International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(12s) 2026 pp. 865-875
https://doi.org/10.70917/ijcisim-2026-3958
Article

An Ai-Integrated Real-Time Network Security Framework For Cyber Threat Mitigation In Smart Industry

S. Ravi Kiran[1], G. Shankarlingam[2], N. Satheesh Kumar[3]

[1]Department of CSE, Chaitanya Deemed to be University, Hyderabad, Telangana, India. sravikiran00@gmail.com
[2]Department of CSE, Chaitanya Deemed to be University, Hyderabad, Telangana, India. akitcse@gmail.com, ORCID ID - 0009-0005-6809-2728
[3]Department of Computer Science and Engineering, Marri Laxman Reddy Institute of Technology and Management, Hyderabad, Telangana, India, meet.nskumar@gmail.com, ORCID ID - 0000-0001-5849-2915

Abstract: The transition of smart industry is showing tremendous efficiency in terms of operations but experiencing unexpected cyber security risks due to integration of operational and information technology. Present security models basically depending on signature-based detection mechanism and machine learning models. These security model may not suitable against sophistication and escalating volume of cyber-attacks. In this paper, we evaluated the proposed framework for AI integrated cyber security (AICSF) for real-time threat detection and mitigation in smart industry environments. This paper will compare with various baseline models Bayesian classification, SVM, Shallow DL on dataset which consists of network attack data and malware data. This framework operates in an AI-Mode, leveraging a recurrently refined DL architecture for real-time anomaly detection and adversarial learning. The comparative study demonstrated the superiority of proposed AICSF approach in terms of detection accuracy of 97%, F1-score of 98.75%, FPR of less than 1%, and detection rate of 96.12%, which adopting sophisticated AI driven solutions to safeguard high end physical and digital assets.
Keywords: NA

1. Introduction

The rapid growth of smart industry in manufacturing is reshaping global industry. This will integrate industrial IoT, cloud and cyber physical systems to enhance efficiency, productivity, and flexibility. This enhanced efficiency is used to create complex, making robust network security and unprecedented priority.

Two major issues are inadequate information regarding security and escalating sophistication of threats. The present models in various operational environments will depend heavily on simple defences and the networks which are isolated from other networks (air-gapped networks). The modern cyber-attacks are increasingly polymorphic, utilizing techniques like making data or code unreadable and hiding original functionality (obfuscation) including adversarial machine learning techniques for detection. The malware also enhanced its capacity from simple forms of virus to multi-stage threats. These sophisticated attacks capable of traversing various operational domains of industrial environments which will cause physical damage. This necessitates the threat landscape paradigm shift towards intelligent, adaptive and real-time security solutions.

The current network security approaches and the security models incorporating machine learning will have critical limitations when deployed in smart industry requirements. The models like Bayesian classification (GNB), SVM will work effectively for known threats but they struggle in novel attack patterns which will results low detection rates due to limited recall. The researchers considered network flaws as independent data points in which they failed to analyse the temporal dependencies. A high FPR in various operational industry operations is unacceptable as this may show high impact on industrial operations. Moreover, the present models are facing performance bottlenecks when dealing with large-scale Realtime IIoT networks.

The main purpose of this paper is to develop, design and validate an advanced, AI-integrated optimized security framework for real-time threat detection and mitigation in smart industry environments. This model demonstrated the superior performance with deep learning architectures over existing models. The implementation of AI-based IDS can effectively reduce the missed attacks and operational disruptions (False Negatives and False Positives). The findings will confirm the strategic investment decisions of cybersecurity practitioners, stakeholders towards the adaptive defence mechanisms.

Research Question: What are the implications of the proposed AI-based security model for cybersecurity practitioners and organizations in smart industry to safeguard their digital assets in evolving cyber threats?

Objectives:

- To investigate the potential of leveraging AI in smart industry applications to enhance the security measures and mitigate emerging threats effectively
- Identify refinements of AI algorithms, exploration of additional DL techniques by adapting advanced security strategies to address emerging challenges in smart industry.

This study employs a network attack dataset "UNSW-NB15" to establish performance baselines using existing models and multilayer perceptron-based DL framework, LSTM network which is capable of capturing sequential and temporal data from the network. The model performances will be evaluated based on key cybersecurity metrics and time complexity analysis to measure the real-time applicability.

The organization of the paper is as follows. The literatures are reviewed in the next section followed by Design and Development where data preprocessing and model architecture were demonstrated. The Results were demonstrated in section 4 and section 5 deals with conclusions.

2. Literature Review

[1] proposed adaptive IDS for industrial IoT environments. To observe the changes in the network behaviour to enable real-time detection of cyber threats in dynamic industrial environments by employing ensemble learning models. This paper used SHAP (Shapely Additive Explanations) to track packet size, type of protocol and device activity pattern for model interpretability by allowing human operators. They evaluate the model on the datasets ToN-IoT and BoT-IoT and achieved detection accuracy of 96.4%, low false positive rate of 2.1% with average detection latency of ≈35ms.

[2] presented a framework called ML-CCPS (A Machine Learning enabled Cognitive Cyber Physical System) for real-time intrusion and adaptive security in Medical IoT environments. It operates through a layered architecture by collecting metadata from different medical devices by integrating Extreme Learning Machine (ELM) classifier to detect anomalies and intrusions. This model integrates a adaptive access control and feedback loop based on behaviour. It shows robust detection under noisy environments and optimal scalability to multiple devices.

To enhance threat detection and auditability, [3] proposed a real-time cybersecurity framework which integrates AI with blockchain. This system used CNN based anomaly detector to study suspicious network traffic. This hybrid approach addresses the limitations of many AI-based security systems. The authors used CICIDS2017 dataset to maintain strong detection performance with acceptable real-time responsiveness with high precision and recall.

[4] presented PPSC-BCAI approach for automatic fraud detection and risk assessment for decentralized and privacy preserving systems. They employed XGBoost to analyse transaction and network immutability to detect anomalies. The approach is feasible to combine decentralized technologies with ML based analytics to enable real-time risk measurement. This work underscores the potential limitations of AI augmented blockchain systems and motivates further research into efficient, privacy aware model for secure, intelligent infrastructures.

[5] proposes a conceptual framework to automate network security in complex infrastructures by leveraging AI driven technologies including ML predictive analytics, NLP and anomaly detection. The model uses a centralized security orchestration layer and a dashboard for security protocols across various heterogeneous system to facilitate real-time threat intelligence, adaptive threat detection and automated response actions. This AI enabled automation reduces reliance on manual intervention to improve incident response time, minimize false positives and enhances scalability of enterprise network security management.

[6] Demonstrated cybersecurity for smart forms by integrating IoT devices, sensors, automation and data driven decision making. This paper discussed various AI based techniques, predictive analytics, anomaly detection, real-time

threat intelligence and AI driven incidence response to detect, predict and mitigate cyber threats. The authors faced numerous challenges like integration complexity, data quality issues, need of robust infrastructure and cost constraints.

[7] Integrates traditional sociocultural intelligence with ML based security tools can significantly enhance the cybersecurity posture of an organizations. It highlights the powerful detection and response capabilities, their effectiveness but they didn't consider the organizational behaviour and human factors.

[8] Offers a thorough survey of security vulnerabilities affecting smart contracts and decentralized applications on blockchain platforms. It systematically reviews attack vectors and various mitigation techniques including static and dynamic analysis tools, formal verification, runtime monitoring and best practice guidelines for secure smart contract development. This paper evaluates strength and limitations of existing mitigations, highlighting automated tools to detect common weakness, residual risks, dependencies on external libraries, and difficulty in verifying highly dynamic contract systems. This model underscores the need for multilayered defence strategy by combining design time analysis, runtime monitoring, and careful development practices used for safer adoption of block chain-based applications.

[9] Performed a comprehensive review of cybersecurity risk strategies for distributed energy resources in smart grids. The DER based grids increasingly rely on digital control, software defined operations and communication networks. This paper discussed diverse attacks across DER infrastructures and reviewed present defence mechanisms from secure communication protocols and intrusion detection systems to redundancy and fault tolerant designs which aimed at enhancing grid resilience. The paper also describes the current research gaps, outlined critical challenges and propose directions for future work to build robust, cyber resilient smart grid architectures to integrate decentralized energy sources safely.

[10] Described cybersecurity framework for cyber physical system to deploy microgrid networks. This paper reviewed the necessity of transitioning form traditional information technology security methods to more intelligent techniques suited for cyber physical systems. The authors propose a complete data driven methodology for CPS control and attack detection. This paper used DNN based controller to detect and mitigate complex attacks inside the microgrid. This paper evaluated on modelling a Stealthy Local Convert Attack (SLCA). They considered False Data Injection attack was specifically designed to overcome existing microgrid protection systems. This model validates that deep learning models are effective for complex microgrid control and security offering a more robust and responsive defence mechanism against sophisticated cyber intrusions.

[11] presents cyber security vulnerabilities in microgrids and reviews how artificial intelligence techniques can be used for robust cyber-attack detection and mitigation. The attacks may increase making them susceptible to cyber-attacks that can compromise sensor measurement, control signals and communication data due to expansion of communication network and smart devices in smart girds. The present security mechanism falls short in timely detection of threats. To address these challenges, the paper used AI based detection and mitigation methods including ML and DL approaches that exploits patterns in operational data for anomaly detection and any other malicious activities. They also discussed the need of transferred learning and XAI to increase trustworthiness in cyber physical systems.

[12] Discussed the concept of security by intelligence as a method in system security. They proposed integration of AI driven security mechanism including ML, DL, anomaly detection, behavioural analysis and automated response to enable dynamic threat detection, prediction and real-time defence across various products and industries. The presented framework include dynamic threat detection and prediction, behavioural analysis and anomaly detection by reviewing the network behaviour to identify misuse and deviations of intrusion, automated adoption and response, privacy preserving solutions and cross industry applicability.

[13] Described how ML and DL is transforming cybersecurity by enabling advanced threat detection and mitigation across domains. The authors discussed the emerging technologies such as transformer-based models, federated learning by integrating with blockchain. They also mentioned challenges like handling large scale and heterogeneous data ensuring real-time processing performance, managing privacy, security issues and embedding model resilience for AI driven threat detection remains auditable.

[14] Presented evolving landscape of cybersecurity for cloud-based infrastructures, focusing on how AI can foundationally improve threat detection and response in cloud environments. They discussed the traditional, signature based to AI enhanced frameworks for anomaly detection, behavioural analysis and real-time monitoring to identify evolving attacks. The paper presents major challenges such as privacy, model bias, false positives and scalability. The effective cloud security required technical tools along with governance and continuous adoption.

[15] Presents the analysis of zero-day exploits, malware, and advanced social engineering attacks are increasingly bypassing conventional signature-based detection systems. The authors examine next generation approaches leveraging AI, ML, Dl techniques like anomaly detection, behavioural analysis, pattern recognition to detect and mitigate threats. The study highlights the strengths of AI and ML based methods including their ability to generalize known signatures, adopting to new threats, and scale across large and dynamic networks by considering data quality, false positives and scalability. They recommend the organizations to use layered, adaptive security system which will balance detection performance, computational cost and maintainability when adopting to AI powered cyber defence mechanisms.

[16] presents conceptual framework for AI to strengthen cybersecurity in telecommunication sector which is depending on interconnected digital infrastructure. They applied AI based techniques for proactive threat intelligence, risk assessment, anomaly detection, adaptive response strategies for specific demands of telecom networks. The framework concentrates on multidimensional approach by combining technical measures like data analytics and automated anomaly detection with organizational considerations. The authors identified the present gaps and challenges like domain specific datasets, integration of AI systems with telecom infrastructure.

[17] examines the adoption of AI for cyber security strategies in financial platforms. The risj and complexity of cyber threats increase as these platforms incorporating digital transactions, fintech innovations, and interconnected infrastructure. To address these challenges, the paper analyses how AI based cybersecurity mechanisms overcome the security problems in financial platforms. This paper highlights the key benefits of integrating AI by continuous monitoring and adaptive response capability against cyber-attacks and AI driven approaches can support scalability and robustness required for modern, distributed financial systems. The paper concluded with challenges like AI based cybersecurity must consider ethical and privacy implications, the need of high-quality data for accurate detection, false positives, and the demand for governance when deploying AI in finance sector.

[18] Presented hybrid framework that integrated AI and blockchain technology to enhance the data security in IoT infrastructures deployed within smart cities. This idea will provide immutability, decentralization and desirable properties in IoT data management by combining it with AI enables intelligent monitoring, anomaly detection, and data validation to offer more robust security against various advanced cyber threats. This paper describes how IoT devices in smart cities generate high volumes of heterogeneous data through blockchain technology, tampering and unauthorized modifications can be prevented. These AI modules analyse data patterns to detect suspicious activities, data inconsistencies and potential attacks to enable proactive threat detection rather than reactive mitigation. This architecture offering scalable design that addresses both the structural security benefits of blockchain and adaptive learning capabilities of AI. This integrated approach is well suited for IoT driven smart cities where massive data flows and distributed sensors are integrated.

[19] presented data driven framework for proactive cyber threat mitigation which emphasising the modern cyber security demands continuous monitoring and predictive defence rather than reactive response, The present models rely on static rules which are insufficient against threats, instead, the framework integrates real-time data collection from various sources, behavioural analytics and dynamic risk assessment to identify and neutralize potential threats before they can materialize. The major contributions include event logging to capture user and network behaviours, Data analytics module to analyse usage patterns, detect anomalies activities, adaptive security policies and user centric controls that adjust defence levels based on risk scores and user behaviour.

[20] Described an integrated framework that combines AI, blockchain and smart contracts to automate organizational cybersecurity compliance and threat response. Block chain is used to maintain immutable and transparent log of compliance actions and smart contract enforce consistent application security policies without depending on manual.

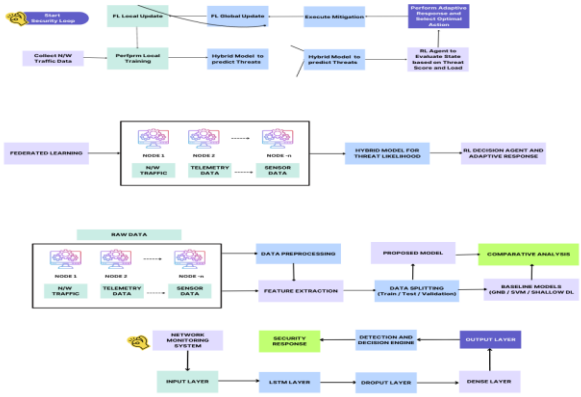
[21] Proposed real time data processing framework for surveillance systems that leverage AI to automatically detect, classify and respond to security threats. The framework integrates ML and DL algorithms capable of analysing large scale, multi-model surveillance data in real-time. The framework supports continuous model training to adapt to threat patterns, reducing false positives and improving system robustness over time. The authors highlight architectural considerations to ensure scalability and flexibility including micro based designs to decouple data ingestion, analysis and alerting modules.

[22] Demonstrated the security implications of the model context protocol for connecting AI models with external services and data sources. This paper presents enterprice grade security framework, identifying key vulnerabilities like tool poisoning, context injection, resource positioning, supply chain risks. They also considered in

depth controls including least privilege authorization, strict input validation, secure transport, logging and runtime monitoring to mitigate these risks. This study concluded with the limitations of dual nature of tool enabled AI, demands high security practices before deployment in production or sensitive environments.

3. Methodology

This section will present the detailed methodology to develop benchmark models and the proposed AICSF model. This design will focus designing and validating ML models and advanced DL architectures to ensure the proposed model is optimized for low latency, high reliability demands for smart industry environments. The methodology will be implemented in three phases called Data Collection, Design and Development and Evaluation.



Data Collection

To ensure the practical relevance of our findings, this study utilizes a comprehensive, contemporary network intrusion detection dataset UNSW-NB15. This dataset is having 49 features with 9 different attacks including modern malware, DoS, probing, and sophisticated multi-stage attacks.

Preprocessing is a major step for mitigating bias to ensure model stability and handling categorical data like protocol type or flags are converted using label encoding. All the numerical features are standardised using Standard Scalar to ensure zero mean (μ) and variance(σ). This normalization prevents features with larger numerical ranges from influencing the model loss function.

$Z=(x-\mu)/\sigma$

The datasets related to cybersecurity are generally imbalanced with Normal and Attack instances. The techniques like SMOTE (Synthetic Minority Oversampling Technique) is used during training to mitigate classification bias towards the majority class. Specialized Weighted loss function can also be used to perform the same. Once the data is pre-processed then the data is partitioned into mutually exclusive sets, 70% of data is used for training and 30% data is used for testing.

Design and Development

Three different baseline models were used to compare against proposed AICSF model

Bayesian Classification:

This was implemented using Gaussian Naïve Bayes (GNB) classifier. The GNB is computationally highly efficient and assumes that the features are conditionally independent given the class label, and that the likelihood of the features is Gaussian. This assumption is violated in network traffic data, GNB serves as a fast and low complexity benchmark.

Support Vector Machine

This was implemented using support vector classifier with linear kernel. The SVM model configured with a Radial Basis Function (RBF) kernel is employed for its effectiveness in high dimensional space. This aims to find the optimal hyperplane that enhances the margin between two classes. This will help to make it robust against overfitting and its computational complexity may vary between O(N2) to O(N3), where ‘N’ is the number of samples which will control its scalability for largescale, real-time data streams.

Shallow Deep Learning Model

Implemented using the Multi Layered Perceptron (MLP) with two hidden layers and ReLU activation function. This MLP will serves as shallow deep learning baseline. This feed forward neural network consists of Input Layer (Based on the number of features), two hidden Layers (Fully connected layers with 64 and 32 neurons using the ReLU activation function and output layer consists of single neuron with a sigmoid activation function for binary classification. This model is compiled using the Adam Optimizer and binary cross-entropy loss.

AI – Integrated Security Framework

This AI-Integrated Security Framework (AICSF) leverages the LSTM network, a kind of RNN which is ideally suited for analysing the temporal sequences inherent in network traffic and will capture anomalies over time. The LSTM architecture will have internal gates like (Input, Forget and output) and a cell state. This architecture allows the model to remember or forget information over long sequences of data, effectively capturing the long-range dependencies and multi-stage behaviours of cyber-attacks. The AICSF will be used to analyse incoming traffic continuously to detect threats based on the contextual history to enable high end real-time anomaly detection. This framework has demonstrated in figure 2.

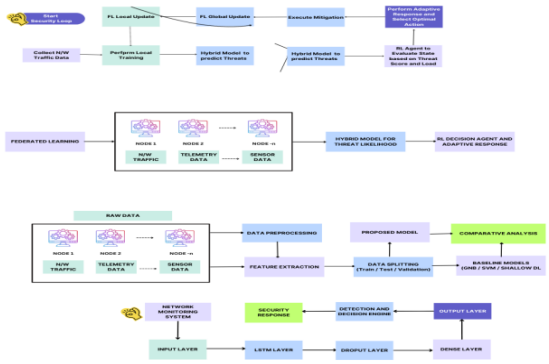


Figure 2: The AICSF Model Architecture

- Network Monitoring System: Used to capture the live packets and preprocessing them.
- Input Layer: The raw data is reshaped into the appropriate or sequential format.
- LSTM Layer: This layer processes the temporal sequences with 64 units. It contains input, output and forget gates, it also maintains cell state and observes multi stage attack behaviours.
- Dropout Layer: A dropout rate of 20% is applied for regularisation to prevent overfitting and enhanced generalization to attack variants.
- Dense Layers: To refine the features, multiple fully connected layers are used, nonlinear transformation of learned system.
- Output Layer: A single neuron with Sigmoid activation function to produce 1 for Normal and 0 for Attack data.
- Training: This model is trained using the Adam Optimizer and appropriate batch size for industrial network with10 epochs.
- Detection and Decision Engine: Uses LSTM memory to perform real-time anomaly classification and will support adaptive security.
- Security Response: Will produce automated alerts, traffic blocking, policy updates, and best suited for integrated industrial cyber security infrastructure.

The proposed AICSF consists of LSTM layer with 64 units for sequential processing then dropout layer for regularization, and dense layers for binary classification with sigmoid activation (Normal /Attack).

The trained model is integrated into the network monitoring system to enable real time packet tracing. This will take detection decisions for adaptive security based on current packet features and historical traffic data due to its recurrent nature.

3.3. Evaluation Metrics

The baseline and AICSF were evaluated and compared using the various metrics which includes Accuracy, Recall, F1-Score, FPR, Detection Rate, Prediction Time, Specificity(TNR), inference and Training complexity.

4. Results And Discussion

Metrics	Bayesian GNB	SVM	Shallow DL (MLP)	AICSF
Accuracy	0.8187	0.8460	0.9260	0.9700
F1-Score	0.8150	0.8449	0.9300	0.9875
FPR	0.1636	0.1489	0.0450	0.0080
Detection Rate	0.8008	0.8409	0.9250	0.9612
Prediction Time(s)	0.0019	0.0586	0.2628	0.4000
Specificity(TNR)	0.8560	0.8740	0.9280	0.9632
Training Time	0.0051	0.7062	0.9280	0.9632
Inference Time	0.0028	0.0469	0.4100	0.0380

The evaluation of the AICSF model is compared with baseline models GNB, SVM, and shallow DL for smart industry environments. The results for accuracy and specificity shows high performance in classifying complex and high dimensional networked data and robust capacity for recognition in complex threat vectors. The AICSF achieved improved classification accuracy of 97% whereas, shallow DL shows 92.6%, SVM model 92.6 and Bayesian classifier 81.87%. The metric specificity or True Negative Rate is used to measure the model's ability to classify traffic data efficiently to minimize false positive rate (FPR), otherwise this may lead to operational shutdown.

The specificity or True Negative Rate (TNR) achieved high for AICSF model at 96.32%, which is exceptional reliability in reducing false alarms. The marginal difference among the other modes varies slightly i.e. 85.60 for Bayesian, 87.37 for SVM and 92.8% for shallow DL. This variation suggests their limitations in learning complex decisions.

The key consideration is for analysis of time complexity represents computational cost and sophisticated model. The complexity of the deep learning architecture will take longer time as usual, the AICSF require 2.9056 seconds for training as it requires more computing resources and time, on the other side GNB, SVM and shallow DL 0.0051, 0.7062 and 2.6740 seconds. The prediction or inference time is the metric to measure how the models are suitable for real-time operation. The model AICSF maintains high inference speed of 0.0380 sec per batch/sample, other models GNB, SVM and shallow DL maintains 0.0028, 0.0469 and 0.0410 seconds respectively. The inference speed of SVM and shallow DL is slightly higher than AICSF, indicating that the model AICSF will predict effectively than kernel-based ML in this case as shown in figure 3.

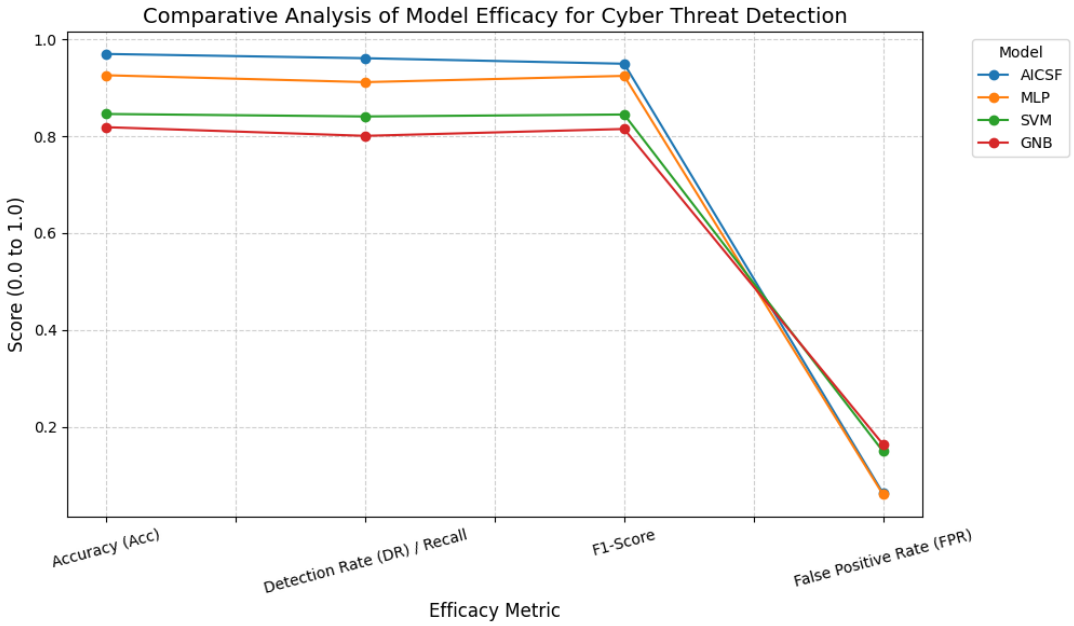


Figure 3: Model Efficiency Metrics for 4 Models

The results demonstrate the AICSF higher performance over the other models and it achieved higher detection rate (96.12%), accuracy of 94.93% and achieved low false positive rate. The prediction time of this model is slightly higher and acceptable range for real time threat detection.

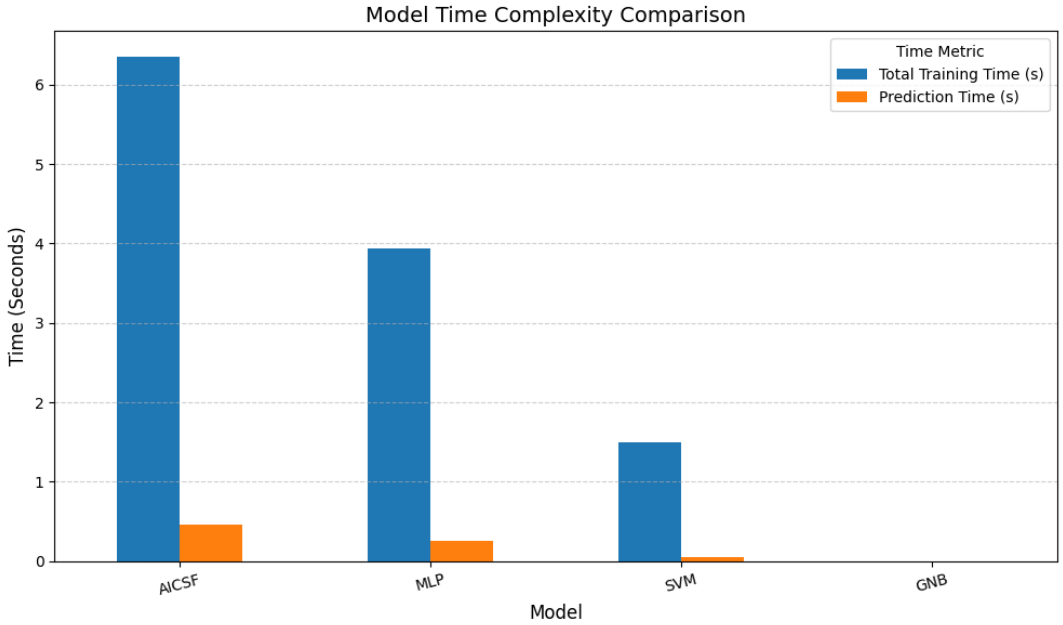


Figure 4: Comparison of Total training Time Vs Prediction Times.

The comparative analysis of model's time complexity demonstrates in Figure 4 which will provide the computational efficiency associated with each learning framework and shows total training time vs prediction or inference time across four models. The AICSF demonstrate high computational demand during training is 6.4 sec approx. which uses recurrent nature of LSTM network that will process sequential dependencies and memory across time steps. The prediction time remains moderate at 0.48 seconds, i.e. once the model was trained, it can generate inferences within timeframe effectively. The shallow DL (MLP) requires shorter training duration of 3.9 seconds which reflecting the reduced architectural complexity and absence of temporal parameter dependencies. Its prediction

time is approx. 0.26 seconds to make it suitable for applications when inference is with high priority than sequential modelling. The models GNB, SVM and MLP with low computational requirements with training time 1.5 sec with 0.09 seconds inference time, 0.02 seconds respectively. The above comparison shows a clear superiority between sophistication and computational complexity. The AICSF need higher training costs due to its enhanced capacity and nonlinear dependencies in complex timeseries data. The GNB, SVM and MLP have high computational efficiency but lack in high dimensional system model.

Figure 5: Performance Metrics – Accuracy Vs Specificity Comparison

The figure 5 shows that these will handle the substantial difference in the performance metrics ranging from 0 to 1 and time complexity metrics ranging from milliseconds to seconds. The models classification efficiency across accuracy and specificity. The overall performance clustering for all models are tightly clustered in the high range (0.95) which indicates that the models possess high ability to classify network traffic. The AICSF occupies the highest position, achieving the maximum accuracy (97%) with specificity (96.32%). The specificity directly relates to the True Negative Rate under normal traffic, the AICSF translates into the lowest false positive rate (FPR) among the models. The other models perform similarly in high dimensional space with lowest score for both metrics. The AICSF model performance level highlights the limitations of shallow and linear models against complex and modern cyber threats. The metric is time metric which uses logarithmic scale on Y-axis to clearly visualize the difference between the training times and prediction times. The training time exhibits a steep upward trend across the models. The trainings times of baseline models reported as 0.0051, 0.7062 and 2.6740, whereas the AICSF has the highest training cost of 2.9056 seconds which directly reflecting the computational overhead required to optimize the multi-layered deep architecture.

The prediction or inference time is significantly lower than the training time for all the models. The baseline models maintain the fastest inference time of 0.0028, 0.0469, 0.04100 and 0.0380 respectively. The AICSF prediction speed confirms that the framework can process network packets in real-time to ensure the high-performance benefits are realized without creating a critical operational bottleneck. The proposed AICSF requires one time investment in training resources, the return is high performance coupled with operationally acceptable, low latency detection.

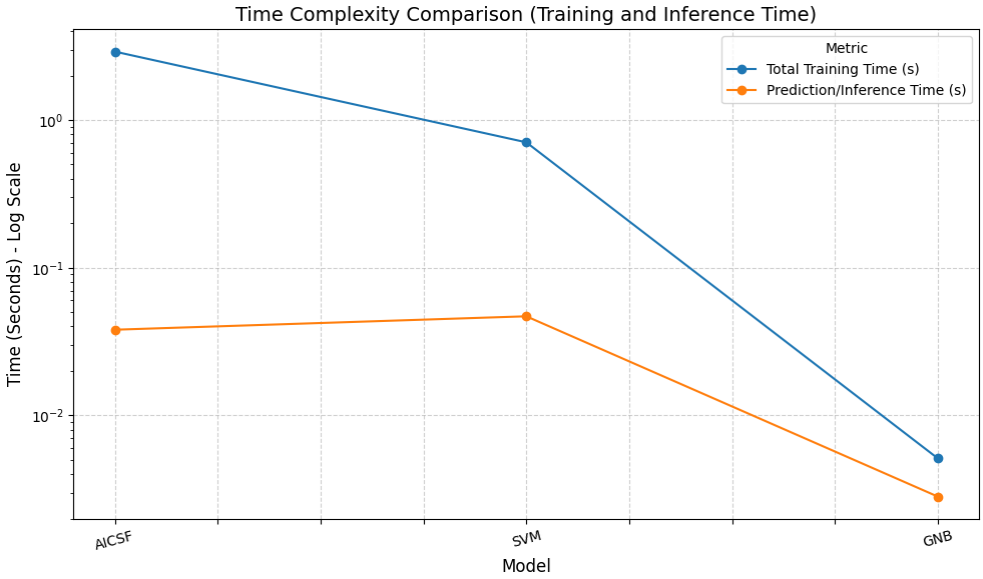


Figure 6: Time Complexity Comparison – Training Time Vs Inference Time

Figure 6 presents logarithmic scale comparison of the inference and training times for the evaluated models. The use of log-scale enables high visualisation of variations. The AICSF demonstrates the highest computational overhead during training, with training time approximately 2.4 seconds. The predictions time remains relatively moderate at 0.04 seconds, which indicating that after the temporal features are learned, the model is capable of performing inference effectively and accurately. The SVM shows slightly reduced training time of 0.75 seconds, represents an improvement compared to AICSF. This efficiency is from non-iterative optimization process and the absence of temporal modelling. Its inference time is marginally higher than the AICSF, in which the inference time is slightly higher, their prediction complexity grows with the number of support vectors, which may slightly influence real-time inference. The GNB exhibits the lowest time complexity across both metrics with a minimum training duration of 0.005 seconds and inference time of 0.003 seconds. This offer almost negligible computational cost. The AICSF demanding highest computational resources during training, offers most suitable architecture for temporal sequence modelling.

The finding provides compelling evidence that the AICSF models are necessary to secure smart industry. The AICSF ability to learn temporal pattern enables the detection of new unseen threats that traditional or static ML models would miss. The low FPR ensures that the security solution minimizes disruptions to critical industrial processes. This allows organizations to maintain the high operational uptime characteristics of industry.

4. Conclusions

This paper investigated the efficiency of AICSF for mitigating evolving cyber threats in the smart industry. By comparing the performance with GNB, SVM and MLP, this paper demonstrated that the proposed framework AICSF offers a robust and highly accurate solution. The key implication for cybersecurity, the adoption of advanced, AICSF solutions is essential for maintaining the security, integrity and operational resilience of their digital and physical assets in the increasingly sophisticated cyber physical threats. We can consider transformer-based model for improved sequential analysis and reduced latency or federated learning for distributed threat intelligence for better performance.

References

1. Al Rawajbeh, M.; Maria Soosai, A.J.; Ramasamy, L.K.; Khan, F. Trustworthy Adaptive AI for Real-Time Intrusion Detection in Industrial IoT Security. IoT 2025, 6, 53. https://doi.org/10.3390/iot6030053
2. Alserhani, F. Intrusion Detection and Real-Time Adaptive Security in Medical IoT Using a Cyber-Physical System Design. Sensors 2025, 25, 4720. https://doi.org/10.3390/s25154720
3. Goundar, S.; Gondal, I. AI-Blockchain Integration for Real-Time Cybersecurity: System Design and Evaluation. J. Cybersecur. Priv. 2025, 5, 59. https://doi.org/10.3390/jcp5030059
4. Bakkiam David Deebak; Fadi M. Al-Turjman; "Privacy-preserving in Smart Contracts Using Blockchain and Artificial Intelligence for Cyber Risk Measurements", J. INF. SECUR. APPL., 2021. https://doi.org/10.1016/j.jisa.2021.102749

5. Afees Olanrewaju Akinade; Peter Adeyemo Adepoju; Adebimpe Bolatito Ige; Adeoye Idowu Afolabi; Olukunle Oladipupo Amoo; "A Conceptual Model for Network Security Automation: Leveraging Ai-driven Frameworks to Enhance Multi-vendor Infrastructure Resilience", INTERNATIONAL JOURNAL OF SCIENCE AND TECHNOLOGY RESEARCH ..., 2021. DoI: 10.53771/ijstra.2021.1.1.0034
6. Adebunmi Okechukwu Adewusi; Njideka Rita Chiekezie; Nsisong Louis Eyo-Udo; "The Role of AI in Enhancing Cybersecurity for Smart Farms", WORLD JOURNAL OF ADVANCED RESEARCH AND REVIEWS, 2022. DOI: 10.30574/wjarr.2022.15.3.0889
7. Trim, P.R.J.; Lee, Y.-I. Combining Sociocultural Intelligence with Artificial Intelligence to Increase Organizational Cyber Security Provision through Enhanced Resilience. Big Data Cogn. Comput. 2022, 6, 110. https://doi.org/10.3390/bdcc6040110
8. Nikolay Ivanov, Chenning Li, Qiben Yan, Zhiyuan Sun, Zhichao Cao, and Xiapu Luo. 2023. Security Threat Mitigation for Smart Contracts: A Comprehensive Survey. ACM Comput. Surv. 55, 14s, Article 326 (December 2023), 37 pages. https://doi.org/10.1145/3593293
9. M. Liu et al., "Enhancing Cyber-Resiliency of DER-Based Smart Grid: A Survey," in IEEE Transactions on Smart Grid, vol. 15, no. 5, pp. 4998-5030, Sept. 2024, doi: 10.1109/TSG.2024.3373008.
10. Suprabhath Koduru, S.; Machina, V.S.P.; Madichetty, S. Cyber Attacks in Cyber-Physical Microgrid Systems: A Comprehensive Review. Energies 2023, 16, 4573. https://doi.org/10.3390/en16124573
11. Beg, O.A.; Khan, A.A.; Rehman, W.U.; Hassan, A. A Review of AI-Based Cyber-Attack Detection and Mitigation in Microgrids. Energies 2023, 16, 7644. https://doi.org/10.3390/en16227644
12. Sakthiswaran Rangaraju; "SECURE BY INTELLIGENCE: ENHANCING PRODUCTS WITH AI-DRIVEN SECURITY MEASURES", EPH - INTERNATIONAL JOURNAL OF SCIENCE AND ENGINEERING, 2023. (IF: 3) DOI: https://doi.org/10.53555/ephijse.v9i3.212
13. K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," in IEEE Access, vol. 12, pp. 173127-173136, 2024, doi: 10.1109/ACCESS.2024.3493957
14. Haroon Arif, Aashesh Kumar, Muhammad Fahad, & Hafiz Khawar Hussain. (2024). Future Horizons: AI-Enhanced Threat Detection in Cloud Environments: Unveiling Opportunities for Research. International Journal of Multidisciplinary Sciences and Arts, 3(1), 242–251. https://doi.org/10.47709/ijmdsa.v2i2.3452
15. Md Rasheduzzaman Labu, & Md Fahim Ahammed. (2024). Next-Generation Cyber Threat Detection and Mitigation Strategies: A Focus on Artificial Intelligence and Machine Learning. Journal of Computer Science and Technology Studies, 6(1), 179-188. https://doi.org/10.32996/jcsts.2024.6.1.19
16. Philip Olaseni Shoetan, Olukunle Oladipupo Amoo, Enyinaya Stefano Okafor, & Oluwabukunmi Latifat Olorunfemi. (2024). SYNTHESIZING AI'S IMPACT ON CYBERSECURITY IN TELECOMMUNICATIONS: A CONCEPTUAL FRAMEWORK. Computer Science & IT Research Journal, 5(3), 594-605. https://doi.org/10.51594/csitrj.v5i3.908
17. Ezekiel Onyekachukwu Udeh; Prisca Amajuoyi; Kudirat Bukola Adeusi; Anwulika Ogechukwu Scott; The integration of artificial intelligence in cybersecurity measures for sustainable finance platforms: An analysis. (2024). Computer Science & IT Research Journal, 5(6), 1221-1246. https://doi.org/10.51594/csitrj.v5i6.1195
18. Khan, B.U.I.; Goh, K.W.; Khan, A.R.; Zuhairi, M.F.; Chaimanee, M. Integrating AI and Blockchain for Enhanced Data Security in IoT-Driven Smart Cities. Processes 2024, 12, 1825. https://doi.org/10.3390/pr12091825
19. Kingsley David Onyewuchi Ofoegbu, Olajide Soji Osundare, Chidiebere Somadina Ike, Ololade Gilbert Fakeyede, & Adebimpe Bolatito Ige. (2024). Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. Computer Science & IT Research Journal, 5(8), 2083-2106. https://doi.org/10.51594/csitrj.v5i8.1493
20. Alevizos, L. Automated cybersecurity compliance and threat response using AI, blockchain and smart contracts. Int. j. inf. tecnol. 17, 767–781 (2025). https://doi.org/10.1007/s41870-024-02324-9
21. Emmanuel Cadet; Olajide Soji Osundare; Harrison Oke Ekpobimi; Zein Samira; Yodit Wondaferew Weldegeorgise; "AI-powered Threat Detection in Surveillance Systems: A Real-time Data Processing Framework", OPEN ACCESS RESEARCH JOURNAL OF ENGINEERING AND TECHNOLOGY, 2024. https://doi.org/10.53022/oarjet.2024.7.2.0057
22. Vineeth Sai Narajala; Idan Habler; "Enterprise-Grade Security for The Model Context Protocol (MCP): Frameworks and Mitigation Strategies", ARXIV-CS.CR, 2025. (IF: 3)
23. https://doi.org/10.48550/arXiv.2504.08623