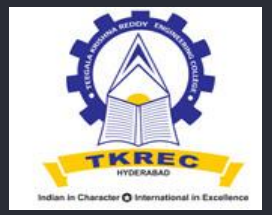


TEEGALA KRISHNA REDDY ENGINEERING COLLEGE

Department of Computer Science & Engineering

HEAD OF THE DEPARTMENT
Dr. CH.V.PHANI KRISHINA
Professor

PROJECT COORDINATORS
Dr. J. RAJARAM
Professor
Dr. VADIVALAN NATARAJAN
Professor

CYBER THREAT DETECTION BASED ON ARTIFICIAL NEURAL NETWORKS USING EVENT PROFILES

INTERNAL GUIDE

DR K BHARGAVI

Professor

TEAM MEMBERS

Manasa Deshpande : 18C21A0557

B. Sai Vaishnavi : 17UR1A0504

G. Akshitha : 18R91A05J6

V. Priyanka : 19R95A0527

OBJECTIVES

1. ABSTRACT
2. EXISTING SYSTEM
3. PROPOSED SYSTEM
4. HARDWARE & SOFTWARE REQUIREMENTS
5. SYSTEM ARCHITECTURE
6. FUNCTIONAL REQUIREMENTS

ABSTRACT

One of the major challenges in cybersecurity is the provision of an automated and effective cyber-threats detection technique. In this paper, we present an AI technique for cyber-threats detection, based on artificial neural networks. The proposed technique converts multitude of collected security events to individual event profiles and use a deep learning-based detection method for enhanced cyber-threat detection. For this work, we developed an AI-SIEM system based on a combination of event profiling for data preprocessing and different artificial neural network methods, including FCNN, CNN, and LSTM. The system focuses on discriminating between true positive and false positive alerts, thus helping security analysts to rapidly respond to cyber threats.Consequently, the experimental results of this study ensure that our proposed methods are capable of being employed as learning-based models for network intrusion-detection, and show that although it is employed in the real world, the performance outperforms the conventional machine-learning methods.

EXISTING SYSTEM

- First, learning-based detection methods require labeled data, which enable the training of the model and evaluation of generated learning models. Furthermore, it is not straightforward to obtain such labeled data at a scale that allow accurate training of a model.

- Second, most of the learning features that are theoretically used in each study are not generalized features in the real world, because they are not contained in common network security systems. Hence, it makes difficult to utilize to practical cases.

- Third, using an anomaly-based method to detect network intrusion can help detect unknown cyber threats; whereas it can also cause a high false alert rate Triggering many false positive alerts is extremely costly and requires a substantially large amount of effort from personnel to investigate them.

- Fourth, some hackers can deliberately cover their malicious activities by slowly changing their behavior patterns. Even when appropriate learning- 7 based models are possible. attackers constantly change their behaviors, making the detection models unsuitable.

LIMITATIONS OF EXISTING SYSTEM

 It works on covering attacks related exclusively to intrusion detection, malware analysis, and spam detection, and do not cover malicious domain names commonly used by botnets.

 The majority of IPS solutions have a high false positive rate and are limited in detecting any unknown or new attacks.

 Limitations for an IPS such as the challenges of volume, accuracy, low-frequency attacks.

 The SIEM analysts spend an immense amount of effort and time to differentiate between true security alerts and false security alerts in collected events.

PROPOSED SYSTEM

We present an AI-SIEM system which can discriminate between true alerts and false alerts based on deep learning techniques. Our proposed system can help security analysts rapidly to respond cyber threats.

The main contributions of our work can be summarized as follows:

- Our proposed system aims at converting a large amount of security events to individual event profiles for processing very large-scale data. We developed a generalizable security event analysis method by learning normal and threat patterns from a large amount of collected data, considering the frequency of their occurrence.

- Our event profiling method for applying artificial intelligence techniques, unlike typical sequence-based pattern approaches, provides featured input data to employ various deep learning techniques.

- For the applicability, we evaluate our system with real IPS security events from a real security operations center (SOC) and validate its effectiveness through performance metrics, such as the accuracy, true positive rate (TPR), false positive rate (FPR) and the F-measure.

SOFTWARE REQUIREMENTS

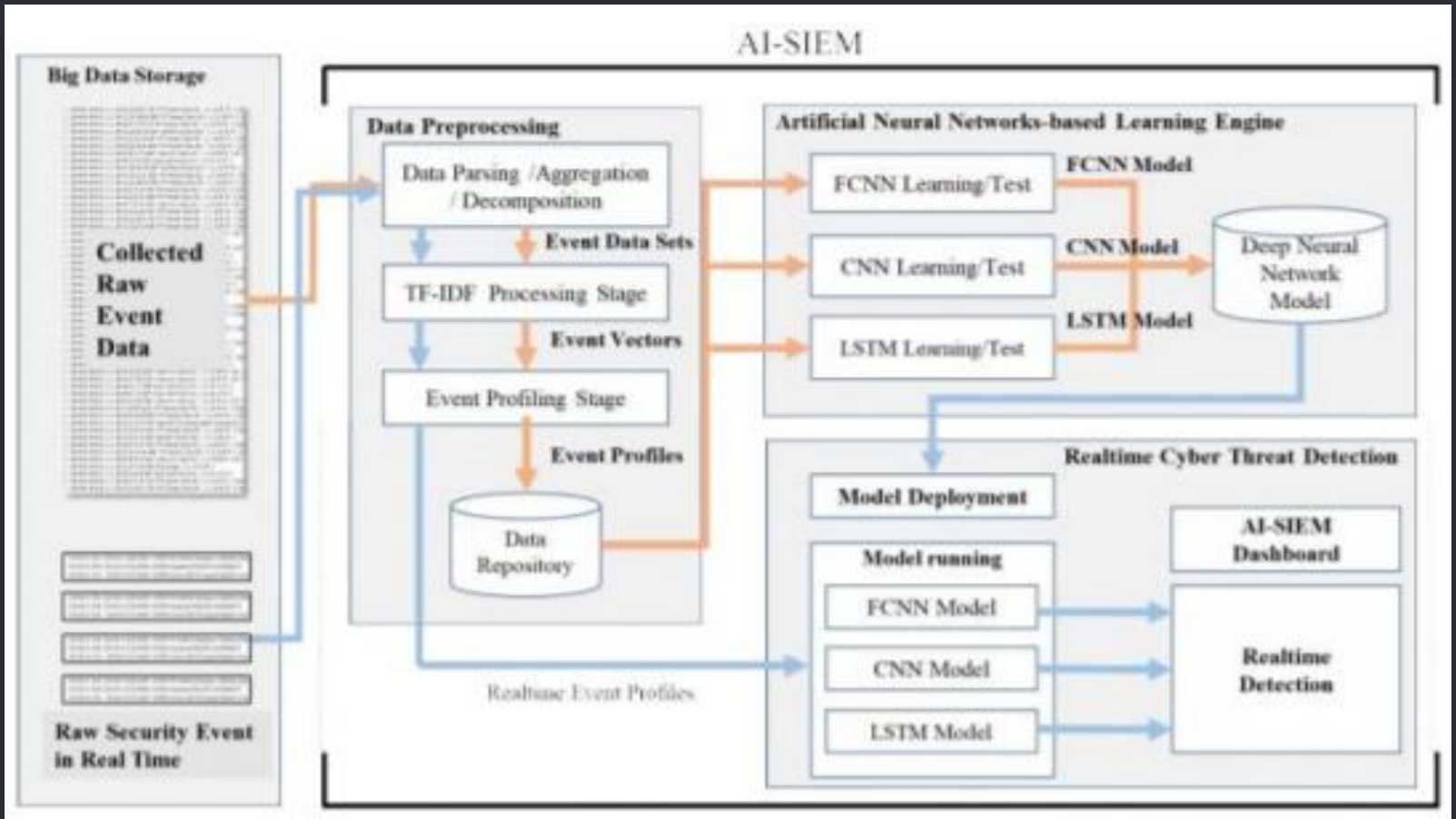
SOFTWARE REQUREMENTS

- Operating System : Windows XP/7 to 10
- Front End : Python Tkinter
- Database Connectivity : MySQL.

HARDWARE REQUIREMENTS

- Processor : Intel dual core
- Ram : 4GB
- Hard Disk : 20 GB

SYSTEM ARCHITECTURE



SYSTEM ARCHITECTURE

- The Architecture of the proposed AI-SIEM system for artificial intelligence-based threat detection. The AI-SIEM system employs not only deep learning techniques but also data preprocessing mechanism that enables the handling of very large-scale network events.

- Specially, the main goal of the AI-SIEM is to automatically analyze network security events related to true alerts for detecting cyber-threats and execute multiple analysis engines. It also utilizes the processing capability of the several graphical processing unit (GPU) cores for faster and parallel analysis.

- The AI-SIEM system comprises three main phases: The data preprocessing, artificial neural networks-based learning engine, and real-time threat detection phase.

- The first preprocessing phase in the system, termed event profiling, aims at providing concise inputs for various deep neural networks by transforming raw data. In the data preprocessing phase, data aggregation with parsing, data normalization stage using TF-IDF mechanism, and event profiling stage are consecutively performed in the AI-SIEM system.

- The second AI-based learning engine employs three artificial neural networks for modeling. For the data learning stage, the preprocessed data are fed into the three artificial neural networks, and each ANN performs learning to find the most accurate model.

- Finally, in real-time threat detection, each ANN model mechanically classifies each security raw event using the trained model, and the dashboard shows the only recognized true alerts to security analysts for reducing false ones.

FUNCTIONAL REQUIREMENT

The functional requirements are designed to carry out to the clients. The requirements used by the clients should be very well defined for the operation of the system. The clients understand what the services to be provided, objectives to be defined and how the system will react with input.

 To decompose a large amount of collecting events into individual event occurrence profiles, we apply the TF-IDF mechanism.

 To generate the event profiles by computing the similarity value among each TF-IDF event sets and appointed base points

 The generated event profiles are fed into the input-layer of the FCNN, CNN, and LSTM models, which are executed in AI-SIEM.

 Consequently, using two well-known benchmark datasets and two real datasets collected from operating IPS, we aim to show the applicability of our system for defending IT systems against the cyber threats.

THANK YOU