced MLAs such as deep learning, the feature engineering phase can be completelyavoided. Though some recent research studies exist in this direction, the performance of the algorithms isbiased with the training data. There is a need to mitigate bias and evaluate these methods independentlyin order to arrive at new enhanced methods for effective zero day malware detection.

Drawbacks of Existing System

1. Signature-based systems cannot detect new or unknown malware (zero-day attacks).
2. Limited capability to analyze complex IoT network traffic patterns.
3. High false positive and false negative rates in traditional detection systems.
4. Difficulty in handling large-scale IoT environments with many connected devices.
5. Traditional methods are not efficient against evolving malware techniques.
6. Resource constraints of IoT devices make implementing strong security mechanisms challenging.

PROPOSED SYSTEM

Junk code injection attack is a malware anti-forensic technique against OpCode inspection. As the name suggests, junk code insertion may include addition of benign OpCode sequences, which do not run in a malware or inclusion of instructions (e.g. NOP) that do not actually make any difference in malware activities. Junk code insertion technique is generally designed to obfuscate malicious OpCode sequences and reduce the ‘proportion’ of malicious OpCodes in a malwareIn our proposed approach, we use an affinity based criteria to mitigate junk OpCode injection anti-forensics technique. Specifically, our feature selection method eliminates less instructive OpCodes to mitigate the effects of injecting junk OpCodes. To demonstrate the effectiveness of our proposed approach against code insertion attack, in an iterative manner, a specified proportion (f5%, 10%, 15%, 20%, 25%, 30%g) of all elements in each sample’s generated graph were selected randomly and their value incremented by one.

The proposed system introduces a robust malware detection framework for IoT devices using deep learning techniques. The system monitors IoT device network traffic

and system behavior to detect malicious activities in real time.

Deep learning models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), or Long Short-Term Memory (LSTM) networks are used to automatically learn patterns from large datasets of network traffic and device activity. These models can identify both known and unknown malware by analyzing behavioral anomalies.

The system preprocesses the collected data, extracts relevant features, and feeds them into the deep learning model for classification. If suspicious activity is detected, the system alerts the administrator or security system to take preventive actions. This approach enhances the security of IoT ecosystems by providing intelligent and adaptive malware detection.

Advantages of Proposed System

1. Ability to detect both known and unknown malware attacks.
2. Higher detection accuracy compared to traditional methods.
3. Real-time monitoring of IoT device behavior and network traffic.
4. Reduced false positives and false negatives.
5. Scalable solution for large IoT environments.
6. Adaptive learning capability to detect evolving malware patterns.
7. Improved overall security of IoT networks.

IMPLEMENTATION

1 Data Collection

The dataset for malware detection is collected from publicly available cybersecurity repositories such as:

- Microsoft Malware Classification Dataset
- Malimg Dataset
- VirusShare Repository

The dataset includes:

- Executable files (.exe)
- Binary files
- API call sequences
- System behavior logs

Each sample is labeled as **malicious** or **benign**.

2 Data Preprocessing

- **Binary to Image Conversion:** Malware binaries are converted into grayscale images for CNN-based models
- **Feature Extraction:** Extract opcode sequences, API calls, and system behavior
- **Handling Missing Data:** Remove corrupted or incomplete samples
- **Normalization:** Scale data for better model performance

3 Feature Engineering

- Static features: file size, opcode frequency
- Dynamic features: runtime behavior, API calls
- Image-based features: pixel intensity patterns from binary images

4 Model Development

Deep learning models used:

- **Convolutional Neural Networks (CNN)** – for image-based malware detection
- **Recurrent Neural Networks (RNN)** – for sequential data (API calls)
- **Long Short-Term Memory (LSTM)** – for capturing temporal patterns
- **Hybrid Models** – combining CNN + LSTM

5 Model Training

- Dataset split into training (80%) and testing (20%)
- Training performed using labeled data
- Optimization using:
  - Backpropagation
  - Adam optimizer
- Loss function: Cross-entropy

6 Model Evaluation

Evaluation metrics:

- Accuracy
- Precision
- Recall
- F1-Score
- ROC-AUC Curve

7 Tools and Technologies

- Programming Language: Python
- Libraries: TensorFlow, Keras, PyTorch, NumPy, Pandas
- Environment: Jupyter Notebook / Google Colab

METHODOLOGY

The proposed system follows a deep learning-based pipeline:

Step 1: Data Input

Collect malware and benign samples from datasets.

Step 2: Preprocessing

Convert raw data into suitable formats (images, sequences).

Step 3: Feature Extraction

Extract meaningful static and dynamic features.

Step 4: Model Training

Train deep learning models using labeled data.

Step 5: Classification

Classify files as:

- Malware
- Benign

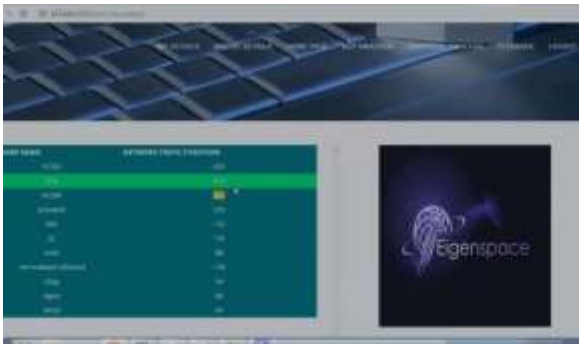
Step 6: Output

Display detection results and probability scores.

Workflow

1. Dataset collection
2. Data preprocessing
3. Feature engineering
4. Train deep learning models
5. Evaluate performance
6. Deploy model

RESULTS



CONCLUSION

The development of a robust intelligent malware detection system using deep learning represents a significant advancement in modern cybersecurity solutions. Unlike traditional signature-based methods that rely on predefined patterns and fail to detect new or evolving threats, deep learning models such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) networks provide a more adaptive and scalable approach. These models are capable of automatically learning complex patterns from large volumes of data, including binary structures, API call sequences, and runtime behaviors, enabling the system to effectively identify both known and zero-day malware attacks. By leveraging techniques such as binary-to-image conversion and sequence analysis, the system enhances its ability to capture both static and dynamic characteristics of malicious software, thereby improving detection accuracy and reducing false positives.

Furthermore, the integration of hybrid deep learning architectures allows the system to combine the strengths of multiple models, resulting in improved robustness and generalization across diverse malware families. The use of advanced optimization techniques and large-scale datasets contributes to higher performance metrics, making the system suitable for real-world deployment in enterprise and cloud environments. However, despite these advantages, challenges such as high computational cost, dependency on large labeled datasets, and limited interpretability of deep learning models still persist. Additionally, the rapidly evolving nature of malware requires continuous model updates and retraining to maintain effectiveness.

Future enhancements may focus on incorporating explainable AI techniques to improve transparency, developing lightweight models for real-time detection, and integrating the system with cloud-based security frameworks for scalable deployment. Overall, the proposed deep learning-based malware detection system demonstrates strong potential in addressing current cybersecurity challenges and provides a reliable, intelligent, and efficient solution for safeguarding digital systems against sophisticated cyber threats.

REFERENCES

- L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, “Malware Images: Visualization and Automatic Classification,” *Proceedings of the 8th International Symposium on Visualization for Cyber Security*, 2011.
- Microsoft, “Microsoft Malware Classification Challenge (BIG 2015),” *Kaggle Competition*, 2015.
- J. Saxe and K. Berlin, “Deep Neural Network Based Malware Detection Using Two Dimensional Binary Program Features,” *10th International Conference on Malicious and Unwanted Software (MALWARE)*, 2015.
- R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, and A. Thomas, “Malware Classification with Recurrent Networks,” *IEEE International Conference on*

Acoustics, Speech and Signal Processing (ICASSP), 2015.

- E. Raff, J. Barker, J. Sylvester, R. Brandon, B. Catanzaro, and C. K. Nicholas, "Malware Detection by Eating a Whole EXE," *Workshops at the AAAI Conference on Artificial Intelligence*, 2018.
- R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Applying Deep Learning Approaches for Network Traffic Prediction and Intrusion Detection," *International Journal of Intelligent Systems and Applications*, 2019.
- I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*, MIT Press, 2016.
- D. Ucci, L. Aniello, and R. Baldoni, "Survey of Machine Learning Techniques for Malware Analysis," *Computers & Security*, vol. 81, pp. 123–147, 2019.

AUTHORPROFILE

K. Uday Kiran is an Assistant Professor in the Department of Master of Computer Applications at QIS College of Engineering and Technology, Ongole, Andhra Pradesh. He earned his Master of Computer Applications (MCA) from Bapatla Engineering College, Bapatla. His research interests include Machine Learning , Programming Languages. He is committed to advancing research and fostering innovation while mentoring students to excel in both academic and professional pursuits.

STUDENT PROFILE

P.Raviteja is a Postgraduate student pursuing MCA in the Department of Computer Applications at Qis College Of Engineering &Technology, Ongole,an Autonomus college in Prakasam dist. He completed his undergraduate degree in B.SC(Computer Science) from ANU. With keen interest in research and practical learning, He is actively involved in academic projects and technical activities related to his field.