Leveraging AI for Fraud Detection in Identity and Access Management: A Focus on Large-Scale Customer Data

Venugopal Tamraparani

Vice President, Marlabs Piscataway , NJ , USA, Email: Venugopal.tp@gmail.com

Received: 15.10.2023 Revised: 27.11.2023 Accepted: 12.12.2023

ABSTRACT

Due to the increasing complexity of theft, organizations handling substantial consumer data must implement sophisticated identity and access management (IAM) systems. This study examines the application of artificial intelligence (AI) in detecting fraud within Identity and Access Management (IAM) systems, particularly those managing extensive customer datasets. The study examines the challenges arising from the vast volume, rapidity, and diversity of data, together with the evolving nature of fraud schemes. Artificial intelligence (AI) encompasses machine learning algorithms, anomaly detection models, and pattern recognition methodologies. These can swiftly identify potential scam scenarios that traditional approaches may overlook. The research examines the advantages and disadvantages of employing AI for fraud detection. It addresses concerns regarding data quality, false positives, and system scalability. Enhancing scam protection necessitates continuous training of models, as evidenced by real-world examples, and the integration of AI into current identity and access management systems. This report provides valuable recommendations for firms seeking to enhance their IAM systems through the utilization of AI technologies.

Keywords: Artificial Intelligence, Fraud Detection, Identity and Access Management (IAM), Anomalies

1. INTRODUCTION

Insider threat has emerged in enterprise security and received increasing attention over last several years. A survey [1] by Haystack shows 56% of respondents feel that insider attacks have become more frequent. Privileged IT users such as administrators with access to sensitive information, pose the biggest insider threat. IT assets such as databases, file servers and mobile devices are top assets at risk.

In the world of growing connectivity, information is considered to be one of the most prized assets. Due to this reason, the number of threats that are imposed upon corporate data is also high. These threat vectors, hence, pose serious challenge for protecting information. Threat from external sources have received considerable efforts for prevention through the use of various network components installed, like next-gen firewalls, antivirus programs, Intrusion Detection Systems (IDS), etc. On the other hand, insider threats, which have better knowledge of the critical assets within the organization and increased access, are difficult to detect and stop by network components, as these act as a legitimate user and often go undetected. This has encouraged increased amount of insider threats. Compromised users in Advanced Persistent Threat (APTs), careless employees using unsecured application service account instead of named account, users with malicious intents, spies from other organizations and dissatisfied employees constitute are some of the cases which are identified as insider threat[1]. According to latest insider threat report by Gurucul, regardless of the origin, action taken by them potentially harm organization and 49% of those organizaion have no effective detection of insider threat in place[2]. Hacking trails for outsiders are hard to hide whereas malicious insiders are equally difficult [3] to detect based on the signature based profiles of the users.

Identity and access management (IAM) is a business and security discipline that enables the right people, software, and hardware, as appropriate to job roles and functionality, to have access to the tools required to perform assigned duties, without also granting them access to those that are not needed and/or present a security risk to the enterprise. Organizations that utilize IAM can streamline operations by managing identities without requiring individuals to log into applications as administrators. Identity and access management is a vital initiative for any enterprise because it supports the crucial need to enable the appropriate access to tools and resources in increasingly diverse technological ecosystems and to comply with ever-changing privacy and security regulations. IAM affects many aspects of the enterprise, not just IT, and requires strategic business planning in addition to specialized technical capabilities.

A. IAM Concepts

The core of identity and access management, is, of course, identity. The objective of IAM is to assign one digital identity per individual or other entity, which must then be controlled, managed, and supported throughout its lifecycle. Another important concept is digital resource, defined as any combination of data and applications, such as software, databases, application programming interfaces (APIs), devices, and more, in a computer system. When a team member, customer, device, robot, or any other entity with an identity needs access to an organization's resources, identity and access management confirms the identity and controls its access to the digital resource. IAM Terminology Before diving into a deep discussion of identity and access management, it's helpful to know brief definitions of related terms, including:

Access management: Access management is defined as the practices and tools that monitor and manage network access. Identity management solutions, whether on-premises or cloud-based, typically include features like authentication, authorization, and trust and security auditing.

Active directory (AD): AD, a user-identity directory service, is a proprietary Microsoft product that is widely available through the Windows Server operating system. Integrations allow access to be seamlessly provisioned and deprovisioned, easing IT team workloads. Biometric authentication: This security method uses unique characteristics such as fingerprints, retinas, and facial features to authenticate usersas in Figure 1.

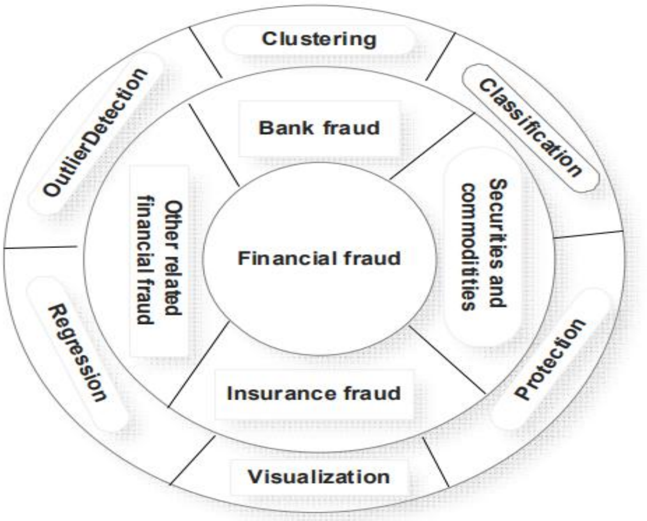

Figure 1: Conceptual Framework for Classification of Frauds

Cloud infrastructure entitlement management (CIEM): CIEM is the process of managing identities and access across increasingly complex cloud infrastructure environments. A least privilege approach is utilized to ensure that users only have access to the resources they need, and only for long as they need them.

Deprovisioning: Deprovisioning is the act of removing user access to applications, systems, and data within a network.

Digital identity: A digital identity consists of user attributes (such as name, government ID number, email address, biometrics, and other personally identifiable information), and digital activity and behavioral patterns (such as browsing history, downloads, and operating system).

Identity and access management (IAM): IAM is a specialty discipline within cybersecurity designed to ensure only the right people can access the appropriate data and resources, at the right times and for the right reasons.

Identity as a service (IDaaS): IDaaS is an is an application delivery model that allows users to connect to and use identity management services from the cloud. Identity governance: Identity governance is the act of using IT software and systems to manage user access and compliance. Identity provisioning: A key component of the identity governance framework, identity provisioning manages user accounts and ensures users have access to the right resources and are using them appropriately.

Multi-factor authentication (MFA): MFA is an access management tool that combines two or more security mechanisms for accessing IT resources, including applications and devices. Principle of least privilege: To protect data and applications, access is only granted to an identity for the minimum length of time required, and is only permitted to the resources required to perform the task.

Privileged access management (PAM): Privileged access is limited to users such as administrators who must have access to applications, systems, or servers for implementation, maintenance, and updates. Since breaches to these credentials could be catastrophic to the enterprise, PAM tools separate these user accounts from others and track activities associated with them closely.

Role-based access management (RBAC): RBAC allows the enterprise to create and enforce advanced access by assigning a set of permissions. The permissions are based on what level of access specific user categories require to perform their duties. In other words, different people in the organization can have completely different levels and types of access privileges based solely on factors such as their job functions and responsibilities.

Separation of duties (SoD): Also known as Segregation of Duties, Separation of Duties is a security principle used by organizations to prevent error and fraud. This internal control relies on RBAC to prevent error.

Single sign-on (SSO): SSO is an authentication service allowing a user to access multiple applications and sites using one set of credentials.

User authentication: A fundamental task of IAM systems is to validate that an identity is who or what it claims to be when logging in to and utilizing applications and data. Most people are familiar with the traditional authentication that occurs when a user enters a username and password into a sign-in screen; modern user authentication solutions, and those of the future, utilize artificial intelligence and other technical advancements for improved safeguarding of organizational assets.

2. LITERATURE REVIEW

Distributed data mining and machine learning techniques could be used to fight efficiently and alleviate the effect or prevent cybercriminals' actions, especially in the presence of large data sets [4]. In particular, classification is used efficiently for many cybersecurity applications, i.e. classification of user behaviour, risk and attack analysis, intrusion detection systems, etc. However, in this particular domain, different data sets often have a different number of features, and each attribute could have different importance and cost. Furthermore, the entire system must also work if some features are missing. Therefore, a single classification algorithm performing well for all the data sets would be unlikely, especially in the presence of changes and with constraints of real time and scalability.

a framework based on the elastic stack to process and store the data from the different users and generate an ensemble of classifiers to classify user behaviour and exploit this classification to detect anomalies in their behaviour efficiently. In practice, the system uses the high-performance architecture provided by ELK, running on top of a Kubernetes-based platform and adopts a distributed evolutionary algorithm for classifying the user based on their digital footprints, derived from many logs. In addition, as a new resulting task, the framework permits the individuation of the anomalies in user behaviour. Indeed, the classification algorithm previously introduced inis here used as a preliminary step for identifying likely anomalies by associating a class of risk to all the tuples differing by a predefined threshold by the usual behaviour of the user/group.

Recently, in the literature, there has been a growing interest in the task of monitoring user behaviour and actions and using machine learning-based approaches to analyse the resulting logs to minimise or prevent cybersecurity risks or frauds.

The authors try to cope with high-class imbalance, changing target concepts and other real-time issues (heterogeneous attributes, cold start problem, etc.) of anomaly detection by using a user-centred algorithm operating with identity and access management (IAM) real logs. Experimental results on the CERT insider data set show that two different methods must be used for masquerades and discovering malicious users. In the former case, user identification is sufficient, while for the latter, it is necessary to introduce graph features representing user context and relations to other entities.

Table 1: Description and data sources for the HFUser data set

Records	**Features**	**Users (Groups)**
2220	85 + 3	10 (3)
Data sources		
DS-1	DS-2	DS-3
Activity keyboard (5 features)	Mouse movement (16 features)	Cpu usage (16 features)
	Mouse click (16 features)	Memory usage (16 features)

	Mouse zone (16 features)	

The second data set is the context-aware data set described, which contains the information security awareness (ISA) scores assessed from the three data sources (namely, the questionnaires, mobile agent and network traffic monitor) by conducting a long-term user study involving 162 smartphone users, downloadable from here.

he arrival of smart cities powered by the Internet of Things (IoT) has revolutionized the functioning and development of urban areas. These cities leverage digital interconnections and an extensive network of sensors to improve operational efficiency, sustainability, and their inhabitants' overall quality of life. However, the proliferation of IoT devices has led to an unprecedented influx of data into urban environments. This data plays a critical role in a smart city's real-time operations and decision-making processes but also presents significant challenges, particularly about security and management. One of the most critical challenges is the detection of anomalies within this urban data.

Anomaly detection involves identifying patterns or events that deviate significantly from a data set's normal or expected behavior. This task is of paramount importance in the context of smart cities, as it covers a broad spectrum of applications, ranging from identifying manipulations in the electrical grid to detecting cyber threats and anticipating failures in critical urban systems. Early detection of anomalies is not only advantageous; it is imperative to prevent unplanned disruptions, ensure the safety of citizens, and maintain the integrity of urban systems. Within the intricate fabric of a smart city, IoT devices serve as nerve endings, continuously monitoring and collecting data from various aspects of urban life, including energy consumption, transportation, environmental conditions, and security. These devices generate a wealth of information that can be leveraged to optimize urban services, improve resource management, and improve overall urban resilience. However, this influx of data also makes smart cities vulnerable to many threats, including cyberattacks, equipment malfunctions, and natural disasters. The consequences of these threats can range from service interruptions to significant economic losses and even threats to human lives. Therefore, the ability to identify and mitigate anomalies in real-time becomes not only a technological aspiration but a critical need.

This work delves into the critical role that anomaly detection models play in IoT-enabled smart cities and evaluates their effectiveness in reinforcing the safety and efficiency of urban systems. To fulfill this purpose, research has been carried out covering the applicability of anomaly detection models in various urban scenarios. Furthermore, its performance is rigorously evaluated and juxtaposed with existing approaches, comprehensively assessing its effectiveness. Again, a comprehensive analysis of the strengths and limitations of these models is performed, accompanied by a visual presentation of the comparative results. This work deepens the understanding of how IoT-enabled anomaly detection models can significantly contribute to the safety and efficiency of smart cities. This contribution creates a safer and more efficient urban environment for citizens, allowing real-time anticipation and resolution of critical problems.

A. Hypotheses

Investigators conducting studies need research questions and hypotheses to guide analyses. Starting with broad research questions (RQs), investigators then identify a gap in current clinical practice or research. Any research problem or statement is grounded in a better understanding of relationships between two or more variables. For this article, we will use the following research question example:

1. What a user knows, like a passphrase or the solution to a secret inquiry.
2. Possession - anything the user must physically possess, like a physical credit card.
3. Biological characteristics of the user, such fingerprints or a face scan, are examples of inborn identification methods.
4. You can be sure that it was really you using that card by checking your location at the time of authentication.
5. What time or times are the authentication attempts being made?

3. PROPOSED METHODOLOGY

Financial fraud fraud is a serious ethical problem in the business world. The research primary goal is to detect financial fraud fraud and offer a workable solution to this problem. Financial fraud fraud has resulted in billions of dollars in losses worldwide for victims and financial institutions. Even though there are many security measures in place to prevent fraud, attackers are always devising new techniques to deceive unsuspecting victims. The banking industry and other financial institutions place a premium on fraud detection. The proposed model use historical fraud data to improve its ability to identify future instances of fraud. While fraud detection algorithms based on mining data had been tried, they had not shown any promising results. The research makes use of supervised learning methods applied to a highly skewed and imbalanced dataset considered from Kaggle.

Feature selection is a crucial part of data preparation to avoid over fitting due to the curse of dimensionality reduction. Through the process of feature selection, superfluous or unimportant details are eliminated. Filter and wrapper are the two most well-known approaches, and both have their advantages and drawbacks. The wrapper method has some drawbacks, such as the high processing cost and reliance on the algorithm as an evaluation function to select the features. On the other hand, the filter approach has the drawback of only searching for features independently, therefore features that are highly dependent on one another will be missed.

A ML based feature selection strategy that combines filter and wrapper approaches is an alternate solution that is less exhaustive and has less drawbacks. In order to determine the degree of similarity between the numerical characteristics, a correlation-based filter was employed. Positive features that were highly associated were omitted from the prediction model to prevent over fitting and to conserve computational resources. This research presents a Related Feature Subset Model for Financial fraud Fault Detection for accurate detection of financial fraud frauds. The proposed model architecture is shown in Figure 2.

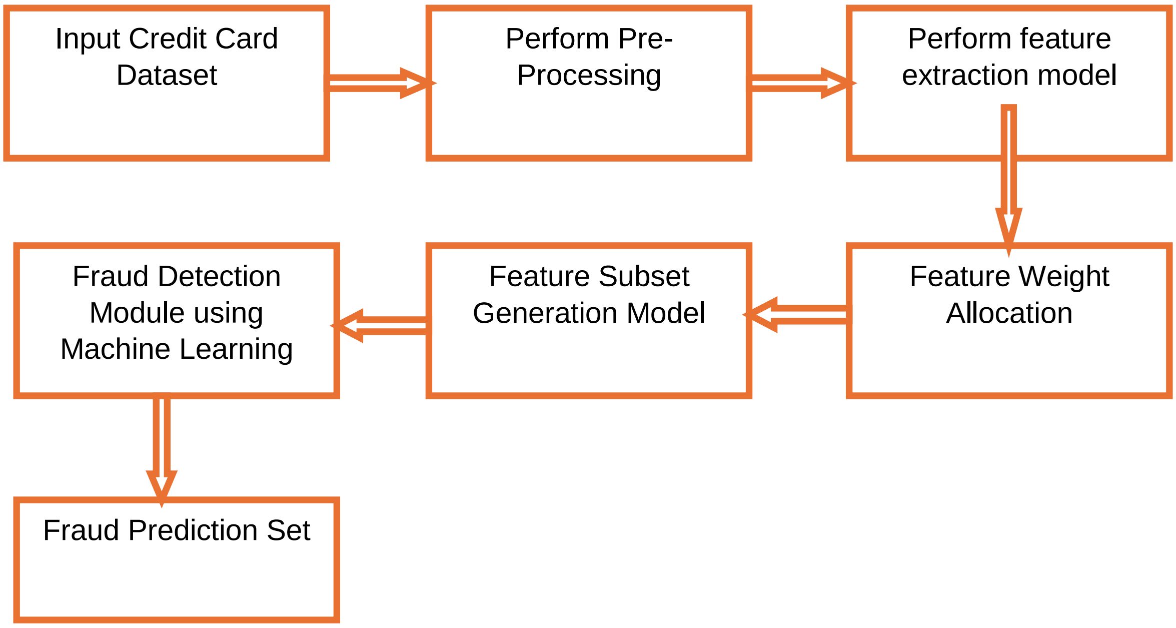
Input Credit Card Dataset
Perform Pre-Processing
Perform feature extraction model
Feature Weight Allocation
Feature Subset Generation Model
Fraud Detection Module using Machine Learning
Fraud Prediction Set

Fig 2: Proposed Model Architecture

Algorithm RF-CFD

{

Input: Financial fraud Fraud Dataset {CCFDSET}

Output: Fraud Prediction Set {FPSET}

Step-1: Load the dataset and then analyze the records to perform pre processing on the dataset. The pre processing cleans the data from the available ones. The pre processing is performed as

Step-2: As a method of dimensionality reduction, feature extraction organises large amounts of raw data into more manageable parts. In order to process these massive data sets, a great deal of computational power is needed because of the sheer amount of variables involved. To reduce the amount of data that needs to be processed while still providing an accurate and complete description of the original data set, a number of techniques have been developed under the feature extraction process. The feature extraction process is performed as

Step-3: The parameters employed in each layer of the model are reflected in the model's weights. The weights are allocated based on the correlation factor and the highly correlated features are removed and most useful features are considered.

Step-4: From the features extracted, the feature subset is generated which considers the most useful features that is used for financial fraud fraud detection.

Step-5: The financial fraud fraud detection is performed by training the model using the feature subset.

Machine learning algorithms can identify suspicious activity on a financial fraud and prevent further losses. The first step in using a model to predict potential instances of fraud is to collect and organize raw data for use in training that model. Machine learning provides solutions for detecting financial fraud fraud, including the use of learning algorithms to classify transactions as authentic or fraudulent, financial fraud profiling to predict whether legitimate cardholders or malicious actors are using the cards, and outlier detection methods to identify records of transactions that are significantly different from the norm.

Financial fraud fraud is a big problem in today's interconnected global economy. Worldwide, fraud results in massive financial losses. As a result, many banks have invested in studying the problem and creating tools to help identify and stop financial fraud fraud. The major goal of this research is to develop a ML model that efficiently and accurately identify fraudulent transactions for financial fraud issuers. Computer software that may rapidly construct a prediction system for detecting financial fraud fraud by automatically picks suitable Machine Learning algorithms, adjusting their hyper-parameter variables, and evaluating performance on a highly skewed dataset.

There is zero overhead in terms of user setting of method parameters during model training. It also requires little work to apply the model, retrain this whenever new data becomes available, produce visualizations of the findings, and communicate them across the many levels of management in the organization.

A. Source of information and tools for analysis:

The proposed model is implemented in python and executed in Google Colab. The proposed model is compared with the traditional Enhanced financial fraud fraud detection based on attention mechanism and LSTM deep model (FDAM-LSTM) model.

Data preprocessing, or the manipulation or removal of data before to its usage, is a crucial part of the data mining process, as it ensures or improves performance. Any action taken on raw data in order to get it ready for further processing is referred to as data preprocessing, and it is part of the larger data preparation process. It is a crucial first stage in the data mining process and has been for a long time.

1. The data preprocessing secure accuracy levels of the existing and proposed models.
2. The feature extraction time levels of the existing and proposed models
3. The feature weight allocation secure accuracy levels of the traditional and proposed models
4. The feature subset generation time levels of the proposed and the traditional method.
5. The feature subset generation secure accuracy levels of the traditional and proposed models
6. The proposed model fraud detection time levels is less than the existing models
7. The fraud detection secure accuracy levels of the proposed model is high than the existing models

4. PERFORMANCE ANALYSIS

Criminals are more likely to resort to online payment fraud in an attempt to circumvent payment providers' security measures, as the popularity of such transactions has grown. With the ultimate goal of preventing fraud in an online payment system and devising countermeasures against attacks, there is a lot of pressure to investigate any security vulnerabilities that could be exploited. Detecting potentially fraudulent financial transactions as early as possible is an important aspect of this research. The development of online payment systems has led to an increase in demand for automated detection technologies that can detect and stop fraudulent transactions in real-time.

With the spread of smartphones, there is an increase in the usage of mobile payment methods, which piques the interest of scammers. Numerous fraud detection algorithms that employ supervised machine learning have been developed in response to the aforementioned body of literature. Nonetheless, suitable labelled data are scarce, and the considerable class imbalance in financial fraud data reduces detection performance. Given the monetary ramifications of fraud detection systems, this study seeks to propose an improved logistic regression framework for detecting fraudulent behaviour. The system was validated using a massive dataset of over 3 million Internet transactions. This study presents a Linked Feature Set with Enhanced Logistic Regression (LFS-ELR) Model for accurately detecting online payment fraud. Results from a comparison with the standard Fine-Grained Co-Occurrences for Behavior-Based Fraud Detection in Online Payment Services (FGCO-BFD-OPS) show that the proposed model delivers respectable results. The fraud prediction set is calculated using the formulas shown below.

Feature extraction is a form of dimensionality reduction that involves partitioning an initial set of raw data into more manageable subsets. One of the characteristics of these massive data sets is the large number of variables that must be processed, which requires a significant amount of computational power. The process of selecting and/or combining variables to create features is known as feature extraction. This effectively reduces the amount of data that must be handled while accurately and thoroughly characterizing the initial data set. Table 1 shows the feature extraction time levels of the proposed and traditional models.

Table 1: Feature Extraction Time Levels

Size of the Dataset	FDAM-LSTM	Proposed RF-CFD
5	12.0	6.0
10	14.0	7.8
15	15.9	9.3
20	17.7	11.2
25	21.4	13.5
30	21.4	14.6

The feature extraction accuracy levels of the suggested and current models are displayed in Table 2.

Table 2: Feature Extraction Accuracy Levels

Size of the Dataset	FDAM-LSTM	Proposed RF-CFD
5	78.2	82.7
10	80.9	84.5
15	82.1	86.4
20	84.5	88.2
25	86.7	90.2
30	88.3	92.6

Feature selection is the process of using only the data that is relevant to the model and removing noise from it to limit the number of variables that are fed into the model. It is the technique of automatically identifying appropriate features for a machine-learning model based on the type of problem being addressed. This can be accomplished by selectively including or removing significant features while leaving them unchanged. Thus, data noise and size can be reduced. Table 3 shows the Feature Selection Accuracy Levels of the existing and proposed models.

Table 3: Feature Selection Accuracy Levels

Size of the Dataset	FDAM-LSTM	Proposed RF-CFD
5	82.1	88.1
10	82.6	90.5
15	84.7	92.1
20	87.4	94.8
25	89.4	96.2
30	90.7	97.8

The detection of modern payment fraud makes use of machine learning based ELR model and statistical analysis to continually monitor transactions and evaluate the level of risk that is connected with each transaction. This may require comparing lacks of different pieces of transactional data to various models of fraud that are already known to exist. Scammers take advantage of the payment request option that is available in apps that support the UPI in order to obtain the PIN or OTP that is required to authorize a transaction. They start the process of requesting payment and then contact the person in question to inquire about the OTP or PIN, claiming that this information is necessary on their end in order to finalize a transaction. The Figure 4 represents the Online Payment Fraud Detection Accuracy Levels of the proposed and existing models.

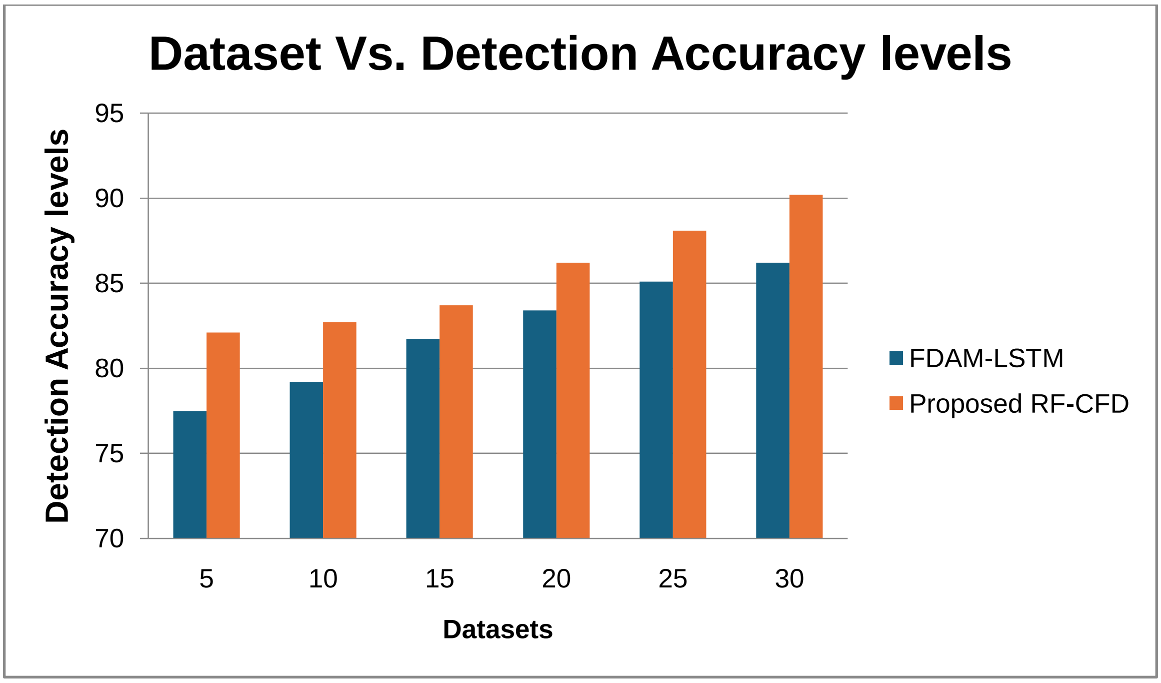

Figure. 4 Dataset Vs. Detection Accuracy levels

Evaluation Metrices

		Predicted Class	
		Normal(-)	Anomaly(+)
Actual	Normal(-)	TN	FN
	Anomaly(+)	FP	TP

Based on above table, different performance parameters are calculated in evaluation of model.
True positive Rate OR Recall:

$$TPR = \frac{TP}{TP + FN}$$

Accuracy:

$$Accuracy = \frac{TP + TN}{TN + FP + FN + TP}$$

Precision:

$$Precision = \frac{TP}{FP + TP}$$

F1 score:

$$F1score = 2 * \frac{Precision * Recall}{Precision + Recall}$$

ROC:
Receiver Operating Characteristic Curve The graph representing cost against benefit to show the relationship between Recall(TPR) and False Postive rate at different threshold values is called ROC curve.

This relation between these two quantities differs and plotting these values, we can get a curve. The area covered with the curve is directly proportional to the performance of the model.

CONCLUSIONS

This research works presents use of one class modelling on normal data of CERT r4.2 data set. The model overfitted on non-malicious normal during training period data produces high reconstruction error when malicious samples are fed during the testing period. The work focuses on using GRU units in place of traditional LSTM units for use in autoencoder model for modelling non-malicious user behavior. This paper presents an overview of UBA architecture and platform for detecting anomalous user behaviors within enterprise. The platform, composed of four components working independently, is suitable for running on distributed platforms. The anomaly detection component contains an ensemble of OCSVM, RNN and Isolation Forest. Strictly filtering strategy is applied and can improve the performance and robustness no matter whether there exist anomalies in the training set. The sequences of events contain valuable information about users and we will focus on anomaly detection of sequence data. Besides, the peer group analysis, which may play an important role in practice, can be introduced into the UBA platform in the future.

REFERENCES

[1] 2021 insider threat report gurucul.pdf, July 2017.

[2] Folino G, Guarascio M, Papuzzo G (2019) Exploiting fractal dimension and a distributed evolutionary approach to classify data streams with concept drifts. Appl Soft Comput 75:284–297

[3] Ullah, W.; Min Ullah, F.U.; Ahmad Khan, Z.; Wook Baik, S. Sequential Attention Mechanism for Weakly Supervised Video Anomaly Detection. Expert. Syst.

[4] Alhakami, W.; Alharbi, A.; Bourouis, S.; Alroobaea, R.; Bouguila, N. Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection. IEEE Access 2019, 7, 52181–52190. [Google Scholar] [CrossRef]