Unified Security Operations Dashboard (USOD)

1st Ghulam Mohayudin
Information and Communication Engineering
Islamia University of Bahawalpur
Bahawalpur, Pakistan
ighulammohayudin@gmail.com

2nd Ali Sami
Information and Communication Engineering
Islamia University of Bahawalpur
Bahawalpur, Pakistan
saminagri0111@gmail.com

3rd Zuhaib Iqbal
Information and Communication Engineering
Islamia University of Bahawalpur
Bahawalpur, Pakistan
zuhaibiii14@gmail.com

4th Iftikhar Rasheed
Information and Communication Engineering
Islamia University of Bahawalpur
Bahawalpur, Pakistan
iftikhar.rasheed@iub.edu.pk

***Abstract*—The increasing complexity and diversity of cyber threats demands integrated, intelligent and Unified security solutions. The Unified Security Operations Dashboard (USOD) addresses this problem by combining AI-powered threat intelligence, automated incident response, forensic logs saving, and multi-cloud security monitoring into a centralized platform. This review is written after reading over 50 research papers and their relevance to USOD's objectives. Key findings highlight the effectiveness of Artificial Intelligence, Machine and Deep learning for threat detection, SOAR platforms for automation, blockchain for secure logging, and unified cloud monitoring for visibility. These technologies improve Cybersecurity, but their integration into a cohesive system remains unexplored. USOD aims to bridge this gap by offering a scalable and comprehensive solution to diverse modern security challenges.**

***Index Terms*—Cybersecurity, Artificial Intelligence, Incident Response, Digital Forensics, Multi-Cloud Security, Blockchain**

I. Introduction

The rapid evolution of cyber threats has outpaced traditional security measures, necessitating centralized, intelligent platforms [1]. The Unified Security Operations Dashboard (USOD) integrates AI-driven threat intelligence, automated incident response, forensic logs saving, and multi-cloud monitoring to enhance efficiency and reduce response times [2]. Leveraging technologies like TensorFlow, Ansible, Terraform, Hyperledger Fabric, and cloud security services, USOD aims to provide a scalable, adaptive security ecosystem. This review synthesizes over 50 peer-reviewed studies to assess advancements in these areas, identifying trends, challenges, and their applicability to USOD. By examining AI applications, automation frameworks, forensic methodologies, and multi-cloud security, the paper provides a foundation for USOD's development and highlights research gaps in unified security platforms.

II. Literature Review

A. AI-Powered Threat Intelligence

Artificial Intelligence (AI) and Machine Learning (ML) have transformed cybersecurity by enabling proactive threat detection [1], [3]–[5]. Supervised and unsupervised models, implemented in frameworks like TensorFlow and Scikit-learn, excel in anomaly detection and threat prediction [6], [7]. Deep learning techniques, such as convolutional neural networks, achieve high accuracy in identifying malware from network traffic [8]. Recent studies explore deep reinforcement learning, which adapts to evolving threats through environmental interactions [9]. However, challenges like model interpretability and adversarial attacks persist [10]. These advancements align with USOD's goal of real-time threat analysis using historical and behavioral data [11].

B. Automated Incident Response

Automated incident response minimizes mitigation times through predefined workflows [12], [13]. Security Orchestration, Automation, and Response (SOAR) platforms, such as Cortex XSOAR, integrate tools like Ansible and Terraform to automate policy enforcement [14], [15]. AI/ML enhances SOAR by enabling intelligent decision-making, reducing false positives [15]. Studies highlight SOAR's integration with SIEM systems for streamlined responses [16]. Yet, handling complex, multi-stage attacks remains a challenge [12]. USOD's automated response module leverages AI-driven insights to trigger context-aware actions, building on SOAR principles.

C. Forensic Investigation Tools

Digital forensics ensures accurate incident analysis and compliance [17], [18]. Blockchain technologies, like Hyperledger Fabric, provide tamper-proof logging for attack timeline reconstruction [19]–[21]. Recent research explores cloud forensics, addressing distributed environment challenges [3], [22]–[24]. Standardization remains a hurdle [17]. USOD's forensic toolkit uses blockchain to secure logs, supporting reliable evidence management and regulatory compliance [25], [26].

DOI: https://doi.org/10.67535/tsp.000001.029
Published under the ICACNC 2025 Proceedings

D. Multi-Cloud Security Monitoring

Multi-cloud environments require unified monitoring for comprehensive visibility [27], [28]. SIEM-based approaches integrate alerts from AWS Security Hub, Azure Sentinel, and GCP Security Command Center, enhancing threat detection [28]. Interoperability and data silos pose challenges [29]–[32]. USOD's API-driven integration provides real-time insights and compliance tracking across clouds, addressing these issues. Using multiple cloud services enhances the visibility and scaling of large amount of data.

III. USOD System Architecture

The USOD architecture, as shown in Figure 1, integrates advanced AI/ML algorithms using tensorflow and scikit-learn, automation and orchestration tools, blockchain forensics logging and cloud monitoring into a cohesive cybersecurity platform. This section details the architecture, focusing on the AI/ML algorithms and their integration with other USOD components.

A. Architecture Design

The block diagram (Figure 1) organizes USOD into five components with clear data flow as **User Interface**, **Threat Intelligence Engine**, **Automation & Orchestration**, **Forensics Logging**, and **Multi-Cloud Monitoring**. Each of these serve a unique and important part in overall functionality of the whole USOD app. The **User Interface** utilizes React.js along with Next.js for dynamic dashboards, Express.js for server-side logic, and Chart.js for analytics visualization, providing insights, alerts, and forensic analysis with Javascript being primary language for this purpose. [33], [34]. Security logs are processed in **Threat Intelligence Engine** using AI/ML algorithms (listed above), implemented via TensorFlow and Scikit-learn, to detect anomalies, classify threats, and predict future attacks [35], [36]. Each of the AI algorithm presented in block diagram servers a unique purpose that is different from other algortithms. Next component is **Automation & Orchestration**, it employs Ansible for incident response workflows and Terraform for infrastructure management, automating threat mitigation and policy enforcement [37], [38]. The **Forensics Logging** uses Hyperledger Fabric for tamper-proof forensic logging and Elasticsearch for efficient log analysis. [39], [40]. **Multi-Cloud Monitoring** integrates AWS Security Hub, Azure Sentinel, and GCP Security Command Center for unified visibility across cloud platforms, feeding security logs to the Threat Intelligence Engine. It provides a unifies system scattered through mutliple platforms making it much easier and faster for users to access our USOD app flawlessly [41]–[43]. The extra part of our diagram is **Extensibility** which means that it supports future integrations, such as federated learning or zero-trust architectures, ensuring adaptability to emerging threats.

B. AI/ML Algorithms for Threat Intelligence

The Threat Intelligence Engine employs a suite of machine learning and deep learning algorithms, implemented using TensorFlow and Scikit-learn, to analyze security logs and network traffic. The selected algorithms are:

- **Anomaly Detection**: We will use multiple unsupervised AI models for anomaly detection. **Isolation Forest** is an unsupervised machine learning algorithm that identifies anomalies in high-dimensional security logs by isolating outliers [44]. This algorithm will be used to isolate logs and security events that deviate from the normal. This makes it effective to differentiate between a legitimate and abnormal traffic. **One-Class SVM** is also an unsupervised anomalies detection algorithm that identifies anomalies falling outside a specific boundary. [45]. It makes it best algorithm to detect anomalities slightly deviating from base line. It is particularly useful in our USOD project for finding unusual behavior in network traffic, login patterns, or system activity. **Autoencoders** being an unsupervised model uses neural networks to reconstruct normal data, flagging anomalies from compressed form with high reconstruction errors [46]. As this model is only trained on normal data, so when presented with abnormal data gives significant error. USOD traffic that was never used in training of this data will be flagged by it.
- **Threat Classification**: Threat is classified using many supervised machine learning algorithms.**Random Forest Classifier** is a supervised machine learning algorithm that combines decision trees for robust threat classification [47]. It combines multiple decision trees to enhance model quality and accuracy. It works by creating group of trees trained on a large network dataset, then aggregates the results of these trees by voting. **Gradient Boosting Classifier** is also a supervised machine learning algorithm that enhances the classification accuracy through boosting [48].In boosting technique a powerful model is created by combining multiple simpler models in sequence. The error in one of the model is corrected by next model. The traffic of USOD when analyzed through muitple models in Gradien Boosting Classifier flaggs abnormal traffic from normal one. **Convolutional Neural Networks (CNN)**: is a supervised machine learning algorithm that analyzes network traffic patterns to identify threats by extracting spatial features of presented graphical network traffic [49]. This algorithm is specially designed to work on images and graphs. It is greatly adapted in cybersecurity and relevant technologies. USOD network traffic is generated using **Charts.js**, a library in JavaScript, specially used to create visual form of data provided.
- **Sequence Prediction**: Sequence of future anomalies is predicted using sequence prediction. It uses **Long Short-Term Memory (LSTM) Networks** is a type of Recurrent Neural Network (RNN) to predict future threat sequences based on historical data [50]. It is preferred for modeling sequential data and long-range dependencies. As the USOD analyze and evaluates a huge amount of data including logs, ips, alerts, attacks and other data forms.

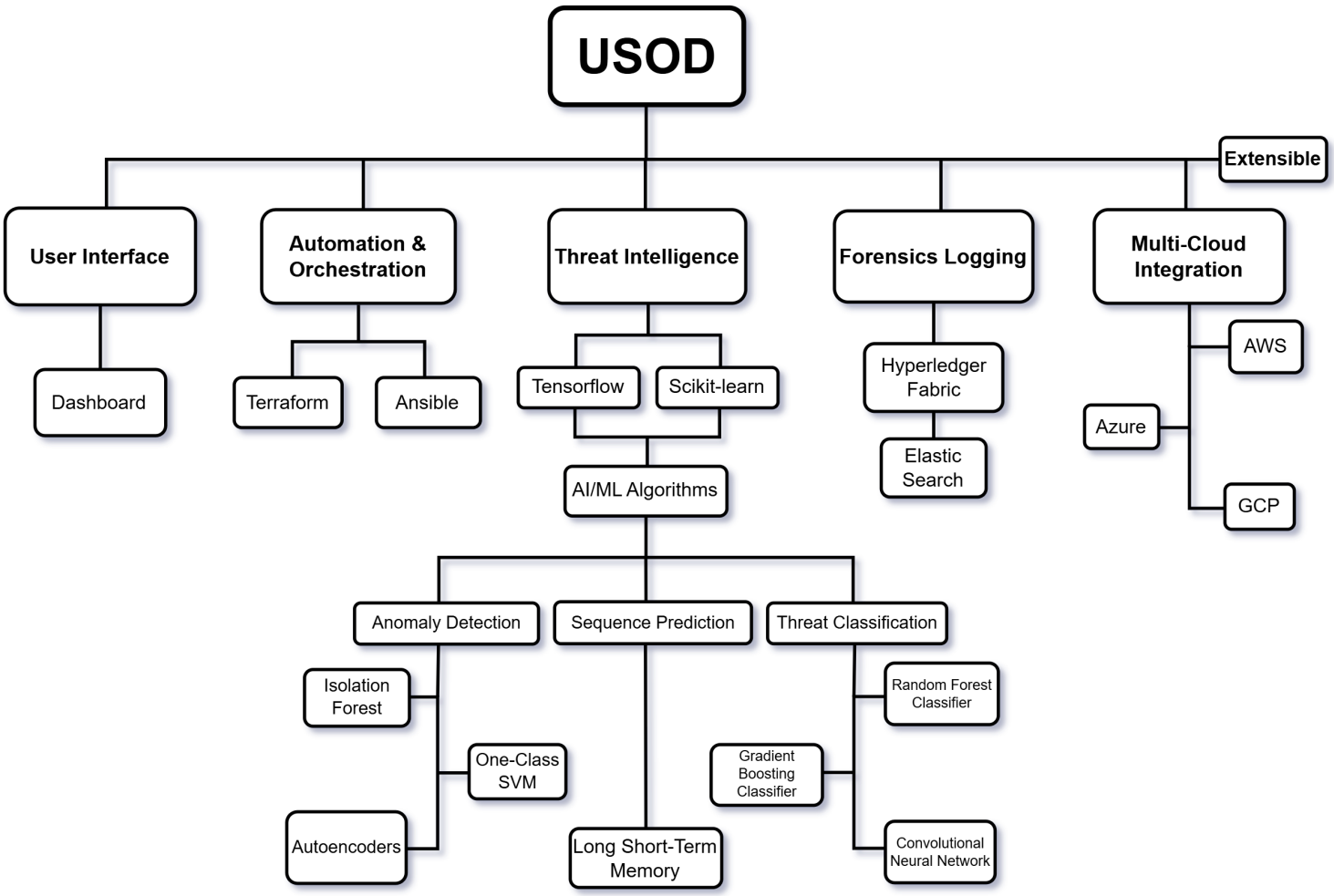

Fig. 1. The diagram illustrates five key components: User Interface (Dahshboard), Automation & Orchestration (Ansible, Terraform), Threat Intelligence Engine (AI/ML Models for Anomaly Detection: Isolation Forest, One-Class SVM, Autoencoders; Threat Classification: Random Forest, Gradient Boosting, CNN; Sequence Prediction: LSTM; supported by TensorFlow), Forensics Logging (Hyperledger Fabric, Elasticsearch, Terraform), Multi-Cloud Monitoring (AWS Security Hub, Azure Sentinel, GCP Security Command Center) and Extensibility (supports future integrations like federated learning).

These datasets can be used to train our LSTM and predict the future attacks and attacks frequency.

Security logs flow from Multi-Cloud Monitoring to the Threat Intelligence Engine, where AI/ML algorithms detect and classify threats. Threat alerts trigger automated responses via Ansible and Terraform, with incident details logged in Hyperledger Fabric and analyzed using Elasticsearch. The User Interface provides real-time insights and control, ensuring efficient security operations.

This architecture ensures USOD's scalability and adaptability to evolving cyber threats.

IV. Discussion

The literature underscores the potential of AI, automation, forensics, and multi-cloud monitoring to enhance cybersecurity [1], [15], [17], [27]. AI improves detection accuracy by using multiple models each using different approach then others, SOAR streamlines responses and automation, blockchain ensures log integrity, and unified monitoring enhances visibility. However, integrating these into a single platform is underexplored [3]. USOD addresses this gap with a modular architecture, combining AI-driven analytics, automated workflows, secure logging, and cloud integration. Challenges include model interpretability, automation scalability, forensic standardization, and cloud interoperability, which USOD mitigates through extensible design and advanced technologies.

V. Conclusion

This review highlights how Unified Security Operations Dashboard comprising of Automation and Orchestration along with Threat Intelligent System using multiple Artificial Intelligence and Machine Learning algorithms, forensics logging on Hyperledge Blockchain and Multi-cloud monitoring to work on real-time analysis can improve overall security structure of an organization and strengthens its overall capability to detect and defend against network attacks. USOD's development will contribute to efficient, adaptive security operations,

addressing literature gaps. Future research should focus on standardized integration frameworks and adding advanced AI models that will analyze and interpret network traffic in better and more efficient way. We can expand the multi-cloud support in future and enhance the visualization and analytics using interactive tools and predictive capabilities. Scalability and performance also needs to be improved in future given that the project is comprehensive and needs to be implemented at organizational level to be of full potential. We can also enhance the Blockchain part of the USOD along with AI-driven Orchestration and Zero-trust integration.

REFERENCES

[1] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, p. 101804, 2023.

[2] A. J. G. De Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial intelligence-based cyber security in the context of industry 4.0—a survey," *Electronics*, vol. 12, no. 8, p. 1920, 2023.

[3] A. H. Salem, S. M. Azzam, O. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of ai-driven detection techniques," *Journal of Big Data*, vol. 11, no. 1, p. 105, 2024.

[4] I. Jada and T. O. Mayayise, "The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review," *Data and Information Management*, vol. 8, no. 2, p. 100063, 2024.

[5] M. E. Bonfanti, "Artificial intelligence and the offence-defence balance in cyber security," *Cyber Security: Socio-Technological Uncertainty and Political Fragmentation. London: Routledge*, pp. 64–79, 2022.

[6] L. Ofusori, T. Bokaba, and S. Mhlongo, "Artificial intelligence in cybersecurity: A comprehensive review and future direction," *Applied Artificial Intelligence*, vol. 38, no. 1, p. 2439609, 2024.

[7] J.-h. Li, "Cyber security meets artificial intelligence: a survey," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 12, pp. 1462–1474, 2018.

[8] N. Mohamed, "Current trends in ai and ml for cybersecurity: A state-of-the-art survey," *Cogent Engineering*, vol. 10, no. 2, p. 2272358, 2023.

[9] M. Sewak, S. K. Sahay, and H. Rathore, "Deep reinforcement learning for cybersecurity threat detection and protection: A review," in *International Conference On Secure Knowledge Management In Artificial Intelligence Era*. Springer, 2021, pp. 51–72.

[10] R. Raimundo and A. Rosário, "The impact of artificial intelligence on data system security: A literature review," *Sensors*, vol. 21, no. 21, p. 7029, 2021.

[11] S. Verma and N. Gupta, "Application of artificial intelligence in cybersecurity," *Innovations in Computer Science and Engineering: Proceedings of 7th ICICSE*, pp. 65–72, 2020.

[12] H. Karlzen and T. Sommestad, "Automatic incident response solutions: a review of proposed solutions' input and output," in *Proceedings of the 18th International Conference on Availability, Reliability and Security*, 2023, pp. 1–9.

[13] C. M. Patterson, J. R. Nurse, and V. N. Franqueira, "Learning from cyber security incidents: A systematic review and future research agenda," *Computers & Security*, vol. 132, p. 103309, 2023.

[14] H. Mouratidis, S. Islam, A. Santos-Olmo, L. E. Sanchez, and U. M. Ismail, "Modelling language for cyber security incident handling for critical infrastructures," *Computers & Security*, vol. 128, p. 103139, 2023.

[15] J. Kinyua and L. Awuah, "Ai/ml in security orchestration, automation and response: Future research directions." *Intelligent Automation & Soft Computing*, vol. 28, no. 2, 2021.

[16] F. E. Catota, M. G. Morgan, and D. C. Sicker, "Cybersecurity incident response capabilities in the ecuadorian financial sector," *Journal of Cybersecurity*, vol. 4, no. 1, p. tyy002, 2018.

[17] S. L. Garfinkel, "Digital forensics research: The next 10 years," *digital investigation*, vol. 7, pp. S64–S73, 2010.

[18] A. Shaaban and N. Abdelbaki, "Comparison study of digital forensics analysis techniques; findings versus resources," *Procedia Computer Science*, vol. 141, pp. 545–551, 2018.

[19] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "A systematic literature review of blockchain cyber security," *Digital Communications and Networks*, vol. 6, no. 2, pp. 147–156, 2020.

[20] R. Prakash, V. Anoop, and S. Asharaf, "Blockchain technology for cybersecurity: A text mining literature analysis," *International Journal of Information Management Data Insights*, vol. 2, no. 2, p. 100112, 2022.

[21] S. M. Idrees, M. Nowostawski, R. Jameel, and A. K. Mourya, "Security aspects of blockchain technology intended for industrial applications," *Electronics*, vol. 10, no. 8, p. 951, 2021.

[22] A. Adel, "A conceptual framework to improve cyber forensic administration in industry 5.0: qualitative study approach," *Forensic Sciences*, vol. 2, no. 1, pp. 111–129, 2022.

[23] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain: research and applications*, vol. 3, no. 2, p. 100067, 2022.

[24] S. Mahmood, M. Chadhar, and S. Firmin, "Cybersecurity challenges in blockchain technology: A scoping review," *Human Behavior and Emerging Technologies*, vol. 2022, no. 1, p. 7384000, 2022.

[25] V. Wylde, N. Rawindaran, J. Lawrence, R. Balasubramanian, E. Prakash, A. Jayal, I. Khan, C. Hewage, and J. Platts, "Cybersecurity, data privacy and blockchain: A review," *SN computer science*, vol. 3, no. 2, p. 127, 2022.

[26] S. Johar, N. Ahmad, W. Asher, H. Cruickshank, and A. Durrani, "Research and applied perspective to blockchain technology: A comprehensive survey," *Applied Sciences*, vol. 11, no. 14, p. 6252, 2021.

[27] Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-Rimy, "Secure cloud infrastructure: A survey on issues, current solutions, and open challenges," *Applied Sciences*, vol. 11, no. 19, p. 9005, 2021.

[28] E. Tuyishime, T. C. Balan, P. A. Cotfas, D. T. Cotfas, and A. Rekeraho, "Enhancing cloud security—proactive threat monitoring and detection using a siem-based approach," *Applied Sciences*, vol. 13, no. 22, p. 12359, 2023.

[29] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, "An analysis of security issues for cloud computing," *Journal of internet services and applications*, vol. 4, pp. 1–13, 2013.

[30] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Data security and privacy in cloud computing," *International Journal of Distributed Sensor Networks*, vol. 10, no. 7, p. 190903, 2014.

[31] A. W. Malik, D. S. Bhatti, T.-J. Park, H. U. Ishtiaq, J.-C. Ryou, and K.-I. Kim, "Cloud digital forensics: Beyond tools, techniques, and challenges," *Sensors*, vol. 24, no. 2, p. 433, 2024.

[32] S. Alam, M. Shuaib, W. Z. Khan, S. Garg, G. Kaddoum, M. S. Hossain, and Y. B. Zikria, "Blockchain-based initiatives: current state and challenges," *Computer Networks*, vol. 198, p. 108395, 2021.

[33] React.js Team, "React.js official documentation," https://reactjs.org/docs/getting-started.html, 2025.

[34] Chart.js Team, "Chart.js documentation," https://www.chartjs.org/docs/latest/, 2025.

[35] TensorFlow Team, "Tensorflow official website," https://www.tensorflow.org/, 2025.

[36] Scikit-learn Team, "Scikit-learn documentation," https://scikit-learn.org/stable/, 2025.

[37] Ansible Team, "Ansible documentation," https://docs.ansible.com/, 2025.

[38] Terraform Team, "Terraform documentation," https://www.terraform.io/docs, 2025.

[39] Hyperledger Fabric Team, "Hyperledger fabric documentation," https://hyperledger-fabric.readthedocs.io/, 2025.

[40] Elasticsearch Team, "Elasticsearch official website," https://www.elastic.co/elasticsearch/, 2025.

[41] AWS Security Hub Team, "Aws security hub documentation," https://docs.aws.amazon.com/securityhub/, 2025.

[42] Azure Sentinel Team, "Azure sentinel overview," https://docs.microsoft.com/en-us/azure/sentinel/, 2025.

[43] Google Cloud Security Command Center Team, "Google cloud security command center documentation," https://cloud.google.com/security-command-center/docs, 2025.

[44] F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation forest," in *2008 eighth ieee international conference on data mining*. IEEE, 2008, pp. 413–422.

[45] B. Schölkopf, J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, "Estimating the support of a high-dimensional distribution," *Neural computation*, vol. 13, no. 7, pp. 1443–1471, 2001.

[46] M. Sakurada and T. Yairi, "Anomaly detection using autoencoders with nonlinear dimensionality reduction," in *Proceedings of the MLSDA 2014 2nd workshop on machine learning for sensory data analysis*, 2014, pp. 4–11.
[47] L. Breiman, "Random forests," *Machine learning*, vol. 45, pp. 5–32, 2001.
[48] J. H. Friedman, "Greedy function approximation: a gradient boosting machine," *Annals of statistics*, pp. 1189–1232, 2001.
[49] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning," *nature*, vol. 521, no. 7553, pp. 436–444, 2015.
[50] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.