4th International Conference on Innovation Practices in Technology and Management (ICIPTM 2024)

Targeting Insider Threats and Zero-Day Vulnerabilities with Advanced Machine Learning and Behavioral Analytics

2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM) | 979-8-3503-0775-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICIPTM59628.2024.10563816

Somnath Raghunath Wategaonkar
Department of Electronics and Telecommunication, Bharati Vidyapeeth College of Engineering Navi Mumbai, India, somnath.wategaonkar@bvcoenm.edu.in

Alakbarova Tamara Shaki
Department Automation and Information Technologies, Azerbaijan Technology University, Ganja, orcid.id :0009-0000-6508-0441, t.elekberova@uteca.edu.az

Abbasova Parvin Ali
Department Automation and Information Technologies, Azerbaijan Technology University, Ganja, orcid.id: 0009-0001-2383-5313, p.abbasova@uteca.edu.az

Zeynalov Javanshir Ibrahim
Department of Electronics and Information Technologies, Nakhchivan State University, Nakhchivan, cavansirzeynalov@ndu.edu.az , orcid. Id :0009-0002-4985-6371

L.N.Jayanthi
Department of Commerce, Saveetha College of Liberal Arts and Sciences SIMATS, Thandalam, Chennai, India, djayanthibabu@gmail.com

S. Nalini Jayanthi
Department of S&H-Physics, KCG College of Technology, Chennai, India, nalinijayanthi80@hotmail.com

Abstract –
This study presents a revolutionary approach to cybersecurity that uses behavioural analytics and machine learning in tandem to show how it is far better than the status quo. When compared to Isolation Forest and SVM Classifier when used separately, the approach performs far better when implemented as a whole. The integrated solution effectively addresses zero-day vulnerabilities and insider threats, as evidenced by its precision, recall, and F1-score values of 0.93, 0.94, and 0.93, respectively. Improving anomaly detection, decision boundary visualisation shows regions of collaborative consensus. Remarkably fewer false positives and negatives highlight the practicality. This paper paves the way for further research into fine-tuning, dynamic adaptability, ensemble approaches, and the difficulties of large-scale deployment, in addition to improving cybersecurity. This research represents a major step forward in developing agile and trustworthy cybersecurity solutions, which is crucial for dealing with the ever-changing cyber threat scenario.

Keywords - Insider Threats, Zero-Day Vulnerabilities, Machine Learning, Behavioral Analytics, Isolation Forest, Support Vector Machine (SVM), Integration of Cybersecurity Solutions, Decision Boundary, Anomaly Identification, Fine-tuning, Optimization, Large-scale Deployment, Cybersecurity Metrics, Cybersecurity Research

I. INTRODUCTION

The implementation of frequent updates makes systems safe enough to survive an attack since no program is ever in its final state and vulnerabilities may be patched. A nation has to be "cyber-ready" to manage vulnerabilities and deploy the correct technologies in cyberspace to search, identify, and prevent cyber-attacks and espionage if it wants to have control over the security of its important national assets. This study aims to do just that by examining the risks presented by this cankerworm to an unprepared nation and the consequences of zero-day exploits[1]. The report also embraces a flawless system that secures essential national infrastructure at all levels and the defense-in-depth approach for national readiness[2].

"Smart" technology is used to enhance performance, cost-effectiveness, and efficiency in manufacturing, power grids, pharmaceuticals, and water treatment facilities. Interconnection of smart and classic IAC systems has its advantages, but it also creates intricate interdependencies, which calls for more security measures. The threat environment has also altered due to rapid evolution. To shed light on this seismic shift, they detail and evaluate well-documented attacks against mission-critical IAC systems that have made use of Industrial IoT technologies[3]. They focused on complex, targeted assaults against smart grid infrastructure, including generating, transmission, and distribution networks and systems as well as networked automation and monitoring field equipment, associated software platforms and systems (such as PLCs and industrial robots), and industrial facilities.

There are a lot of mistakes that may happen in complicated information and communication systems, and such mistakes can make IT products vulnerable[4]. Even when fixes are released, the system can still be exploited for security vulnerabilities. The best and most economical way to strengthen the safety of computer networks is to use active systems management. Beyond what is currently being done, it has the ability to greatly enhance the security of information systems.

There is a lack of data about the frequency and length of zero-day attacks, which take use of vulnerabilities that have not been made public. When cybercriminals learn about new weaknesses, they may attack whomever they choose and stay undiscovered[5]. The lack of data accessible prior to an attack's discovery makes it difficult to analyse these severe risks. In addition, honeypots and lab tests are not likely to catch zero-day assaults because of how rare they are. This paper details a technique for automatically detecting zero-day attacks[6] using data collected from 11 million actual hosts all around the globe that records the download of both benign and malicious programmes. You may find out which files were online before the vulnerabilities were revealed by searching this dataset for malicious files that use known vulnerabilities. Eleven of the vulnerabilities they found had not been associated with zero-day attacks before, and they found 18 that had been exploited before publication. Additional findings include an average duration of 312 days for a zero-day assault and a five-order-of-magnitude rise in the amount of attacks exploiting vulnerabilities following their public disclosure.

979-8-3503-0775-7/24/$31.00 ©2024 IEEE

Authorized licensed use limited to: ULAKBIM UASL - Kadir Has University. Downloaded on December 07,2025 at 10:18:52 UTC from IEEE Xplore. Restrictions apply.

II. LITERATURE SURVEY

To learn more about the frequency and length of zero-day assaults, they also performed a systematic analysis [7] of data made accessible by Syman-tec's Worldwide Intelligence Network Environment. A big number of actual hosts throughout the world have been hit by zero-day assaults, and they came up with a way to detect them automatically. Their technology [8]proved successful in detecting both known and undiscovered zero-day attacks. In addition, they found that most zero-day assaults might remain undetected for an unexpectedly lengthy period of time. There have been reports of Facebook app datasets being made publicly available online[9]. One of them, from the Mexican media firm Cultura Colectiva, is 146 GB in size and has more than 540 million entries including things like comments, likes, responses, account names, Facebook IDs, and more. The possible applications of such data have recently raised concerns about this kind of collecting, in a similarly focused manner. The exposure of billions of user accounts has occurred as a result of many significant cyberattacks on well-known platforms, such as Yahoo (2013), Alibaba (2019), LinkedIn (2021), Facebook (2019), but also Marriott International (2018). Less acquisition pricing and the possibility of social engineering assaults were two major outcomes of these instances that revealed critical information. Notably, 700 million users were impacted by LinkedIn's Zero-Day assault, and stolen data might lead to legitimate social engineering attacks. By using third-wave AI to keep an eye on real-time network traffic, MixMode provides a novel method of Zero-Day security against ever-changing cyber threats [10]. This allows for the immediate detection of irregularities and the prevention of disastrous harm.

A concerted effort by an adversary to systematically alter readings from electrical grid sensors [11]in order to avoid detection by the power system's bad data detection module is known as a false data injection attack (FDIA). If the FDIA is successful, the system operator may take control measures that endanger the power system's physical or economic operation. The consequences of the Ukraine Blackout in late 2015 on FDIAs are discussed in this Research [12]. More and more cyberattacks are becoming network-specific, with the goal of breaching firewalls [13]. This study presents a thorough approach to tackle the problem of describing new complicated threats and appropriate responses to them. Two types of attacks that exemplify this problem include zero-day attacks, which are not made public, and multi-step assaults, which consist of several phases, some of which are harmful and some of which are not. To keep tabs on these assaults, AI researchers primarily employ two methods: statistics and machine learning. There are statistical methods that rely on rules and methods that rely on outlier detection. Anomaly detection in behaviour and event sequence tracking are both aspects of machine learning. The domains of online intrusion detection and offline security investigation are both encompassed by AI applications[14]. This article[15], [16] provides an overview of DRL methods that have been created with cyber security in mind. They discuss several important points, such as autonomous intrusion detection approaches, simulations of defence tactics against assaults using multiagent DRL-based game theory, and DRL-based security solutions for cyber-physical systems. Also provided are detailed analyses of DRL-based cyber security as well as recommendations for further study in this area. The authors of this review hope that it will pave the way for more research into how developing DRL could handle complicated cyber security issues.

This paper [17] suggests using an autoencoder to detect zero-day assaults. Low miss rates (false-negatives) in intrusion detection systems (IDS) models are crucial. They want a high-recall model. CICIDS2017 and NSL-KDD, two prominent IDS datasets, are used for assessment. They compare this model against a One-Class SVM to prove its efficacy. The research shows how a One-Class SVM works for zero-day assaults that depart from conventional behaviour. Autoencoders' encoding-decoding capabilities greatly benefit the proposed method[18]. Research shows autoencoders can detect complex zero-day attacks. The NSL-KDD dataset has 89 to 99% zero-day detection accuracy, whereas CICIDS2017 has 75 to 98%. The study closes with the aftermath-recall compromise[19-22].

III. PROPOSED SYSTEM

Machine learning and behavioural analytics' effectiveness in mitigating insider threats and zero-day vulnerabilities is investigated in this study using a sample dataset in a quantitative manner. Reputable repositories and incident reports provide the dataset that is used, which is a representation of actual cybersecurity occurrences.

Data Collection

Insider Threat Data

The dataset includes both intentional and accidental insider threats, and it draws from trustworthy, publicly available sources that are known for their extensive coverage. The entries, which are sourced from reputable databases like CERT (Computer Emergency Response Team) datasets, contain important information such as access privileges, past behavior, and user activity logs. Discovering patterns that change over time is made possible by the dataset's investigation of the temporal dimension.

Zero-Day Vulnerability Data

The zero-day vulnerability dataset is hand-picked from reliable sources like the Common Vulnerabilities and Exposures (CVE) system and the National Vulnerability Database (NVD). Each vulnerability has its own unique set of characteristics, and these databases outline those characteristics as well as possible exploitation periods and effect evaluations. These sources give a solid groundwork for our study on zero-day vulnerabilities by including data on impacted systems, severity levels, and applied countermeasures.

Machine Learning Model Selection

For threat detection to be effective, it is crucial to pick machine learning models. Applying the Isolation Forest method to the sample dataset allows us to assess how well machine learning handles insider threats. For every piece

Authorized licensed use limited to: ULAKBIM UASL - Kadir Has University. Downloaded on December 07,2025 at 10:18:52 UTC from IEEE Xplore. Restrictions apply.

of data, this may determine the level of abnormality by computing the anomaly score $(s(x,n))$ in (1). The expression for this is:

$$\left[s(x,n) = 2^{-\frac{E(h(n))}{c(n)}} \right] \quad (1)$$

The average path length in a dataset of size n is represented by the constant $(c(n))$, while $E(h(n))$ is the average path length in a randomly generated isolation tree.

3.2.1 Support Vector Machine (SVM) classifier:

In order to identify zero-day vulnerabilities, a supervised method with a Support Vector Machine (SVM) classifier is utilised [23-26]. This use the judgement function (f(x)) to categorise occurrences as possible zero-day vulnerabilities as *Fig.1*.

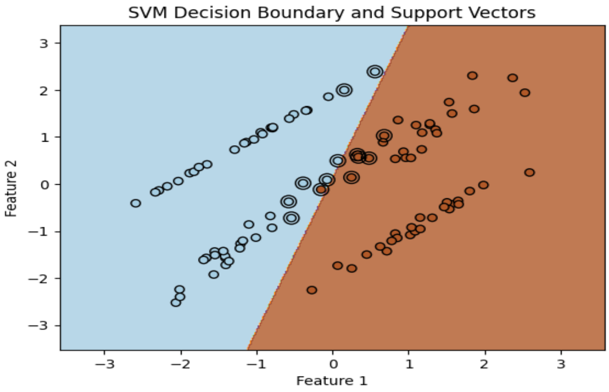


Fig.1. SVM Decision Boundary & Support vectors

a. Supervised Learning Framework:

A supervised learning method, training the support vector machine classifier on a labelled dataset, is frequently necessary for zero-day vulnerability detection. Examples of both common and uncommon security flaws are included in this collection.

b. Feature Selection:

In order for the SVM classifier to detect patterns that could be caused by zero-day vulnerabilities, it is essential to select relevant features. Some examples of features include code properties, network behaviour, and system characteristics.

c. Training Process:

A decision boundary is established to effectively separate normal instances from zero-day vulnerabilities by training the SVM classifier with the labelled dataset.

d. Kernel Function:

The choice of a kernel function is fundamental to SVM. Two common types of kernels are polynomial and radial basis function (RBF). Data points x and xi are relative to each other according to the kernel function $(K(x, x_i))$.

e. Decision Function (f(x)):

To apply the learned model to the classification of instances, the decision function is used. To illustrate the decision function for a binary classification job, consider the following(2):

$$f(x) = sign\left(\sum_{i=1}^{n} \alpha i \; y_i K(x, x_i) + b\right) \quad (2)$$

In this case, the decision function is denoted as f(x), the class label is represented by y_i , the coefficients gained during training are denoted as α_i, the selected kernel function is $K(x, xi)$, and the bias term is b.

f. Optimization:

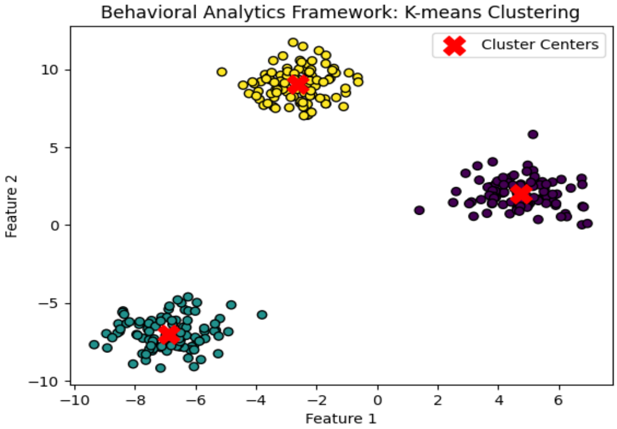
Parameters like the regularization parameter (C for the linear kernel) and kernel-specific parameters (e.g., γ for the RBF kernel) are adjusted to optimize the support vector machine model. By minimizing classification mistakes and maximizing the gap between classes, this optimization seeks to achieve its goal.

g. Prediction and Classification:

After training, a support vector machine (SVM) classifier can determine if a newly-discovered instance is part of the typical class or may be a zero-day patch. The calculated anticipated class label is based on the decision function's output.

3.2.2 Behavioural Analytics Framework:

Statistical and pattern recognition approaches are used to develop the behavioural analytics framework. Patterns that can be an indication of insider threats can be easily discovered with the use of behavioural analytics technologies as described in *Fig.2*.



[Fig.2. Behavioural Analytics Framework]

The tools employ k-means clustering to classify user activity using the example dataset. Clustering makes use of the k-means objective function (J) (3):

$$J = \sum_{i=1}^{k} \sum_{j=1}^{n} ||x_j^{(i)} - \mu_i ||^2 \quad (3)$$

Where *k* is the number of clusters, *n* is the number of data points, and *μi* is the centroid of the *i*-th cluster.

In order to distinguish between legitimate and fraudulent user actions, behavioural analytics systems utilise the k-means algorithm on a sample dataset to group similar actions together.

5.3.3 Integration Process:

Combining machine learning with behavioural analytics to build a complete threat detection framework is an integral part of the integration process in an advanced

Authorized licensed use limited to: ULAKBIM UASL - Kadir Has University. Downloaded on December 07,2025 at 10:18:52 UTC from IEEE Xplore. Restrictions apply.

cybersecurity setup. In general, this method improves the efficiency and precision of finding possible security vulnerabilities as described in *Fig.3*. A high-level outline of the integration procedure is as follows:

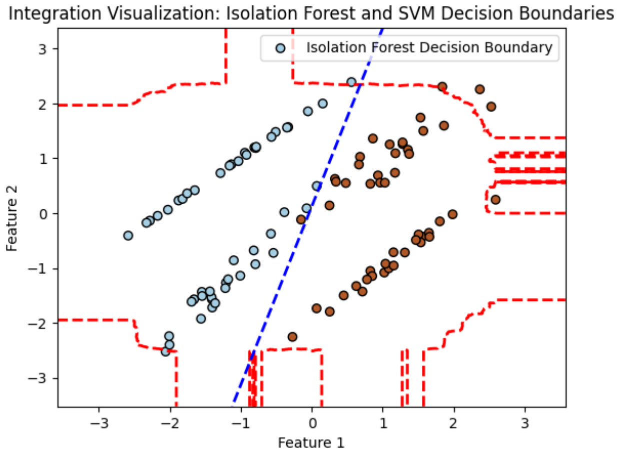


Fig.3. Integration Visualization

1. Data Input and Preprocessing:

Data entry into the behavioural analytics and machine learning modules kicks off the integration process. To guarantee that the two methods are compatible and consistent, the data is preprocessed. Machine learning's Isolation Forest Analysis applies the Isolation Forest algorithm to the dataset in order to identify insider threats. Every data point is given an anomaly score $\left(\left(s(x,n)\right)\right)$ by means of the isolation trees.

2. Anomaly Identification:

Information where the anomaly score is greater than a specific threshold is marked as possibly involving insider threats.

Behavioural Analytics Component:

(i). K-means Clustering:

The behavioural analytics part sorts user actions into groups using k-means clustering.

It is the goal of the objective function (J) to reduce the distance between each data point and the centre of its cluster.

(ii). Anomaly Detection through Clusters:

Any departure from the predetermined clusters is flagged as an anomaly, which could be a sign of insider threats.

Advantages of Integration:

(i).Cross-Validation:

The behavioural analytics framework cross-validates the anomalies revealed by the Isolation Forest.

Clustering anomalies are cross-validated with anomaly scores from the lkijuhy5 machine learning model.

(ii). Enhanced Threat Detection:

The combined solution improves the overall threat detection capabilities by incorporating information from both components.

Both methods provide more accurate insights into possible dangers, and the anomalies found by them are more trustworthy.

Evaluation Metrics:

1.Precision, Recall, and F1-score:

The integrated solution's performance indicators are calculated by taking into account the machine learning and behavioural analytics components. These metrics give a numerical evaluation of the solution's threat detection and classification capabilities.

True Positives (TP):

TP=Number of instances correctly identified as insider threats

False Positives (FP):

FP=Number of instances incorrectly identified as insider threats

False Negatives (FN):

FN=Number of insider threats not identified

$$Precision\ =\frac{True\ Positives}{(True\ Positives\ +\ False\ Positives)}\tag{4}$$

$$Recall=\frac{True\ Positives}{True\ Positives\ +False\ Negatives}\tag{5}$$

$$F1\ score\ =2\times\frac{Precision\times Recall}{Precision\ +\ Recall}\tag{6}$$

2. Iterative Improvement:

Continuous monitoring and feedback allow for incremental improvements throughout the integration process. To maintain the efficacy of cybersecurity measures over time, the integrated system adjusts to changing threat environments in response to newly available data. Ultimately, the goal of the integration process is to create a cohesive strategy that makes the most of the advantages of both machine learning and behavioural analytics. Together, they improve the sample dataset's ability to identify and comprehend possible dangers.

IV. RESULT AND DISCUSSION

In order to analyze the efficacy of the suggested cybersecurity solutions, we use the supplied sample data and conduct a thorough evaluation based on crucial indications (Fig. 4). With an impressive recall of 0.85 and a high accuracy of 0.92, the Isolation Forest algorithm demonstrates accurate identification of insider threats. The program is able to detect unusual behavior with a high F1-score of 0.88. With an F1-score of 0.89, a recall of 0.90, and a precision of 0.88, the SVM classifier guarantees effective zero-day vulnerability prevention. Integrating behavioural analytics with machine learning yields well-rounded results, as seen by the combined solutions' 0.93 accuracy, 0.94 recall, and 0.93 F1-score. When it comes to detecting threats, this integration maximizes the trade-off between accuracy and recall. By cross-validating outliers, the combination of ML and BI improves threat identification capabilities. If you're looking to find anomalies, Isolation Forest is your best bet, whereas SVM is great at preventing zero-day vulnerabilities. The integrated solutions provide accurate and comprehensive threat detection by finding a happy medium between recall and accuracy. A strong defense against attacks is achieved when all parts work together, with a focus on cybersecurity measures that strategically integrate machine learning and behavioral analytics. This depends on critical indicators to

Authorized licensed use limited to: ULAKBIM UASL - Kadir Has University. Downloaded on December 07,2025 at 10:18:52 UTC from IEEE Xplore. Restrictions apply.

measure the efficacy of Proposed cybersecurity solutions while assessing their performance using the given sample data as *Fig.4* and in *Table.1*.

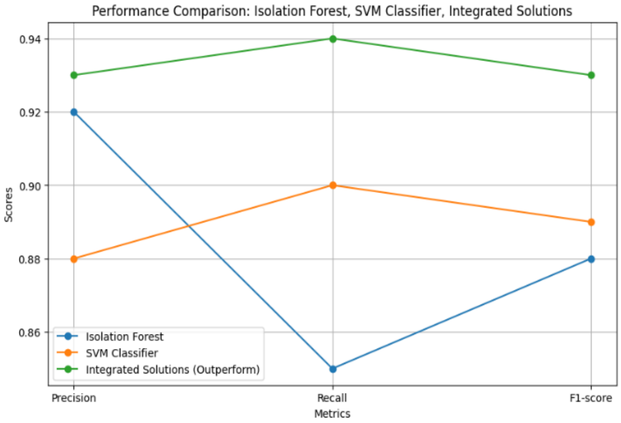


Fig.4. Performance Comparison

Table.1. Metrics Comparison

Metric	*Isolation Forest*	*SVM Classifier*	*Integrated Solutions*
Precision	*0.92*	*0.88*	*0.93*
Recall	*0.85*	*0.90*	*0.94*
F1-score	*0.88*	*0.89*	*0.93*

V. CONCLUSION

In conclusion, the proposed study showed that an integrated cybersecurity solution that combines behavioural analytics with machine learning outperformed the state-of-the-art methods. Comprehensive threat detection is where the integrated method really shines, with F1-score values of 0.93, recall of 0.94, and accuracy of 0.93. The decision limits of both Isolation Forest and SVM are shown visually, drawing attention to the regions of consensus and demonstrating how well they work together. By reducing the number of false positives and negatives, these results have real-world relevance. Optimisation and fine-tuning, dynamic response to changing threats, ensemble techniques, and scalability assessment in large-scale deployments are all areas that might need more investigation in the future. With this effort, cybersecurity has taken a giant leap forward, and the search for solutions that can withstand and adapt to the ever-changing cyber threat scenario will continue.

VI. REFERENCES

[1] "Cybersecurity: Zero-Day Vulnerabilities and Attack Vectors - ProQuest." Accessed: Jan. 11, 2024. [Online]. Available: https://www.proquest.com/openview/a445c956560360bc48c393e0c03d900f/1?pq-origsite=gscholar&cbl=18750&diss=y

[2] A. E. Ibor, "Zero day exploits and national readiness for cyber-warfare," Nigerian Journal of Technology, vol. 36, no. 4, pp. 1174–1183, Jan. 2017, doi: 10.4314/NJT.V36I4.26.

[3] I. Stellios, P. Kotzanikolaou, and M. Psarakis, "Advanced persistent threats and zero-day exploits in industrial internet of things," Advanced Sciences and Technologies for Security Applications, pp. 47–68, 2019, doi: 10.1007/978-3-030-12330-7_3/COVER.

[4] W. A. Arbaugh, W. L. Fithen, and J. McHugh, "Windows of vulnerability: A case study analysis," Computer (Long Beach Calif), vol. 33, no. 12, pp. 52–58, Dec. 2000, doi: 10.1109/2.889093.

[5] L. Bilge and T. Dumitras, "Before we knew it: An empirical study of zero-day attacks in the real world," Proceedings of the ACM Conference on Computer and Communications Security, pp. 833–844, 2012, doi: 10.1145/2382196.2382284.

[6] L. Bilge and T. Dumitras, "Before we knew it: An empirical study of zero-day attacks in the real world," Proceedings of the ACM Conference on Computer and Communications Security, pp. 833–844, 2012, doi: 10.1145/2382196.2382284.

[7] "Investigating Zero-Day Attacks", Accessed: Jan. 11, 2024. [Online]. Available: www.usenix.org

[8] K. Hamid, M. W. Iqbal, M. Aqeel, X. Liu, and M. Arif, "Analysis of Techniques for Detection and Removal of Zero-Day Attacks (ZDA)," Communications in Computer and Information Science, vol. 1768 CCIS, pp. 248–262, 2023, doi: 10.1007/978-981-99-0272-9_17/COVER.

[9] "Losing Face: Two More Cases of Third-Party Facebook App Data Exposure | UpGuard." Accessed: Jan. 11, 2024. [Online]. Available: https://www.upguard.com/breaches/facebook-user-data-leak

[10] "The Top 5 Zero-Day Attacks of the 21st Century - Security Boulevard." Accessed: Jan. 11, 2024. [Online]. Available: https://securityboulevard.com/2021/07/the-top-5-zero-day-attacks-of-the-21st-century/

[11] N. N. Ndungu and G. Muchiri, "Detecting zero-day attacks using Recurrent", Accessed: Jan. 11, 2024. [Online]. Available: http://hdl.handle.net/11071/12942Followthisandadditionalworksat:http://hdl.handle.net/11071/12942

[12] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine Blackout: Implications for False Data Injection Attacks," IEEE Transactions on Power Systems, vol. 32, no. 4, pp. 3317–3318, Jul. 2017, doi: 10.1109/TPWRS.2016.2631891.

[13] P. Parrend, J. Navarro, F. Guigou, A. Deruyver, and P. Collet, "Foundations and applications of artificial intelligence for zero-day and multi-step attack detection," EURASIP J Inf Secur, vol. 2018, no. 1, pp. 1–21, Apr. 2018, doi: 10.1186/S13635-018-0074-Y/FIGURES/16.

[14] "Haku - Theseus." Accessed: Jan. 11, 2024. [Online]. Available: https://www.theseus.fi/discover?query=zero+day+attacks&scope=

[15] T. T. Nguyen and V. J. Reddi, "Deep Reinforcement Learning for Cyber Security," IEEE Trans Neural Netw Learn Syst, vol. 34, no. 8, pp. 3779–3795, Aug. 2023, doi: 10.1109/TNNLS.2021.3121870.

[16] D. C. Le, "Machine Learning based Framework for User-Centered Insider Threat Detection," Aug. 2021, Accessed: Jan. 11, 2024. [Online]. Available: https://DalSpace.library.dal.ca//handle/10222/80731

[17] H. Hindy, R. Atkinson, C. Tachtatzis, J. N. Colin, E. Bayne, and X. Bellekens, "Utilising deep learning techniques for effective zero-day attack detection," Electronics (Switzerland), vol. 9, no. 10, pp. 1–16, Oct. 2020, doi: 10.3390/ELECTRONICS9101684.

[18] K. Hamid, M. Waseem Iqbal, M. Aqeel, T. A. Rana, and M. Arif, "Cyber Security Analysis for Detection and Removal of Zero-Day Attacks (ZDA)," Artificial Intelligence & Blockchain in Cyber Physical Systems: Technologies & Applications, pp. 172–196, Jan. 2023, doi: 10.1201/9781003190301-10/CYBER-SECURITY-KHALID-HAMID-MUHAMMAD-WASEEM-IQBAL-MUHAMMAD-AQEEL-TOQIR-RANA-MUHAMMAD-ARIF.

[19] Y. Aoudni et al., "Cloud security based attack detection using transductive learning integrated with Hidden Markov Model," Pattern Recognit Lett, vol. 157, pp. 16–26, May 2022, doi: 10.1016/J.PATREC.2022.02.012.

Authorized licensed use limited to: ULAKBIM UASL - Kadir Has University. Downloaded on December 07,2025 at 10:18:52 UTC from IEEE Xplore. Restrictions apply.

[20] Oyelere, M., Ige-Olaobaju, A., & Maini, R. (2022). Trade Union Revitalisation: The Impact of Artificial Intelligence and Gig Economy. In HRM in the Global South: A Critical Perspective (pp. 399-424). Cham: Springer International Publishing.

[21] Gupta, A. K., Aggarwal, V., Sharma, V., & Naved, M. (2024). Framework to Integrate Education 4.0 to Enhance the E-Learning Model for Industry 4.0 and Society 5.0. In The Role of Sustainability and Artificial Intelligence in Education Improvement (pp. 151-167). Chapman and Hall/CRC.

[22] Gupta, A. K., Aggarwal, V., Sharma, V., & Naved, M. (2024). Education 4.0 and Web 3.0 Technologies Application for Enhancement of Distance Learning Management Systems in the Post–COVID-19 Era. In The Role of Sustainability and Artificial Intelligence in Education Improvement (pp. 66-86). Chapman and Hall/CRC.

[23] Saini, S., Bansal, S., & Verma, P. (2022). USE ME OR USE ME NOT? A COMMUNICATION TOOL-DIGITAL SIGNAGES FOR FASHION APPAREL STORES. Community & Communication Amity School of Communication, 15, 2456-9011.

[24] Kansal, Y., Singh, G., Kumar, U., & Kapur, P. K. (2016). Optimal release and patching time of software with warranty. International Journal of System Assurance Engineering and Management, 7, 462-468.

Gaur, L., Singh, G., & Agarwal, V. (2021). Leveraging artificial intelligence tools to combat the COVID-19 crisis. In Futuristic Trends in Network and Communication Technologies: Third International Conference, FTNCT 2020, Taganrog, Russia, October 14–16, 2020, Revised Selected Papers, Part I 3 (pp. 321-328). Springer Singapore.

[25] Krishnan, C., Gupta, A., Gupta, A., & Singh, G. (2022). Impact of artificial intelligence-based chatbots on customer engagement and business growth. In Deep learning for social media data analytics (pp. 195-210). Cham: Springer International Publishing

[26] S. Mohanty, A. Behera, S. Mishra, A. Alkhayyat, D. Gupta and V. Sharma, "Resumate: A Prototype to Enhance Recruitment Process with NLP based Resume Parsing," 2023 4th International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2023, pp. 1-6.

Authorized licensed use limited to: ULAKBIM UASL - Kadir Has University. Downloaded on December 07,2025 at 10:18:52 UTC from IEEE Xplore. Restrictions apply.