A Comprehensive Review of ML-Based Cloud Security: Biometric Authentication, Threat Detection, and Malware Analysis

Muhammad Abdullah Bajwa *, Mina Fatima *, Sufyan Munawar *, Farhan Hassan Malik *,
*Department of Information and Communication Engineering, Faculty of Engineering and Technology,
The Islamia University of Bahawalpur, Punjab, Pakistan

***Abstract*—A comprehensive review of machine learning (ML) techniques for enhancing cloud security through biometric authentication, threat detection, and malware analysis. It explores how advanced ML and deep learning models—such as CNNs, RNNs, BiLSTM, SVMs, and Random Forest—are applied to safeguard cloud environments. The review categorizes over 60 recent studies, highlighting key methods for intrusion detection, malware classification, and anomaly detection. Special attention is given to multimodal biometric authentication using ECG, fingerprint, and facial recognition, as well as the integration of adaptive encryption and multi-factor authentication (MFA) for robust access control. Practical use cases in healthcare, IoT, and secure remote services are discussed, alongside emerging trends such as Zero Trust Architecture and self-learning AI. By synthesizing state-of-the-art research, this study provides a layered framework for developing intelligent, resilient, and privacy-preserving cloud security systems.**

***Index Terms*—Cloud Security, Machine Learning, Biometric Authentication, Threat Detection, Malware Analysis, Encryption, Deep Learning, Multi-factor Authentication**

I. Introduction

An ML-based framework for ECG biometric authentication, improving data quality with new preprocessing techniques and quality metrics. It defines three key use cases—hospital, security checks, and wearables—and introduces a time-slicing method for better training data. A MATLAB toolbox is also provided to support implementation and research [1]. The paper provides a comprehensive systematic review of machine learning applications in cloud security. It analyzes 63 studies from 2004 to 2019, identifying 11 major cloud security areas such as DDoS, data privacy, and intrusion detection [2]. A layered security approach for backup systems using encryption and multi-factor authentication (MFA). It evaluates encryption methods like AES, RSA, and ECC, and MFA techniques including OTPs and biometrics. The study emphasizes combining both to enhance data protection, prevent breaches, and mitigate cyber threats. It also analyzes real-world cases and suggests improvements for better security and usability [3]. A robust multi-factor authentication system for secure remote access to cloud-based healthcare services using biometrics and artificial intelligence. It combines fingerprint, facial, and iris recognition with AI models for anomaly detection and adaptive authentication. Testing showed high accuracy and usability, significantly outperforming traditional methods. The solution emphasizes privacy, scalability, and user accessibility, aiming to enhance trust and adoption in healthcare [4]. An AI-driven framework for real-time threat detection in cloud environments using machine learning. It combines various ML techniques to detect known and emerging threats, addresses implementation challenges, and validates effectiveness through case studies. Key focus areas include scalability, accuracy, and operational efficiency [5].

Artificial intelligence enhances cloud security through real-time threat detection, predictive analytics, and automated response. It addresses challenges like false positives, data privacy, and adversarial attacks. The study also emphasizes future trends like self-learning AI and integration with Zero Trust models for stronger, adaptive security [6]. A machine learning-based cloud security framework combining multi-factor authentication and adaptive cryptography. It uses passwords, conditional attributes, and fingerprints, with dynamic dual-encryption algorithms selected based on predicted cyber-attacks. A hybrid CNN-transformer model achieves high attack prediction accuracy (96.8%), allowing real-time adaptation of encryption strategies. This approach enhances protection against threats like spoofing, phishing, and credential stuffing in cloud environments [7].

Artificial Intelligence and machine learning, particularly neural networks, enhance biometric security through multi-modal authentication systems. It reviews neural architectures like CNNs, RNNs, and GANs used for integrating biometric traits (e.g., face, fingerprint, voice). The study evaluates fusion techniques, real-world applications, and challenges like data privacy and algorithmic bias. It concludes that AI-powered multimodal systems offer greater accuracy, resilience, and scalability compared to unimodal systems [8]. A secure IoT-cloud healthcare framework using fused ECG and PPG signals for biometric authentication. It employs homomorphic encryption and BiLSTM models, achieving 100 percent accuracy. The system ensures strong protection, scalability, and real-time authentication for personalized healthcare [9]. An integrated network security framework that combines machine learning and multi-factor authentication (MFA) to enhance intrusion detection. It uses advanced ML models like XGBoost and deep learning techniques, along with data preprocessing

DOI: https://doi.org/10.67535/tsp.000001.033
Published under the ICACNC 2025 Proceedings

and SMOTE to handle imbalanced datasets. The system is validated using real-world datasets and achieves high accuracy in detecting threats. The study also explores the role of blockchain in strengthening data integrity and presents a structured methodology for secure, scalable network protection [10]. A machine learning framework for detecting advanced API threats like DDoS and injection attacks. It uses models like LSTM, SVM, and Random Forest, with LSTM achieving the highest accuracy. The study highlights real-time detection, adaptive thresholds, and suggests future use of Explainable AI [11].

Big Data and AI/ML are transforming cybersecurity by enabling real-time threat detection and predictive modeling. It highlights the use of supervised, unsupervised, and deep learning methods like neural networks, SVMs, and graph neural networks for detecting anomalies in massive data streams. It also discusses data collection, preprocessing, and challenges like integration, scalability, privacy, and ethical concerns. The study emphasizes that intelligent, adaptive systems are essential for defending against modern cyber threats [15]. Machine learning enhances cybersecurity by enabling systems to detect complex, evolving threats through pattern recognition and anomaly detection. It discusses ML methods like supervised, unsupervised, and deep learning for threat identification, behavior analysis, and intrusion detection. The study highlights real-world applications, benefits, and challenges such as adversarial attacks and ethical concerns. It concludes that machine learning is essential for building adaptive, automated, and resilient cyber defense systems in today's digital landscape [16].

The growing importance of cybersecurity as digital systems become essential to national infrastructure. It discusses various types of cyber threats, from script kiddies to nation-state actors, and presents strategies for prevention, detection, and response. Key security mechanisms like authentication, access control, intrusion detection, and software assurance are explained. The paper emphasizes the need for proactive, well-engineered security systems and highlights critical vulnerabilities in Windows and Unix platforms [17]. An in-depth survey of modern cybersecurity threats driven by emerging technologies like cloud computing, social media, smartphones, and critical infrastructure systems. It highlights the evolution of malware, vulnerabilities in hardware/software/networks, and the inadequacy of traditional perimeter defenses. New attack vectors such as botnets, social engineering, and insider threats are discussed. The authors propose advanced detection strategies, policy integration, and emphasize future research in trust management, secure architectures, and privacy preservation [18]. The growing complexity and volume of cybersecurity threats, especially due to increased digitalization and the use of personal devices (BYOD). It identifies malware, ransomware, phishing, cryptojacking, and APTs as top attack types, emphasizing that most breaches stem from human error and outdated defenses. It also reviews evolving attack vectors like malicious email attachments, supply chain attacks, and infected USBs. The authors recommend a layered defense approach involving antivirus software, firewalls, training, and data access restrictions to improve cyber resilience [19]. The transformative role of IoT, machine learning, and deep learning in healthcare, highlighting applications in home healthcare, m-health, and hospital management, while addressing challenges like security, interoperability, and data quality. It emphasizes IoT's potential to enhance patient outcomes through real-time monitoring and personalized care, identifying research gaps in model interpretability, privacy, and real-time performance for future advancements [20].

A comprehensive scientometric analysis of global research trends at the intersection of machine learning and cybersecurity from 2016 to 2025. It identifies key contributors, emerging topics, and collaborative networks using bibliometric tools, offering strategic insights for future interdisciplinary research and policy formulation in AI-driven cybersecurity [21]. The integration of big data, cybersecurity, and ERP systems, proposing deep learning as a solution to enhance security and operational efficiency. It highlights the challenges of managing complex data and cyber threats, supported by case studies demonstrating practical deep learning applications in ERP cybersecurity [22].

II. Cyber Security Threat's and Challenges

A comprehensive review of 33 recent studies (2020–2024) applying deep learning, reinforcement learning, and ensemble methods to intrusion detection systems. It evaluates these advanced techniques for their effectiveness in enhancing detection accuracy and adaptability, identifies existing challenges, and outlines future research directions for developing robust and intelligent network security solutions [23]. Cybersecurity challenges in Digital Twin (DT) technology, categorizing DTs into five types and analyzing associated risks, common attacks, and security strategies like encryption and machine learning. It highlights sector-specific vulnerabilities and proposes future research directions for scalable, adaptive security frameworks to enhance DT resilience [24]. In the contemporary digital era, cybersecurity has emerged as a critical domain, driven by the rapid expansion of cloud infrastructure, the proliferation of online services, and the widespread adoption of Bring Your Own Device (BYOD) policies. Across multiple studies, including surveys and analytical frameworks, it is evident that organizations and individuals alike face an increasingly complex and evolving threat landscape. Among the most persistent and damaging threats are malware attacks, especially polymorphic malware which constantly changes its code to avoid detection. Reports show that up to 95% of malware samples now exhibit polymorphic characteristics, making traditional signature-based antivirus solutions insufficient.

An extensive review of phishing attacks, covering classic and modern techniques, including spear phishing, smishing, vishing, and QRishing. It categorizes phishing based on the medium, vector, and technical approach, revealing how attackers exploit human psychology and technical flaws. Real-world examples like Steam scams and Ukraine's power grid attack emphasize phishing's devastating impact. The study highlights

TABLE I
REVIEW OF EXISTING TECHNIQUES FOR MACHINE LEARNING BASED CLOUD SECURITY

Ref.	Technique	Dataset/Tool	Findings/Results	Limitations
[12]	Machine Learning (e.g., Decision Trees, SVM)	ISOT Dataset	Achieved 95.9% of accuracy	Struggled with accuracy when tested on a different dataset (ISOT).
[13]	Machine Learning Algorithms(Logistic Regression, Random Forest, K-Nearest Neighbors (KNN),Naïve Bayes)	PIMA Indian Diabetes Dataset	Achieved 81.17% accuracy and 0.82% Precision	Limitations include small dataset size, limited feature diversity, and missing deeper data preprocessing or validation methods.
[14]	Cryptographic Technique e.g., Multi-Factor Authentication (MFA) using Digital Signature	No Specific dataset/tool used	Lightweight, MITM protection, scalable	DoS/DDoS , Sybil vulnerabilities

the need for awareness, technical defenses, and proactive anti-phishing strategies [25].

A significant emerging threat discussed in several papers is cryptojacking, where attackers hijack computing resources to mine cryptocurrencies such as Monero and Bitcoin. This trend has seen a 400 percent increase, fueled by its stealth, profitability, and minimal risk compared to other attack types. Studies report botnets like Smominru infecting over 500,000 devices, generating millions of dollars in illicit revenue. Similarly, Advanced Persistent Threats (APTs), often state-sponsored, have been highlighted for their stealth, persistence, and capacity to bypass traditional defenses while targeting government, academic, and corporate systems over extended periods.

The Internet of Things has introduced a new frontier of vulnerabilities. Devices with minimal built-in security are often exploited to form botnets, as seen with the Mirai attack, which conducted one of the largest DDoS attacks in history. IoT vulnerabilities are compounded by poor patch management, insecure protocols, and default credentials.

All papers agree that the human factor remains a critical weakness. Lack of awareness, poor password hygiene, and susceptibility to social engineering are cited as leading causes of breaches.

Surveys show that 63% of breaches involve stolen or weak credentials, and 93% of organizations have experienced compromise, many more than once per year. This underscores the need for comprehensive user education, periodic security audits, and strict access controls.

In response to these threats, the reviewed literature strongly advocates for a multi-layered defense strategy. This includes the integration of machine learning models for behavior-based anomaly detection, biometric authentication for access control, encryption standards (RSA, AES) to protect data integrity, and Zero Trust Architectures (ZTA) to ensure continuous verification and least-privilege access. The use of smart contracts within blockchain environments was also explored for securing transaction systems in cloud-based e-commerce.

AI security challenges, including data privacy, adversarial attacks, model inversion, and IP theft, while evaluating advanced solutions like homomorphic encryption, secure multi-party computation, federated learning, and confidential computing. It highlights CYSEC's ARCA Trusted OS and Attested Launch protocol, which utilize trusted execution environments to ensure robust AI security across distributed deployments [29].

III. DETECTION TECHNIQUES

Machine learning Based Detection

- **Random Forest , Decision Trees (RF,DT) :** Random Forest and Decision Trees as traditional machine learning approaches used in malware detection tasks. These models serve as benchmarks for evaluating the performance and certification of more advanced AI-based malware detectors. Although not central to the proposed method, RF and DT are cited in related work for their simplicity and effectiveness. Their mention supports the comparative analysis of model robustness, accuracy, and privacy [30]. Random Forest and Decision Trees as part of machine learning-based authentication techniques in IoT security. Specifically, Random Forest is utilized in malware detection and classification of runtime behaviors, as mentioned in Branch et al.'s study. These models are appreciated for their flexibility and ability to handle various forms of cyber-attacks. However, metrics like False Positive/Negative rates were not deeply evaluated in the cited implementation [14]. As part of machine learning approaches for detecting cyber attacks in Industrial IoT systems. These models are noted for their high accuracy, especially in mitigating DDoS attacks using ML classifications. In particular, tree-based models and XGBoost decision-making trees achieved over 99% accuracy in threat detection. Their efficiency in classifying anomalous traffic highlights their suitability for security in IIoT environments. [31]
- **Support Vector Machines (SVM) :** SVM as an effective machine learning technique for malware detection in IoT environments. SVMs are applied to tasks like object localization, intrusion detection, and anomaly classification, showing high accuracy (up to 98 percent) in certain applications. Variants like linear SVM and ellipsoidal SVM were explored to enhance detection and manage outliers in data. Furthermore, hybrid models that combine SVM with deep belief networks were proposed

TABLE II
REVIEW OF EXISTING TECHNIQUES FOR DEEP LEARNING BASED CLOUD SECURITY

Ref.	Technique	Dataset/Tool	Findings/Results	Limitations
[26]	Deep Learning (e.g., CNN, RNN, LSTM)	Cloud/Fog/Edge platforms Tools:Specialized hardware (e.g., GPUs, FPGAs for acceleration)	accuracy ranging from 84% to over 99%, with LSTM and CNN variants	Data Dependency, Imbalanced and Noisy Data
[27]	Deep Learning Algorithms(Generative Adversarial Networks (GANs), Autoencoders	TensorFlow, PyTorch (implied).	Superior for complex tasks like NLP, image processing, and sequential modeling.	Black-box model, Computational cost
[28]	Cryptographic Technique e.g., SHA-512 Hash Function, Homomorphic Encryption (HE)	Dataset and Tools e.g.,MNIST, Python and Cryptographic library	Achieved Accuracy 98.9% and precision 0.94	Increased Computational Cost, Limited to MNIST

for improved performance in real-world data sets [32]. Support Vector Machines (SVM) as part of a machine learning-based methodology for Android malware detection. SVMs are used in both static and dynamic analysis, particularly in a hierarchical classification system for distinguishing malware types. A kernel-based SVM is applied to permission-based features for classifying apps as malicious or benign. The approach demonstrates high accuracy and is optimized using ROC curve analysis for improved detection performance [33]. Support Vector Machines (SVMs) as one of the classical machine learning algorithms used for IoT security applications. SVMs are referenced as effective for classifying complex patterns in data to detect threats like unauthorized access or cyber-attacks. Though the focus is mainly on broader ML/DL integration, SVMs are listed among the potential solutions. Their utility is noted for tasks such as intrusion detection and data classification in constrained environments [34].

- **K-Nearest Neighbors (KNN) :** K-Nearest Neighbors (KNN) as one of the traditional machine learning models commonly used in cybersecurity tasks, including intrusion and malware detection. KNN is acknowledged for its simplicity and effectiveness in classification problems within adversarial machine learning scenarios. Although not central to the proposed solutions, it is referenced as part of the model suite evaluated for robustness. KNN is noted to be vulnerable to adversarial attacks, emphasizing the need for robust defense strategies in ML-based cybersecurity systems [35]. K-Nearest Neighbors as one of the machine learning algorithms applied in ransomware detection. KNN is used to classify ransomware samples by analyzing behavior patterns extracted from dynamic analysis such as API calls and network activity [36].The summary of the prominent machine learning techniques has been given in Table I.

Deep learning Based Detection

- **Convolutional Neural Networks (CNN) :** CNNs are employed for feature extraction from network traffic data to identify patterns related to cyber threats. Their ability to detect anomalies and intrusions makes them effective in enhancing real-time threat detection. The integration of CNNs contributes to the framework's high accuracy in detecting network attacks in smart environments [37]. CNNs as a type of deep learning model employed for cybersecurity tasks like malware and intrusion detection. CNNs are particularly effective when cybersecurity data are transformed into image-like formats, enabling pattern recognition. Their layered architecture aids in extracting hierarchical features crucial for accurate classification. The paper highlights CNNs' strong performance in Android malware detection and classifying various network threats [38]. CNN's as part of the future advancements in fraud detection within financial cybersecurity systems. CNNs are recognized for their ability to analyze complex data patterns, which enhances the performance of machine learning-based fraud detection models. They are expected to contribute to more scalable and adaptive systems. Although CNNs are not the central focus, their potential in detecting sophisticated threats is acknowledged in the proposed framework [39].

- **Recurrent Neural Networks (RNN) :** RNN's process time-series data from inertial sensors to identify individuals based on their walking behavior. The system combines GRU's with template protection mechanisms to enhance privacy and security. The use of GRU's supports effective learning of sequential features in behavioral biometric data for robust authentication [40]. RNNs, particularly in the form of BiLSTM models, to enhance network intrusion detection systems. These models are capable of capturing temporal dependencies in network traffic data, which helps in identifying patterns associated with cyber threats. This hybrid deep learning approach significantly improves the accuracy and robustness of threat detection in dynamic network environments [10]. An adaptive threat detection model for cloud-assisted IoT systems using RNN-based architectures. Specifically, RNN layers were employed with disjoint training and testing models to detect malware across varied IoT environments. These RNNs process sequences of data to capture temporal patterns relevant to malicious behavior. The approach improved malware detection accuracy but introduced higher computational complexity [32]. The summary of the prominent deep learning techniques is given in Table II.

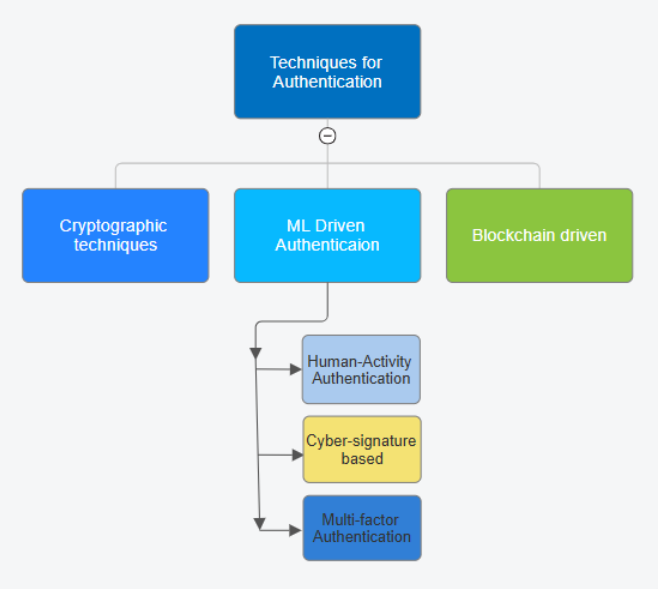

Fig.1. Comprehensive classification of Authentication techniques for IoT.

IV. Conclusion

A detailed review of machine learning-driven frameworks for enhancing cloud security through biometric authentication, threat detection, and malware analysis. It highlights how integrating deep learning models like CNN, RNN, and BiLSTM with traditional ML techniques (e.g., SVM, Random Forest, KNN) enables robust identification of cyber threats across diverse environments. The study emphasizes the critical role of adaptive encryption, multi-factor authentication, and real-time anomaly detection in securing sensitive cloud applications such as healthcare and IoT. It concludes that a layered, intelligent security architecture—powered by AI and supported by Zero Trust principles—is essential for building resilient, scalable, and privacy-preserving cloud infrastructures in the future.The paper also highlights the use of biometric modalities—like ECG signals, fingerprints, and facial recognition—for secure identity verification within multi-factor authentication (MFA) systems. In conclusion, this comprehensive review lays the groundwork for developing intelligent, scalable, and self-adaptive cloud security systems. It encourages further exploration into explainable AI, federated learning, and AI-driven policy automation to enhance trust, accountability, and resilience in cloud-centric digital infrastructures.The study demonstrates how machine learning enhances the accuracy and efficiency of threat identification and response in real time.

References

[1] K. K. Swamy, S. N. Likhitha, P. S. Keerthi, P. Nandini, and V. Srinidhi, "Designing secure and efficient biometric-based secure access mechanism for cloud services ml," *Turkish Journal of Computer and Mathematics Education*, vol. 14, no. 3, pp. 667–671, 2023.

[2] A. B. Nassif, M. A. Talib, Q. Nasir, H. Albadani, and F. M. Dakalbab, "Machine learning for cloud security: a systematic review," *IEEE Access*, vol. 9, pp. 20 717–20 735, 2021.

[3] L. White and S. A. Fathima, "Encryption and multi-factor authentication in backup systems: A layered approach to securing data."

[4] O. AKINOLA, "Robust authentication mechanisms integrating biometrics and ai for securing remote access to cloud-based healthcare services," *World Journal of Advanced Research and Reviews*, vol. 23, no. 3, 2024.

[5] S. K. Sundaramurthy, N. Ravichandran, A. C. Inaganti, and R. Muppalaneni, "Ai-driven threat detection: Leveraging machine learning for real-time cybersecurity in cloud environments," *Artificial Intelligence and Machine Learning Review*, vol. 6, no. 1, pp. 23–43, 2025.

[6] B. John, "Ai-driven threat detection and mitigation in cloud environments," 2025.

[7] K. Sasikumar and S. Nagarajan, "Enhancing cloud security: A multi-factor authentication and adaptive cryptography approach using machine learning techniques," *IEEE Open Journal of the Computer Society*, 2025.

[8] V. Kolluri, S. Jain, M. Malaga, and J. Das, "Advancing biometric security through ai and ml: A comprehensive analysis of neural network architectures for multimodal authentication systems."

[9] V. S. Satukumati, "Revolutionizing healthcare: A comprehensive framework for personalized iot and cloud computing-driven healthcare services with smart biometric identity management."

[10] R. K. Mahmood, A. I. Mahameed, N. Q. Lateef, H. M. Jasim, A. D. Radhi, S. R. Ahmed, and P. Tupe-Waghmare, "Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection," *Journal of Robotics and Control (JRC)*, vol. 5, no. 5, pp. 1502–1524, 2024.

[11] P. Ranjan and S. Dahiya, "Advanced threat detection in api security: Leveraging machine learning algorithms," *International Journal of Communication Networks and Information Security*, vol. 13, no. 1, 2021.

[12] D. Bhamare, T. Salman, M. Samaka, A. Erbad, and R. Jain, "Feasibility of supervised machine learning for cloud security," in *2016 International Conference on Information Science and Security (ICISS)*. IEEE, 2016, pp. 1–5.

[13] Á. L. García, J. M. De Lucas, M. Antonacci, W. Zu Castell, M. David, M. Hardt, L. L. Iglesias, G. Moltó, M. Plociennik, V. Tran *et al.*, "A cloud-based framework for machine learning workloads and applications," *IEEE access*, vol. 8, pp. 18 681–18 692, 2020.

[14] M. Weqar, S. Mehfuz, and D. Gupta, "Authentication in iot networks via machine learning and deep learning: A review," in *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. IEEE, 2024, pp. 1–6.

[15] S. Lekkala, R. Avula, and P. Gurijala, "Big data and ai/ml in threat detection: A new era of cybersecurity," *Journal of Artificial Intelligence and Big Data*, vol. 2, no. 1, pp. 32–48, 2022.

[16] U. I. Okoli, O. C. Obi, A. O. Adewusi, and T. O. Abrahams, "Machine learning in cybersecurity: A review of threat detection and defense mechanisms," *World Journal of Advanced Research and Reviews*, vol. 21, no. 1, pp. 2286–2295, 2024.

[17] R. A. Kemmerer, "Cybersecurity," in *25th International Conference on Software Engineering, 2003. Proceedings.* IEEE, 2003, pp. 705–715.

[18] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of computer and system sciences*, vol. 80, no. 5, pp. 973–993, 2014.

[19] G. Tsochev, R. Trifonov, O. Nakov, S. Manolov, and G. Pavlova, "Cyber security: Threats and challenges," in *2020 International Conference Automatics and Informatics (ICAI)*. IEEE, 2020, pp. 1–6.

[20] A. Kumar and R. K. Dewang, "Comprehensive insights into healthcare iot: the role of machine learning and deep learning approaches," *Multimedia Tools and Applications*, pp. 1–42, 2025.

[21] K. Razzaq and M. Shah, "Advancing cybersecurity through machine learning: A scientometric analysis of global research trends and influential contributions," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, p. 12, 2025.

[22] V. N. Annapareddy, "The intersection of big data, cybersecurity, and erp systems: A deep learning perspective," *Journal of Artificial Intelligence and Big Data Disciplines*, vol. 2, no. 1, pp. 45–53, 2025.

[23] N. Kalpani, N. Rodrigo, D. Seneviratne, S. Ariyadasa, and J. Senanayake, "Cutting-edge approaches in intrusion detection systems: a systematic review of deep learning, reinforcement learning, and ensemble techniques," *Iran Journal of Computer Science*, pp. 1–31, 2025.

[24] N. Alhumam, M. H. Rahman, and A. Aljughaiman, "A comprehensive review on cybersecurity of digital twins issues, challenges, and future research directions," *IEEE Access*, 2025.

[25] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Future internet*, vol. 12, no. 10, p. 168, 2020.

[26] S. Ahmad, I. Shakeel, S. Mehfuz, and J. Ahmad, "Deep learning models for cloud, edge, fog, and iot computing paradigms: Survey, recent advances, and future directions," *Computer Science Review*, vol. 49, p. 100568, 2023.
[27] C. Janiesch, P. Zschech, and K. Heinrich, "Machine learning and deep learning," *Electronic markets*, vol. 31, no. 3, pp. 685–695, 2021.
[28] M. Tayyab, M. Marjani, N. Jhanjhi, I. A. T. Hashim, A. A. Almazroi, and A. A. Almazroi, "Cryptographic based secure model on dataset for deep learning algorithms," *CMC Comput. Mater. Contin*, vol. 69, pp. 1183–1200, 2021.
[29] E. Amri, M. Catalano, Y. Paulus, and Y. Roelvink, "Artificial intelligence security."
[30] N. Bena, M. Anisetti, G. Gianini, and C. A. Ardagna, "Certifying accuracy, privacy, and robustness of ml-based malware detection," *SN Computer Science*, vol. 5, no. 6, p. 710, 2024.
[31] N. Singh, R. Buyya, and H. Kim, "Securing cloud-based internet of things: challenges and mitigations," *Sensors*, vol. 25, no. 1, p. 79, 2024.
[32] S. Sasikala and S. Janakiraman, "A review on machine learning-based malware detection techniques for internet of things (iot) environments," *Wireless Personal Communications*, vol. 132, no. 3, pp. 1961–1974, 2023.
[33] S. Soviany, A. Scheianu, G. Suciu, A. Vulpe, O. Fratu, and C. Istrate, "Android malware detection and crypto-mining recognition methodology with machine learning," in *2018 IEEE 16th International conference on embedded and ubiquitous computing (EUC)*. IEEE, 2018, pp. 14–21.
[34] P. Sharma, S. Jain, S. Gupta, and V. Chamola, "Role of machine learning and deep learning in securing 5g-driven industrial iot applications," *Ad Hoc Networks*, vol. 123, p. 102685, 2021.
[35] J. Xu, Y. Wang, H. Chen, Z. Shen *et al.*, "Adversarial machine learning in cybersecurity: Attacks and defenses," *International Journal of Management Science Research*, vol. 8, no. 2, pp. 26–33, 2025.
[36] S. Razaulla, C. Fachkha, C. Markarian, A. Gawanmeh, W. Mansoor, B. C. Fung, and C. Assi, "The age of ransomware: A survey on the evolution, taxonomy, and research directions," *IEEE Access*, vol. 11, pp. 40 698–40 723, 2023.
[37] A. Mishra, "Ai-powered cybersecurity framework for secure data transmission in iot network."
[38] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity threats and their mitigation approaches using machine learning—a review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 527–555, 2022.
[39] O. E. Ejiofor, "A comprehensive framework for strengthening usa financial cybersecurity: integrating machine learning and ai in fraud detection systems," *European Journal of Computer Science and Information Technology*, vol. 11, no. 6, pp. 62–83, 2023.
[40] W. Joosen, "Security and assessment of biometric authentication: Attacks, defenses, and metrics," 2023.