ISSN: 2634 - 8853

Journal of Engineering and Applied Sciences Technology

SCIENTIFIC Research and Community

Review Article

Open Access

Enhancing Identity and Access Management Systems with Behavioral Analytics: A Novel Approach to Detecting Anomalous Activities

Shanmugavelan Ramakrishnan

USA

ABSTRACT

The detection of malicious user conduct that does not result in an alert for an access violation or a data breach may prove to be a difficult task by itself. With the stolen login credentials, the intruder who is conducting espionage will initially make an effort to acquire data from the company network that he is authorised to access in a stealthy manner while attempting to avoid being discovered. This article presents a description of the User Behaviour Analytics Platform, which was designed to collect logs, extract features, and detect atypical users who may include possible insider threats. The platform was developed at the beginning of this article. A multi-algorithm ensemble that incorporates OCSVM, RNN, and Isolation Forest is also described. This is in addition to the previous point. Under the conditions of the experiment, it was proved that the system, which is made up of a collection of unsupervised anomaly detection algorithms, is able to recognise unusual patterns of user behaviour. The suggested study makes an effort to identify behaviours that are considered to be insider threats and to keep an eye out for any behaviour that is deemed to be unexpected or suspicious by the model. This behaviour is considered to be anomalies because it results in a high level of reconstruction error inside the model. During the training phase of the model, feature vectors that have been derived from user log activities are implemented within a predetermined time frame of each day. This strategy makes use of an autoencoder that is based on Gated Recurrent Units (GRU) in order to model user behaviour on a daily basis and identify abnormal insider threat spots. Errors generated by normal data are negligible since the model has been overfitted with normal data. However, when it comes to the malevolent category of aberrant data, the autoencoder produces a massive mistake. Computer Emergency Response Team (CERT) r4.2 is the name of the dataset used in this study. The feature vectors used are computed from the daily occurrences of a specific action by the users. GRU autoencoder is utilised for the purpose of behaviour learning.

***Corresponding author**
Shanmugavelan Ramakrishnan, USA.

Received: April 07, 2022; **Accepted:** April 16, 2022; **Published:** April 25, 2022

Keywords: Malicious, RNN, Behaviour Analytics, IAM System

Introduction

The prevalence of insider threats to company security has increased dramatically within the last several years. Approximately 56 percent of responders to a poll conducted by Haystack [1] believe that the frequency of insider assaults has increased. The most common type of insider threat is posed by privileged users of information technology, such as administrators who have access to sensitive data. Databases, file servers, and mobile devices are examples of prominent examples of assets that are at danger.

Information is often regarded as one of the most valuable things in today's fast-paced and increasingly interconnected world. The amount of dangers that are posed to the data of corporations is likewise rather big because of this reason. The protection of information is consequently made significantly more difficult by these attack vectors. As a result of the implementation of a variety of network components, such as next-generation firewalls, antivirus software, Intrusion Detection Systems (IDS), and so on, significant efforts have been made to avoid threats that originate from external sources. On the other hand, insider threats are difficult to identify and block by network components since they appear as legitimate users and frequently go unreported. This makes it difficult to identify and block insider attacks. It is more difficult to detect and stop insider threats that have expanded access and a greater awareness of the important assets that are contained within the business. Because of this, there has been an increase in the number of threats that come from within the organisation. Cases that are considered to be insider threats include users who have been compromised in Advanced Persistent Threats (APTs), employees who are careless and use an unsecured application service account instead of a named account, users who have malicious intentions, spies from other organisations, and dissatisfied employees [1]. These are just some of the examples of insider threats. The acts that they carry out have the potential to do harm to the organisation, and according to the most current insider threat survey conducted by Gurucul, only 49% of those organisations have an effective detection mechanism in place for insider threats [2]. This is true regardless of the origin of the actions that they carry out. From the outside, it is difficult to conceal hacking tracks, but it is similarly difficult to detect hostile insiders based on signature-based profiles of the users [3]. This is because it is difficult to conceal hacking trails from outsiders.

Definition of Identity and Access Management

Identity and access management, also known as IAM, is a business and security discipline that enables the appropriate individuals, software, and hardware, according to the nature of their job roles and the functionality they perform, to have access to the tools that are necessary to carry out their assigned responsibilities. However, it does not grant these individuals access to tools that are not required and/or that pose a security risk to the organisation. By managing IDs without requiring individuals to log into programmes as administrators, it is possible for organisations that use identity and access management (IAM) to streamline their processes. Because it supports the fundamental requirement to provide the proper access to tools and resources in more different technical ecosystems and to comply with ever-changing privacy and security rules, identity and access management is an initiative that is essential for any business. This is because it is a necessary initiative. It is necessary to have strategic business strategy in addition to specialised technical competencies in order to implement IAM because it has an impact on many elements of the firm, not just IT.

IAM Concepts

Identity, of course, is the most important aspect of identity and access management. By assigning a single digital identity to each person or other entity, the goal of identity and access management (IAM) is to ensure that this identity is controlled, maintained, and supported during its entire existence. One other essential idea is the digital resource, which may be defined as any combination of data and applications that are present in a computer system. Examples of digital resources include software, databases, application programming interfaces (APIs), devices, and many others. When a member of a team, a client, a device, a robot, or any other entity with an identity needs access to the resources of an organisation, identity and access management verifies the identification of the required entity and regulates its access to the digital resource. Languages Used in IAM It is helpful to have a basic understanding of the definitions of related terms before delving into a more in-depth discussion of identity and access management. These examples include:

Access Management

The techniques and tools that are used to monitor and manage network access are what people mean when they talk about access management. Identity management solutions, whether they are hosted on-premises or in the cloud, often incorporate capabilities such as authentication, authorization, trust and security auditing, and other similar characteristics.

Active Directory (AD)

An identity directory service, often known as Active Directory (AD), is a proprietary product developed by Microsoft and made generally accessible through the Windows Server operating system. The responsibilities of IT teams are reduced thanks to integrations, which make it possible to provision and deprovision access in a smooth manner. Users are authenticated through the use of biometric authentication, which is a security approach that makes use of user-specific traits such as fingerprints, retinas, and facial features.

Cloud Infrastructure Entitlement Management (CIEM)

Identity and access management is the practice of managing identities and access across cloud infrastructure systems that are becoming increasingly complicated. An strategy known as "least privilege" is utilised to guarantee that users are only granted access to the resources that they require, and only for the duration of time that they require them. Deprovisioning: Deprovisioning is the process of eliminating user access to data, applications, and systems that are contained within a network architecture.

Digital Identity

User attributes, such as a name, government ID number, email address, biometrics, and other personally identifiable information, as well as digital activity and behavioural patterns, such as browsing history, downloads, and operating system, are the components that make up a digital identity.

Identity and Access Management (IAM)

Identity and access management (IAM) is a subfield of cybersecurity concerned with identifying and vetting users to make sure they have authorised access to sensitive information at the right times.

Identity as a Service (IDaaS)

Users are able to connect to and make use of identity management services from the cloud through the usage of an application delivery mechanism known as identity as a service (IDaaS). Identity governance refers to the process of utilising information technology (IT) tools and systems in order to regulate user access and fulfil compliance requirements. The providing of identities: The identity provisioning system is an essential part of the identity governance architecture. It is responsible for managing user accounts and ensuring that users have access to the necessary resources and are making proper use of those resources.

Multi-factor Authentication (MFA)

In order to manage access to resources in the realm of information technology, such as devices and apps, multi-factor authentication (MFA) uses a combination of two or more security procedures. Based on the principle of least privilege: Access is only allowed to an identity for the shortest amount of time necessary to complete the work, and it is only granted to the resources that are necessary to carry out the task. This is done to ensure the safety of both the data and the applications.

Privileged Access Management (PAM)

Individuals who are required to have access to programmes, systems, or servers for the purposes of implementation, maintenance, and updates are prohibited from having privileged access. Examples of such individuals include administrators. The PAM tools isolate these user accounts from those of other users and closely monitor the activities that are linked with them. This is done because any compromise of these credentials might have disastrous consequences for the organisation.

Role-Based Access Management (RBAC)

A set of permissions can be assigned to an enterprise using RBAC, which enables the enterprise to develop and enforce advanced access. The authorizations are determined by the level of access that particular user types need in order to carry out their responsibilities. In other words, various individuals within the organisation can have completely different levels and types of access privileges depending simply on characteristics such as the positions they hold and the responsibilities they are responsible for.

Separation of Duties (SoD)

The notion of separation of duties, which is often referred to as segregation of duties, is a security philosophy that is utilised by groups in order to prevent errors and fraud. For the purpose of error prevention, this internal control utilises RBAC.

Single Sign-On (SSO)

SSO, or single sign-on, is a type of authentication solution that enables users to access different websites and applications by utilising a single set of credentials.

User Authentication

In the process of logging in to and making use of applications and data, one of the primary responsibilities of identity and access management (IAM) systems is to verify that an identity is who or what it claims of being. The majority of people are familiar with the traditional authentication that takes place when a user enters a username and password into a sign-in screen. Modern user authentication solutions, as well as those that will be implemented in the future, make use of artificial intelligence and other technological advancements in order to secure organisational assets more effectively.

Literature Review

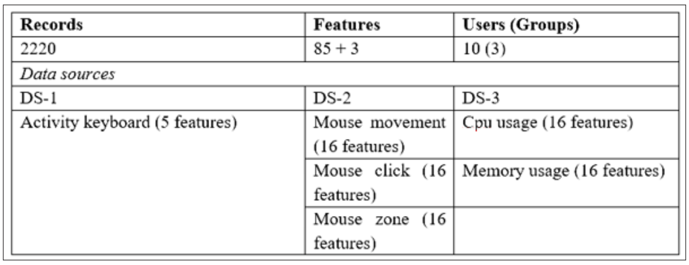
Distributed data mining and machine learning techniques could be used to effectively battle cybercriminals, reducing their effects or stopping their actions, when dealing with enormous data sets [4]. Some examples of classification's many useful uses in cybersecurity include user behaviour classification, intrusion detection systems, risk and attack analysis, and similar fields. However, in this specific domain, separate datasets often include a wide range of attributes, and the weight and expense of each attribute can differ. To add insult to injury, the entire system must function properly even if certain features are absent. Because of this, it is highly improbable that a single classification method would be able to perform effectively for all of the data sets, particularly when there are changes present and when there are limits regarding real time and scalability [5].

A system that utilises the elastic stack to not only store and evaluate data from multiple users, but also to generate a group of classifiers capable of classifying user behaviour and then efficiently identifying any anomalies in this categorization. The solution takes advantage of ELK's high-performance architecture when put into action. Using a distributed evolutionary algorithm, it sorts users according to their digital footprints collected from a mountain of logs; it runs on top of a Kubernetes-based infrastructure. Furthermore, the framework enables the detection of any user behaviour anomalies, a newly-minted duty brought about by the framework. In point of fact, the classification technique that was shown in is utilised in this context as a preliminary step for the purpose of finding possible anomalies [6]. This is accomplished by assigning a class of risk to each and every tuple that distinguishes itself from the typical behaviour of the individual or group by a predetermined threshold.

The issue of keeping tabs on user activity and using algorithms based on machine learning to decipher the resulting logs in order to forestall or identify cybercrime has recently garnered a lot of attention [7]. This interest has been reflected in the literature.

In their attempt to tackle multiple real-time anomaly detection difficulties, the authors of employ a user-centered solution that works with identity and access management (IAM) real logs [8]. Among these pressing challenges are the following: the cold start problem, heterogeneous features, and the high-class imbalance. Additionally, there are fluctuating target concepts. Two separate methods are required to detect malicious individuals and masquerade actions, according to experiments performed on the CERT insider data set. When it comes to the first scenario, it is sufficient to just identify the user. However, when it comes to the second scenario, it is essential to incorporate graph elements that describe the user context and their relationships to other entities.

Table 1: A Description of the HF User Data Collection, along with the Sources of the Data



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)	

There is extensive description of the second data set, the context-aware data set. As part of a long-term user study involving 162 smartphone users, this data set provides the information security awareness (ISA) scores that were evaluated from three data sources: surveys, mobile agent, and network traffic monitor. You may get the dataset by going here [9].

Smart cities, made possible by the proliferation of Internet-connected devices, have revolutionised city planning and development. The operational efficiency, sustainability, and overall quality of life of the people who live in these cities are all improved through the utilisation of digital linkages and a vast network of sensors [10]. Conversely, cities are now flooded with data due to the proliferation of Internet of Things devices. These data not only play an important position in the real-time operations and decision-making processes of a smart city, but they also create substantial issues, notably with regard to administration and security [11]. Among the most formidable challenges is the need to detect outliers in this urban data.

The process of discovering patterns or events that significantly depart from the normal or expected behaviour of a data set is referred to as algorithmic anomaly detection. In the context of smart cities, this work is of the utmost significance because it involves a wide range of applications. There are many different ways in which it can be utilised. The identification of manipulations in the electrical grid, the detection of cyber threats, and the anticipation of failures in significant metropolitan systems are all examples of these applications [12,13]. Not only is the early detection of anomalies valuable, but it is also vital in order to prevent unplanned interruptions, assure the safety of inhabitants, and preserve the integrity of urban systems.

The gadgets that are connected to the Internet of Things serve as nerve ends inside the complex fabric of a smart city. They continuously monitor and collect data from a wide range of urban living areas. Consumption of energy, transportation, transportation conditions, environmental circumstances, and safety are all included in these elements. A great deal of information is generated by these devices, which can be put to use to improve the management of resources, optimise urban services, and strengthen the overall resilience of urban regions. However, this influx of data also makes smart cities vulnerable to a wide range of threats, including cyberattacks, equipment failures, and natural disasters. Smart cities are becoming increasingly dependent on the internet. These hazards have the potential to result in a broad variety of consequences, some of which include disruptions in service, significant economic losses, and even the possibility of endangering human lives. As a consequence of this, the capability to identify and eliminate irregularities in real time shifts from being a technological aim to becoming an important requirement.

The objective of this research is to analyse the crucial role that anomaly detection models play in smart cities that are enabled by the Internet of Things (IoT), as well as to evaluate the effectiveness with which these models contribute to the improvement of urban systems and the safety of such systems [14]. In order to achieve this goal, research has been carried out to explore the likelihood of anomaly detection models being applicable in a number of different urban environments. In addition to this, its performance is submitted to a rigorous review, and it is compared to other methods that are already in use, which provides a comprehensive evaluation of its effectiveness. Once again, a comprehensive analysis of the benefits and drawbacks of these models is carried out, and in addition to that, a visual representation of the outcomes of the comparison is carried out [15]. The findings of this study add to a more comprehensive understanding of the ways in which anomaly detection models that are enabled by the Internet of Things (IoT) have the potential to significantly contribute to the safety and efficiency of smart cities. As a result of this contribution, the urban environment is made safer and more efficient for the people who live there, and it also makes it feasible to foresee and solve critical problems in real time [16,17].

Methodology

The use of analysts to probe attacks is laborious and costly due to the sheer volume of logs and alerts that analysts must examine. For the purpose of detecting any changes in user behaviour, each action is contrasted with the compatible baseline. Within milliseconds or less, our UBA platform can begin to compile logs detailing events pertaining to users and their session activity. Having a risk label or score that discloses human risk assigned to each user is incredibly useful and significant for security analysts when they check or monitor employees for peculiar behaviours or attacks. This assessment is based on the findings of the detection process. The architecture, which is comprised of four different components, is shown in Figure 1. Detailed explanations of each of them are provided in the following.

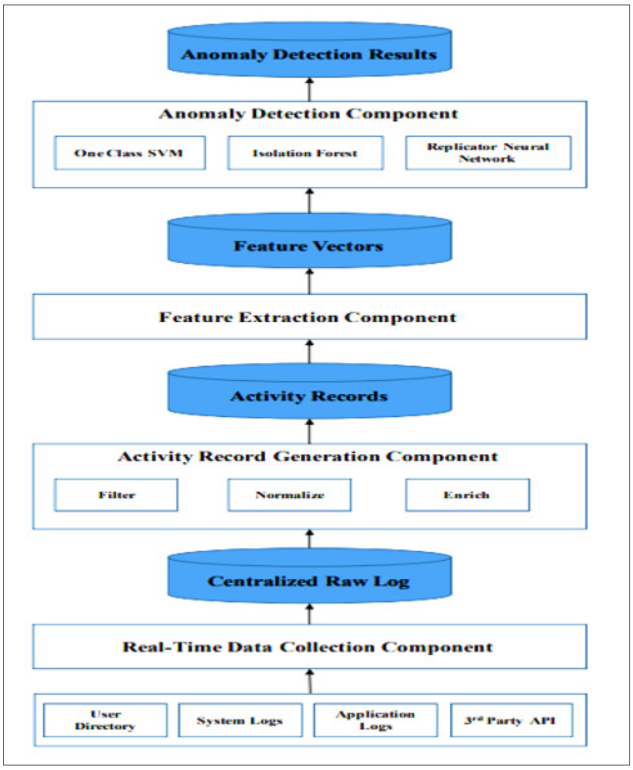

Anomaly Detection Results
Anomaly Detection Component
One Class SVM
Isolation Forest
Replicator Neural Network
Feature Vectors
Feature Extraction Component
Activity Records
Activity Record Generation Component
Filter
Normalize
Enrich
Centralized Raw Log
Real-Time Data Collection Component
User Directory
System Logs
Application Logs
3rd Party API

Figure 1: Platform Architecture for Analytics on User Behaviour

System Architecture

GRU has been proposed as a method for simulating activities carried out by insiders. It has been demonstrated in previous research that it has provided favourable outcomes for situations in which variable length input/output units are utilised, while also being architecturally straightforward and utilising a short training phase in comparison to LSTM. CERT, version r4.2, is a standard dataset that contains logs from a variety of independent sources. Using a time-based system, the events are arranged on distinct files to depict the activities of the users on a daily basis. Numerical representations, such as the aggregation of occurrence frequencies, are utilised to aggregate these events. A feature vector is the result of combining these representations. The training of the model makes use of these feature vectors. Normal data are the only ones that are included in the training set. The result of this is that the model will learn to behave in a manner that is said to as faux non-anomalous.

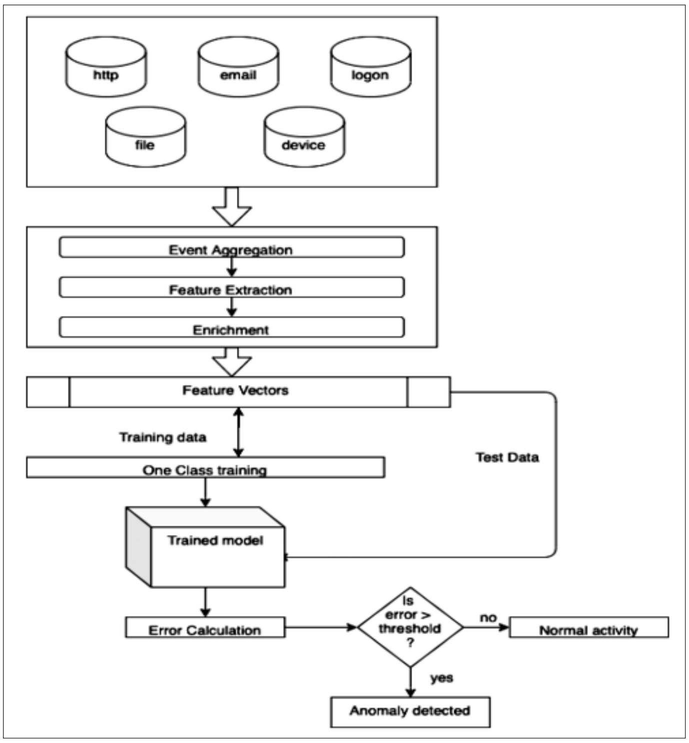


Figure 2: System Architecture

Experiment Scenario

In the case of a file server that is located within an organisation, authorised personnel are able to access the server in order to retrieve files and data with varying levels of authority, which is often specified by the administrator. It is possible, for instance, to read, write, upload, download, or delete directories or files. In order to prevent unauthorised access or rogue user activity, it is important to monitor all processes and access points. This is necessary since documents and data are valuable pieces of information.

Dataset

The data collection component that was discussed before is responsible for collecting the logs from the FTP server. Each of the eight different types of logs that are gathered correlates to one or more of the different categories of occurrences. For instance, the Download Log is solely used to represent Download Events, and it contains information such as the timestamp, the user name, the SUCCESS/FAIL flag, and the client IP address. Due to the fact that multiple events share the same format, it is impossible to differentiate between them based on the content of the UPLOAD LOG. It might stand in for a number of other events, such as a remote copy, a file or directory upload, or a file creation.

GRU Unit

LSTM models were commonly employed for time sequence-based temporal data analysis since vanilla RNN models had a number of shortcomings that needed to be addressed. A gated model structure known as GRU, which is a version of LSTM, is one in which the model utilises gated structures rather than the usual tanh value models typically used.

Results and Discussion

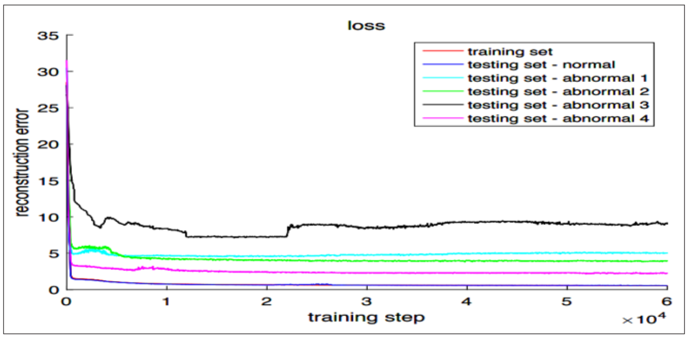


Figure 3: Standard Deviation of the Replicator Neural Network's Reconstruction Accuracy during Training

During the RNN training process, the mean reconstruction error of five different categories of test data is displayed in Figure 3. The training set contains 2.06% anomalies. During the training phase, the convergence occurred, and anomalous data had a greater reconstruction error, which allowed for the possibility of separation. The anomalous data in the testing dataset has an average reconstruction error of 4.947, 3.887, 8.627, and 2.409, while the normal data dataset has a far lower average reconstruction error of 0.539.

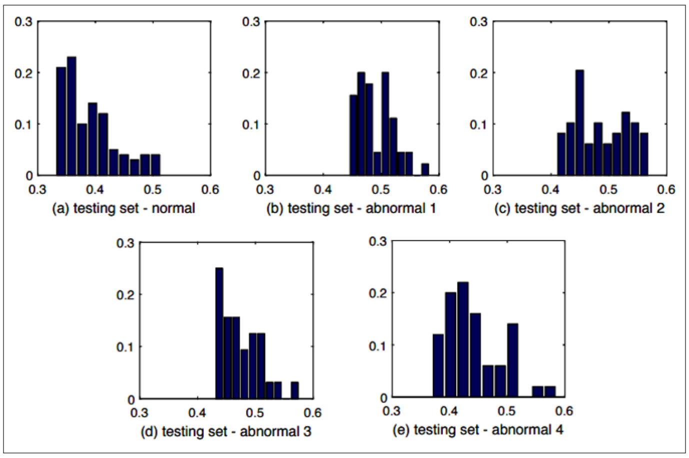


Figure 4: Isolation Forest Anomaly Score for Various Types of Test Data

The scores of some data, however, are rather similar to one another, as shown in Figure 4, particularly the data of operations that take place outside of working hours. While we were simulating each type of anomaly data, we found that just a few dimensions of the data were anomalous. Random selection is used to determine the characteristic and split point during the training stage.

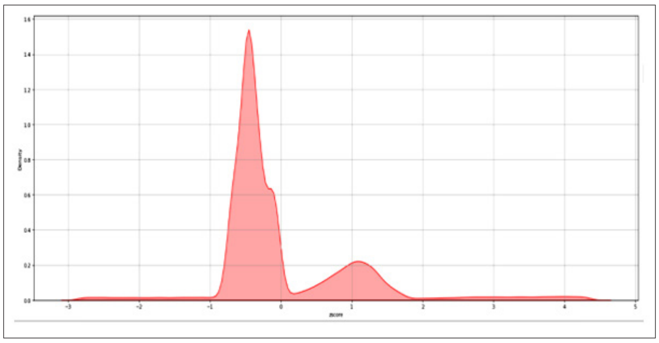


Figure 5: Data Distribution Curve for Logon

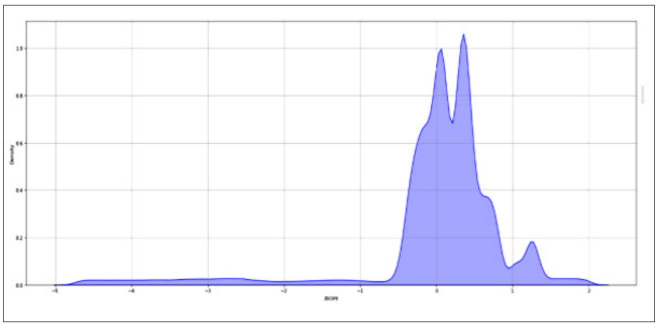


Figure 6: Cumulative Distribution of Logoffs

Table 2: Event Source and Statistics

Parameter	Values
Activation Function	ReLU
Optimizer	Adam
Learning Rate	0.001
Decay rate	1e-6
Loss Function	Mae
No.of Epoch	100
Batch Size	256

The regular office hours were specified in the data set as 9 a.m. to 5 p.m. Because of this cutoff period's inability to be strictly applied, the results were even worse. A probability distribution chart was developed in order to modify the new cutoff period. With one standard deviation, the normal was changed by three hours, from seven in the morning to seven in the evening. Afterwards, the frequency distribution table was constructed in the same multi-index data frame that also housed the composite feature table, and this table was preserved and updated there. In order to arrive at a numerical value of 0-1, the values included inside this data frame were optimised through the use of maximum normalisation. Additionally, these are depicted in figures 5 and 6,

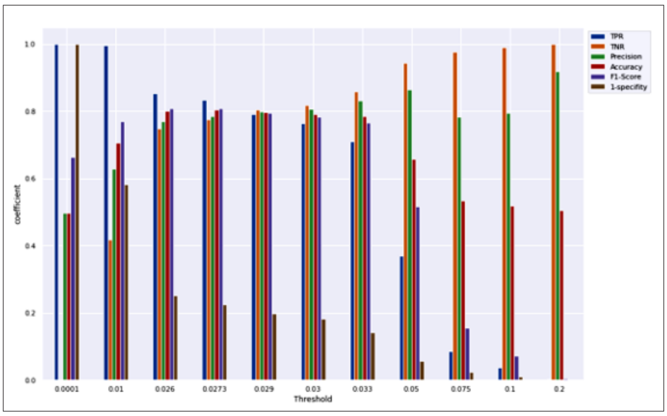


Figure 7: Model Performance at Different Threshold

Figure 8 displays the calculated values that are derived from various anomaly detection threshold values. The graphic clearly shows that the model is doing a good job of identifying unusual events at lower thresholds, but it is not very good at identifying negative values. With each successively higher threshold value, the model's ability to differentiate between the two types of data improves dramatically, reaching its peak performance at a value that is nearly 0.03.

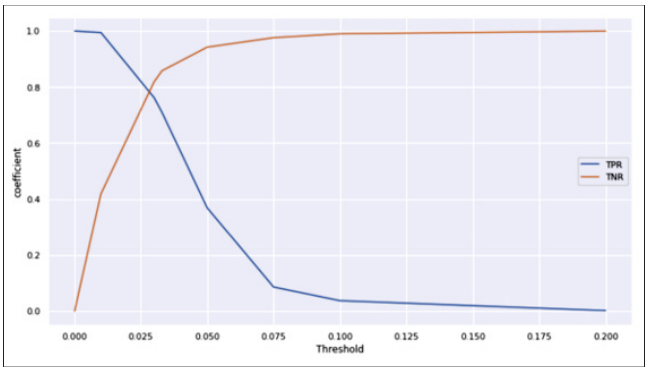


Figure 8: Optimum Threshold Calculation

The optimal classification threshold, represented by the intersection of the TPR and TNR charts, is determined using these varied values; Figure 8 shows the result. When the misclassification for both classes was minimised, the model's precision was 80.1% and the f1 score was 79.4%.

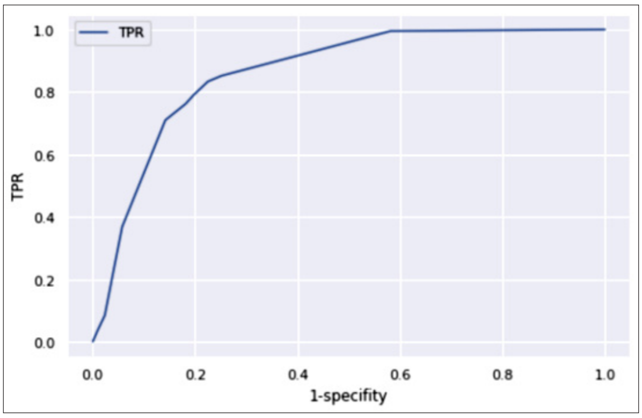


Figure 9: Curve of ROC

The area under the curve (AUC) value of 0.8732 was attained at the ideal threshold, as shown in Figure 9, which illustrates the ROC curve.

Evaluation Metrices

Table 3: Confusion Matrix

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

In order to evaluate the model, various performance metrics are computed using this table.

Recall or True Positive Rate

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

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

The Receiver's Operating Characteristic Curve At different threshold settings, the relationship between false positive rate (FPR) and recall (TPR) can be seen on a receiver operating characteristic (ROC) curve, a cost-benefit graph. A curve can be obtained by charting the values of these two quantities, which have a different relation. The model's accuracy is proportionate to the area under the curve.

Conclusions

This study demonstrates the application of one-class modelling on normal data extracted from the CERT r4.2 dataset. The model, which was trained on regular, non-malicious data, produces a large reconstruction error when dangerous samples are added to the model during testing. The approach aims to represent benign user behaviour by using GRU units in autoencoder models instead of the more common LSTM units. In order to help readers better understand how UBA works in an operational setting, this article will give a high-level description of the architecture and platform. Because it is made up of four different components that each operate separately, the platform is appropriate for use on distributed platforms like those. OCSVM, RNN, and Isolation Forest are the three components that make up the ensemble that is the anomaly detection component. The strict filtering technique is implemented, and regardless of whether or not there are abnormalities in the training set, it has the potential to improve both performance and robustness simultaneously. Anomaly identification in sequence data will be our primary focus since event sequences provide crucial information about their users. Finally, the UBA platform may eventually include the peer group analysis, which might be very useful in real-world settings.

References

1. Holger Schulze (2021) insider threat report gurukul. Cybersecurity Insiders https://www.cybersecurity-insiders.com/wp-content/uploads/2021/06/2021-Insider-Threat-Report-Gurucul-Final-dd8f5a75.pdf.
2. (2020) 5 Real-Life Examples of Breaches Caused by Insider Threats.
3. Balaram Sharma, Prabhat Pokharel, Basanta Joshi (2020) User Behavior Analytics for Anomaly Detection Using LSTM Autoencoder - Insider Threat Detection. In Proceedings of the 11th International Conference on Advances in Information Technology Bangkok Thailand 1-9.
4. 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
5. Folino G, Godano CO, Pisani FS (2022) A scalable architecture exploiting elastic stack and meta ensemble of classifiers for profiling user behaviour. In: González-Escribano A, José Daniel 1-25.
6. Garcia Torquati M, Skavhaug A, Arturo González-Escribano, Massimo Torquati (2022) 30th Euromicro International Conference on Parallel, Distributed and Network-Based Processing, PDP 2022, Valladolid, Spain. IEEE 189-196.
7. Hilal W, Gadsden SA, Yawney J (2022) Financial fraud: a review of anomaly detection techniques and recent advances. Expert Syst Appl 193: 116429.
8. Garchery M (2021) User-centered intrusion detection using heterogeneous data. PhD thesis, Universität Passau https://d-nb.info/1226425569/34.
9. Solomon A, Michaelshvili M, Bitton R, Shapira B, Rokach L, et al. (2022) Contextual security awareness: a context-based approach for assessing the security awareness of users. Knowl Based Syst 46: 108709.
10. Zaidan MA, Xie Y, Motlagh NH, Wang B, Nie W, et al. (2022) Dense Air Quality Sensor Networks: Validation, Analysis, and Benefits. IEEE Sens. J 22: 23507-23520.
11. Ullah W, Min Ullah, FU, Ahmad Khan Z, Wook Baik S (2023) Sequential Attention Mechanism for Weakly Supervised Video Anomaly Detection. Expert. Syst. Appl 230: 120599.
12. Shukla S, Thakur S, Breslin JG (2022) Anomaly Detection in Smart Grid Network Using FC-Based Blockchain Model and Linear SVM. In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Springer 13163.
13. Prathapchandran K, Janani TA (2021) Trust Aware Security Mechanism to Detect Sinkhole Attack in RPL-Based IoT Environment Using Random Forest—RFTRUST. Comput Netw 198: 108413.
14. Khatkar M, Kumar K, Kumar B (2022) Unfolding the Network Dataset to Understand the Contribution of Features for Detecting Malicious Activities Using AI/ML. Mater. Today Proc 59: 1824-1830.
15. Ullah W, Hussain T, Baik SW (2023) Vision Transformer Attention with Multi-Reservoir Echo State Network for Anomaly Recognition. Inf. Process Manag 60: 103289.
16. Alhakami W, Alharbi A, Bourouis S, Alroobaea R, Bouguila N (2019) Network Anomaly Intrusion Detection Using a Nonparametric Bayesian Approach and Feature Selection. IEEE 7: 52181-52190.
17. Prazeres N, Costa RLDC, Santos L, Rabadao C (2023) Engineering the Application of Machine Learning in an IDS Based on IoT Traffic Flow. Intell Syst Appl 17: 200189.