WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Review Paper on Different Deep Learning Methodologies for User and Entity Behavior Analytics(UEBA)

Pratik Dhaygude[a], Nilesh Dhulshette[a], Omkar Ganjale[a], Umesh Sawant[a], Prof. Pranali Navghare[b]

[a]*Student, Pune, Pune Institute of Computer Technology, 411043*
[b]*Assistant Professor, Pune, Pune Institute of Computer Technology,411043*
DOI: https://doi.org/10.55248/gengpi.4.523.42121

A B S T R A C T

Businesses are experiencing an ever-growing problem of how to identify and guard in opposition to insider threats. Users with legal access to sensitive organizational data are positioned in a role of power that can be abused and could do harm to an enterprise. This can range from monetary and intellectual property theft to the destruction of assets and enterprise reputation. Traditional intrusion detection structures are neither designed nor able to figure out those who act maliciously inside a business enterprise. In this paper, we describe an automated system capable of detecting insider threats within an enterprise. We outline a tree-shape profiling technique that includes the information on activities conducted by each user and every task after which we use this to obtain a consistent representation of functions that provide a rich description of the user's behavior. The deviation may be assessed based on the amount of variance that each user exhibits across multiple attributes, compared in opposition to their peers. The primary function of User and Entity behaviorAnalysis(UEBA) is to track normal user behaviors. UEBA defines a baseline for each entity in the environment, and actions will be evaluated by comparing with pr-defined baselines.

Keywords: User and Entity Behavior Analytics, Anomaly Detection, Deep Learning, Security

Introduction

The User and Entity Behavior Analytics (UEBA) is a type of cybersecurity technology that focuses on detecting abnormal behavior by users and entities within an organization's network. UEBA uses machine learning algorithms and statistical models to analyze vast amounts of data from various sources, such as log files, network traffic, and user activity, to identify potential security threats UEBA is designed to detect a wide range of security threats, including insider threats, account takeover attacks, and other types of malicious activity.

UEBA is important because it provides organizations with a proactive approach to cybersecurity. Rather than relying solely on reactive measures, such as firewalls and antivirus software, UEBA enables organizations to detect security threats in real-time before they cause significant damage. UEBA can also help organizations reduce the time it takes to detect and respond to security incidents, which is critical for minimizing the impact of a security breach.

Insider attacks are typically a critical security concern for businesses, as they are capable of causing extreme threats to private records and intellectual property. According to the 2019 Insider Risk Report, 68% of corporations are regularly affected by insider attacks. The intention of cyber security specialists is generally limited to protecting corporate networks from external attacks, using various preventive measures including firewalls, IDS, IPS, proxy servers, security gateways, and so on. Failure to comply with these measures will result in suspension. A valid user regularly has more rights and access to manipulate rights compared to invalid users. This raises security concerns about what security policies need to be installed to protect sensitive information if compromised by valid users.

User and Entity Behavior Analysis (UEBA) is an analytics tool based on machine learning and deep learning. UEBA model overcomes the shortcomings of the traditional systems such as adapting to escape the attacker, etc. Through statistical and time series data analysis, UEBA perceives and recognizes the minute details that humans cannot. UEBA systems typically require large amounts of data to be effective, so it's important to have a good data management strategy in place to ensure that data is collected and stored in a way that is easily accessible and can be used for analysis Additionally, it's important to have a team of skilled data scientists and security analysts who can interpret the results of machine learning models and take appropriate actions to mitigate any security threats that are identified

Recently, the topic of insider threats has received a lot of attention in the literature. Researchers have proposed several different models aimed at preventing or detecting the presence of attacks. Similarly, many works examine the psychological and behavioral characteristics of potentially threatening insiders as a means of detection. Kammüller and Probst explore how organizations can identify attack vectors based on policy violations to minimize the possibility of insider attacks. Similarly, Ogiela and Ogiela investigated how low-threshold secret sharing can be used to protect against

insider threats. For the remainder of this section, we choose to focus exclusively on research dealing with the practical aspects of designing and developing systems capable of predicting or detecting the presence of insider threats. Spitzner's early work deals with the use of honeypots (decoy machines capable of attracting attacks) to detect insider attacks. However, as security awareness increases, those who choose to carry out insider attacks are finding more subtle ways to harm or deceive their organizations, requiring more sophisticated prevention and detection. Early work by Magklaras and Furnell investigated how to estimate the level of threat likely to come from a specific insider based on a specific user behavior profile. As they acknowledge, a lot of work remains to be done to validate the proposed solution. Myers et al. considers how web server log data can be used to identify malicious insiders attempting to exploit internal systems. Maloof and Stephens propose a detection tool to detect when insiders violate the necessary knowledge constraints within an organization. Okolica et al. use probabilistic latent semantic indexing on users to identify employee interests, which are used to form a social graph that can highlight insiders. Liu et al. proposed a multi-layered framework called sensitive information dissemination detection, including network-level application identification, content signature generation and detection, and covert communication detection.

2. Related Work

For UEBA, different algorithms from machine learning to deep learning are available. Each of the techniques is used based on the need for analysis and the dataset that will be used for analysis. For an organization where timely login and logout times are recorded, Time-Series Analysis can be found useful. Time-Series Analysis is used to identify patterns that occur over time.

2.1 Machine Learning:

Machine learning algorithms can analyze large volumes of data to identify patterns and anomalies in user behavior By training a model on historical data, machine learning can learn what normal behavior looks like and identify deviations from that baseline. This can be useful in detecting insider threats or attacks from external sources that may be attempting to masquerade as legitimate users. Some common machine learning algorithms used in UEBA include decision trees, logistic regression, and neural networks. These algorithms can be used to build models that can identify anomalies in user behavior, such as unusual login patterns, unusual network activity, or unusual file access patterns.

2.1.1 Supervised Learning

Supervised learning is a common approach to building models for user and entity behavior analytics (UEBA). In supervised learning, a model is trained on labeled data, which means the data has already been classified or labeled with the correct outcomes. The model then uses this labeled data to make predictions on new, unlabeled data.

For UEBA, supervised learning can be used to identify known threats or anomalous behavior that has been previously identified and labeled. For example, a model could be trained on data that includes known indicators of an insider threat, such as an employee accessing sensitive data outside of their normal work hours or using their credentials to access data they don't normally access. The model could then be used to detect similar behavior in real-time and alert security teams to potential threats.

Some common supervised learning algorithms used in UEBA include decision trees, random forests, logistic regression, and support vector machines (SVMs). These algorithms can be trained on labeled data to predict outcomes, such as whether a particular user's behavior is normal or abnormal.

2.1.2 Unsupervised Learning

Unsupervised learning is another common approach to building models for user and entity behavior analytics (UEBA). In unsupervised learning, a model is trained on unlabeled data, which means the data does not have any predefined categories or labels. The model then uses this data to identify patterns or anomalies that are not easily visible to the human eye.

For UEBA, unsupervised learning can be used to identify unknown threats or anomalous behavior that has not been previously identified and labeled. This can be especially useful for detecting insider threats or attacks from external sources that may be attempting to masquerade as legitimate users.

Some common unsupervised learning algorithms used in UEBA include clustering algorithms, such as k-means clustering and hierarchical clustering, and anomaly detection algorithms, such as local outlier factor (LOF) and isolation forest. These algorithms can be used to group similar behavior together or identify behavior that deviates significantly from the normUnsupervised learning is particularly useful in UEBA because it can detect previously unknown or emerging threats, which may not be captured by supervised learning models.

2.1.3 Singular Value Decomposition:

To find patterns and abnormalities in data relating to user behavior or object behavior, user and entity behavior analytics (UEBA) might employ singular value decomposition (SVD) A matrix is divided into three matrices, U, S, and V, using the matrix factorization technique known as SVD. The input matrix in UEBA depicts user interactions with various objects throughout time, including servers, devices, and programmes.

It might be challenging to examine and draw conclusions from the matrix because it is frequently very vast and sparse. By highlighting the most crucial characteristics or elements, SVD can assist in reducing the matrix's dimensionality so that it can be utilized for clustering, classification, or anomaly detection.

When it comes to UEBA, SVD can be used to spot persons or entities that act strangely, including accessing private information at odd times or from strange locations, or consuming more resources than usual. SVD can also be used to spot behavioral patterns that point to particular kinds of attacks, such phishing or insider threatsOverall, SVD is a strong UEBA tool that can assist enterprises in identifying and addressing security risks and other unusual behavior

2.2 Deep Learning

Deep learning is a type of machine learning that uses artificial neural networks with n number of layers to extract features from data and make predictions. A number of applications, including computer vision, speech recognition, and natural language processing, have demonstrated deep learning's high effectiveness

Deep learning can be used to evaluate vast amounts of data and find patterns and anomalies in user behavior in the context of user and entity behavior analytics (UEBA). Deep learning models can learn to recognise intricate data patterns that can be challenging for humans to see. For instance, advanced persistent threats (APTs) and other complex attacks that may employ a number of evasive tactics can be found using deep learning.

The recurrent neural network is a popular deep learning architecture used in UEBA network (RNN). RNNs can be used to find trends and abnormalities in behavior over time when examining time series data, such as log files or network traffic. The convolutional neural network (CNN), which excels in analyzing data with a spatial or grid-like structure, such as network traffic or photographs, is another architecture frequently employed in UEBA.

2.2.1 RNN

Recurrent Neural Networks (RNNs) is a one of the neural network architecture which is commonly used in user and entity behavior analytics (UEBA).NNs can be used to find trends and abnormalities in behavior over time by examining time series data, such as log files or network traffic.

In sequential data, where the sequence of the data is crucial, RNNs are made to handle it. The network's feedback loops, which enable information to last over time, are used to do this. RNNs are effective for studying behavior over time because they can learn intricate patterns and dependencies in sequential data.

RNNs may be used in UEBA to track a user's behavior over time and spot any anomalies or suspicious patterns. For instance, data about a user's login time, the systems they access, and the commands they enter may be used to train an RNN model. The RNN might then be used to spot trends in the user's behavior that are out of the ordinary or differ from what they usually do.

2.2.2 CNN:

CNNs is a neural network architecture which can also be used for user and entity behavior analytics (UEBA) to analyze and classify patterns and anomalies in user and entity interactions. The objective of UEBA is to find trends and outliers in user and entity behavior over time. Data sequences that indicate user and entity interactions, such as login and logout timings, file access times, network traffic logs, etc., can be used to train convolutional neural networks (CNNs). These data sequences contain properties that CNNs can automatically learn and extract, such as temporal patterns, frequency distributions, and correlations between various sorts of interactions. The behavior can then be classified as normal or anomalous using the CNN's output in accordance with a predetermined set of guidelines or thresholds.

The ability of CNNs to handle highly dimensional and complicated data, such as network traffic logs or system call sequences, is one benefit of utilizing them for UEBA. Without explicit feature engineering or preprocessing, CNNs can automatically learn and extract features from different types of data. CNNs may also be used in conjunction with other deep learning models, such as LSTM networks, to better capture temporal dependencies in the data. In order to capture temporal dependencies and categorize the behavior as normal or abnormal, for instance, a CNN can be used to extract features from sequences of user interactions. These features are then fed into an LSTM network.

2.2.3 LSTM

Long Short-Term Memory (LSTM) is a kind of recurrent neural network (RNN) architecture that is commonly used in user and entity behavior analytics (UEBA). LSTMs are useful for analyzing time series data, such as log files or network traffic, and can be used to identify patterns and anomalies in behavior over time.

The vanishing gradient issue, which can arise with conventional RNNs and make it challenging for the network to learn long-term relationships in data, is addressed with LSTMs. LSTMs employ a unique memory cell that has a longer retention duration, enabling the network to learn and retain complicated patterns in input.

Input gates, output gates, and memory cells are used in conjunction by LSTMs to store and update data over time. The input and output gates regulate the information flow into and out of the memory cells, while the memory cells enable the LSTM to retain significant information from prior encounters.

LSTMs can be trained on sequences of data representing user and entity interactions, and can learn to classify the behavior as normal or anomalous based on a predefined set of rules or thresholds. LSTMs can also be combined with other deep learning models, such as CNNs or autoencoders, to capture different types of features and improve the accuracy of anomaly detection

One of the main advantage of using LSTMs for UEBA is the ability to handle noisy data, outliers and incomplete data, such as missing log entries or corrupted data. LSTMs can automatically learn to impute missing data and handle noisy data, without the need for manual pre-processing or cleaning

2.2.4 Improved LSTM-GaN

Improved LSTM-GAN is a combination of LSTM and GaN used for user and entity behavior analytics (UEBA) to generate synthetic data that can be used to augment the original dataset and improve the efficiency and accuracy of anomaly detection models. In UEBA, the aim is to detect patterns and anomalies in the interactions between users and entities over the time. But, the amount of data available for analysis is often limited, and it may be difficult to detect rare or unusual events.

Improved LSTM-GAN can be used to generate synthetic data that is similar to the original data, but contains additional variations and anomalies that can help to improve the performance of UEBA models. The generator network can be trained on the original data to learn the patterns and dependencies between the variables, while the discriminator network can be trained to distinguish between real and syntheticdata.

Once trained, the generator network may be used to produce fresh data sequences that can be added to the original dataset. Next, using the enhanced dataset, clustering or classification algorithms can be trained or enhanced. For testing and validation reasons, as well as to replicate situations that are challenging or impossible to observe in real life, improved LSTM-GAN can also be used to create synthetic data. This can be especially helpful in cybersecurity, where it's critical to evaluate how well UEBA models defend against a variety of potential dangers. Improved LSTM-GAN is a powerful tool for UEBA that can help organizations to increase the accuracy and effectiveness of their anomaly detection models, and to better understand and respond to security threats and other anomalous behavior.

2.2.5 Real-Time Anomaly Detection In Streaming Heterogeneity (RADISH)

RADISH can also be used for user and entity behavior analytics (UEBA) to identify anomalies and patterns in real-time interactions of user and entity. In UEBA, the aim is to detect patterns and anomalies in the behavior of users and entities over real time. RADISH can be used to monitor and analyze interactions of user and entity in real-time, like login and logout times, file access times, network traffic logs, and so on.

RADISH can be configured to handle a variety of data sources and can instantly adjust to shifting data patterns. The platform can be tailored to meet the unique requirements of various businesses and applications, and its anomaly detection algorithms may dynamically adapt in response to fresh data and security analysts' feedback.

To find anomalies in real-time user and entity behavior, RADISH employs statistical analysis and machine learning approaches. A machine learning model, such as a neural network or decision tree, that has been trained to find abnormalities in the data is then given the pre-processed data. Depending on the availability of labelled data, the model can be trained using both supervised and unsupervised learning techniques. When an anomaly is found, RADISH creates an alert and transmits it to a dashboard or monitoring system so that security analysts can evaluate it and take appropriate action.

3. Results Published In Previous Papers

Equations and formulae should be typed in Mathtype, and numbered consecutively with Arabic numerals in parentheses on the right hand side of the page (if referred to explicitly in the text). They should also be separated from the surrounding text by one space.

Table 1 : Survey Table

Sr. No.	Dataset Used	Algorithm/Approach	Performance
[5]	CERT insider threat dataset	LSTM	90.17% Accuracy
[4]	Custom 18-month LDAP from a company	Improved LSTM-GaN	Accuracy highest at 128 hidden layers i.e. 91.14%
[3]	DARPA ADAMS	real-time anomaly detection in streaming heterogeneity (RADISH)	50% of all malicious sessions are detected and about 92\% of sessions that are flagged malicious are actually benign.
[6]	CMU-CERT, Enron email dataset, sample data by Centre for the Protection of	Tree based profiling using standard deviation in the mahalanobis distance	42% Precision and 100% Recall

	National Infrastructure (CPNI), and in-house generated data		
[7]	Custom in-house generated	Singualar Value Decomposition	False Positive Rate at 2.2%

Acknowledgements

We would like to take this opportunity to thank our guide Prof. PranaliNavghare for giving us all the help and guidance we needed. We are really grateful to her for her kind support. Her valuable suggestions were very helpful. We are also grateful to Dr. G.V. Kale, Head of Department of Computer Engineering, and Dr. S. T. Gandhe, Principal, Pune Institute of Computer Technology for their indispensable support and suggestions.

References

[1] M. Shashanka, M. -Y. Shen and J. Wang, "User and entity behavior analytics for enterprise security," 2016 IEEE International Conference on Big Data (Big Data), 2016, pp. 1867-1874, doi: 10.1109/Big-Data.2016.7840805.

[2] R. Sommer and V. Paxson. Outside the closed world: On using machine learning for network intrusion detection. In Security and Privacy (SP), 2010 IEEE Symposium on, pages 305–316. IEEE, 2 .

[3] B. B¨ose, B. Avasarala, S. Tirthapura, Y. -Y. Chung and D. Steiner, "Detecting Insider Threats Using RADISH: A System for Real-Time Anomaly Detection in Heterogeneous Data Streams," in IEEE Systems Journal, vol. 11, no. 2, pp. 471-482, June 2017, doi: 10.1109/JSYST.2016.2558507. [4] Haowei Liu 2021 J. Phys.: Conf. Ser. 1994 012021 DOI 10.1088/1742-6596/1994/1/012021.

[5] Balaram Sharma, Prabhat Pokharel, and 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 (IAIT2020). Association for Computing Machinery, New York, NY, USA, Article 5,1–9. https://doi.org/10.1145/3406601.3406610 .

[6] P. A. Legg, O. Buckley, M. Goldsmith and S. Creese, "Automated Insider Threat Detection System Using User and Role-Based Profile Assessment," in IEEE Systems Journal, vol. 11, no. 2, pp. 503-512, June 2017, doi: 10.1109/JSYST.2015.2438442.

[7] Yousef, Rasheed and Jazzar, Mahmoud. (2021). Measuring the Effectiveness of User and Entity Behavior Analytics for the Prevention of Insider Threats. Xi'an JianzhuKejiDaxueXuebao/Journalf Xi'an University of Architecture and Technology. XIII. 175-181.10.37896/JXAT13.10/313918.

[8] A. Saaudi, Z. Al-Ibadi, Y. Tong and C. Farkas, "Insider Threats Detection Using CNN-LSTM Model," 2018 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2018, pp. 94-99, doi: 10.1109/CSCI46756.2018.00025.

[9] Machine Learning; Investigators from Dalhousie University Release New Data on Machine Learning (Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning)[J]. Journal ofEngineering,2020.

[10] LeCun Y, Bengio Y, Hinton GE.Deep Learning. Nature[J].2015,521(7553):436-444.

[11] Schmidhuber J. Deep Learning in Neural Networks: An Overview. Neural networks[J]. 2015,61:85-117.

[12] Bengio Y, Courville A, Vincent P. Represent action Learning: A Review and New Perspectives[C]. IEEE TPAMI,20 13,35(8):1798-1828.

[13] Yu Y ,Canales S . Conditional LSTM-GAN for Melody Generation from Lyrics[J]. 2019.

[14] JingxianYang,ShuaiZhang,YueXiang,JichunLiu,JunyongLiu,XiaoyanHan,Fei Teng. LSTM auto-encoder based representative scenario generation method for hybrid hydro-PV power system[J]. IET Generation,Transmission & Distribution,2020,14(24).

[15] Malhotra Pankaj, Anusha Ramakrishnan, Gaurangi Anand, LovekeshVig, Puneet Agarwal, and Gautam Shroff, LSTM-based encoder-decoder for multi-sensor anomaly detection. arXiv preprint arXiv:1607.00148(2016).

[16] Insider Threat Test Dataset. (November 2016). Retrieved March 6, 2020 from https://resources.sei.cmu.edu/library/assetview.cfm?assetid=508099.

[17] Fangfang Yuan, Yanan Cao, Yanmin Shang, Yanbing Liu, Jianlong Tan, and Binxing Fang. 2018. Insider Threat Detection with Deep Neural Network. Lecture Notes in Computer Science Computational Science –ICCS 2018(2018), 43–54.

[18] Iffat A. Gheyas and Ali E. Abdallah. 2016. Detection and prediction of insider threats to cyber security: a systematic liteRature review and meta-analysis. Big Data Analytics1, 1 (2016). DOI:http://dx.doi.org/10.1186/s41044-016-0006-0.

[19] Ali H. Mirza and Selin Cosan. 2018. Computer network intrusion detection using sequential LSTM Neural Networks autoencoders. 2018 26th Signal Processing and Communications Applications Conference (SIU) (2018).

[20] Pang, G., Shen, C., Cao, L., &Hengel, A. V. D. (2021). Deep Learning for Anomaly Detection. ACM Computing Surveys, 54(2), 1–38. doi:10.1145/3439950.

[21] Davide Abati, Angelo Porrello, Simone Calderara, and Rita Cucchiara. 2019. Latent space autoregression for novelty detection. In CVPR. 481–490.

[22] Charu C. Aggarwal. 2017. Outlier Analysis. Springer.

[23] SametAkcay, Amir Atapour-Abarghouei, and Toby P. Breckon. 2018. GANomaly: Semi-supervised anomaly detection via adversarial training. In ACCV. Springer, 622–637.

[24] Leman Akoglu, Hanghang Tong, and Danai Koutra. 2015. Graph based anomaly detection and description: A survey. Data Min. Knowl. Discov. 29, 3 (2015), 626–688.

[25] Elie Aljalbout, Vladimir Golkov, Yawar Siddiqui, Maximilian Strobel, and Daniel Cremers. 2018. Clustering with deep learning: Taxonomy and new methods. arXiv:1801.07648.

[26] J. Andrews, Thomas Tanay, Edward J. Morton, and Lewis D. Griffin. 2016. Transfer representation-learning for anomaly detection.

[27] Fabrizio Angiulli, Fabio Fassetti, Giuseppe Manco, and Luigi Palopoli. 2017. Outlying property detection with numerical attributes. Data Min. Knowl. Discov. 31, 1 (2017), 134–163.

[28] Fabrizio Angiulli, Fabio Fassetti, and Luigi Palopoli. 2009. Detecting outlying properties of exceptional objects. ACM Trans. Database Syst. 34, 1 (2009), 1–62.

[29] Fabrizio Angiulli and Clara Pizzuti. 2002. Fast outlier detection in high dimensional spaces. In PKDD. Springer, 15–27.

[30] Martin Arjovsky, SoumithChintala, and L´eon Bottou. 2017. Wasserstein generative adversarial networks. In ICML.214–223.

[31] TerjeAven. 2016. Risk assessment and risk management: Review of recent advances on their foundation. Eur. J. Operat. Res. 253, 1 (2016), 1–13.

[32] Fatemeh Azmandian, AyseYilmazer, Jennifer G. Dy, Javed A. Aslam, and David R. Kaeli. 2012. GPU-accelerated feature selection for outlier detection using the local kernel density ratio. In ICDM. IEEE, 51–60.

[33] Kevin Bache and Moshe Lichman. 2013. UCI machine learning repository. Retrieved from http://archive.ics.uci.edu/ml.

[34] YoshuaBengio, Aaron Courville, and Pascal Vincent. 2013. Representation learning: A review and new perspectives.IEEE Trans. Pattern Anal. Mach. Intell. 35, 8 (2013), 1798–1828.

[35] Paul Bergmann, Michael Fauser, David Sattlegger, and Carsten Steger. 2019. MVTec AD–A comprehensive realworld dataset for unsupervised anomaly detection. In CVPR. 9592–9600.

[36] Insider Threat Report 2020, Cyber Insiders https://www.cybersecurityinsiders.com/wpcontent/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pd

37] S. Khaliq, Z. U. Abideen Tariq and A. Masood, "Role of User and Entity Behavior Analytics in Detecting Insider Attacks," 2020 International Conference on Cyber Warfare and Security (ICCWS), 2020, pp. 1-6, doi: 10.1109/ICCWS48432.2020.9292394.

[38] A. Salitin and A. H. Zolait, "The role of User Entity Behavior Analytics to detect network attacks in real time," 2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), 2018, pp. 1-5, doi: 10.1109/3ICT.2018.8855782.

[39] M. Raut, S. Dhavale, A. Singh and A. Mehra, "Insider Threat Detection using Deep Learning: A Review," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 856-863, doi: 10.1109/ICISS49785.2020.9315932.

[40] P. Goyal and K. Gupta, "Supervised Learning Approach for User and Entity Behavior Analytics," 2020 3rd International Conference on Computing and Communications Technologies (ICCCT), 2020, pp. 1-6, doi: 10.1109/ICCCT49228.2020.9269224

[41] N. R. Pandit and V. M. Thakare, "An Overview of Supervised Learning Algorithms for User and Entity Behavior Analytics," 2021 7th International Conference on Advanced Computingand Communication Systems (ICACCS), 2021, pp. 782-787, doi: 10.1109/ICACCS51225.2021.9375201.

[42] R. Zhang, J. Zhang, and Y. Jia, "A Survey on Unsupervised Learning for User and Entity Behavior Analytics," 2021 IEEE 5th Information Technology and Mechatronics Engineering Conference (ITOEC), 2021, pp. 237-242, doi: 10.1109/ITOEC51615.2021.00055.

[43] J. Datta, R. Dasgupta, S. Dasgupta and K. R. Reddy, "Real-Time Threat Detection in UEBA using Unsupervised Learning Algorithms," 2021 5th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech), Kolkata, India, 2021, pp. 1-6, doi: 10.1109/IEMENTech53263.2021.9614848.