The Deep Intru-Net for anomaly detection in massive IoT networks

Abstract

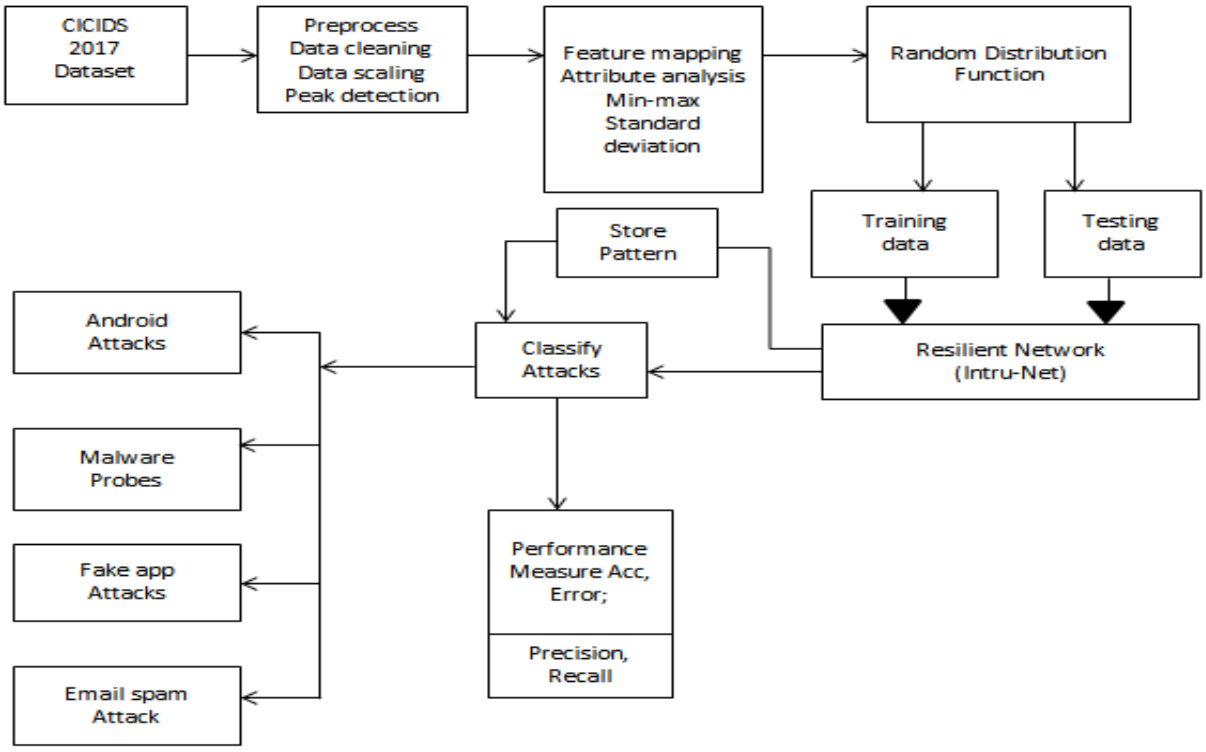
The massive development of the internet of things enabled various applications in smart devices, mobiles, laptops, and equipment that are configured with the common internet to provide flexible access. numerous users benefited by the reliability of the internet as a common medium. on the similar scope of work, the intrusion attacks threaten the system security. The data stored in the cloud needs to be protected from network anomalies. The presented system is focused on development of novel deep learning architecture with tuned layers for better performance. The presented system considers the CICIDS2017 dataset. The system considers the CICIDS dataset as the reference information and creates an architecture using Deep Intru-Net to test. The dataset is divided into training data of 80% and testing data of 20%. The dataset holds the recorded patterns of network anomalies. The Deep Intru-Net learns the frequent pattern of anomaly in the network and detects the occurrence of similar patterns. The improved iterations increase the learning strength of the system. The performance evaluation is made using accuracy value estimation and the proposed network achieved 98% accuracy.

INTRODUCTION

Smart devices, including smartphones, smartwatches, and other Internet of Things (IoT) devices, have become an essential part of our daily lives. These devices generate and store vast amounts of personal and sensitive data, making them an attractive target for cyber-attacks. Traditional security measures, such as firewalls and intrusion detection systems (IDS), are not always effective in detecting and preventing these attacks. Therefore, there is a growing need for more advanced security measures that can detect and prevent cyber-attacks on smart devices.

Deep Intrusion Detection System (IDS) is a promising security measure that can detect and prevent cyber-attacks on smart devices. Deep IDS is a type of IDS that uses machine learning algorithms, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, to analyze network traffic and system activity data to identify patterns that indicate potential security threats. The system is designed to extract various features, such as statistical and behavioral

features, from the raw data to identify patterns that indicate potential security threats.



PROPOSED SYSTEM

The Deep Intru-Net is an AI-based system that uses deep learning algorithms to detect anomalies in massive IoT networks. The system is designed to work with large-scale networks that may have millions of connected devices generating massive amounts of data.

The system has three main components:

Data Preprocessing: The raw data generated by IoT devices is preprocessed to remove any noise or errors. The preprocessing step may include data cleaning, filtering, and normalization.

Feature Extraction: The preprocessed data is then transformed into features that can be used by the deep learning algorithms. The feature extraction step may include statistical analysis, signal processing, and other techniques to extract relevant features from the data.

Deep Neural Network: The system uses a deep neural network to learn the normal behavior patterns of the IoT network. The deep neural network is trained using the features extracted from the preprocessed data. Once trained, the neural network can identify any deviations from the learned patterns and flag them as anomalous behavior.

ADVANTAGES

Real-time detection: The system can process data in real-time, allowing for early detection of potential security threats or system failures.

Scalability: The system is designed to work with large-scale IoT networks and can handle massive amounts of data.

Accuracy: The system uses deep learning algorithms, which have been shown to be highly accurate in detecting anomalies in complex data.

EXISTING SYSTEM

Autoencoder is a type of unsupervised learning algorithm that is designed to learn a compressed representation of input data. It consists of two parts: an encoder and a decoder.

The encoder compresses the input data into a lower-dimensional representation, and the decoder reconstructs the data from this compressed representation.

During training, the autoencoder is trained to minimize the reconstruction error between the input data and the reconstructed data.

Anomalies can be detected using the reconstruction error: if the reconstruction error for a particular data point is higher than a predefined threshold, it is flagged as an anomaly.

DISADVANTAGES

Autoencoder requires a large amount of data to train effectively. If the dataset is small or unrepresentative of the true distribution of data, the autoencoder may not be able to learn accurate representations of normal behavior.

Autoencoder may struggle with detecting anomalies that are dissimilar to any of the normal behavior patterns it has learned. If the network experiences a novel type of attack, the autoencoder may not be able to detect it.

Autoencoder can be computationally expensive, especially if the input data has a high dimensionality. This can make it difficult to use in real-time applications.

CONCLUSION

The widespread growth of the internet of things made it possible for a variety of apps to be installed in smart devices, mobile devices, laptops, and other pieces of equipment that are set to allow flexible access to the internet. There have been a lot of people who have benefitted from the dependability of the internet as a common medium. On the same scale of operations, the intrusion assaults pose a danger to the system's level of security. The data that is kept in the cloud has to have some kind of defense against network irregularities. The primary emphasis of the system that is now being presented is the construction of a revolutionary deep learning architecture that features layers that have been optimized to improve performance. The CICIDS2017 dataset is taken into account by the system that is provided. The CICIDS dataset is taken into account by the system as the reference information, and Deep Intru-Net is used to do testing on the architecture that is developed. The dataset is split into training data comprising 80% of the total and testing data making up the remaining 20%. The documented patterns of network irregularities are included in the dataset. The Deep Intru-Net is able to understand the common pattern of anomaly that occurs in the network and recognize when other patterns with the same characteristics arise. The capacity of the system to learn is increased as a result of the better iterations. The accuracy value estimate is what's used to do the performance assessment, and that showed that the suggested network was accurate 98% of the time.