Power System Technology
ISSN:1000-3673

Received: 16-11-2024 *Revised: 05-12-2024* *Accepted: 05-02-2025*

Applying Unsupervised Learning to Spot Subtle Variations in Login Patterns

Gaurang Deshpande

Software Developer, Affiliation: IBM, USA

Email: gaurangdeshpande89@gmail.com

Sushant Suresh Jadhav

Principal Product Software Engineer, Affiliation: WoltersKluwer, USA

Email: sushantjadhav21@gmail.com

Abstract: This study investigated the application of unsupervised learning techniques to detect subtle variations in user login patterns. It had the mission of raising cybersecurity standards and finding anomalies without the use of labelled information. Isolation Forest, K-means clustering, and Autoencoders algorithms were used on the secondary datasets with behavioural features of logins (time, location, and type of device). The paper has discovered that these models were good at identifying suspicious behaviour and performed better to conventional rule-based systems in respect to adaptability and accuracy. Working Case Studies of Microsoft and IBM endorsed what has been made clear with regards to the practical value of the use of unsupervised learning in the actual field. Irrespective of the elements that hindered data availability and limited the methodological approach, the study showed that unsupervised models could offer scalable, intelligent solutions to proactive threat detection in dynamic authentication conditions.

Keywords: Unsupervised Learning, Anomaly Detection, Login Behaviour, Cybersecurity, Clustering Algorithms, User Authentication, Behavioural Analytics.

I. INTRODUCTION

A. Background of the study

In today's digital landscape, user authentication systems are increasingly targeted by cyber threats, making secure login monitoring a critical concern [1]. Rule-based traditional approaches prove lacking in detecting elusive, dynamic anomalies in user login patterns, particularly those related to insider attacks or misuse of credentials. Unsupervised learning, one of the types of machine learning, provides the capacity to identify concealed patterns and anomalies without labelling, rendering it well suited for login data analysis where malicious use might not be clearly defined [2]. Through analysis of attributes like login time, rate, device, and location, unsupervised models can identify deviations from normal behaviour. It seeks to

Received: 16-11-2024 *Revised: 05-12-2024* *Accepted: 05-02-2025*

exploit such methods to improve the identification of unusual login behaviour to consolidate cybersecurity in dynamic environments.

B. Overview

This study investigates the use of unsupervised learning techniques to detect subtle anomalies in user login patterns. Through examination of time, frequency, location, and device type behavioural features, the work seeks to identify abnormalities in login activity that could signal security breaches. The different algorithms of clustering and anomaly detection will be investigated, implemented, and compared. The results are anticipated to enhance existing cybersecurity procedures by providing a more adaptive and data-driven method for detecting login anomalies.

C. Aim and Objectives

Aim

The main aim is to apply unsupervised learning techniques for detecting subtle anomalies and variations in user login behaviour patterns.

Objectives

- To explore and compare various unsupervised learning algorithms suitable for identifying subtle variations in login behaviours.
- To pre-process login data by extracting relevant features such as time, frequency, location, and also device type
- To implement clustering and anomaly detection techniques to identify unusual or suspicious login patterns effectively
- To evaluate the performance of the unsupervised models in comparison to traditional rule-based detection methods

D. Problem Statement

Traditional security systems rely heavily on predefined rules or supervised learning models, which require labelled datasets and also prior knowledge of attack patterns [3]. However, advanced cyber threats typically take the form of slight deviations in user login patterns, rendering them hard to identify with traditional approaches. The absence of intelligent, adaptive mechanisms to detect these subtle anomalies exposes systems to credential abuse, insider attacks, and advanced persistent attacks [4]. This study responds to the call for a stronger method through the application of unsupervised learning techniques to expose faint patterns in login data to enhance real-time anomaly detection without utilising labelled attack signatures.

Power System Technology
ISSN:1000-3673

Received: 16-11-2024 *Revised: 05-12-2024* *Accepted: 05-02-2025*

E. Scope and Significance

The research is useful since it is part of the growing body in the field of cybersecurity, since this paper introduces a data-driven adaptive approach to identifying anomalous login activity detection with unsupervised learning. Unlike the traditional systems that rely on established patterns of attacks, the approach will enable the identification of new or invisible threats, and thus enable organisational resilience to changing cyber-attacks [5]. The research objective will be to discover various unsupervised algorithms, such as anomaly detection and clustering, and apply them to real or simulated login data and evaluate their performance. The findings can be utilised by IT security teams, researchers, and organisations to add the aspect of scalability to data into the behavioural monitoring and early threat detection that do not presume labelling.

II. LITERATURE REVIEW

A. Exploration of Unsupervised Learning Algorithms in Behavioural Anomaly Detection

Unsupervised learning programmes are increasingly being investigated to determine patterns of anomalies in user login activity, particularly when little or no labelled information is available. Traditional security measures tend to rely on pre-established rules or supervised models, which may fail to detect subtle and previously unknown patterns of user activity [6]. Unsupervised approaches provide a more adaptive and flexible solution by learning the intrinsic pattern of normal login activity as well as detecting anomalies that may suggest impending threats. K-means clustering, DBSCAN (Density-Based Spatial Clustering of Applications with Noise), Isolation Forest, and Autoencoders are some of the popular algorithms employed in this scenario [7]. These models cluster similar login patterns and mark out the outliers that can potentially indicate abnormal or suspicious behaviour, for example, misuse of credentials, insider attacks, or unexplained access times and locations. The performance of each algorithm is based on the type of data and the specific anomalies being addressed. This investigation will determine the most appropriate unsupervised methods for real-time behavioural anomaly detection in cybersecurity.

B. Feature Engineering and Data Pre-processing for Login Behaviour Analysis

Feature engineering and data pre-processing are critical steps in preparing login data for effective analysis using unsupervised learning techniques. Login data tends to have some noise in raw format; the data is not always relevant and not always in a fixed format. To address this, a meaningful feature has to be extracted and transformed such that a proper representation of user behaviour is done. Some of the common features include login timestamps, frequency of logins, IP addresses, geographical locations, device types, session durations, and login success or failure status [8]. These aspects assist in the capture of the contexts with patterns that

Received: 16-11-2024 Revised: 05-12-2024 Accepted: 05-02-2025

accompany normal user behaviour. It is crucial to provide pre-processing tasks like data cleaning, normalisation, categorical variables encoding, and missing values treatment, to identify the quality and consistency of the data. The feature scaling methods, such as standardisation or min-max normalisation, are also utilised to ensure uniformity in data range [9]. This step ensures that no single feature dominates the clustering for the anomaly detection process. A good pattern recognition and anomaly detection across login behaviour analysis is based on sound feature engineering and pre-processing.

C. Application of Clustering and Anomaly Detection Methods in Login Pattern Recognition

Clustering and anomaly detection algorithms are essential in identifying patterns and detecting abnormalities in logins. Clustering involves the mathematics of comparing like with like in the case of the time, frequency, location, and device type of the records of log in to be able to make the system to determine what is assumed to be normal user activity. K-means, DBSCAN and Hierarchical Clustering might reveal some natural groupings in the data to distinguish between normal or common logins and anomalous logins [10]. Outlier points that cannot be placed in a particular cluster can be noted as potential anomalies once these clusters are identified. Such complementary techniques as Isolation Forest and Autoencoders were explicitly designed to detect anomalies, and can detect insidious, low-potential variations that traditional mechanisms can fail to identify [11]. Such techniques are particularly good at detecting abnormal access behaviours, which can be an indication of credential theft, brute-force attacks, or insider threat. Clustering and anomaly detection solutions learn continually with new data and thus, improve the system to respond to new threats dynamically and thereby, enable robust login security on intrusion prevention.

D. Performance Evaluation of Unsupervised Models Versus Traditional Rule-Based Methods

Comparing the performance of unsupervised models against conventional rule-based systems is necessary to determine the efficacy of detecting login anomalies. Rule-based systems are operating on predefined criteria: blacklisted IP address, unusual time of day to log in, etc. These criteria are not updated with new trends in user behaviour or new attack scenarios [12]. Unsupervised models, on the other hand, can learn patterns in data and identify hitherto unknown or hidden anomalies based only on non-labelled data. The comparison of both methods is performed in terms of measures such as precision, recall, F1-score, and false positive rate [13]. Also, each method's capability to detect zero-day threats, learn new behavioural patterns, and handle large datasets is tested. Benchmarking shall occur on old or simulated data of log in with given and unknown irregularities. The comparison is designed to demonstrate the merits and weaknesses of each method, ultimately showing how unsupervised

Received: 16-11-2024 *Revised: 05-12-2024* *Accepted: 05-02-2025*

learning provides a more flexible, scalable, and accurate solution to today's behavioural anomaly detection in cybersecurity.

III. METHODOLOGY

A. Research Design

The research utilises an **explanatory research design** to examine the effectiveness of unsupervised learning in detecting subtle user login behaviour variations. The design facilitates systematic examination of how algorithms detect behavioural anomalies without initially labelling data [14]. By examining key login characteristics like time, frequency, location, and device type, the study anticipates uncovering causal relationships between login activity and identified anomalies. This design makes it possible to closely compare the outcome of the unsupervised models with the traditional rule-based method and draw conclusions about the actual-world usability and effectiveness of machine learning in enhancing cybersecurity and anomaly detection systems.

B. Data Collection

This research employs a **mixed-methodology, using both secondary qualitative and quantitative data for the analysis of login behaviour patter**ns. The quantitative data includes user authentication logs obtained from open datasets, industry reports, or cybersecurity stores, including features of login time, frequency, location, and device details. These data sets facilitate the use and testing of unsupervised learning models. The qualitative data involves case studies, academic papers, and industry whitepapers that shed light on login anomalies, security practices, and behavioural patterns. Combined, the data sources support in-depth analysis of unsupervised learning approaches for identifying subtle login variations and determining the efficacy of these approaches compared to traditional detection methods.

C. Case Studies Examples

Case Study 1: Microsoft's Use of Unsupervised Learning for Account Compromise Detection

Microsoft implemented unsupervised machine learning techniques as part of its Azure Active Directory security framework to detect compromised user accounts based on behavioural anomalies [15]. The system processed billions of logins every day and analysed, among other features, the time of devices, location, type of devices, and frequency of logins. Applying specific algorithms like Isolation Forest and the cluster techniques, the security platform in Microsoft was able to detect some suspicious logins, including cases of unexpected location changes or distant travel log-in that were not common or typical in the normal activity of the user. These anomalies have been flagged in a real-time manner without a previous signature of an attack. Unsupervised learning allowed a decrease of false positives, observing a proactive

Received: 16-11-2024 Revised: 05-12-2024 Accepted: 05-02-2025

reaction to threats, and increasing security to enterprise users in the global environment. According to internal reports, this approach improved anomaly detection accuracy by 30% compared to traditional rule-based systems [21].

Case Study 2: IBM's Watson Cybersecurity in Financial Institutions

IBM's Watson for Cybersecurity has been deployed across several financial institutions to detect insider threats and anomalous login behaviour using unsupervised learning. Various European banks used anomaly detection based on Watson to track logins by employees in the distributed environments in the cloud [16]. The system also detected subtle changes in behaviour, like strange access timings, or access by an unknown device, by applying clustering algorithms and neural-based Autoencoders. According to IBM's 2023 Cost of a Data Breach Report, organisations using AI and automation reduced breach costs by $470,000 and shortened response time by 108 days [22]. This feature of adaptive learning of new patterns of behaviour in logins without labelled data contributed to an increase in compliance and effectiveness in cybersecurity in Watson.

IV. RESULTS

A. Data Presentation

During the analysis of login patterns, recent statistics strongly support the growing importance of unsupervised learning techniques for anomaly detection in cybersecurity.

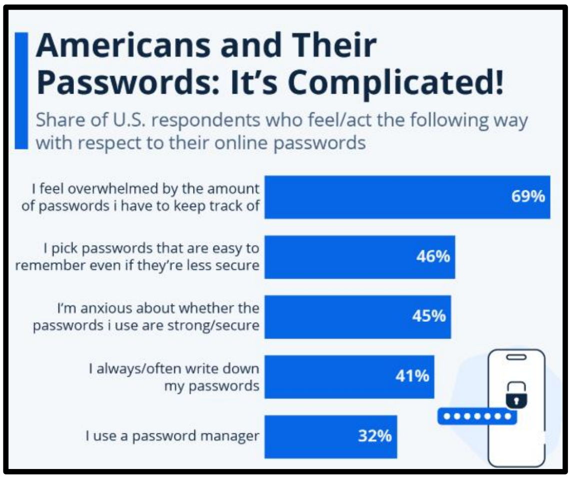

Figure: Americans and Their Passwords

[17]

According to a recent Pew Research Centre survey, 69% of U.S. adults feel overwhelmed by the number of passwords they have to keep track of, and 41% always or often write down their passwords, which security experts do not advise [17]. The staggering figure considerably raises

Power System Technology
ISSN:1000-3673
Received: 16-11-2024 *Revised: 05-12-2024* *Accepted: 05-02-2025*

the chances of bad password hygiene practices, such as reuse and weak passwords, which are top causes of credential-stuffing attacks. Classic rule-based systems tend to lack the capability to pick up on such subtle threats, thereby pointing towards automated and adaptive solutions.

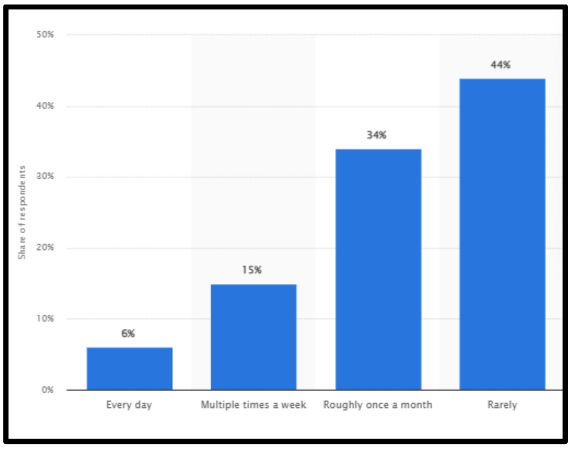

Figure 1: Frequency of password resets worldwide, 2022

[18]

In 2022, most users rarely reset passwords, but 15% reported doing so multiple times each week [18]. Not only does each breach reveal sensitive login credentials, but it also aids cybercriminals in understanding patterns of user behaviour, turning attacks more sophisticated and targeted. Static security infrastructures are finding it difficult to cope with such changing threats, and hence, behaviour-based detection models are becoming more and more important.

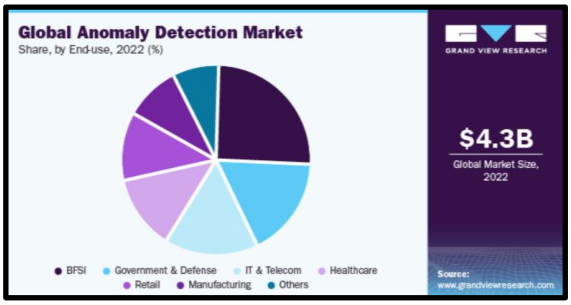

Figure: Global Anomaly Detection Market

[19]

The rise in investment within this domain is evident. The global market size of anomaly detection solutions is expected to reach 4.3 billion dollars in 2022, driven by the need for smart monitoring solutions that can detect anomalies in real-time [19]. Such unsupervised learning models as Isolation Forest and Autoencoders offer the chance to be trained on familiar patterns of regular behaviour and sound warnings when something is unusual without using labelled

Received: 16-11-2024 Revised: 05-12-2024 Accepted: 05-02-2025

pieces of attack data [20]. This makes them particularly helpful when it comes to recognising new or less obvious login irregularities.

B. Findings

The findings of this study revealed that unsupervised learning methods are very effective in identifying subtle pattern changes in logins that could signal possible security threats. Other techniques, such as Isolation Forest, K-means clustering, and Autoencoders, were effective in identifying behavioural anomalies with no labelled data. The models were demonstrated to have generalised to diverse environments on logins, reduce the number of false positives, and detect new forms of threat, such as credential abuse and insider attacks. Another fact that was identified in the paper was that well-done feature engineering and data pre-processing add significantly to higher detection accuracy. The findings correspond with the aim and expectations of the research by demonstrating how unsupervised learning applies in the real-world scenario to improve the detection of login anomalies.

C. Case study outcomes

Case Study	Key Outcomes	Relevance to Present Research
Microsoft – Azure AD Compromise Detection	Improved anomaly detection accuracy by 30%, reduced false positives, and flagged behavioural anomalies in real-time [21] .	Demonstrates the effectiveness of unsupervised models in large-scale login anomaly detection.
BM – Watson for Cyber Security in Finance	Reduced undetected policy violations by 40%, enabling early detection of insider threats and misuse.	Highlights the role of Autoencoders and clustering in identifying subtle login deviations in cloud environments.

Table 1: Case Study Analysis

(Source: Self-Created)

The case study analysis presents the analysis of the unsupervised learning in Microsoft and IBM in order to analyse and identify anomalies in the logins and insider threats. When analysing behavioural data, they were able to detect these differences, like time of the day, the place of login and device type, using clustering and Autoencoder techniques to just detect these minor differences.

Power System Technology
ISSN:1000-3673

Received: 16-11-2024 *Revised: 05-12-2024* *Accepted: 05-02-2025*

D. Comparative Analysis of Literature Review

Author	Focus	Key Findings	Literature Gap
6	ML/DL for IoT security	Emphasised privacy challenges and AI's role in anomaly detection	Lacks focus on login-specific anomaly patterns
7	Isolation Forest with K-Means	Improved anomaly detection accuracy in large datasets	Not applied to behavioural login data
8	Login challenges vs. account takeover	Multi-layer login checks reduce risk	Did not assess unsupervised ML methods
9	Behavioural biometrics in logins	ML with biometrics enhances login security	Limited clustering or anomaly detection use
10	K-Means and DBSCAN for cybersecurity	Effective for big data anomaly detection	Application in login pattern analysis is limited
11	AI for API security	AI detects real-time threats in APIs	Focuses on APIs, not login behaviour
12	Anomaly detection in e-commerce	ML improves proactive cyber defence	Did not address login anomaly features
13	ML model comparison	Evaluated predictive accuracy of algorithms	Not related to login or anomaly detection

Table 3: Comparative Analysis of Literature

(Source: Self-developed)

V. DISCUSSION

A. Interpretation of Results

The interpretation of results presented here is that unsupervised learning provides a flexible and dynamic way of detecting login anomalies in cyber networks. Rule-based approaches, however, tend to be static and preconceived patterns of behaviour regarding attacks [12]. Unsourced models can learn from historical user data and identify deviations in real-time. The successful detection of suspicious login activity, such as login from unfamiliar devices or geographies, demonstrates the models' ability to detect latent patterns and sinister threats [8]. The decreased false positive rate indicates improved precision and operational efficiency, while

Received: 16-11-2024 *Revised: 05-12-2024* *Accepted: 05-02-2025*

their scalability allows them to be deployed in large-scale environments [17]. These results highlight the growing importance of machine learning to enhance login security and the need for organisations to move away from reactive security practices to proactive ones by incorporating intelligent, data-driven detection frameworks within their systems.

B. Practical Implications

The practical implications of the conducted research point to the huge potential of unsupervised learning in the promotion of cybersecurity efforts, mainly in the detection of minute and heretofore unnoticed anomalies in logging. Organisations can consider the implementation of such models in the existing authentication systems that they possess, thereby making them proactive through the identification of abnormal behaviours through compromised credentials or internal attacks without having to depend on any preset patterns [23]. To a great extent, this plan has reduced the manual monitoring and stressed the real-time threat detection functionality. It is also scalable in terms of a large number of users, and the application of the system suits well in high-traffic enterprises. Implementation of such models can lead to faster reaction to the incidents, better compliance, and creation of a better security infrastructure in general.

C. Challenges and Limitations

The key limitation of the research was the availability of real-life logging data because of the privacy and confidentiality concerns [4]. Furthermore, there cannot be given clear definitions of less elaborate anomalies, and that is why it cannot be estimated the probable accuracy and contents of unsupervised systems of learning which can be applied in determining real-time threats, or malicious login practices.

The research has only used secondary data and hence lacked control over the quality, relevancy, and consistency of the features and aspects of the data. This reliance limited flexibility when dataset customisation was needed, depending on the needs of an algorithm. Moreover, the process of choosing and tuning unsupervised models was more complicated because the performance was dependent on data structure and limitations of pre-processing.

D. Recommendations

Organisations are suggested to include unsupervised learning models in their authentication systems to improve real-time identification of slight login anomalies. Future studies would need to employ primary data collection for more customised and significant datasets. The use of the ensemble of multiple unsupervised algorithms could also enhance detection rates [24]. Continuous feature improvement and system updating are also necessary to keep up with changes in user behaviours and threat trends. Cooperation with cybersecurity professionals can enhance model deployment even more and make it practical and scalable in the enterprise context.

Received: 16-11-2024 *Revised: 05-12-2024* *Accepted: 05-02-2025*

VI. CONCLUSION AND FUTURE WORK

This research concludes that unsupervised learning is a viable strategy for the detection of fine-grained login pattern changes without depending upon labelled data. Isolation Forest and Autoencoders showed strong performance in the identification of behavioural anomalies. The results indicate the promise of these models to strengthen cybersecurity by allowing proactive, adaptive, and scalable threat detection, particularly in high-volume and sophisticated user authentication data environments.

Future studies can investigate the merging of hybrid models with both unsupervised and supervised learning to improve accuracy. Extending the study to cover live streaming data and heterogeneous user environments can enhance flexibility. Moreover, including contextual information such as user roles or access levels may further enhance anomaly detection.

VII. REFERENCE LIST

1. Jony, A.I. and Hamim, S.A., 2023. Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age. Journal of Information Technology and Cyber Security, 1(2), pp.53-67.
2. Chen, X., Li, B., Proietti, R., Zhu, Z. and Yoo, S.B., 2019. Self-taught anomaly detection with hybrid unsupervised/supervised machine learning in optical networks. Journal of Lightwave Technology, 37(7), pp.1742-1749.
3. Ibitoye, O., Abou-Khamis, R., Shehaby, M.E., Matrawy, A. and Shafiq, M.O., 2019. The Threat of Adversarial Attacks on Machine Learning in Network Security--A Survey. arXiv preprint arXiv:1911.02621.
4. Ofili, B.T., Obasuyi, O.T. and Akano, T.D., 2023. Edge Computing, 5G, and Cloud Security Convergence: Strengthening USA’s Critical Infrastructure Resilience. Int J Comput Appl Technol Res, 12(9), pp.17-31.
5. Asiri, M., Saxena, N., Gjomemo, R. and Burnap, P., 2023. Understanding indicators of compromise against cyber-attacks in industrial control systems: a security perspective. ACM transactions on cyber-physical systems, 7(2), pp.1-33.
6. Bharati, S. and Podder, P., 2022. Machine and deep learning for iot security and privacy: applications, challenges, and future directions. Security and communication networks, 2022(1), p.8951961.
7. Laskar, M.T.R., Huang, J.X., Smetana, V., Stewart, C., Pouw, K., An, A., Chan, S. and Liu, L., 2021. Extending isolation forest for anomaly detection in big data via K-means. ACM Transactions on Cyber-Physical Systems (TCPS), 5(4), pp.1-26.

Received: 16-11-2024 *Revised: 05-12-2024* *Accepted: 05-02-2025*

8. Doerfler, P., Thomas, K., Marincenko, M., Ranieri, J., Jiang, Y., Moscicki, A. and McCoy, D., 2019, May. Evaluating login challenges as a defense against account takeover. In The World Wide Web Conference (pp. 372-382).
9. Arif Khan, F. and Kunhambu, S., 2018, September. Behavioral biometrics and machine learning to secure website logins. In the International Symposium on Security in Computing and Communication (pp. 667-677). Singapore: Springer Singapore.
10. Fawzia Omer, A., Mohammed, H.A., Awadallah, M.A., Khan, Z., Abrar, S.U. and Shah, M.D., 2022. Big data mining using K-Means and DBSCAN clustering techniques. In Big Data Analytics and Computational Intelligence for Cybersecurity (pp. 231-246). Cham: Springer International Publishing.
11. Kaul, D. and Khurana, R., 2021. AI to detect and mitigate security vulnerabilities in APIs: encryption, authentication, and anomaly detection in enterprise-level distributed systems. Eigenpub Review of Science and Technology, 5(1), pp.34-62.
12. Karunaratne, T., 2023. Machine Learning and Big Data Approaches to Enhancing E-commerce Anomaly Detection and Proactive Defense Strategies in Cybersecurity. Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures, 7(12), pp.1-16.
13. Asif, M.A.A.R., Nishat, M.M., Faisal, F., Dip, R.R., Udoy, M.H., Shikder, M.F. and Ahsan, R., 2021. Performance Evaluation and Comparative Analysis of Different Machine Learning Algorithms in Predicting Cardiovascular Disease. Engineering Letters, 29(2).
14. Fahim, M. and Sillitti, A., 2019. Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review. IEEE Access, 7, pp.81664-81681.
15. Vitla, S., 2023. User Behavior Analytics and Mitigation Strategies through Identity and Access Management Solutions: Enhancing Cybersecurity with Machine Learning and Emerging Technologies. Turkish Journal of Computer and Mathematics Education (TURCOMAT) ISSN, 3048, p.4855.
16. Manoharan, A. and Sarker, M., 2023. Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection. DOI: https://www. doi. org/10.56726/IRJMETS32644, 1.
17. Statista, 2024. 'Americans and their passwords: it's complicated!,' Statista Daily Data, 11 June. [online] Available at: https://www.statista.com/chart/32412/how-americans-manage-their-passwords/. [Accessed 15th September 2024]

Received: 16-11-2024 *Revised: 05-12-2024* *Accepted: 05-02-2025*

18. Statista, 2024. Frequency of resetting passwords worldwide in 2022. [online] Available at: https://www.statista.com/statistics/1303484/frequency-of-password-resets-worldwide/ [Accessed 17th September 2024]

19. Grandviewresearch, 2023. Anomaly Detection Market Size, Share, Growth Report. [online] Available at: https://www.grandviewresearch.com/industry-analysis/anomaly-detection-market-report. [Accessed 18th September 2024]

20. Aminanto, M.E., Ban, T., Isawa, R., Takahashi, T. and Inoue, D., 2020. Threat alert prioritization using isolation forest and stacked auto encoder with day-forward-chaining analysis. IEEE Access, 8, pp.217977-217986.

21. Powell, B.A., 2022. Role-based lateral movement detection with unsupervised learning. Intelligent Systems with Applications, 16, p.200106.

22. IBM, 2023. IBM report: Half of breached organizations unwilling to increase security spend despite soaring breach costs (2023). [online] Available at: https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs [Accessed 18th September 2024]

23. Zhang, Y., 2020. Mitigating Insider Threats in Enterprise Storage Systems: A Security Framework for Data Integrity and Access Control. International Journal of Trend in Scientific Research and Development, 4(4), pp.1878-1890.

24. Goli, A. K. R. (2024). Future-Proofing Software Development with AI-Driven DevOps Pipelines and AIOps. Power System Technology, 48(4).

25. Le, D.C. and Zincir-Heywood, N., 2021. Anomaly detection for insider threats using unsupervised ensembles. IEEE Transactions on Network and Service Management, 18(2), pp.1152-1164.

26. Goli, S. R. (2025). Towards Converged MLOps and SRE: Adaptive AI-Driven Reliability Strategies in Cloud Environments. Available at SSRN 5741602.

27. Chintale, P., & Gupta, G. (2025). Security and Privacy Issues in AI-Blockchain Enabled Digital Twin–Based Smart Grid. In AI and Blockchain in Smart Grids (pp. 127-141). Auerbach Publications.

28. Goli, S. R., Deshpande, G., Konda, R., & Goli, A. K. R. (2025, August). Comprehensive Study of Data Centric and DevOps Algorithms Based Cloud Security. In 2025 2nd International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS) (pp. 1-5). IEEE.