Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (4), 2022, 12-20
Impact Factor-2.05

MACHINE LEARNING-DRIVEN CYBERSECURITY ANALYSING NETWORK TRAFFIC AND USER BEHAVIOUR FOR INTRUSION DETECTION

[1]Sreekar Peddi
Tek Leaders, Texas, USA
sreekarpeddi95@gmail.com

[2]Dharma Teja Valivarthi
Tek Leaders, Texas, USA
teja89.ai@gmail.com

[3]Swapna Narla
Tek Yantra Inc, California, USA
swapnanarla8883@gmail.com

[4]Sai Sathish Kethu
Neura Flash, Georgia, USA
skethu86@gmail.com

[5]Durai Rajesh Natarajan
Estrada Consulting Inc, California, USA
durairajeshnatarajan@gmail.com

[6]S. Rathna
SNS College of Technology,
Coimbatore, Tamil Nadu, India.
rathnajack@gmail.com

ABSTRACT

Guaranteeing network environment security implies precise identification of unauthorized or malicious user behaviour and unusual traffic patterns. Standard signature-based techniques tend to fail under new or zero-day attacks, as they are based on pre-defined attack signatures. For these reasons, this paper introduces a Machine Learning (ML)-based approach, which integrates network traffic monitoring and user behaviour observation through Recurrent Neural Networks (RNNs). The system conforms important features like a packet size, protocol type, flow duration, and user session frequency, followed by necessary preprocessing operations such as missing value imputation and normalization. During the classification step, the RNN model allocates data instances to the "Anomaly Defect" or "Anomaly Non-Defect" class respectively. Performance testing emphasizes the performance of the solution, attaining a high rate of precision as 98.2% and accuracy as 98.5%, showing strong reliability in suppressing false positives but correctly identifying threats. Future progress can consider using federated learning for privacy-based model training, expanding the system to identify more types of cyber threats, and integrating continuous learning to adjust according to changing patterns of attacks

Keywords: *Recurrent Neural Networks (RNNs), Anomaly Defect, Cyber threats, Cybersecurity, Network Traffic Analysis. Machine Learning (ML).*

1. INTRODUCTION

Network Intrusion Detection Systems (NIDS) monitor and analyse network traffic for any signs of irregularities or security breaches [1]. The systems protect organizations by identifying potential indications of cyber threats before they can cause real damage [2]. Intrusion detection is pivotal for protecting sensitive data, system integrity, and unauthorized access [3]. For instance, Denial of Service (DoS) attacks are one of the common intrusions that flood the intended target with heaps of traffic, thus draining its resources to give away the service [4]. Distributed

Available online at www.jcsonline.in Journal of

Current Science & Humanities

10 (4), 2022, 12-20

Impact Factor-2.05

denial-of-service attacks, on the other hand, use multiple systems in attacking the target, making detection even more difficult [5]. To elaborate on that, Port Scanning techniques identify open ports to exploit vulnerabilities in a system while Man-in-the-Middle (MitM) attacks will intercept and alter communications between two entities without their knowledge [6]. Such intrusion detection systems thus become the closer eye discerning these threats through the examination of such irregularities in network traffic patterns, protocol usage, flow durations, and unexpected traffic spikes [7]. Besides the abnormality found in network traffic, user behavioural inspection is a crucial characteristic of intrusion detection [8].

Intrusion detection techniques have advanced nowadays with their two main categories of signature-based and anomaly-based detection [9]. Signature-based detection uses the predefined signatures or patterns of known attacks [10]. It checks incoming traffic on the network or user activity against the library of attack signatures to flag any arrival of attacks by that [11]. This approach is much efficient for observing common attacks [12]. But it becomes ineffective with novel or zero-day attacks since it cannot detect the attacks as such or with any other means since there is no attack pattern established for it [13]. On the contrary, anomaly-based detection is a method where the normal behavior of network traffic or user activity is trained and any deviations from the learned models are considered as intrusions [14]. The strength of this method is in its ability to identify new attacks that have never been seen before [15]. However, the ability of almost every method that relies on anomaly becomes a high false positive rate [16]. The ML techniques, however, emerged effective in intrusion detection [17].

Regardless of the propitious capabilities exhibited by ML techniques for intrusion detection, various hurdles remain [18]. One key problem is related to imbalanced datasets [19]. Most network traffic datasets are prone to imbalanced situations in which instances of normal traffic vastly outweigh instances of attack traffic, giving rise to models biased toward predicting normal traffic [20]. High rates of false positives diminish the usefulness of any system and create avoidable alerts that lead to alert fatigue [21]. Dimensionality reduction techniques, such as PCA or t-SNE, retain merit for dealing with high-dimensional data and allow the model to concentrate on the most salient features to reduce false positives and increase detection performance [22]. Given the continuous evolution of sophisticated cyber threats, such a system must also be adaptive by continuously learning and retraining with new datasets to capture any newly evolving attack types [23]. Thus, some potential future works would involve hybrid models that combine multiple ML techniques so that they can mutually benefit from the strengths of each and improve detection efficacy [24].

The proposed work aims at incorporating ML-enhanced techniques with network traffic analysis and user behavioural monitoring to supplement intrusion detection systems [25]. The merging of these two critical sources of data allows for distinguishing among conventional, network-based threats and sophisticated ones such as insider attacks or credential stuffing [26]. The hybrid method utilizes the extraction of features from network traffic like flow duration, packet sizes, types of protocol, connection counts, and behavioural activity features of the users like frequency of logins, duration of sessions, and patterns of access [27]. In this integrated approach, an integrated view of system activities is available a view within which attacks may be detected that might not be apparent from pure traffic analysis [28].

2. LITERATURE REVIEW

The role of Information and Communication Technologies (ICTs) in income inequality is multifaceted, especially as it relates to the growth of fixed or mobile connectivity and its socio-economic implications [29]. These technologies can simultaneously reduce or exacerbate inequality depending on various influencing factors such as technological adoption, economic conditions, and political decisions [30]. While ICT alone may not fully account for disparities in income distribution, targeted public policies aimed at reducing digital divides could substantially help mitigate these adverse effects [31].

Cloud computing in smart cities, particularly in health services, enhances task scheduling to optimize overall efficiency and reduce operational delays [32]. Intelligent hybrid models that combine optimization algorithms such as Parallel Particle Swarm Optimization (PPSO) and Particle Swarm Optimization (PSO) significantly improve resource utilization and cut down execution costs. Comparative analysis suggests that PPSO delivers superior scheduling performance compared to traditional PSO techniques [33].

Advancements in tomographic imaging have led to better evaluation of porous materials, especially through the simplified computation of average tortuosity in both 2D and 3D contexts [34]. A Python-based tool for modelling, built on random walks, achieves rapid results and serves as a more efficient alternative to complex simulations [35]. This kind of innovation has made material analysis more accessible for researchers using basic computing infrastructure.

Economic transformation aimed at alleviating poverty relies heavily on expanding production options, reducing costs, diversifying consumption, and enhancing access to government services [36]. Digitalization has the potential to reform these avenues, bringing both benefits and challenges depending on how it is implemented [37]. A comprehensive framework helps evaluate the effects of internet-based financial systems and e-commerce platforms in improving economic conditions, as demonstrated in case studies from developing regions [38].

In the realm of supply chain management, blockchain technology contributes to reducing lead time and streamlining order processes through smart contract integration [39]. These contracts enable real-time visibility, lower administrative expenses, and foster community trust across supply chain stakeholders. This research lays out a foundational blueprint to guide the development of smart contract systems aimed at addressing transparency and trust issues [40].

Digital financial inclusion, particularly when combined with Cloud IoT, significantly affects income equality across both urban and rural populations [41]. The growing emphasis on digital transformation is echoed across business and academic domains, where inclusivity in digital services is becoming a central theme [42]. Service management approaches are being reshaped by these technological advancements to better accommodate diverse socioeconomic contexts [43].

Big Data Business Analytics (BDBA) enhances agility in manufacturing by enabling firms to respond more effectively to market fluctuations and competition [44]. Case studies show that firms with higher BDBA maturity levels are better equipped to deal with turbulent market conditions and demonstrate stronger performance metrics [45]. Agile production strategies informed by data analytics offer scalable solutions that support continuous improvement in manufacturing systems.

Resource efficiency in Automated Guided Vehicle (AGV) manufacturing has been improved using advanced scheduling models, especially for handling diverse and small-batch production orders [46]. An improved PSO-based algorithm outperforms existing models in optimizing task duration and utilization of AGV and machinery [47]. This approach yields critical insights into flexible and responsive AGV-based production environments for modern manufacturing operations [48].

2.1 PROBLEM STATEMENT

The steadily increasing complexity of cyber threats has afforded signature-based ID systems some alleged obsolescence; these systems respond poorly against zero-day attacks and advanced persistent threats and also trigger quite a number of false positives when classified with anomaly-based detection [49]. Rapid increase in network traffic and user pattern behaviour monitoring clearly call for an adaptive and accurate intrusion-detection solution urgently [50]. This study proposes a machine-learning framework that combines network traffic analysis and monitoring of user behaviour for the online detection of both known and unknown threats. The design is focused around getting higher machine-learning techniques and develop the system with appropriate processing of large data while minimizing the false positives and learn continuously from new advanced patterns of attack to increase overall security stance [51].

3. PROPOSED METHODOLOGY

In the proposed Cybersecurity Figure 1 intrusion detection methodology, the Cybersecurity Intrusion Detection Dataset, containing network traffic and user behaviour data, comes into play in its very first stage. The processes of preprocessing include dealing with missing values wherein numerical features are normalized to ensure uniform data. Feature extraction applies key metrics like Transmission Control Protocol (TCP) characteristics that include packet size, protocol type, and flow duration to identify the attack patterns. Afterward, it employs an anomaly detection system to recognize the unusual behaviour. The system uses RNN to classify the data stream as either normal or anomalous traffic. The performability of the proposed methodology plays a key role in the effective identification and classification of network traffic and, hence, detection of cyber threats, both known and unknown.

Available online at www.jcsonline.in Journal of
Current Science & Humanities
10 (4), 2022, 12-20
Impact Factor-2.05

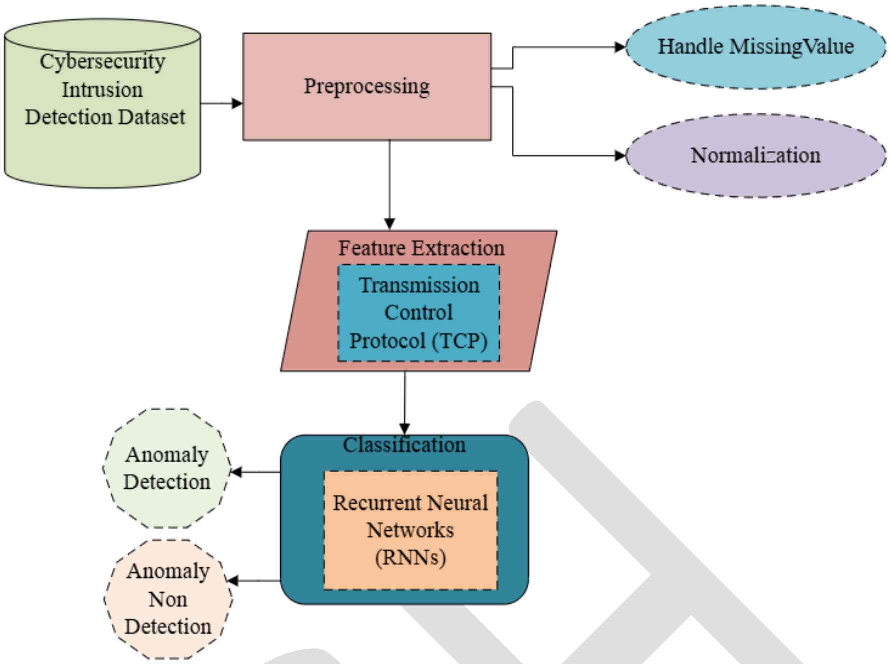

Figure 1: *Overall Architecture for Proposed Methodology*

3.1 DATA COLLECTION

The dataset called Cybersecurity Intrusion Detection Classification has been developed to detect cyber intrusions on the basis of network traffic and user behavior The principal features of the dataset are network packet size, which helps in recognizing abnormal traffic patterns such as reconnaissance or DoS attempts, and protocol type, indicating the type of communication used. In addition, packet inter-arrival time is important to uncover anomalies either from DDoS or slow Loris attacks. Turning to user behavior, features such as login frequency can help uncover brute-force or credential stuffing attacks by detecting unusual login patterns. All these features spanning network-based and user behavior-based attributes provide substantial information about any cyber threat, equipping the ML model with a clear separation line to distinguish normal and malicious activities.

3.2 PRE-PROCESSING

Another important aspect of ML is preprocessing, which involves preparing raw data for possible feeding to any model for testing its performance. It usually includes missing value handling, feature scaling, and encoding categorical variables. It is an absence handling imputation intern replacement of missing data by meaningful such as the mean or the median of available data. Scaling the data within a specific range, where no feature would dominate over others due to scale, is termed normalization. Thus, if the preprocessing is done correctly, the model can generalize well and give more accuracy and reliability in its predictions.

3.2.1Handle Missing Value

Missing value treatment is a very crucial preprocessing phase in ML. R datasets seldom ever are without missing information; missing information could occur due to errors in data collection, system failures, or incomplete responses. The existence of missing values could potentially bias subsequent results, leading to wrong conclusions and degrading model performance. There could be several approaches to dealing with missing data, which could depend on what type of data is being used, how much information is missing, and how this may bear on the analysis. Handling with mean imputation is modelled using Equation (1):

$$X_{ij}^{\text{imputed}} = \frac{1}{n}\sum_{k=1}^{n} X_{ik} \tag{1}$$

where, X_{ij}^{imputed} is the imputed value for the missing data point in feature f_i at the j^{th} row,X_{ik} represents the observed values of feature f_i from the k^{th} row,n is the number of non-missing values for feature f_i. This formula calculates the mean of the available (non-missing) data in feature f_i and replaces the missing value with this mean.

3.2.2 Normalization

Normalization is one of the pre-processing techniques that scale real-valued data into a definite range, typically [0, 1], thereby not allowing any feature to dominate another because of the scale on which it is measured. It is especially important when using ML algorithms like k-Nearest Neighbours (k-NN), Support Vector Machines (SVM), or Neural Networks since their output or performance will be highly sensitive to input feature scaling. Min-Max scaling normalization process is presented in Equation (2):

$$X_{\text{norm}} = \frac{X - X_{\min}}{X_{\max} - X_{\min}} \tag{2}$$

where, X is the original value,$X_{\min}$ is the minimum value in the feature, $X_{\max}$ is the maximum value in the feature, X_{norm} is the normalized value (scaled to the range $[0,1]$).

3.3 FEATURE EXTRACTION USING TRANSMISSION CONTROL PROTOCOL (TCP)

TCP data-based feature extraction is a key component of intrusion detection in cyber security. Packet size, flow duration, TCP flags, and bytes per flow are just a few features that provide insightful information regarding network behaviour. For instance, suspicious packet sizes or suspicious flow durations could indicate potential DoS/DDoS attacks or session hijacking attacks. In addition, TCP flag observation helps to detect attacks like SYN floods, while sequence numbers and bytes per flow can help to detect data exfiltration or port scanning. These derived features help ML algorithms to better detect malicious traffic patterns as well as improve intrusion detection systems. TCP Expressed the Equation (3):

$$\text{Avg Packet Size } = \frac{1}{N_{\text{packets}}} \sum_{i=1}^{N_{\text{packets}}} P_i \tag{3}$$

where, P_i is the size of the i^{th} TCP packet in bytes, N_{packets} is the total number of TCP packets exchanged during a particular connection or flow,$\sum_{i=1}^{N_{\text{packets}}} P_i$ is the summation of the sizes of all N_{packets} TCP packets in the flow.

3.4 CLASSIFICATION USING RNN

RNNs refer to one type of neural network that is capable of dealing with data that has some sequential aspect to it by remaining in a hidden state to enable it to remember previous inputs from the sequence. Unlike feedforward networks, RNNs have feedback of the actions taken on the different time steps, which offers temporal dependencies suitable to this kind of network. Time series prediction, natural language processing, and even speech recognition can use RNNs widely. Input is applied at a time step, then the hidden state is updated, and the value at that time step is output. In this feedback, one can learn sequential patterns and predict according to the sequence of the data. RNN Expressed the Equation (4):

$$h_t = f(W_h h_{t-1} + W_x x_t + b) \tag{4}$$

where,h_t is the hidden state at time step t,W_h and W_x are weight matrices for the previous hidden state and the current input,b is the bias term,f is the activation function, h_t at each time step t ased on the previous hidden state h_{t-1} and the current input x_t . In detecting anomalies using RNN, the model yields a probability score designed to classify the input sequence as having an " Anomaly defect" (anomalous) or " Anomaly non-defect" (normal). The probability indicates the degree to which the sequence is considered defective, with higher scores meaning that the sequence is most likely anomalous and lower ones indicating that this sequence is normal. There is a predetermined threshold for this output, usually, above which the sequence qualifies as a defect and below which it is classified as non-defect. This threshold can be modified according to the different needs of a detection system.

4. RESULTS AND DISCUSSIONS

Its performance test as a model on major performance measures like Accuracy, Precision, Recall, and F1-Score validates its superior ability of classifying accurate normal and abnormal network traffic with high precision. Their resultant high values show the model is highly correct in marking valid and malicious activity with low false negatives and false positives. The confusion matrix also enforces these results with evident distinction between the "Anomaly Defect" and "Anomaly Non-Defect" classes and verification that the model is highly robust and reliable. The results are strongly favourable to the model being good enough to be used in real-world applications with correct and efficient detection of anomalies.

4.1 PERFORMANCES METRICS

Performance metric results and comparisons for a few models sets such as Accuracy, Precision, Recall, and F1-Score are illustrated Figure 2. All the metrics are quite high, thus verifying the model's ability to discern between the normal traffic and abnormal traffic with a high degree of confidence. The parameter Accuracy simply refers to how correct the model has been. On the contrary, Precision refers to how well the model avoids generating false positives by predicting that a certain traffic flow is an anomaly when, in fact, it is. Recall will tell us how well the model detects all actual anomalies, while the F1 Score will.

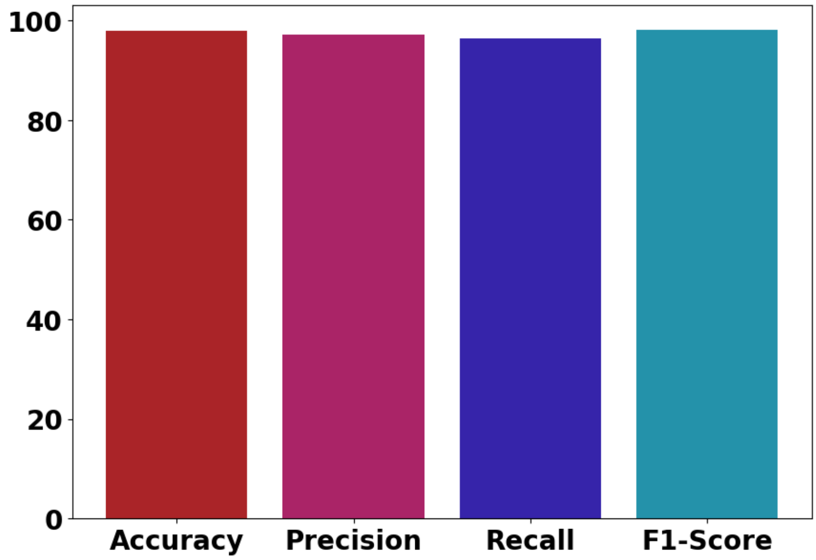

Figure 2*: Performance Metrix*

4.2 CONFUSION MATRIX

Confusion matrix Figure 3 shows the discrimination ability of the model between "Anomaly Defect" and "Anomaly Non-Defect" classes. The model marked 2,526 defect and 2,200 non-defect cases correctly, with the two classes highly discriminated from one another. Misclassifications were very minimal, with only 9 non-defect samples incorrectly labeled as defects and 10 defect samples incorrectly labeled as non-defects. These findings establish high accuracy of classification, minimal error rates, and maximal model reliability, and thus it is appropriate to utilize in applications where exact anomaly detection is paramount.

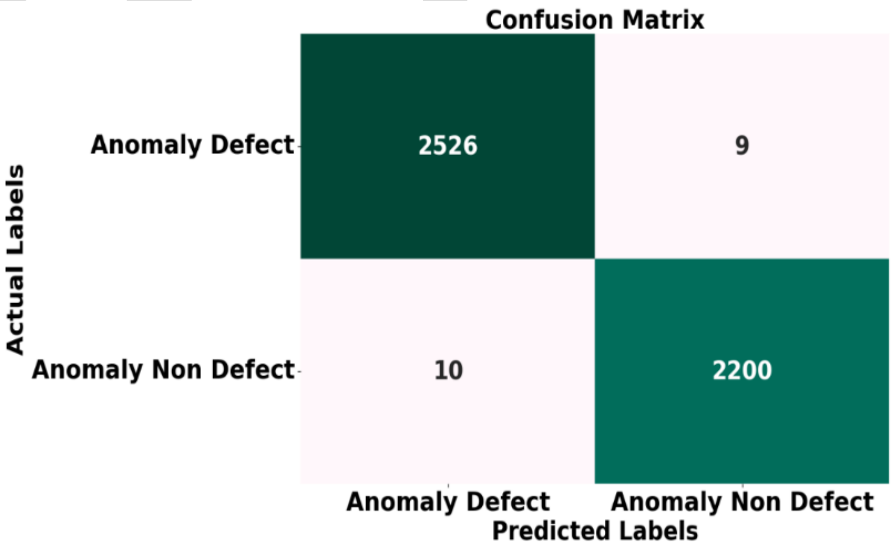

Figure 3*: Confusion Matrix*

5. CONCLUSION AND FUTURE WORK

It needs to be able to detect malicious or unauthorized user traffic and activity patterns to protect the network. The traditional detection methods, including signature-based detection, cannot detect new or zero-day attacks since they are pattern-dependent. In an effort to overcome these limitations, this research presents a ML-based solution involving network traffic monitoring and user behaviour monitoring utilizing RNNs. The model needs to learn important features such as packet length, protocol type, flow duration, and frequency of user sessions, and preprocessing involves imputation of missing values and normalization. RNNs are employed in the classification task to produce outputs categorized into "Anomaly Defect" or "Anomaly Non-Defect" classes. Performance metrics indicate excellent model performance with accuracy at 98.2% and precision at 98.5%, effectively weeding out false positives while maintaining correct detection, to ensure that it can scale into the Future work the integration of federated learning to facilitate decentralized environments, scaling the model to identify numerous patterns of attacks, and using continuous learning algorithms to facilitate compatibility with new threat techniques.

REFERENCES

[1] Alguliyev, R. M., Imamverdiyev, Y. N., Mahmudov, R. S., & Aliguliyev, R. M. (2021). Information security as a national security component. Information Security Journal: A Global Perspective, 30(1), 1-18.
[2] Basani, D. K. R. (2021). Leveraging Robotic Process Automation and Business Analytics in Digital Transformation: Insights from Machine Learning and AI. International Journal of Engineering Research and Science & Technology, 17(3).
[3] Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. Government Information Quarterly, 37(1), 101419.
[4] Sareddy, M. R. (2021). Advanced quantitative models: Markov analysis, linear functions, and logarithms in HR problem solving. International Journal of Applied Science Engineering and Management, 15(3).
[5] Durai, K. N., Subha, R., & Haldorai, A. (2021). A novel method to detect and prevent SQLIA using ontology to cloud web security. Wireless Personal Communications, 117(4), 2995-3014.
[6] Bobba, J. (2021). Enterprise financial data sharing and security in hybrid cloud environments: An information fusion approach for banking sectors. International Journal of Management Research & Review, 11(3), 74–86.
[7] S Awad, W. (2020). A framework for improving information security using cloud computing. International Journal of Advanced Research in Engineering and Technology, 11(6).
[8] Narla, S., Peddi, S., & Valivarthi, D. T. (2021). Optimizing predictive healthcare modelling in a cloud computing environment using histogram-based gradient boosting, MARS, and SoftMax regression. International Journal of Management Research and Business Strategy, 11(4).
[9] Bruma, L. M. (2020). An approach for information security risk assessment in cloud environments. Informatica Economica, 24(4), 29-40.
[10] Kethu, S. S., & Purandhar, N. (2021). AI-driven intelligent CRM framework: Cloud-based solutions for customer management, feedback evaluation, and inquiry automation in telecom and banking. Journal of Science and Technology, 6(3), 253–271.
[11] Lian, J. W. (2021). Understanding cloud-based BYOD information security protection behaviour in smart business: In perspective of perceived value. Enterprise Information Systems, 15(9), 1216-1237.
[12] Srinivasan, K., & Awotunde, J. B. (2021). Network analysis and comparative effectiveness research in cardiology: A comprehensive review of applications and analytics. Journal of Science and Technology, 6(4), 317–332.
[13] Elmurzayevich, M. O. (2020). Cloud technology to ensure the protection of fundamental methods and use of information. International Journal on Integrated Education, 3(10), 313-315.
[14] Narla, S., & Purandhar, N. (2021). AI-infused cloud solutions in CRM: Transforming customer workflows and sentiment engagement strategies. International Journal of Applied Science Engineering and Management, 15(1).
[15] Rupra, S. S., & Omamo, A. (2020). A cloud computing security assessment framework for small and medium enterprises. Journal of Information Security, 11(4), 201-224.
[16] Budda, R. (2021). Integrating artificial intelligence and big data mining for IoT healthcare applications: A comprehensive framework for performance optimization, patient-centric care, and sustainable medical strategies. International Journal of Management Research & Review, 11(1), 86–97.
[17] Syafrizal, M., Selamat, S. R., & Zakaria, N. A. (2020). Analysis of cybersecurity standard and framework components. International Journal of Communication Networks and Information Security, 12(3), 417-432.
[18] Ganesan, T., & Devarajan, M. V. (2021). Integrating IoT, Fog, and Cloud Computing for Real-Time ECG Monitoring and Scalable Healthcare Systems Using Machine Learning-Driven Signal Processing Techniques. International Journal of Information Technology and Computer Engineering, 9(1).
[19] Jaeger, L., Eckhardt, A., & Kroenung, J. (2021). The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis. Information & Management, 58(3), 103318.

[20] Pulakhandam, W., & Samudrala, V. K. (2021). Enhancing SHACS with Oblivious RAM for secure and resilient access control in cloud healthcare environments. International Journal of Engineering Research and Science & Technology, 17(2).

[21] Alrehaili, A., Mir, A., & Junaid, M. (2020). A retrospect of prominent cloud security algorithms. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 9(3), 749-755.

[22] Jayaprakasam, B. S., & Thanjaivadivel, M. (2021). Integrating deep learning and EHR analytics for real-time healthcare decision support and disease progression modeling. International Journal of Management Research & Review, 11(4), 1–15. ISSN 2249-7196.

[23] Geetha, R., Suntheya, A. K., & Srikanth, G. U. (2020). Cloud integrated iot enabled sensor network security: research issues and solutions. Wireless Personal Communications, 113(2), 747-771.

[24] Jayaprakasam, B. S., & Thanjaivadivel, M. (2021). Cloud-enabled time-series forecasting for hospital readmissions using transformer models and attention mechanisms. International Journal of Applied Logistics and Business, 4(2), 173-180.

[25] Feng, S., Xiong, Z., Niyato, D., Wang, P., Wang, S. S., & Shen, S. X. (2020). Joint pricing and security investment in cloud security service market with user interdependency. IEEE Transactions on Services Computing, 15(3), 1461-1472.

[26] Dyavani, N. R., & Thanjaivadivel, M. (2021). Advanced security strategies for cloud-based e-commerce: Integrating encryption, biometrics, blockchain, and zero trust for transaction protection. Journal of Current Science, 9(3), ISSN 9726-001X.

[27] AlZubi, A. A., Al-Maitah, M., & Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Computing, 25(18), 12319-12332.

[28] Garikipati, V., & Pushpakumar, R. (2019). Integrating cloud computing with predictive AI models for efficient fault detection in robotic software. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(5).

[29] Tariq, M. I., Tayyaba, S., Ali Mian, N., Sarfraz, M. S., De-la-Hoz-Franco, E., Butt, S. A., ... & Rad, D. V. (2020). Combination of AHP and TOPSIS methods for the ranking of information security controls to overcome its obstructions under fuzzy environment. Journal of Intelligent & Fuzzy Systems, 38(5), 6075-6088.

[30] Ayyadurai, R., & Kurunthachalam, A. (2019). Enhancing financial security and fraud detection using AI. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(1).

[31] Wu, Y. C., Sun, R., & Wu, Y. J. (2020). Smart city development in Taiwan: From the perspective of the information security policy. Sustainability, 12(7), 2916.

[32] Basani, D. K. R., & Bharathidasan, S. (2019). IoT-driven adaptive soil monitoring using hybrid hexagonal grid mapping and kriging-based terrain estimation for smart farming robots. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(11).

[33] Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems, 15(4), 565-584.

[34] Kodadi, S., & Purandhar, N. (2019). Optimizing secure multi-party computation for healthcare data protection in the cloud using hybrid garbled circuits. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(2).

[35] Mansour, R. F., & Parah, S. A. (2021). Reversible data hiding for electronic patient information security for telemedicine applications. Arabian Journal for Science and Engineering, 46(9), 9129-9144.

[36] Devarajan, M. V., & Pushpakumar, R. (2019). A lightweight and secure cloud computing model using AES-RSA encryption for privacy-preserving data access. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(12).

[37] Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. Journal of applied security research, 16(4), 490-513.

[38] Allur, N. S., & Thanjaivadivel, M. (2019). Leveraging behavior-driven development and data-driven testing for scalable and robust test automation in modern software development. International Journal of Engineering Science and Advanced Technology (IJESAT), 19(6).

[39] Mirtsch, M., Kinne, J., & Blind, K. (2020). Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. IEEE Transactions on Engineering Management, 68(1), 87-100.

[40] Ramar, V. A., & Kumar, V. R. (2019). Enhancing data privacy and security in cloud healthcare solutions using elliptic curve cryptography (ECC). International Journal of Engineering Technology Research & Management, 3(5), 2456-9348.

[41] Khan, A., Ibrahim, M., & Hussain, A. (2021). An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. International Journal of Information Management Data Insights, 1(2), 100015.

[42] Induru, V., & N, P. (2019). Enhanced network intrusion detection using long short-term memory for improved security analysis. International Journal of Engineering Technology Research & Management, 3(3), 2456-9348.

[43] Durowoju, O., Chan, H. K., & Wang, X. (2020). Investigation of the effect of e-platform information security breaches: a small and medium enterprise supply chain perspective. IEEE Transactions on Engineering Management, 69(6), 3694-3709.

[44] Bhadana, D., & Arulkumaran, G. (2019). STAMS-enabled genomic smart farming: A spectrotemporal intelligence framework for adaptive zone treatment and crop optimization. International Journal of Engineering Technology Research & Management, 3(6), 2456-9348

[45] Reddy, A. R. P., & Ayyadapu, A. K. R. (2020). Automating Incident Response: Ai-Driven Approaches To Cloud Security Incident Management. Chelonian Research Foundation, 15(2), 1-10.

[46] Chaluvadi, A., & Kumar, R. L. (2019). Cloud-based heart disease classification system using deep neural networks and IoT data integration. International Journal of Engineering Technology Research & Management, 3(7), 2456-9348

[47] Faisal, A., & Zulkernine, M. (2021). A secure architecture for TCP/UDP-based cloud communications. International Journal of Information Security, 20(2), 161-179.

[48] Vasamsetty, C., & Palanisamy, P. (2019). Anomaly detection in cloud healthcare networks using deep learning. International Journal of Business Management and Economic Review, 2(2), 54.

[49] Aldallal, A., & Alisa, F. (2021). Effective intrusion detection system to secure data in cloud using machine learning. Symmetry, 13(12), 2306.

[50] Gudivaka, R. K., Gudivaka, R. L., & Karthick, M. (2019). Secure and efficient data management for healthcare IoT devices in cloud-enabled systems using Serpent encryption. International Journal of Business Management and Economic Review, 2(3), 114.

[51] Zhao, S., Li, S., Qi, L., & Da Xu, L. (2020). Computational intelligence enabled cybersecurity for the internet of things. *IEEE Transactions on Emerging Topics in Computational Intelligence*, *4*(5), 666-674.