Smart and Cost-Effective System for Ransomware Identification, Detection and Prevention for IoT Enterprise Networks

Mohammed Mujeebuddin[1], Almahanad Nasser Rashid Al Kalbani[1], Raiyan Mustafa Mulla[1], Badar Saif Said Ali Al Hinai[1], Syed Imran Ali Kazmi[1#] and Muhammad Sohail Hayat[1#]

[1]Middle East College, Muscat, Oman
[#]Advisor

ABSTRACT

As there is an increase of lightweight systems such as smartphones, on the Internet of Things (IoT) paradigm, it is important to strengthen security and prevent ransomware attacks from taking place. Ransomware attacks have become a significant threat to the security of IoT networks, and their impact can be severe and costly for enterprises. Traditional security mechanisms are no longer valid because of the involvement of resource-constrained systems, which require more computation power and resources. To further enhance ransomware detection capabilities, The proposed system uses a combination of machine learning and network monitoring techniques to detect and prevent ransomware attacks in real-time. This Research Study will address the ransomware attack cybersecurity issues using a state-of-the-art solution approach and develop a smart, effective, and affordable prototype solution for identifying, detecting, and preventing ransomware attacks on IoT enterprise networks. Its combination of machine learning and network monitoring techniques offers a robust defense against the growing threat of ransomware attacks, and its cost-effectiveness makes it accessible to enterprises of all sizes. In this Research Study, we aim to demonstrate the proposed framework, design practical implementation of the system.

Introduction

The growth of the Internet of Things (IoT) has caused an abrupt shift in how businesses conduct their operations. The Internet of Things (IoT) has completely changed how we operate, from automating repetitive jobs to remotely monitoring and regulating numerous operations. These advantages do, however, come with considerable security dangers, particularly given the rising frequency of ransomware assaults. A strong system for ransomware detection and prevention must be in place since ransomware attacks may seriously harm an organization's finances and reputation. As attackers may easily modify ransomware to avoid detection, traditional signature-based detection techniques are no longer sufficient to stop ransomware attacks. To recognize ransomware assaults based on their behavior, researchers have suggested innovative techniques, such as machine learning algorithms and behavioral analysis tools. Additionally, as IoT corporate networks may contain thousands of devices, it is critical to have a cost-effective method for detecting and combating ransomware attacks. Without placing a major financial strain on the company, a cost-effective solution that makes use of already-existing infrastructure and resources, such cloud-based servers, may identify and stop ransomware assaults. This research study suggests a unique method for detecting and preventing ransomware attacks in business IoT networks by combining behavioral analysis and machine learning methods. By utilizing already-existing infrastructure and resources to identify and stop ransomware attacks in IoT corporate networks, the suggested method

seeks to be both affordable and scalable. The evaluation's findings show how well the suggested method works at identifying and stopping ransomware assaults while still having a low false-positive rate.

Similar Work

Leveraging Deep Learning Models for Ransomware Detection in the Industrial Internet of Things Environment

The paper (Al-Hawawreh & Sitnikova, 2019) suggests using "Adaptive Computation Time" (ACT), a novel method for training neural networks. Rather than employing a constant amount of computation for all inputs, ACT dynamically modifies the amount of computation carried out by a neural network for each input. This is accomplished by letting the network choose how many computations to do before generating an output. A learnt "halting probability" that is continually updated throughout training determines the number of steps. The ACT approach provides several benefits over conventional neural network training. By eliminating pointless work for simple inputs while enabling more thorough analysis of complicated inputs, it enables more effective use of computer resources. By allowing the network to concentrate on pertinent portions of the input data, it also helps the network to produce predictions that are more accurate. The ACT approach may also be used with different neural network architectures, including feedforward and recurrent networks.

IoT Malware Detection Architecture Using a Novel Channel Boosted and Squeezed CNN

The article (Asam et al., 2022) proposes a novel IoT Malware detection architecture (iMDA) that uses squeezing and boosting dilated CNN to analyze IoT malware using a new benchmark dataset. CNN uses edge-and-smoothing, multi-path dilated convolutional, channel-squeezing, and boosting operations thanks to the iMDA. In split-transform-merge (STM) blocks, the edge and smoothing techniques are used to recover local structure and slight contrast fluctuation from malware pictures. STM blocks carry out multi-path dilated convolutional operations that aid in identifying the overall malware pattern structure. For the purpose of capturing texture differences, channel squeezing and boosting are also used at various granular levels to provide reduced yet noticeable and diversified feature maps. By applying transfer learning, the proposed iMDA has significantly outperformed existing CNNs in terms of performance measures including MCC, F1-Score, AUC, accuracy, precision, and recall. The proposed iMDA's experimental setup, outcomes, and comparison with existing CNNs are also covered in this article as they relate to identifying IoT malware. In conclusion, the research suggests a unique method for identifying IoT malware utilizing an architecture based on deep learning that combines several operations to extract local and global structures of malware patterns. Comparing the suggested method to current CNNs yields encouraging results and suggests a potential tool for enhancing IoT security.

Malware Detection and Classification in IoT Network using ANN

The article (Jamal et al., & 2022) describes an artificial neural network (ANN) based method for malware detection and classification in an Internet of Things (IoT) network. The essay emphasizes how crucial it is to protect IoT devices while outlining the difficulties in doing so, including malware assaults. The authors employ ANNs with ReLU and softmax activation functions that are based on feed-forward and backpropagation architecture. The dataset was divided into train and test data in the proportions of 70% and 30% by the authors. The ANN has an input layer, three hidden

layers, and an output layer with a binary cross entropy loss function for malware detection, while it has three hidden layers, an output layer, and a categorical cross entropy loss function for malware classification. The accuracy, precision, recall, and F1 score are only a few of the performance measures the authors use to assess the suggested strategy. The outcomes demonstrate that the suggested approach performs better than traditional ML algorithms like kNN and Naive Bayes. Future research, according to the authors, might concentrate on applying the suggested technique to identify and categorize assaults on the IoT network that use sensor readings.

Efficient Detection and Classification of Internet-of-Things Malware Based on Byte Sequences from Executable Files

The article (Wan et al., 2020) proposes a method to identify and classify ransomware in Internet of Things (IoT) devices, which have grown susceptible to cyberattacks because of their constrained resources and diverse CPU architectures. Three steps make up the suggested method: gathering ELF files (dataset samples) from various sources, feature extraction and labeling for each sample, and model training and evaluation using a typical machine learning processing pipeline. An ELF file's entry point is utilized to determine whether it is malicious, and N-gram models are employed to construct a numerical feature vector from the bytes that were extracted there. To minimize memory usage during learning, the byte sequence is converted into a sparse representation. Four classification techniques, SVM, KNN, NB, and MLP, which are effective with high dimensional sparse data, are chosen to categorize the samples. While KNN classifies a sample based on the consensus of its k-nearest neighbors, SVM uses the one-against-all convention to solve a multi-class classification problem. MLP is a neural network-based classifier that use backpropagation to train the network, while NB is a probabilistic classifier based on the Bayes theorem. Benefits of the suggested approach include the ability to identify and categorize malware in IoT devices without relying on conventional signature-based approaches or on-device dynamic analysis. It uses machine learning to handle the diverse CPU architectures and constrained resources of IoT devices. The testing results reveal that the method surpasses other cutting-edge methods in terms of accuracy and F1 score, proving the method's efficacy. The suggested method can also be readily expanded to include additional samples and change with the threat environment.

Literature Review

IoT is an revolutionary paradigm that has won a lot significance withinside the previous couple of years because of the mixing of numerous technologies and communique solutions. The fundamental concept in the back of IoT is the pervasiveness of a selection of factors which include clever gadgets, sensors, actuators, and Radio-Frequency Identification (RFID) tags, etc. which have interaction and talk with every different to reap a not unusual place goal. The swiftly developing significance of IoT is due to its excessive effect on nearly normal lifestyles and the conduct of users. Below we offer a few definitions of IoT for a higher understanding for readers According to IoT is described as a global wherein physical items are included with statistics networks, those physical items worried in commercial enterprise procedures as an energetic participant. defines IoT as a self-prepared machine of self-sustaining gadgets that talk with every different to enhance commercial enterprise procedures' efficiency. defines IoT because the connectivity of items to the net the use of RFID, GPS, Sensors, laser scanner or some other statistics sensing tool with a purpose to comprehend identification, monitoring, monitoring and control of items. defines IoT because the capacity of interconnected sensing and actuating gadgets to share statistics throughout numerous platforms. All the above definitions gift the equal concept of IoT as shown in Fig , that IoT affords the interconnection among physical items the use of the net and it's miles a swiftly developing phenomenon this is definitely affecting each discipline of life.

However, this fast boom of IoT has to stand one-of-a-kind challenges, and from these, one such task is that of Ransomware assaults. As mentioned above Ransomware is a kind of malware assault that targets a sufferer's laptop facts and encrypts or locks these facts. The sufferer then wishes to pay the demanded ransom in order to retrieve or get admission to his data. With the boom of IoT, a Ransomware assault is likewise developing rapidly. According to a document via way of means of Symantec, Ransomware assaults extended via way of means of 113% in 2014 and crypto Ransomware extended as much as 4000%. Another document presented via way of means of Kaspersky suggests a 5-time growth in Ransomware assaults among 2012 and 2015. This fast boom of Ransom is now no longer most effective restricted to individuals, instead it's far now focused on organizations as well. Types of Ransomware there are major varieties of Ransomware, Crypto Ransomware and locked Ransomware. Both these Ransomware typically begins off evolved with an electronic mail attachment or an internet link, while the sufferer opens the attachment or the acquired weblink the Ransom assaults the sufferer's laptop via way of means of taking advantage of existing running machine flaws. Fig. suggests us the taxonomy of the Ransomware assaults. In the case of crypto Ransomware, Once Ransomware becomes active, it encrypts a few crucial consumer documents. In this case, Ransomware do now no longer assault the entire tough disk of the sufferer instead it chooses a few crucial documents primarily based totally on report extensions. This assault typically makes use of a 24-bit encryption.

Design

This Project explores and profoundly analyzes the various models to get maximum accuracy results

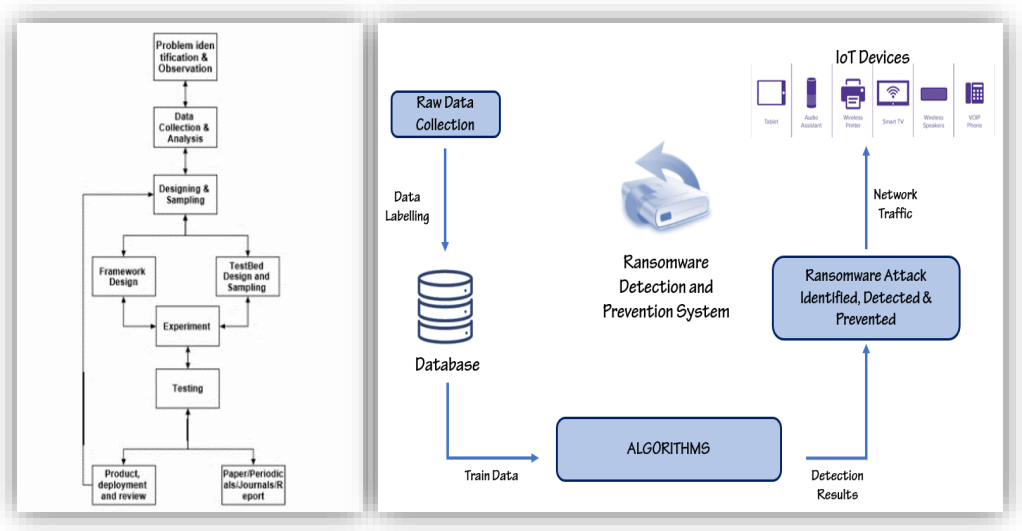

Figure 1. Ransomware Detection and Prevention System

Findings and Future Work

Ransomware attacks have become increasingly common in recent years, and IoT enterprise networks are particularly vulnerable to these types of attacks. To prevent such attacks, it is important to have a smart and cost-effective system for ransomware identification, detection, and prevention.

One potential solution is to use machine learning algorithms to analyze network traffic and identify patterns associated with ransomware attacks. This could involve using supervised learning techniques to train a model on

historical data to identify ransomware attacks, or unsupervised learning techniques to identify anomalous behavior in the network.

Another approach is to use honeypots or decoy devices to attract ransomware attacks and study their behavior. This could provide valuable insights into the tactics and techniques used by attackers, which could inform future prevention and mitigation strategies.

In terms of prevention, it is important to have a robust backup and recovery system in place to minimize the impact of any successful ransomware attacks. Additionally, implementing strong access controls and regularly updating software and firmware can help prevent attacks from exploiting known vulnerabilities.

For future work, researchers could explore the use of blockchain technology to create a decentralized and more secure IoT network. This could involve using blockchain-based smart contracts to enforce access control and ensure the integrity of network communications.

Furthermore, researchers could investigate the potential for using artificial intelligence and machine learning to improve the detection and prevention of ransomware attacks. This could involve developing more sophisticated algorithms that are better able to identify and respond to emerging threats in real-time.

Conclusion

Based on the comments received from the proposal defense and our research assessment result, we have narrowed down our approach to get a maximum result.

- Besides, using more datasets, hyperparameters, and a grid search helped us to find the best parameters associated with the model.
- Based on the new AI/ML models we are better to better to classify and detect IoT-based ransomware attacks in a cloud computing environment.
- Moreover, we find out a solution that ensures the detection of a ransomware attack on IoT devices deployed on a cloud computing environment to secure data.
- Finally, in this research, we examined various models, and algorithms, security analyses to classify and detect IoT-based ransomware attacks on a cloud computing environment.

References

Kothari, C. R. (2019). Research methodology: Method and techniques. Oest, A., Safaei, Y., Doupé, A., Ahn, G.-J., Wardman, B., & Tyers, K. (2019). *Phishfarm: A scalable framework for measuring the effectiveness of evasion techniques against browser phishing blacklists*. Paper presented at the 2019 IEEE Symposium on Security and Privacy (SP).

Yaqoob, I., Ahmed, E., Rehman, M., Ahmed, A., Al-garadi, M., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging security challenges in the Internet of Things. Computer Networks, 129, 444-458. https://www.sciencedirect.com/science/article/abs/pii/S1389128617303468.

Brinson, N. H., Eastin, M. S., & Cicchirillo, V. J. J. J. o. I.A. (2018). Reactance to personalization: Understanding the drivers behind the growth of ad blocking. 18(2), 136-147.

Carmi, E. J. I. R. o. L., Computers, & Technology. (2017). Regulating behaviours on the European Union internet, the case of spam versus cookies. 31(3), 289-307.

Al-Hawawreh, M., & Sitnikova, E. (2019). Leveraging Deep Learning Models for Ransomware Detection in the Industrial Internet of Things Environment. In 2019 Military Communications and Information Systems Conference (MilCIS) (pp. 1-6). Canberra, ACT, Australia. IEEE. doi: https://doi.org/10.1109/MilCIS.2019.8930732. https://ieeexplore-ieee-org.masader.idm.oclc.org/stamp/stamp.jsp?tp=&arnumber=8930732

Asam, M., Khan, S.H., Akbar, A., Ahmed, E., & Hussain, S. (2022). IoT malware detection architecture using a novel channel boosted and squeezed CNN. Scientific Reports, 12, 15498. https://doi.org/10.1038/s41598-022-18936-9
https://www.nature.com/articles/s41598-022-18936-9#Sec3
Jamal, A., Hayat, M. F., & Nasir, M. (2022). Malware Detection and Classification in IoT Network using ANN. Mehran University Research Journal of Engineering and Technology, 41(1), 80+. https://link.gale.com/apps/doc/A689976395/AONE?u=googlescholar&sid=googleScholar&xid=b9641827
Wan, T.-L., Ban, T., Cheng, S.-M., Lee, Y.-T., Sun, B., Isawa, R., Takahashi, T., & Inoue, D. (2020). Efficient Detection and Classification of Internet-of-Things Malware Based on Byte Sequences from Executable Files. IEEE Open Journal of the Computer Society, 1, 262-275. https://doi.org/10.1109/OJCS.2020.3033974.
https://ieeexplore-ieee-org.masader.idm.oclc.org/document/9240051