Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 7 July 2021: 12916 – 12923

Research Article

A User-Centric Machine Learning Framework For Cyber Security Operations Centre

Miss. Jurreyyah Firdaws Mohammad,
UG Scholar, Dept of Computer science Engineering, BITS Pilani, Dubai.Email:
juriya.shayaan@gmail.com

ABSTRACT

Inspectors (SOC) look into warnings to see if they are accurate. However, the majority of warnings are incorrect, and the amount of warnings is more than SCO's capacity to manage all awareness. As a result, malevolent intent is a possibility. It's possible that attacks and compromised hosts are incorrect. Machine learning might be used to reduce the number of false positives and increase the in a real-world setting in this article. We go through common data sources in SOC, their workflow, and how to analyse this data to build a machine learning system that works. This essay is written for two audiences. The first group consists of bright researchers who have no background in data science or computer security but who should develop machine learning algorithms for machine safety. The second category of visitors are Internet security professionals with extensive knowledge and experience in the field, but no Machine Learning experiences exist, and I'd like to build one for them. We utilise the account as an example at the conclusion of the paper to show all of the procedures from data collection to label generation, feature engineering, machine learning algorithm, and sample performance assessments utilising the computer constructed in Seyondike's SOC production.

Keywords—user-centric; machine learning system; cyber security operation center; risky user detection

I INTRODUCTION

By and large, web-connected frameworks, such as equipment, programming, and data, may be protected against assaults using cybersecurity. Cybersecurity refers to a set of technologies and methods designed to protect computers, networks, projects, and data against attacks and unauthorised access, modification, or deletion. As threats become more sophisticated, new technologies like as machine learning (ML) and deep learning (DL) are being used in the cybersecurity network to improve security capabilities. Cybersecurity is a hot topic on the internet these days, and it relies on the computerization of several application spaces, such as accounts, industry, clinical, and a slew of other essential zones [11]. Differentiating between different network assaults, especially those that haven't been seen recently, is a critical issue that has to be resolved as soon as possible [1].

This article summarises previous work in machine learning (ML) and deep learning (DL) approaches for cybersecurity applications, as well as a few examples of each strategy's applicability in cybersecurity jobs. In ML/DL, the approaches described in this study are useful for identifying cybersecurity threats such as programmers and predators, malware, phishing, and network interruption location. In this way, an exceptional obvious quality is placed on an extensive depiction of the ML/DL approaches, with references to actual publications for each ML and DL approach [1].

In addition, consider the challenges and benefits of using machine learning and deep learning for cybersecurity.

2.REALTED WORK

Cybersecurity is the protection of networks, PC-connected devices, projects, and data against harmful attacks or unauthorised access using a variety of innovations. Data innovation security is a term that is frequently used to refer to cybersecurity. Unauthorized access to sensitive data or other types of information might result in a disaster. Security patterns and threat intelligence cybersecurity are at risk throughout the time spent synchronising with new upcoming improvements. However, it is critical to protect data and information against intrusions and to maintain cybersecurity.

Cybersecurity's Difficulties

In the subject of cybersecurity, there are several challenges. The shifting perception of security threats is one of the most challenging aspects of cybersecurity. A traditional approach to cybersecurity was to focus on the most serious known threats while neglecting to secure frameworks against less serious threats.

Different types of cyber-threats

A cyberattack is a malicious attack on computers and servers, as well as electronic frameworks, networks, and information. Counterfeit code is used in cyberattacks to replace unique PC code, logic, or information, resulting in troublesome results that lead to cybercrime. The ultimate goal of cybersecurity is to prevent cyberattacks from happening.

3.SYSTEM ANALYSIS

EXISTING SYSTEM

The majority of business security techniques have concentrated on securing network infrastructure while paying little or are primarily concerned with network level protection. Despite the fact that such an approach is still part of the broader security storey, it has limits in light of the new security problems discussed in the preceding section.

It is concerned with monitoring and analysing network traffic data in order to detect and prevent hostile activities. Risk values were included into and a quantitative risk assessment was undertaken. According to the quantitative analysis, the recommended remedies might lower risk to some level. The cost-effectiveness of the recommended countermeasures will be investigated in the future. It gives users attack details including the type of attack, the frequency, and the target and mitigation techniques utilising an attack tree-based methodology.

PROPOSED SYSTEM

By bringing security closer to end users, user-centric cyber security User security is not the same as user-centric cyber security. Answering people's demands in ways that protect the company network and its assets is what user-centric cyber security is all about. For businesses, user-centric security is more valuable. Cyber-security systems are self-contained, real-time, and durable systems with high performance demands. They're employed in a wide range of applications, including key infrastructures like the national power system, transportation, medical care, and military. These applications necessitate the integration of computer, communication, and control technological systems in order to achieve stability, performance, dependability, efficiency, and resilience. Because of their complexity and cyber-security interconnectedness, these CPSs face security breaches. The attackers are want sensitive information. The project's main goal is to decrease the amount of unnecessary data in the dataset.

4.MACHINE LEARNING ALGORITHM

Algorithms for Machine Learning

In our system, we employed a Multi-layer Neural Network (MNN) with two hidden layers, Random Forest (RF) with 100 Ginisplit trees, Support Vector Machine (SVM) with radial basis function kernel, and Logistic Regression (LR) with radial basis function kernel, among other machine learning methods (LR). In practise, Multi-layer Neural Networks and Random Forests have shown to be effective in our case. The validation results for these models will be supplied later.

Performance Measures for Models

multiple models should be assessed on test holdout data, as is standard procedure. In addition to AUC, we define two further metrics of model quality in Equations (1) to (2):

$$\text{Model Detection Rate} = \frac{\textit{Number of Risky Hosts in Certain Predictions}}{\textit{Total Number of Risky Hosts}} \times 100\% \tag{1}$$

$$\text{Model Lift} = \frac{\textit{Proportion of Risky Hosts in Certain Predictions}}{\textit{Overall Proportion of Risky Hosts}} \tag{2}$$

Active Learning and Model Implementations

Currently, the machine learning system is being used in a real-world production environment. on a regular basis to ensure that it catches the most recent data trends. When fresh alerts are triggered, the risk ratings are created in real time, allowing SOC analysts to take immediate action for high-risk individuals.From data integration through score production, the whole process has been automated. In addition, the system actively learns new ideas from research.

SUPPORT VECTORMACHINE (SVM)

The “Support Vector Machine” (SVM) is a supervised machine-learning method that may be used to both classification and regression problems. It is, however, mostly employed in categorization issues. We depict each data item as a point in n-dimensional space (where n is the number of features you have), with the value of each feature being the coordinate value. After that, we classify the data by looking for patterns the hyper-plane that clearly distinguishes the two classes (look at the below snapshot). In reality, the SVM method is implemented using akernel. The hyperplanein linear SVM is learned by converting the issue with some linear algebra, which is outside the scope of this SVM introduction. The inner product of any two supplied data, rather than the observations themselves, is a significant discovery in the linear SVM. The total of the multiplication of each pair of input values is the inner product between two vectors. The inner product of the vectors [2, 3] and [5, 6], for example, is 2*5 + 3*6 or 28. The following is the equation for creating a prediction for a new input using the dot product between the input (x) and each support vector (xi).

$$f(x) = B0 + \mathrm{sum}(ai * (x,xi))$$

This equation includes computing the inner products of a new input vector (x) with all support vectors in training data. The learning algorithm must estimate the coefficients B0 and ai (for each input) from the training data.

5. SYSTEM ARCHITECTURE

The architecture diagram below depicts the flow of requests from users to the database via servers. The total system is developed in three sections employing three layers: display layer, business logic layer, and data connection layer in this instance. The 3-tire architecture was used to create this project..

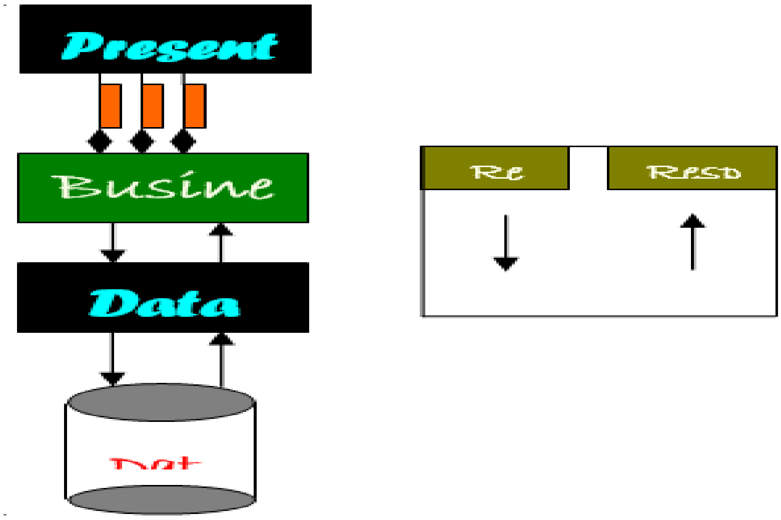


Fig 1: architecture diagram

6.MODULES :

Cyber attack

Cyber threatanalysis is a technique that compares knowledge about internal and external information vulnerabilities relevant to a certain business to real-world cyber-attacks. In terms of cyber security, this threat-oriented strategy to countering cyberattacks provides a seamless shift from reactive to proactive protection. Furthermore, the goal of a threat assessment is to provide best practises for maximising protective instruments in terms of availability, confidentiality, and integrity, without compromising usability or functionality. CYPER ANALYSIS is a term that refers to the examination of a person's A danger might be anything that causes the firm's valued services or items to be disrupted, interfered with, or destroyed. Regardless of whether it is of “human” or “nonhuman” origin, the investigation must examine every aspect that might pose a security concern. Modification Of A Dataset You can conceal certain dataset items from display in the Datasets panel if a dataset in your dashboard has several dataset objects. For example, if you want to import a big quantity of data from a file but don't want to delete it, you may do so.

Data reduction

Using datareduplication, compression, snapshots, and thin provisioning, improve storage efficiency by reducing data and optimising capacity. The most efficient approach to decrease a storage's data is by simply removing undesirable or unnecessary data.

Risk user detection

Immunity against false alarms to avoid consumer humiliation To safeguard all types of products from theft, there is a high detection rate. Entrance/exit layouts are more flexible with wide-exit coverage. A wide selection of appealing designs may be used to enhance any store's decor. For optimum system performance, sophisticated digital controller technology is used.

RESULT

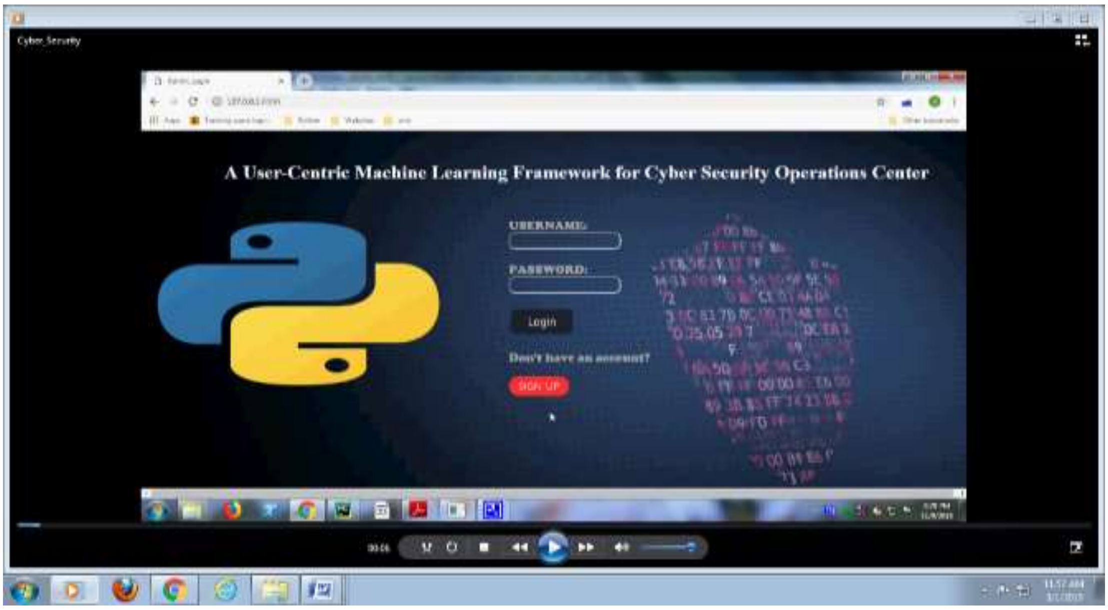
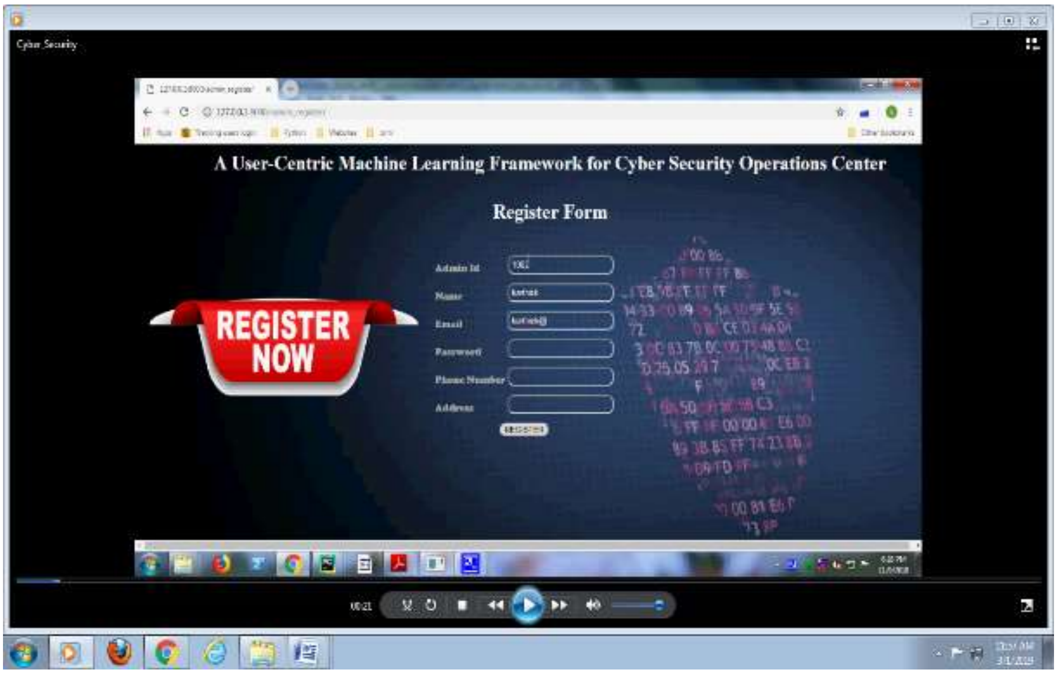

Cyber_Security
A User-Centric Machine Learning Framework for Cyber Security Operations Center
USERNAME:
PASSWORD:
Login
Don't have an account?
SIGN UP

Fig 2: User Login



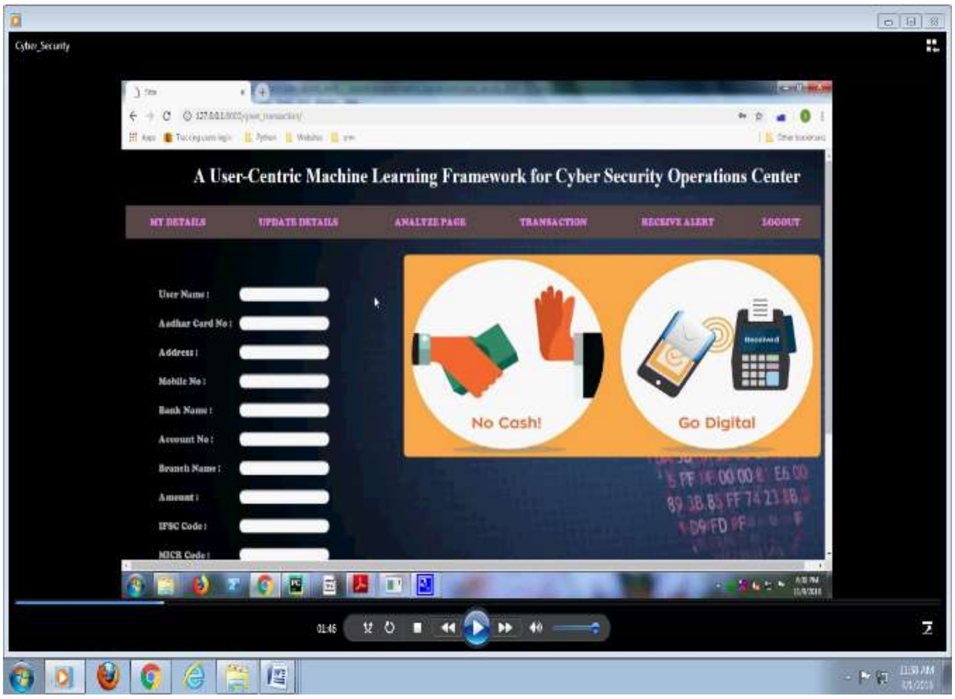
Cyber_Security

A User-Centric Machine Learning Framework for Cyber Security Operations Center

Register Form

Admin Id	1061
Name	kothak
Email	kothak@
Password	
Phone Number	
Address	

Fig 3: Registration Form

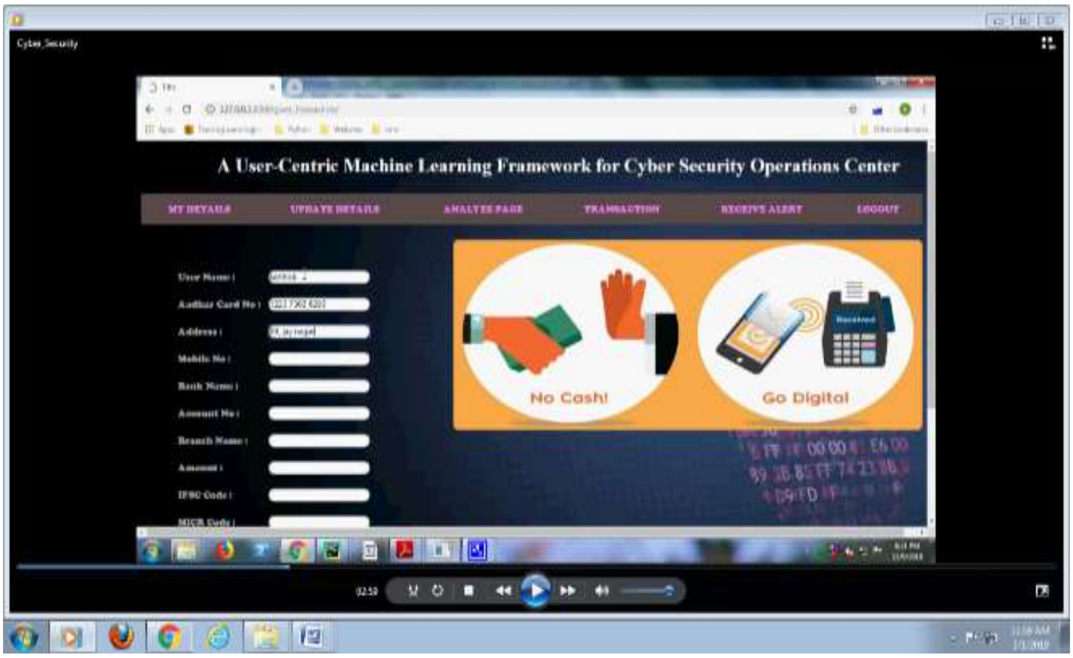


Cyber_Security

A User-Centric Machine Learning Framework for Cyber Security Operations Center

User Name :	
Aadhar Card No :	
Address :	
Mobile No :	
Bank Name :	
Account No :	
Branch Name :	
Amount :	
IFSC Code :	
MICR Code :	

Fig 4: Operation Centre



User Name :

Aadhar Card No :

Address :

Mobile No :

Bank Name :

Account No :

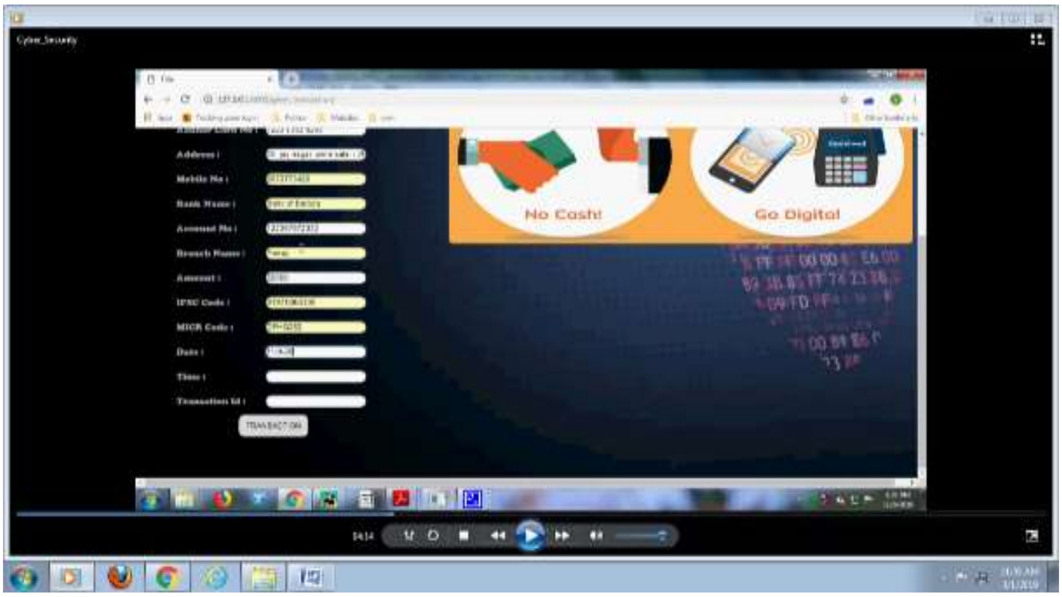
Branch Name :

Amount :

IFSC Code :

MICR Code :

Fig 5: User Info



Address :

Mobile No :

Bank Name :

Account No :

Branch Name :

Amount :

IFSC Code :

MICR Code :

Date :

Time :

Transaction Id :

Fig 6: Transaction Information

CONCLUSION

We provide a user-centered computer learning system that works with vast amounts of data from security logs, awareness data, and inspector intelligence. For the Enterprise System Operating Center, this technique provides a full configuration and solution for risky user detection. To design user-centric features, select machine learning algorithms in the SOC product environment, assess efficiency, IO, host, and users. We show that the learning system can comprehend more insights from the ranks with the most imbalanced and constrained labels, even with We will investigate different learning approaches to better data acquisition, daily model renewal, real-time estimate, completely enhance and organisational risk detection and management in order to increase detection precision. In terms of future research, we should look at alternative learning strategies to increase detection accuracy.

REFERENCES

[1] Sun Institute of Technology. "6 types of daily summary" 2013.

[2] Positive and unbiased data ´ Proceedings of the 18th International Conference on Artificial Intelligence, 2003.

[3] A. L. Banana and e. Givin. IISE Communication Survey and Guidance (18) (2015): 1153-1176 "Finding Methods of Data Downloading and Machine Learning to Detect Internet Theft".

[4] S. Chudhuri and A. Boval. "Comparative Analysis of Machine Learning Methods with Classifiers for Network Discovery", Intelligent Technology and Management for Computers, Communications, Power and Material Monitoring (ISMM), 2015.

[5] N. John et al. "Comparative analysis of SVM and its alignment with other intrusion detection classifications", "Advances in Computers, Communications and Automation" (ICCCA) 2016.

[6] Kekochel. “Reducing Fraud in Invasion Capture Systems Using Data Retrieval Techniques Using Decision Tree Vector Maintenance Machines and Stupid Gulf for Offline Analysis” SoutheastCon, 2016.

[7] M. J. Kang and F. ຜິ. ຜິ. Bumper. 2016 Automotive Technical Conference “Methods for Detecting New Intrusions Using Deep Nervousness for Safety in Automotive Networks” 2016 Automotive Technology Conference