Journal of Informatics and Web Engineering
Vol. 4 No. 3 (October 2025) eISSN: 2821-370X

Zero Trust-The Future of Cybersecurity

Danial Haider[1*], Shougfta Mushtaq[2*], Hasnat Ali[3], Mazliham Mohd Su'ud[4]
[1] Faculty of Computing & Artificial Intelligence, Air University, Service Road E-9, Islamabad, 44000, Pakistan
[2,3,4] Faculty of Computing and Informatics, Multimedia University, Persiaran Multimedia, 63100 Cyberjaya, Malaysia
**corresponding author: (danial.haider@au.edu.pk; ORCiD: 0009-0008-2998-6922)*
**corresponding author: (shouguftawajid@yahoo.com; ORCiD: 0009-0000-5794-8466)*

Abstract - The recent Zero-Trust Architecture (ZTA) is progressively adopted to the develop network security by assuming no implicit trust within or outside an organization's boundary. Though, ZTA faces substantial challenges in detecting sophisticated and developing cyber threats, particularly due to its trust on traditional security mechanisms that struggle to manage internal threats and sophisticated attack techniques. To report these shortcomings, the proposed study discovers the combination of advanced machine learning (ML) and deep learning (DL) performances to improve the anomaly detection proficiencies within ZTA environments. The study develops the CICIDS2017 dataset, which contains diverse and realistic network traffic patterns, to assess the efficiency of nine different models: Naïve Bayes, Logistic Regression, Random Forest, Decision Tree, Gated Recurrent Unit (GRU), Multi-layer Perceptron (MLP), Long Short-Term Memory (LSTM), Bidirectional Long Short-Term Memory (Bi-LSTM), and Convolutional Neural Network (CNN). Concluded comprehensive investigation and performance evaluation, the study validates that ensemble methods such as Random Forest and Decision Tree, together with deep learning models like LSTM and GRU, significantly exceed conventional models in terms of accuracy and detection abilities. The best-performing models attained up to 99.99% accuracy in recognizing malicious network activity. This exceptional performance validates that the strong potential of participating intelligent learning-based methods into ZTA to create scalable and dynamic security solutions with high accuracy. These findings illustrate the value of ML/DL in enhancing the threat detection layer of ZTA, eventually providing a stronger resistance to advanced attacks cyber threats.

Keywords— Machine Learning, Deep Learning, Zero Trust Architecture (ZTA), Cyber Security, Internet of Things (IoT)

Received: 1 March 2025; Accepted: 4 May 2025; Published: 16 October 2025

This is an open access article under the CC BY-NC-ND 4.0 license.

1. INTRODUCTION

In the today's digital landscape, the organizations face progressively sophisticated and insistent cyber threats that conventional boundary-focused security models often considered as " moat-and-castle security model " architectures these can no longer effectively manage. These conventional models primarily focus on the external threats and assume that inherent trust in internal networks, which makes them extremely susceptible to insider attacks and cooperated endpoints [1].

© Universiti Telekom Sdn Bhd.

As the data infrastructures raise more distributed due to the cloud adoption, distant work and the propagation of the IoT devices, there is an urgent need for the security frameworks that ensure the constant authentication, demanding access control and the context-aware threat detection [2].

The Zero Trust Architecture (ZTA) has arisen as a vigorous security pattern that addresses these challenges by imposing the principle of the "never trust, always verify." All users and devices must be uninterruptedly authenticated and authorised, irrespective of their network origin. Zero Trust Network Access (ZTNA), a development of the traditional Virtual Private Networks (VPNs), introduces powdered access controls, micro-segmentation and device posture endorsement to reduce adjacent movement and avoid unauthorised access. Despite its strong point, practical ZTA application still faces the major challenges in the dynamic environments particularly in noticing advanced cyber threats using out-of-date or stationary methods [3].

In multi-cloud surroundings, employing a complete understanding and acceptance of Zero Trust security, counting the incorporation of IoT and AI threat detection, remains a contest. Zero Trust execution significances on performance, user experience, and cost effectiveness within recognised network security constructions are largely unmapped in most studies [4].

This study advances cybersecurity within ZTA by applying deep learning models— Gated Recurrent Unit (GRU), Long Short-Term Memory (LSTM), Bidirectional Long Short-Term Memory (Bi-LSTM), and Convolutional Neural Network (CNN)—to detect complex cyber threats in network traffic using the CICIDS2017 dataset. Unlike traditional perimeter-based security models that are vulnerable to internal threats, ZTA emphasises continuous verification. However, current ZTA implementations often rely on conventional machine learning, which struggles with emerging threats. Deep learning offers a solution, achieving over 99.9% accuracy in detecting sophisticated attacks, surpassing traditional methods presented [5] in adaptability and effectiveness across diverse network environments.

The proposed methodology includes training and testing of these models on the benchmark CICIDS2017 dataset, which act out real-world traffic comprising benign and several types of attack behaviours. Proposed model evaluated each algorithm's performance based on the accuracy, precision, recall and F1-score. Results showed that Decision Tree and Random Forest models achieve the highest accuracy of 99.99%, beating both traditional algorithms and deep learning approaches like GRU and LSTM which still perform robustly at 99.97% accuracy. On the other hand, algorithms such as Naïve Bayes and methods delay behind in detection ability.

The contributions of this work are as follows:

- A proportional performance analysis of nine machine learning and deep learning models for the threat detection in a Zero Trust context.
- Demonstrated that tree-based ensemble models (Decision Tree and Random Forest) attain state-of-the-art detection accuracy on dataset CICIDS2017.
- Identify the limitations of traditional models and the strengths of deep learning in familiarizing to diverse, developing network conditions.
- Providing practical insights into participating AI-based threat detection within ZTA to improve security flexibility.

By addressing the current research gaps such as the limited real-time adaptability, lack of robust detection in active networks and inadequate comparisons among detection algorithms the study contributes to the rising field of intelligent ZTA applications. Further sections of this are divided as Section 2 contains literature review of the latest papers from 2022 to 2025, Section 3 contains research methodology, Section 4 contains results and discussion and Section 5 contains the conclusion.

2. LITERATURE REVIEW

The implication of Zero Trust security in serious infrastructure risk management. The text discovers the essential concepts of ZTA, precisely addressing access control, authentication, encryption, micro-segmentation, and security automation methods. Current challenges in applying ZTA, counting trust and risk computation and Software-Defined Perimeter, are deliberated by the authors. This paper points out potential research areas to expand the implementation

of Zero Trust and highlights the importance of a complete method for its successful acceptance in diverse environments [1].

"Skunk," a merged learning system for enhancing privacy and data derivation in 5G/6G networks through a blockchain design, undertaking the issues of network sharing and security supervision. Skunk implements Zero Trust Security, generating a decentralised architecture that removes the risks tangled to centralised controllers. Using Zero Trust rules, Skunk's sharding-based blockchain architecture allows operations across various network slices through cross-shard communication. 5G/6G environment displays that Skunk can detect IoT device attacks using a use case. The platform encompasses real-time predictions, auditing and future TensorFlow Merged library integration for machine learning functionalities [2].

5G, blockchain, IoT, and artificial intelligence are cooperatively revolutionizing global business. 5G enables widespread IoT ecosystems through faster data rates, ultra-low latency and cost-effective access. The authors propose a zero-trust security model for Future IoT, including a blockchain-based device authentication system, BasIoT, to enable secure admission for a multitude of devices. 5G integration into IoT addresses security, scalability, and standardization challenges while producing new revenue foundations and business models [3].

Design principles with a focus on aggressive resource and budget-friendly, intelligent on-chip sensors for attack exposure. They encourage machine learning for continuous security updates, alike to software reinforcing. This paper underlines the consequence of innovation, encompassing together physical circuit design and algorithms, in inspiring security in distributed systems. These progressions aim to make edge devices extra intelligent, self-sufficient, and secure with dispersed measures. Future developments in varied integration will involve dividing solutions across multiple silicon dice [4].

Real-Time Zero-Trust Security Framework (ZTSF) for dealing and guaranteeing trust in 5G network slices within an open architecture. The ZTSF appraises reliability based on vulnerability, exploitability, and SLA destruction degrees. 5G trusted domains' scalability and vitality are verified by experimental results, future research will explore network security definition, ZTSF enrichment using AES for access control, and protected federated learning development. The work creates the foundation for Zero-Trust Architecture implementation in open 5G networks [5].

Customised ZTA for fortifying intrusion detection within the communication modes and virtualization landscapes of 6G edge computing networks. The framework precisely and professionally detects attacks using a combination of security rules and machine learning algorithms. The exposure process becomes gradually complex, employing standalone and collective methods across multiple wireless nodes as required. 6G integration and detection with high rates and cost savings are future research areas for the ZTA in a drone network [6].

Integrating AI and IoT into a Zero-Trust Network-access control system (ZTN-ACS) to bolster Industry 5.0's elasticity and resilience. The industrial organisers can be securely regained remotely through the scheme, using deep learning for both effective and precise verification of access that aligns with anticipated production outcomes. The system enhances operation scheduling, minimizing false positives and disruptions from adversaries. The ZTN-ACS method improves production uniformity by 12.55% and decreases access interruptions by 11.11% compared to traditional methods. Future suggestion is the use of blockchain technology to enhance concurrency support [7].

Drones used industrially can be vulnerable to cyber-attacks, threatening network security. A drone-specific network intrusion detection system (ZT-NDIS) is offered, together with a multi-agent architecture and a hybrid zero-trust detection method. The system achieves a 99.99% acknowledgment accuracy for low false alarm rate and benign traffic after preprocessing the CICIDS2017 dataset. Real-time testing for both known and unknown cyber threats strengthens drone network security. The ZT-NDIS method aims to address the security contests of drone swarms through agent development and live experimentation [8].

This paper proposes a new method for Network Intrusion Detection Systems (NIDS) that combines Zero Trust security principles with sophisticated machine learning algorithms. The model integrates Auto-Encoder feature extraction, Convolutional Neural Networks, Bi-directional Long Short Term Memory classifiers, and multi-head Self Attention mechanism for enhanced focus on significant features. The model achieved classification accuracies of 93.01%, 89.79%, and 91.72% in experiments on the UNSW-NB15 dataset for 2, 6, and 10 categories. A balanced data sampler was used for training to tackle data imbalance. The model's parameters will be optimised using transfer learning and metaheuristic methods in future studies [9].

CYTØRUS training program emphases on encouraging system architects to learn and implement Zero Trust Architecture design. Based on the analysis, design, development, implementation and evaluation (ADDIE) model, the training highlights system security and scalability through a simulated business scenario. According to attention, relevance, confidence, satisfaction (ARCS) survey evaluations, the program's usefulness in motivating participants is robust for those with work experience than academic background. The sustainability of CYTØRUS motivation will be investigated in future research, together with assessments with other cybersecurity training programs. CYTØRUS goals are to close the cybersecurity skills gap [10].

Implementing Explainable AI (XAI) in marine cyber defences makes NIDS more dependable and comprehensible. The study suggests a zero-trust NIDS system that classifies marine cyberattacks with an extraordinary MCC score of 97.33% and an F1-score of 99%. The research increases model transparency by employing LIME and SHAP. Future efforts will focus on enlightening SHAP's effectiveness, contradicting adversarial XAI misunderstandings and participating federated learning and blockchain for delicate security in NIDS [11].

Zero Trust Architecture arranges defence outside the perimeter, safeguarding data and resources in contradiction of both external and internal threats. The paper identifies shortcomings in current research on ZTA orchestration and automation, precisely focusing on the lack of AI integration. ZTA component automation involves essential trust evaluation and attack detection classifications. AI mechanisms are crucial for optimizing ZTA, particularly amongst emerging technologies such as cloud computing and 5G/6G. Further research is required to systematise and orchestrate Zero Trust Access using AI technology [12].

The study suggests the Zero-Trust Attack (ZETA) framework as a solution for commerce with data renewal and model inversion attacks in independent vehicles through engaging split learning approaches within 5G/6G networks. Split learning permits for joint training despite resource restrictions but is vulnerable to immersive application attacks, like those found in the Metaverse. The ZETA framework enterprise contains simultaneous client data reconstruction with minimal error (0.0032) and enhancing task accuracy to overwhelmed existing defence methods. Further research will include investigative alternative partitioning methods, measuring the impact of hyperparameters through understanding studies and executing homomorphic encryption for advanced defence methods against such attacks [13].

The study declares the ZETA framework, which uses split learning approaches within 5G/6G networks to address data renovation and model inversion attacks in self-governing vehicles. In resource-limited environments, split learning permits concurrent training, albeit vulnerable to immersive submission attacks, like those predominant in the Metaverse. The ZETA framework attains minimal error (0.0032) data renovation and heightened task accuracy, efficiently bypassing prevailing defence methods. Future studies will discover new partitioning mechanisms, measure the effects of hyperparameter modifications, and exploit homomorphic encryption for improved protection in contradiction of attacks [14]

6G mobile networks, with their complex nature and the growing number of associated devices, require a zero-trust architecture to cater to the important security contests posed by scattered architectures. The text strains the reputation of applying strong access control, verification, and encrypted data handover using AI and advanced wireless knowledge. The article proposes practical ways to apply a zero-trust security framework to user service networks, devices, and core networks. The text highlights the use of progressive systems including blockchain, PUFs, digital twins, AI fairness, and semantic communication to reinforce the security architecture. The article forecasts that zero-trust principles will suggestively redesign mobile network security in the future [15].

In response to gradually sophisticated cyber threats, the study highlights the integration of machine learning (ML), mainly CNNs, into ZTA to improve cybersecurity analytics and threat detection. The study highpoints how ML significantly enhances accuracy, efficiency and compliance in classifying known and zero-day threats, outclassing traditional models like Random Forests and SVMs. The research underlines the importance of continuous monitoring, active trust scoring and interactive analytics to support adaptive, real-time security measures. By enabling context-aware decisions and automated responses, ML enhances the flexibility and resilience of ZTA, it reduces false alerts and minimizes the human intervention. Eventually, study presents a data-driven roadmap for building a robust, adaptive security infrastructures capable of developing with modern cyber risks [16].

The research presents an AI-driven, identity-based method to ZTA, focusing on real-time threat detection and access control through interactive analytics and dynamic permission supervision. Traditional access models often fail to reflect evolving user behaviours and contextual threats, that lead to internal vulnerabilities. The proposed system uses

machine learning models like Random Forest, Gradient Boosting and K-means clustering, to analyse login patterns, device types, geolocation and access times and adjust permissions accordingly. Graph-based models segment compromised identities to prevent lateral threat movement within networks. The proposed solution improves response times and accuracy and reduces false positives related to static policies. It addresses key challenges, such as privacy by de-identifying data, ensuring scalability through flexible computing resources and continuously refines its predictions through feedback loops, eventually strengthening dynamic policy execution while maintaining user productivity [17].

This study underscores the vital role of integrating ZTA, AI-driven threat intelligence, and CISA compliance to enhance federal cloud security. As traditional perimeter-based defences are inadequate against modern cyber threats, ZTA enforces continuous verification and least-privilege access, significantly reducing attack surfaces. AI complements this by real-time threat detection, automated anomaly response, and predictive analytics to counter insider threats and sophisticated attacks. Compliance with CISA frameworks, such as FedRAMP and TIC 3.0 ensures standardised security practices and continuous monitoring. While challenges such as AI bias, adversarial risks, and policy gaps persist, the combined use of intelligent automation, behavioural analytics, and regulatory alignment provides a robust foundation to secure federal cloud environments and build long-term cyber resilience [18].

The inclusive study highpoints the transformative role of the ZTA and micro segmentation in modern innovation cybersecurity, thoughtful the boundaries of traditional perimeter-based fortifications against growing threats like insider attacks and broadminded persistent threats (APTs). Prominence the principle of "never trust, always verify," ZTA assurances continuous authentication, least privilege access and robust identity management to protected critical assets. Here micro segmentation, which is a key ZTA section, recovers visibility and limits lateral attacker movement by unravelling workloads at a granulated level. The study precises best practices for application, numeration network discovery, policy definition and constant monitoring using automation and analytics. Empirical indication and case studies validate that micro segmentation improves network resilience, decreases attack surfaces and strengthens compliance despite challenges such as policy complexity and potential performance trade-offs. Looking at addition with AI, SDN and emerging frameworks like SASE and XDR, abilities to realize more adaptive, intelligent and scalable security strategies for dynamic, multi-cloud environments [19].

The paper introduces a novel, combined cybersecurity framework for modern IoT ecosystems that combines Zero-Trust, Zero-Touch provisioning and AI/ML-driven threat detection to secure 5G/6G-enabled IoT networks. By mechanizing secure device onboarding, enforcing continuous authentication and leveraging ensemble machine learning models such as XGBoost and Random Forest, for the real-time Distributed Denial of Service (DDoS) attack detection, the proposed framework ensures robust, scalable and adaptive protection. The key features of this system include dynamic policy enforcement, micro-segmentation and network slicing, which address the developing threat landscape with minimal human interference. The experimental results established the high accuracy and recall of DDoS vector detection, which highlights the efficiency of ensemble-based methods. Future work will enhance data privacy through Federated Learning, reduce bias, recover model efficiency for resource-constrained environments, and increase the explainability of AI decisions, concrete the way for trusted and transparent security systems in the era of industry [20].

Recent occurrences have highlighted the susceptibility of offshore wind infrastructures, making cybersecurity vital. A cost–benefit analysis (CBA) is used to validate cybersecurity reserves by matching costs and risk lessening. A literature review found imperfect research on CBA for offshore wind cybersecurity maximum studies attentive on the general energy sector. The current literature deficiencies detailed modelling of offshore wind, chiefly in terms of effective technology and offshore-specific factors. Future research should discourse these gaps and increase the methodology with more data. The study discloses an opportunity to advance knowledge in offshore wind cyber-physical structures [21].

The proposed study improved pacemaker device cybersecurity by classifying vulnerabilities and endorsing effective plans. It uses machine learning to expect security holes using the WUSTL-EHMS-2020 dataset, that contains network traffic, biometric data and the attack labels. The study compares Support Vector Machines (SVM) and Gradient Boosting Machines (GBM) for risk prediction, with GBM outperforming SVM in precision (99.6% vs 96.7%), accuracy (95.1% vs 92.5%), recall (94.9% vs 42.7%) and F1 score (76.3% vs 59.0%). The results validate that GBM is more effective in predicting cybersecurity threats. Approvals include participating a GBM for threat detection and regularly updating the model. This study highlights the need for robust cybersecurity in pacemakers due to their wireless vulnerabilities [22].

The proposed research focuses on the enhancing cybersecurity consciousness among university students and discovering gamification as a current learning tool. It assesses current consciousness levels, classifies key issues and suggests gamified learning environments to advance cybersecurity education. A gamified platform developed for Multimedia University (MMU) students to discourse financial restrictions with personalised learning and collaborative features. Future progresses will aim to improve scalability, integrate AI for threat detection, participate advanced analytics and adapt content to diverse linguistic and the cultural backgrounds. The proposed platform will also be frequently updated to address developing cybersecurity contests. General, the study highlights gamification's transformative potential in cybersecurity education [23].

3. RESEARCH METHODOLOGY

To deliver a deeper context, the classifiers are trained and evaluated on the CICIDS2017 dataset sourced from Kaggle, that contains more realistic and labelled network traffic data by representing both normal activity and the multiple attack types. The dataset contains detailed features such as packet size, flow duration and protocol behaviour, which offer a robust foundation for intrusion detection. Each classifier was exposed to the same input data to guarantee fair performance evaluation. The visualization in section 4 shows how each model responded to this complex, real-world traffic scenario. It replicates the models' ability to differentiate between benign and malicious designs with changing effectiveness.

This study investigates various ML and deep learning (DL) classifiers within ZTA using the CICIDS2017 dataset. The dataset was initially uploaded to Kaggle, where preprocessing steps included removing null values and duplicates to ensure clean, reliable data for model training and reduce noise. Following this, the dataset was split into training and testing sets. Figure 1 shows the architecture followed in our methodology.

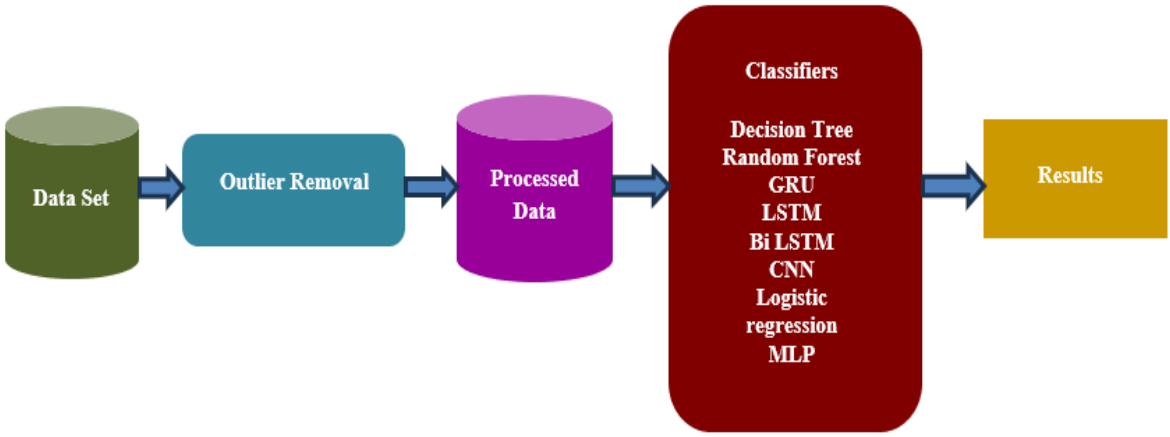


Figure 1. The Architecture Model

Several classifiers were then applied, and their performance was evaluated using accuracy, precision, recall, and F1-score. Python was used throughout the experimental process, which was conducted in the Kaggle environment. The CICIDS2017 dataset underwent systematic preprocessing—noise reduction, handling missing values, and normalizing feature values—to prepare for time-sequential data handling, essential for identifying network patterns. Table 1 shows the classifiers used.

4. RESULTS AND DISCUSSIONS

After examining various DL and ML classifiers including Random Forest, GRU, Decision Tree, LSTM, Bi-LSTM, CNN, Logistic Regression, MLP and Naïve Bayes on CICIDS2017 dataset the performance Metrics such as Accuracy, Precision, Recall and F1-Score are used to assess each model's effectiveness.

Deep learning models as GRU and LSTM show near-perfect results, while traditional models fluctuate in performance. Table 1 shows the results of these classifiers in correspondence to the performance metrics discussed above. It include information as follows:

- **Model Selection and Training:** Deep learning models such as GRU, LSTM, Bi-LSTM, and CNN were selected for their effectiveness in processing sequential data. Each model was trained on network features linked to traffic flow, packet behaviour, and protocol types.
- **Evaluation Metrics and Validation:** Models were assessed based on accuracy, precision, recall, and F1-score to gauge their threat detection capabilities. Performance metrics on a separate test set confirmed the models' generalizability, with results focusing on:
- **Detection Rates**: Highlight each model's detection rate, noting when deep learning models achieve over 99.9% accuracy, surpassing traditional ML methods.
- **False Positives and Negatives**: Examine instances of high false-positive or false-negative rates, especially in certain models like CNN, and analyse contributing factors.
- **Model-Specific Strengths and Limitations**: Identify optimal conditions for each model, considering real-time factors such as latency, which may influence performance.

Table 1. Result Summary of ML and DL Classifiers

Algorithm	Accuracy	Precision	Recall	F1 – Score
Decision Tree	99.99	99.99	99.99	99.99
Random Forest	99.99	99.99	99.99	99.99
GRU	99.97	99.97	99.97	99.97
LSTM	99.97	99.97	99.97	99.97
Bi LSTM	99.96	99.96	99.96	99.96
CNN	99.96	99.96	99.96	99.96
Logistic regression	96.29	96.36	96.29	96.27
MLP	89.91	91.39	89.91	89.65
Naïve Bayes	80.83	85.56	80.83	79.48

Figure 2 shows how each classifier of ML and DL performs based on the performance matrices: Accuracy, Precision, Recall and F1-Score.

Deep learning models like GRU and LSTM constantly achieve over 99.9% across all analysed metrics. On the other hand traditional models such as Naïve Bayes and MLP display lower scores, representing reduced reliability in threat detection.

5. CONCLUSION

This study underlines the deep learning algorithm's ability to tackle the security issues in ZTA. Advanced algorithms like GRU, LSTM, Bi-LSTM, and CNN effectively detect complex security threats and anomalies within network traffic, as demonstrated on the CICIDS2017 dataset. Modern cyber threat complexity surpasses traditional machine learning approaches, which struggle to reach 99.9% detection rates. Deep learning techniques in ZTA can significantly reinforce security measures, providing a powerful solution for organizations in complex and advanced network scenarios. In future, deep learning algorithms can be finetuned to enhance ZTA in cybersecurity.

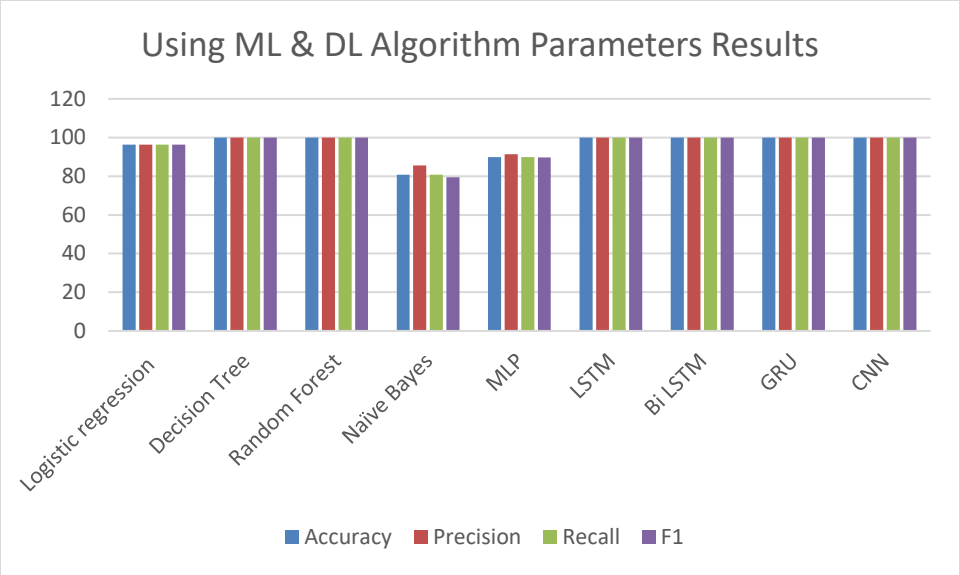


Figure 2. Using ML & DL Algorithm Parameters Results

ACKNOWLEDGEMENT

The authors would like to thank Dr. Mansoor Alam and Assoc. Prof. Dr. Noshina Tariq for constant guidance throughout the writing of this paper.

FUNDING STATEMENT

The authors received no funding from any party for the research and publication of this article.

AUTHOR CONTRIBUTIONS

Danial Haider: Idea, Presentation and Formatting;
Shougfta Mushtaq: Literature Review;
Hasnat Ali: Experimental work.
Mazliham Mohd Su'ud: Proofreading and Supervision

CONFLICT OF INTERESTS

No conflict of interests was disclosed.

ETHICS STATEMENTS

Our study follows The Committee of Publication Ethics (COPE) https://publicationethics.org/. The dataset used in the experiments were available at publicly available platform Kaggle, and all experiments are performed by using Kaggle cloud environment.

REFERENCES

[1] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero Trust Architecture (ZTA): A

comprehensive survey," *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.

[2] E. Bandara, X. Liang, S. Shetty, R. Mukkamala, A. Rahman, and N. W. Keong, "Skunk - A blockchain and zero trust security enabled federated learning platform for 5G/6G network slicing," in *2022 Annual IEEE Communications Society Conference on Sensor, Mesh, and Ad Hoc Communications and Networks (SECON)*, 2022, pp. 109–117. doi: 10.1109/SECON55815.2022.9918536.

[3] S. Li, M. Iqbal, and N. Saxena, "Future industry Internet of Things with Zero-trust security," *Information Systems Frontiers*, 2022, doi: 10.1007/s10796-021-10199-5.

[4] M. Alioto, "Aggressive design reuse for ubiquitous zero-trust edge security—From physical design to machine-learning-based hardware patching," *IEEE Open Journal of the Solid-State Circuits Society*, vol. 3, pp. 1–16, 2022. doi: 10.1109/OJSSCS.2022.3223274.

[5] H. A. Kholidy *et al.*, "Toward zero trust security in 5G open architecture network slices," in *2022 IEEE Military Communications Conference (MILCOM)*, 2022, pp. 577–582. doi: 10.1109/MILCOM55135.2022.10017474.

[6] H. Sedjelmaci and N. Ansari, "Zero trust architecture empowered attack detection framework to secure 6G edge computing," *IEEE Network*, vol. 38, no. 1, pp. 196–202, 2024. doi: 10.1109/MNET.131.2200513.

[7] K. A. Abuhasel, "A zero-trust network-based access control scheme for sustainable and resilient industry 5.0," *IEEE Access,* vol. 11, pp. 116398–116409, 2023. doi: 10.1109/ACCESS.2023.3325879.

[8] S. Ouiazzane, M. Addou, and F. Barramou, "A zero-trust model for intrusion detection in drone networks," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 11, pp. 525–537, 2023. doi: 10.14569/IJACSA.2023.0141154.

[9] A. Z. Alalmaie, P. Nanda, and X. He, "ZT-NIDS: Zero trust, network intrusion detection system," in *2023 International Conference on Security and Cryptography (SECRYPT)*, 2023, pp. 99–110. doi: 10.5220/0012080000003555.

[10] T. Sasada, M. Kawai, Y. Masuda, Y. Taenaka, and Y. Kadobayashi, "Factor analysis of learning motivation difference on cybersecurity training with zero trust architecture," *IEEE Access*, vol. 11, pp. 141358–141374, 2023. doi: 10.1109/ACCESS.2023.3341093.

[11] E. C. Nkoro, J. N. Njoku, C. I. Nwakanma, J. M. Lee, and D. S. Kim, "Zero-trust marine cyberdefense for IoT-based communications: An explainable approach," *Electronics*, vol. 13, no. 2, p. 276, 2024. doi: 10.3390/electronics13020276.

[12] Y. Cao, S. R. Pokhrel, Y. Zhu, R. Doss, and G. Li, "Automation and orchestration of zero trust architecture: Potential solutions and challenges," *Machine Intelligence Research*, vol. 21, no. 2, pp. 294–317, 2024. doi: 10.1007/s11633-023-1456-2.

[13] S. A. Khowaja, P. Khuwaja, K. Dev, K. Singh, L. Nkenyereye, and D. Kilper, "ZETA: Zero-trust attack framework with split learning for autonomous vehicles in 6G networks," in *2024 IEEE Wireless Communications and Networking Conference (WCNC)*, 2024. doi: 10.1109/WCNC57260.2024.10571158.

[14] V. Sobchuk and O. Barabash, "Sequential intrusion detection system for zero-trust cyber defense of IoT/IIoT networks," J*ournal of Cyber Security and Information Technologies*, no. 3, 2024. doi: 10.20998/2522-9052.2024.3.11.

[15] Y. Liu, Z. Su, H. Peng, Y. Xiang, W. Wang, and R. Li, "Zero trust-based mobile network security architecture," *IEEE Wireless Communications*, vol. 31, no. 2, pp. 82–88, 2024. doi: 10.1109/MWC.001.2300375.

[16] E. Ogendi, "Leveraging advanced cybersecurity analytics to reinforce zero-trust architectures within adaptive security frameworks," *International Journal of Research Publication and Reviews*, vol. 6, no. 2, pp. 729–742, 2025. doi: 10.55248/gengpi.6.0225.0729.

[17] S. Ahmadi, "Autonomous identity-based threat segmentation in zero trust architectures," 2025.

[18] B. T. Ofili, E. O. Erhabor, and O. T. Obasuyi, "Enhancing federal cloud security with AI: Zero trust, threat intelligence and CISA compliance," *World Journal of Advanced Research and Reviews*, vol. 25, no. 2, pp. 620–635, 2025. doi: 10.30574/wjarr.2025.25.2.0620.

[19] C. S. Ravi, M. Shaik, V. Saini, S. Chitta, V. Sri, and M. Bonam, "Beyond the firewall: Implementing zero trust with network microsegmentation," 2025.

[20] S. Shakya, R. Abbas, and S. Maric, "A novel zero-touch, zero-trust, AI/ML enablement framework for IoT network security," *arXiv*, 2025. doi: 10.48550/arXiv.2502.03614.

[21] Y. H.-S. Kam, K. Jones, R. Rawlinson-Smith, and K. Tam, "In search of suitable methods for cost-benefit analysis of cyber risk mitigation in offshore wind: A survey," *Journal of Informatics and Web Engineering*, vol. 3, no. 3, pp. 314–328, Oct. 2024. doi: 10.33093/jiwe.2024.3.3.20.

[22] S. T. Jimoh and S. S Al-Juboori, "Cyber-securing medical devices using machine learning: A case study of pacemaker," *Journal of Informatics and Web Engineering*, vol. 3, no. 3, pp. 271–289, Oct. 2024. doi: 10.33093/jiwe.2024.3.3.17.

[23] A. K. A. Razack and M. F. M. Saad, "Enhancing cybersecurity awareness through gamification: Design an interactive cybersecurity learning platform for multimedia university students," *Journal of Informatics and Web Engineering*, vol. 3, no. 3, pp. 21–40, Oct. 2024. doi: 10.33093/jiwe.2024.3.3.2.

BIOGRAPHIES OF AUTHORS

	**Danial Haider** obtained a Master's in Computer Science from COMSATS University, Islamabad, and is advancing in a Ph.D. in Information Security at Air University, Islamabad. Having 4 years of teaching experience, he currently teaches in the Information Technology Department. He has established various applications, including a Python-based face-tracking app and a Drive Watch app, while discovering his research interests. Danial has contributed 3 papers to prestigious journals, focusing on the IoT, machine learning, cryptography and zero trust security. He can be contacted at danial.haider@au.edu.pk.
	**Shougfta Mushtaq** is a interested and skilled Computer Science professional passionate about the education and research. She is a visiting Lecturer at Bahria University Islamabad and pursuing a Ph.D. in Information Technology at Multimedia University Malaysia, focusing in cybersecurity with emphasis on URL phishing attacks in social engineering. Her research purposes to develop robust analysis and mitigation strategies. She seeks to apply her teaching and the research expertise to advance computer science. She can be conducted at shouguftawajid@yahoo.com.
	**Hasnat Ali** is a dedicated cybersecurity professional and is Lecturer at Riphah International University, Islamabad. He is pursuing a Ph.D. in Information Technology at Multimedia University, Malaysia, focusing on Android malware detection using machine learning and deep learning techniques. His knowledge includes cybersecurity frameworks, malware detection, and AI in cybersecurity. He holds certifications such as CEH and GDPR. Passionate about the teaching and research, he aims to contribute implicitly to the cybersecurity field. His contact is: hasnat.ali@riphah.edu.pk | alihasnat51@gmail.com.



Prof. Dato' Mazliham Mohd Su'ud, President and CEO Multimedia University, is a prominent figure in computer engineering. His research contributions include co-authoring numerous published papers, contributing to books and conference proceedings and advancing Higher Technical and Vocational Education & Training (HTVET). He was honoured with the Darjah Sri Sultan Ahmad Shah Pahang (D.S.A.P.) award in 2013 and the Chevalier de l'Ordre national du Mérite from Government of France in 2015 for his significant contributions to the field and international collaboration. He can be contacted at mazliham@mmu.edu.my.