# AI in Cybersecurity: Enhancing Digital Defenses with Anomaly Detection and LSTM-Based Threat Prediction

**Guman Singh Chauhan**
John Tesla Inc, Texas, USA
gumansinghchauhan@ieee.org

**Venkata Surya Teja Gollapalli,**
Centene Management Company LLC,
Missouri, USA,
venkatasuryatejagollapalli@ieee.org

**Kannan Srinivasan**
Saiana Technologies Inc,
New Jersey, USA,
kannansrinivasan@ieee.org

**Rahul Jadon**
CarGurus Inc,
Massachusetts, USA
rahuljadon@ieee.org

**Gamachis Ragasa Gutata**,
College of Engineering and Technology,
Dambi Dollo University, Dambi Dollo, Ethiopia,
gamachisragasa@dadu.edu.et

***ABSTRACT***

*These are the key future areas of research in Applied Artificial Intelligence. In this era of increasingly fast, internet-connected systems, traditional defenses have become inefficient at detecting and responding to various types of sophisticated threats such as malware, phishing, ransomware, distributed denial of service attacks, and more. Such conventional security approaches are not effective with zero-day attacks or new-age evolving attacks. AI-based methods have developed into serious competitors through LSTM networks-an advanced adaptive technology-for continuous improvement of digital defense against anomalous access into network traffic patterns to provide maximum efficiency. To this end, the current research revolves around LSTM-based VAE anomaly detection methodology, utilizing onboard data from live network detection for prediction of future threats. The methodology involves necessary steps that include data pre-processing of Z-score normalization, encoding network traffic into latent representations and then reconstructing the pattern to realize anomaly detection through reconstruction loss and KL divergence. LSTM-based classifier with SoftMax activation is used for threat classification. Testing results indicated improvement in detection accuracy over 90% after 20 epochs of training. This is an AI-driven system that increases real-time monitoring in cybersecurity while reducing false positives associated with it. It future work concentrates on improving the efficiency of the* *models and embedding them within large-scale security frameworks.*

***Keywords**: Cybersecurity, Anomaly Detection, Long Short-term Memory - Variational Auto-Encoder, Threat Prediction, AI-Based Security, Network Traffic Analysis*

## 1. INTRODUCTION

It is true that traditional defenses nowadays are overwhelmed as they are unable to effectively detect and alleviate such attacks as those resulting from sophisticated cyber threats [1]. With intelligent threat detection and response mechanisms, AI-led cybersecurity solutions are now becoming a mandatory part of modern digital defenses [2]. These put up to their mark for heavily age-thorny expansion of the systems connected in the internet, cloud computing, and IoT [3].

This increases the vulnerability of a person's, an organization's and even a government network to cybercrimes such as malware, phishing, ransomware, and DDoS attack[4]. Cyber threats dynamically evolve in real time; therefore, detection of them requires special techniques and cannot be dealt with conventional security techniques [5]. Conventionally, security methods are rule models-based, signature detection, and predefined attack patterns [6]. All these steps have worked sufficiently against known threats, while having some limitations with zero-day attacks, evolving malware, and sophisticated intrusion attempts [7].

Static security models also cause high false positive rates and longer response times and hence are not effective for real-time threat detection [8]. AI-based anomalous detection based on LSTM networks can overcome these limitations and improve threat prediction abilities [9]. Facing this cyber revolution, the traditional methods cease to exist for detection and mitigation purposes [10]. In this case, LSTM, known as a deep learning model, analyzes time-bound patterns of network traffic while detecting anomalies suggesting possible threats [11]. Thus, more accurate detection with fewer false positives and improved defence against growing threats can be achieved with the help of artificial intelligence above [12].

Section 2 discusses the Literature Review. Section 3 gives the problem statement and Section 4 Intelligent Anomaly Detection Using LSTM-VAE. Section 5 describes the evaluation of accuracy metrics, and Section 6 gives a conclusion with suggestions for future directions of research.

## 2. LITERATURE REVIEW

Existing CKD prediction methods such as SVM and Random Forest lack real-time IoMT data accessibility and privacy proposed in [13]. This proposed model CNN-LSTM-Neuro-Fuzzy with AOA optimization improves the accuracy, prevents overfitting, and allows fast and secure prediction in low-resource environments. [14] The effective use of AI-Driven CRM, IoT Analytics, and Cloud Computing promises to revolutionize Banking [15]. However, high cost, risks of security, and issues of integration still pose a challenge [16]. mark for heavily age-thorny expansion of the systems connected in the internet, cloud computing, and IoT. Existing studies evaluate the role of digital finance in ameliorating income inequality using regression models, indicators of financial inclusion, and case studies [17]. At the same time, obstacles include lack of pooled data across various regions and inability to measure long-term socio-economic effects [18]. [19] Existing Research applies Resource-Based View, Explainable AI, and statistical analysis to Cloud IoT-enabled digital financial inclusion. Limitations include issues regarding overall availability of data, differences between regions in regard to adoption, and measurement issues in relating such indicators to the long-term effects on the economy [20].

[21] Existing studies use DBSCAN to find anomalies and CCR for the assessment of bandwidth efficiency in the context of big data-driven mobile network management. Limitations here include computational ineffectiveness coupled with sensitivity to the choice of parameters and then the dynamic network conditions-the entire testing and analyzes are conducted in real time [22]. [23] Studied apply cryptographic techniques and anomaly detection based on AI to protect EHRs in multicloud. While AI improves the real-time detection of threats and compliance with health standards, it is hampered by some limitations, including astronomical computational costs, false positives, and integration difficulties among various cloud architectures [24].

## 3. PROBLEM STATEMENT

The currently available technologies have limitations in computing efficiency [25]; they cannot draw real-time data, nor can they confront the issues of integration in CKD prediction and mobile network management [26]. The SVM and Random Forest could not give real-time prediction and privacy, while the DBSCAN found parameter sensitivity and computation burden as challenges for anomaly detection [27].

On the other hand, the cost involved and integration issues result in diminished effectiveness of cryptographic mechanisms and AI-augmented strategies for anomaly detection in securing EHRs in a multi-cloud environment in real-life scenarios [28]. Although AI and cloud computing have matured, the high costs, security concerns, and integration issues have prevented the design of such scalable and secure systems [29]. This study aims at addressing these challenges through the provision of efficient and flexible models that would be able to tackle these limitations in less resource-consuming environments.

### 3.1 Objectives

These are the findings of the investigation accomplishments:

- Evolving a smart anomaly detection system on LSTM-VAE frameworks for real-time cyber incident guidance and threat prediction.
- Improve detection effectiveness and reduce false positives by fine-tuning the thresholds for loss reconstruction and optimal KL-divergence regularization.
- Install that model in broader security systems for large-scale intrusion of online network threats besides the cloud and IoT environments.
- Use other A.I. models, such as reinforcement learning architectures or transformers, for improving adaptability and optimized performance of modeled software.

## 4. INTELLIGENT ANOMALY DETECTION USING LSTM-VAE

This image depicts a systematic workflow for a cyber threat detection pipeline scenario. The data collection gathers the respective security data from heterogeneous sources. Preprocessing is done using Z-Score normalization on data for standardization and possible better performance of the model. The generated application of that approaches is on anomaly detection, which here involves the use of a LSTM-VAE in the detection of unusual patterns that might signal a possible cyber threat is displayed in Figure (1),

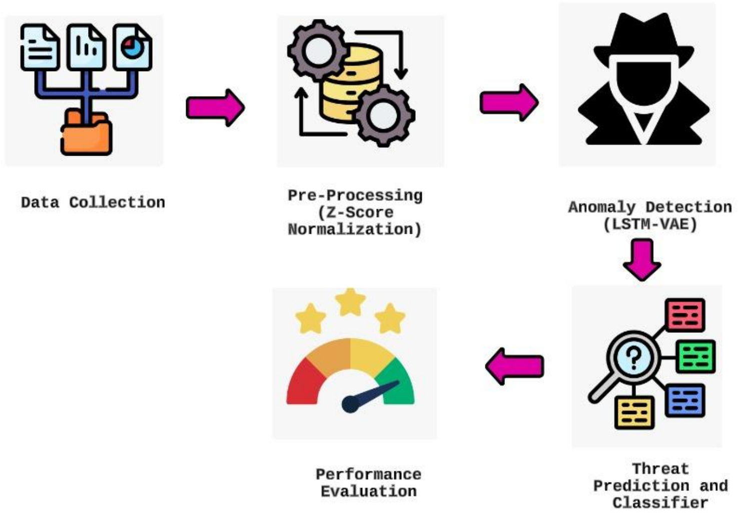
Data Collection
Pre-Processing (Z-Score Normalization)
Anomaly Detection (LSTM-VAE)
Threat Prediction and Classifier
Performance Evaluation

**Figure 1: Block diagram of Anomaly Detection using LSTM-VAE**

Then the detected anomalies are routed into the threat prediction classifier module that evaluates those threats according to learning patterns. Ultimately, the system is put under evaluation for performance, which tests the accuracy and efficiency of the system. Such a methodical way of approaching things, indeed, is crucial to ensure a more robust and efficient cybersecurity framework for detection and mitigation of possible threats.

### 4.1 Data Collection

This network traffic dataset was recorded on Wireshark running under Kali Linux at the University of Cincinnati. With one hour of network traffic stored in CSV format, the entire dataset presents a volume of traffic with the following attributes: timestamp, source and destination IPs, protocol, length, and traffic info. These critical data could provide IP flow statistics to identify the actual applications, and this is of much value for machine learning applications in intrusion detection, anomaly detection, traffic classification, and network performance monitoring [30]. As a public dataset, it serves a great avenue for anything involving training or evaluation of AI-based cybersecurity solutions.

### 4.2 Data Preprocessing using Z-Score Normalization

As features in raw network traffic data vary in their numerical scales, they affect the performance of machine learning models negatively. Z-score normalization converts these values to a mean of 0 and a standard deviation of 1, thus enhancing stability and performance for the model. The Z-score formula is given in Eq. (1),

$$X' = \frac{X-\mu}{\sigma} \tag{1}$$

Where X is the actual feature value, μ is the mean of the feature, σ is the standard deviation, and X' is the normalized value. The difference from Z-score normalization makes features bias-free and more adapted to be used in machine learning for anomaly detection in cybersecurity applications.

### 4.3 Anomaly Detection using LSTM-VAE

Using LSTM-VAEs, normal patterns of network traffic are learned, and anomalies are detected by identifying deviations from expected behaviors.

#### 4.3.1 Encoding Network Traffic-Up

The task of encoding works by compressing the data X into its latent representation Z in such a way that it captures the most relevant features of normal traffic patterns. By modeling normal traffic in this latent space, LSTM-AE can declare any observed network data abnormal if it deviates from the learned patterns significantly. This is represented as Eq. (2)

$$Z = f_{enc}(X) = \mu + \sigma \cdot \epsilon \tag{2}$$

Where, μ and σ determine the distribution of the latent space; while ε introduces variability by being sampled from a standard normal distribution N (0,1).

### 4.3.2 Decoding to Reconstruct Traffic Patterns

The second part of the decoder attempts to reconstruct the original X from Z, the latent representation generated by the encoder, so as to learn the normal patterns of traffic. When the reconstructed data deviates significantly from the input data, the traffic behavior is treated as an anomaly. The decoding refines the representations that enable the network to differentiate normal and abnormal behavior, expressed as Eq. (3)

$$X' = f_{dec}(Z) \tag{3}$$

- **Reconstruction loss (mean squared error)**

Computes the distance between the original input(X) and the reconstructed output(X') in terms of mean square error (MSE); lower the loss is, the better capable it is to accurately reconstruct normal traffic, while a higher reconstruction value would indicate its inability to reconstruct normal traffic due to deviations, thereby possibly signaling an anomaly. It is computed as indicated in Eq. (4):

$$L_{\text{recon}} = \frac{1}{n}\sum_{i=1}^{n} (X_i - X_i')^2 \tag{4}$$

In any case, this network traffic behavior is classified as anomalous once the reconstruction error exceeds the user-specified threshold.

- **KL Divergence Loss**

KL Divergence Loss A penalty on divergence between the learned latent space distribution and standard Gaussian distribution was introduced to smooth the latent space to make it sufficiently structured to generalize better on normal traffic patterns. This loss function is defined as in Eq. (5):

$$L_{KL} = D_{KL}(q(Z \mid X) \| p(Z)) \tag{5}$$

The minimization of KL divergence ensures that our model does not overfit to certain patterns, thus enabling it to detect unseen anomalies in network traffic.

- **Final VAE Loss**

The Final VAE Loss is the weighted sum of the reconstruction loss (MSE) and KL divergence loss, to ensure that there exist equal impulses for accurate reconstruction of data and proper regularization of latent space. It is represented as in Eq.(6),

$$L_{VAE} = L_{\text{recon}} + \beta L_{KL} \tag{6}$$

Here, β weighs the influence of KL divergence; a higher β enforces a more structured latent space, while a lower β concentrates on minimizing reconstruction errors. This synergy ensures that VAE learns the normal patterns of network traffic and detects anomalies where reconstruction error is large.

### 4.4 Prediction and Threat Classification with Softmax Activation

Once anomalies are detected, they will be classified using an LSTM-based classifier into certain kinds of attacks. The final layer of LSTM uses Softmax activation function to arrive at the attack categories as e.g. malware, DDoS, phishing as represented in Eq. (7),

$$P(y_i) = \frac{e^{z_i}}{\sum_{j=1}^{n} e^{z_j}} \tag{7}$$

Where, P(y_i ) is the probability of the sample belonging to class i, zi is the output score for class i, n is the number of attack categories.

- **Classification Loss (Categorical Cross-Entropy Loss)**

Categorical Cross-Entropy measures how well the model carries out prediction of a correct class when taking into accountthe comparison of true labels ($y_i$) against predicted probabilities ($P(y_i)$). It is calculated as Eq. (8),

$$L_{\text{class}} = -\sum_{i=1}^{n} y_i \log(P(y_i)) \tag{8}$$

Where $y_i$ denotes Actual class (1 for correct class and 0 for the others); $P(y_i)$ is the predicted probability for class $y_i$. Lower loss means better alignment of prediction by the model with real labels. This loss function is commonly used in multi-class classification tasks, wherein it ensures that the model gives high probabilities to the right class while lowering those for other classes.

## 5. RESULT AND DISCUSSION

The anomaly detection produces sufficient abnormal network activities using threshold-based methods with red, indicating threat, and blue bar, indicating normal traffic. The training of the model progresses for more than 90% accuracy up from 50% in only 20 epochs. This makes it contextually very stable for learning and never overfits at this level, which is very useful for all real-world applications of cybersecurity behavior.

### 5.1 Detection of Anomalous Network Activity Using Threshold-Based Detection

Anomaly scores across network nodes are illustrated by the bar graph. Nodes where scores exceed the threshold are indicated by red bars and classified as anomalous (possible threats or attacks). Blue bars indicate nodes where the behavior is normal for their scores of anomaly falling under the threshold is displayed in Figure (2),

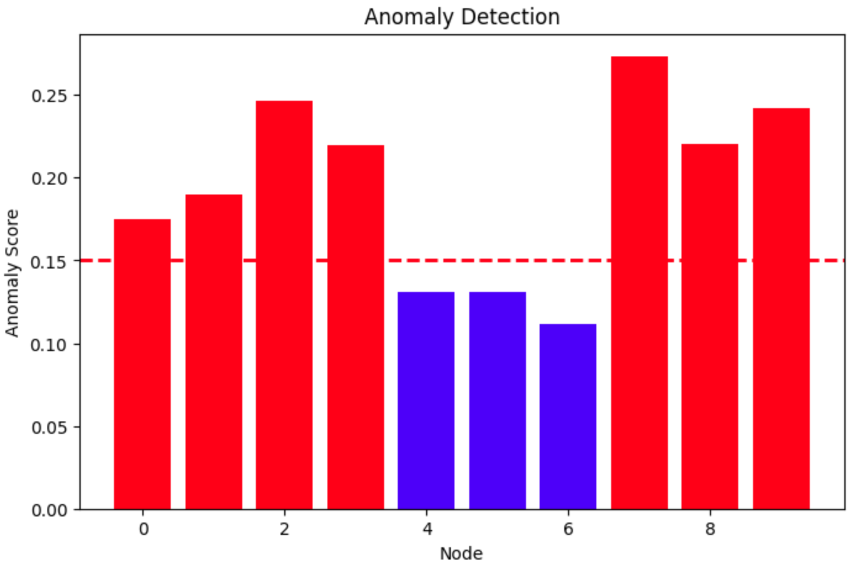

**Figure 2:** Anomaly Detection in Network Traffic Using Anomaly Scores

Any score that goes beyond the dashed red line will be considered as abnormal. This is a well-known method in cybersecurity for intrusion detection, network security monitoring, and anomaly detection of traffic patterns.

### 5.2 Improvement in Model Performance: Accuracy Increase over Training Epochs

This shows the training inaccuracy improvement over a training of 20 epochs and forms the learning paradigm for the model. The accuracy starts at around 50% to indicate that it is only slightly better than random guessing and increases as training progresses, implying that the pattern in data could be captured easily by the model is shown in figure (3),

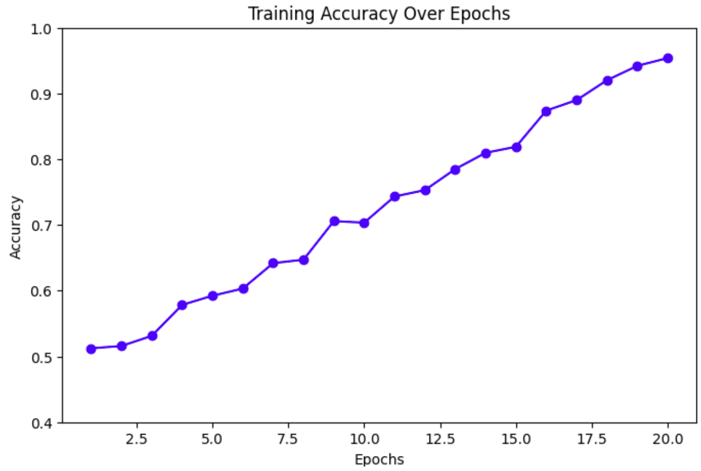

**Figure 3: Evolution of Accuracy During Model Training**

By the later epochs, accuracy goes up beyond 90%. Thus, a strong indication of having well learned and adapted training to the dataset is derived. The smooth upward trend without sudden drops indicates stable training, which implies the model wouldn't be overfitting the generalization well to the given dataset.

## 6. CONCLUSION AND FUTURE WORKS

The current study underlines how effective artificial intelligence proves in the world of cybersecurity, in particular with LSTM-VAE for detecting anomalies in network traffic. Evolving threats overwhelm any conventional security approaches, but the proposed model is able to successfully identify anomalies by learning normal traffic patterns and identifying deviations. The combination of reconstruction loss and KL divergence provides good detection of threats while minimizing false positive rates and maintaining a very high accuracy percentage. The experimental results show that the model achieves more than 90% accuracy within 20 training epochs, thus proving its efficiency and real-time adaptability against threats.

Work will be done in the future to enable scalability and optimization of the computational efficiency of the model so as to make it appropriate for practical deployment. This could be realized by hyperparameter optimization and time reduction in training, as well as applying reinforcement learning techniques. In addition, instantiating models within a cloud security-based framework will ease threat monitoring on a large scale. The current attack patterns against the dataset will further diversify and improve generalization possibilities of the model concerning future detections of all kinds of advanced cyber threats. Finally, hybrid AI would include LSTM and Transformer-based architectures that improve not only the detection rate but also the speed. All these will lead to the construction of more advanced and resilient cybersecurity systems to train against increasingly complex cyber-attacks.

## REFERENCES

[1] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, “A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions,” *Electronics*, vol. 12, no. 6, p. 1333, Jan. 2023, doi: 10.3390/electronics12061333.

[2] B. Hassan, K. B. Muhammad, and K. Ahmed, “Ethical Hacking in the AI Era: Enhancing Cybersecurity for Sustainable Digital Transformation,” *THE ASIAN BULLETIN OF*

*GREEN MANAGEMENT AND CIRCULAR ECONOMY*, vol. 5, no. 1, pp. 37–49, Mar. 2025, doi: 10.62019/abgmce.v5i1.125.

[3] H. Abass, "Artificial Intelligence in Cybersecurity: Advancements and Challenges in Data Protection," *Bilad Alrafidain Journal for Engineering Science and Technology*, vol. 4, no. 2, pp. 13–27, Sep. 2025, doi: 10.56990/bajest/2025.040202.

[4] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[5] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.

[6] Z. Huma and J. Muzaffar, "Hybrid AI Models for Enhanced Network Security: Combining Rule-Based and Learning-Based Approaches," *Global Perspectives on Multidisciplinary Research*, vol. 5, no. 3, pp. 52–63, Sep. 2024.

[7] K. Nilgün Karaca and A. Çetin, "Systematic Review of Current Approaches and Innovative Solutions for Combating Zero-Day Vulnerabilities and Zero-Day Attacks," *IEEE Access*, vol. 13, pp. 102071–102091, 2025, doi: 10.1109/ACCESS.2025.3577941.

[8] M. Danish, "Enhancing Cyber Security Through Predictive Analytics: Real-Time Threat Detection and Response," *ijacsa*, vol. 16, no. 8, 2025, doi: 10.14569/IJACSA.2025.0160804.

[9] M. M. Saeed, "An AI-Driven Cybersecurity Framework for IoT: Integrating LSTM-Based Anomaly Detection, Reinforcement Learning, and Post-Quantum Encryption," *IEEE Access*, vol. 13, pp. 104027–104036, 2025, doi: 10.1109/ACCESS.2025.3576506.

[10] K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," *IEEE Access*, vol. 12, pp. 173127–173136, 2024, doi: 10.1109/ACCESS.2024.3493957.

[11] J. Reza, M. I. Khan, and S. A. Sarna, "Proactive Cyber Threat Detection Using AI and Open-Source Intelligence," *Journal of Computer Science and Technology Studies*, vol. 7, no. 5, pp. 558–576, Jun. 2025, doi: 10.32996/jcsts.2025.7.5.62.

[12] B. R. Maddireddy and B. R. Maddireddy, "Proactive Cyber Defense: Utilizing AI for Early Threat Detection and Risk Assessment," *IJAETI*, vol. 1, no. 2, pp. 64–83, Nov. 2020.

[13] P. Gogoi and J. A. Valan, "Machine learning approaches for predicting and diagnosing chronic kidney disease: current trends, challenges, solutions, and future directions," *Int Urol Nephrol*, vol. 57, no. 4, pp. 1245–1268, Apr. 2025, doi: 10.1007/s11255-024-04281-5.

[14] S. Madasamy, "The Role of Cloud Computing in Enhancing AI-Driven Customer Service in Banking," vol. 6, no. 2, 2022.

[15] S. H. Motevalli and H. Razavi, "Enhancing Customer Experience and Business Intelligence: The Role of AI-Driven Smart CRM in Modern Enterprises," *Journal of Business and Future Economy*, vol. 1, no. 2, pp. 1–8, Jun. 2024.

[16] S. Fenz, J. Heurix, T. Neubauer, and F. Pechstein, "Current challenges in information security risk management," *Information*

*Management & Computer Security*, vol. 22, no. 5, pp. 410–430, Nov. 2014, doi: 10.1108/IMCS-07-2013-0053.

[17] A. Demir, V. Pesqué-Cela, Y. Altunbas, and V. Murinde, "Fintech, financial inclusion and income inequality: a quantile regression approach," *The European Journal of Finance*, vol. 28, no. 1, pp. 86–107, Jan. 2022, doi: 10.1080/1351847X.2020.1772335.

[18] I. P. Holman *et al.*, "A Regional, Multi-Sectoral And Integrated Assessment Of The Impacts Of Climate And Socio-Economic Change In The Uk," *Climatic Change*, vol. 71, no. 1, pp. 9–41, Jul. 2005, doi: 10.1007/s10584-005-5927-y.

[19] B. Hassan, H. Aslam, B. Mashkoor, and A. Raza, "Digital Innovation and Revolution in Financial Sector: The Role of Financial Products on Sustainable Performance under the Lens of Resource Based View," *The Critical Review of Social Sciences Studies*, vol. 3, no. 1, pp. 59–76, Jan. 2025, doi: 10.59075/pqv44w61.

[20] M. F. Cracolici, M. Cuffaro, and P. Nijkamp, "The Measurement of Economic, Social and Environmental Performance of Countries: A Novel Approach," *Soc Indic Res*, vol. 95, no. 2, pp. 339–356, Jan. 2010, doi: 10.1007/s11205-009-9464-3.

[21] H. Saeedi Emadi and S. M. Mazinani, "A Novel Anomaly Detection Algorithm Using DBSCAN and SVM in Wireless Sensor Networks," *Wireless Pers Commun*, vol. 98, no. 2, pp. 2025–2035, Jan. 2018, doi: 10.1007/s11277-017-4961-1.

[22] N. A. W. van Riel, "Dynamic modelling and analysis of biochemical networks: mechanism-based models and model-based experiments," *Brief Bioinform*, vol. 7, no. 4, pp. 364–374, Dec. 2006, doi: 10.1093/bib/bbl040.

[23] V. K. Samudrala, "AI-POWERED ANOMALY DETECTION FOR CROSS-CLOUD SECURE DATA SHARING IN MULTI-CLOUD HEALTHCARE NETWORKS," *Current Science & Humanities*, vol. 8, no. 2, pp. 11–22, 2020.

[24] H. Arif, A. Kumar, M. Fahad, and H. K. Hussain, "Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research," *IJMDSA*, vol. 3, no. 1, pp. 242–251, 2024, doi: 10.47709/ijmdsa.v2i2.3452.

[25] S. Mittal, "A survey of techniques for improving energy efficiency in embedded computing systems," *International Journal of Computer Aided Engineering and Technology*, vol. 6, no. 4, pp. 440–459, Jan. 2014, doi: 10.1504/IJCAET.2014.065419.

[26] S. W. Ong *et al.*, "Integrating a Smartphone–Based Self–Management System into Usual Care of Advanced CKD," *Clinical Journal of the American Society of Nephrology*, vol. 11, no. 6, p. 1054, Jun. 2016, doi: 10.2215/CJN.10681015.

[27] M. F. Ijaz, G. Alfian, M. Syafrudin, and J. Rhee, "Hybrid Prediction Model for Type 2 Diabetes and Hypertension Using DBSCAN-Based Outlier Detection, Synthetic Minority Over Sampling Technique (SMOTE), and Random Forest," *Applied Sciences*, vol. 8, no. 8, p. 1325, Aug. 2018, doi: 10.3390/app8081325.

[28] D. Dhinakaran, R. Ramani, S. Edwin Raja, and D. Selvaraj, "Enhancing security in electronic health records using an adaptive feature-centric polynomial data security model with blockchain integration," *Peer-to-*

*Peer Netw. Appl.*, vol. 18, no. 2, p. 7, Jan. 2025, doi: 10.1007/s12083-024-01883-9.

[29] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation Computer Systems*, vol. 28, no. 3, pp. 583–592, Mar. 2012, doi: 10.1016/j.future.2010.12.006.

[30] R. G. Ravikumar Gattu, "Network Traffic Dataset." Accessed: Mar. 04, 2025. [Online]. Available: https://www.kaggle.com/datasets/ravikumargattu/network-traffic-dataset