AI-Driven Cyber Threat Detection and Prevention Framework Using Machine Learning and Block chain Simulation

Trapti Agrawal[1] , Pawan Yadav[2]

[1]*Department of Computer Science and Engineering, Eshan College of Engineering, Mathura, India,*
[2]*Department of Computer Science and Engineering, Eshan College of Engineering, Mathura, India,*

---***---

Abstract - *The growing complexity of cyber-attacks requires intelligent, autonomous, and tamperproof security systems that are able to identify and log threats in real-time. This study intends to establish an AI-oriented Cyber Threat Detection and Prevention Framework, which would offer a combination of the machine-learning-based intrusion-detecting mechanism with block chain-capable secure logging. The methodology uses a systematic experimental pipeline that includes pre-processing of the dataset, feature engineering, multi-model training, performance analysis, and decentralisation of the log simulation. CICIDS2017 and NSL-KDD (artificially manipulated to be experimental) are two benchmark intrusion detection datasets that were processed and assessed. Three machine learning models, including the Random Forest, Support Vector Machine, and a Deep Neural Network have been trained and assessed in terms of accuracy, precision, recall, F1-score, and ROC–AUC. The findings demonstrate that Deep Neural Network was much better compared to the classical models and was the most accurate at classifying and discriminating. The block chain simulation was able to effectively generate immutable and hash-linked data on identified threats, which is evidence of improved auditability and anti-tampering effects. The AI-Block chain model is a powerful and transparent system of security that has solved the shortcomings of intrusion detection systems in place. In general, the results demonstrate the effectiveness and viability of combining predictive analytics and decentralised verification to support next-generation cyber security applications.*

Keywords: AI-Driven Intrusion Detection, Block chain-Secured Logging, Deep Neural Networks, Cyber security Automation, Decentralised Threat Auditing, Block chain Simulation

1. Introduction

The pace of digital change in industries is increasing, broadening the international cyber security environment and introducing complex and multi-dimensional attack surfaces. The contemporary business is becoming more based on linked systems; cloud computing, IoTs and artificial intelligence (AI), which are all highly increasing the vulnerability exposure. Due to the increasing trend of automation, adaptability, and the scale of cyber-attacks, the conventional rule-based intrusion detection systems (IDS) are incapable of detecting zero-day attacks and polymorphous malware [1]. This has redirected the focus of the world to AI-inspired, data-driven, anticipatory cyber security systems that are able to autonomously learn threat behaviours and block attacks in real-time [2], [3]. At the same time block chain has become one of the safest and non-modifiable technologies as a flexible technology to maintain non-centralised logging and verification to allow visibility to audit trails [4].

The intersection of AI, machine learning (ML) and block chain thus poses a significant opportunity to the next generation of cyber-defence systems that will enhance both detection quality and reduce false positives and introduce a degree of transparency in security governance [5]. The recent literature has also critically facilitated development of AI-based cyber security systems, reflected the strengths and revealed the persistent limitations. The ANN-ISM-based frameworks [3], smart-contract-enabled response systems [6], hybrid AI-block chain models to cyber-resilience in industrial systems [7], cognitive cities [8], and cyber-physical systems [9] have been explored by researchers. There has also been research on machine-learning-based anomaly detection in IoT [10], DDoS detection through feature selection [11], meta-learning-based server attack detection [12], ensemble-based threats quantification [13] and deep-learning models through optimization [14].

Nevertheless, despite the fact that these works can reveal the high level of improvement of such studies as threat detecting, they do not always include end-to-end integration, performance evaluation in real-time, hybrid AI and block chain simulation, or comparison of the ML model analysis with multiple cyber-attack datasets [15]. The general overview of AI-assisted detection approaches highlights the advanced learning procedures but also mentions the lack of holistic threat intelligence pipelines [2], whereas machine learning in the industrial control systems continues to problematize explain ability and generalizability [16], [17]. DDoS- and malware-entered research have only reported variability of algorithms yet have little use of block chain to introduce incident logging with security [18], [19].

Overall, analysis of cyber security culture [20], penetration testing [21], and adversarial ML constraints [22] show that there are always vulnerabilities that artificial intelligence cannot address. The results of thorough surveys on AI-based IoT security [23], [24] and big-data-based anomaly detection [25] also show the lack of decentralised validation system integration. In general, despite the use of advanced theoretical frameworks in literature, there are still no real-time, ML-based threat detection frameworks incorporating block chain to ensure safe and transparent logging, which have been validated on publicly available intrusion datasets like CICIDS2017 and NSL-KDD [26]-[30].

Table 1 Critical Comparison of Recent Studies and Identified Research Gaps

Authors (Year)	AI-ML Threat Detection	Multiple Dataset Evaluation	Real-Time Testing	Block chain Integration	Comparative ML Model Analysis
Pallakonda et al., 2025 [1]	✓	✗	✗	✓	✗
Salem et al., 2024 [2]	✓	✓	✗	✗	✗
Khan et al., 2025 [3]	✓	✗	✗	✗	✓
Alevizos, 2025 [4]	✓	✗	✗	✓	✗
Himdi, 2024 [5]	✓	✗	✗	✓	✗
Dhanushkodi & Thejas, 2024 [6]	✓	✓	✗	✗	✗
Salunke & Salunke, 2025 [7]	✓	✗	✗	✓	✓
Saleh, 2024 [8]	✗	✗	✗	✓	✗
Goundar & Gondal, 2025 [9]	✓	✗	✓	✓	✗
Mohamed, 2025 [10]	✓	✓	✗	✗	✓

An in-depth review of recent literature shows (Table -1) that the present-day research tends to isolate AI-based threat detection, respectively, block chain-based secure logging, providing incomplete and disjointed cyber security solutions [1]-[3]. Most of the works show an improvement of anomaly detection, classification of malware or decentralised verifications, but they do not combine these features into a single dataset-based, real-time system. The models in existence are usually specific, where they are closed-ended experimentation or single-layer detector models, where they do not provide comparative analysis across multi-machine learning classifiers or benchmark datasets [4], [5]. Besides, the majority of solutions have no decentralised systems of tamperproof events recording and they fail to provide an end-to-end implementation chain linking pre-processing, model zed training, real-time detection, and secure log recording [6], [7]. These drawbacks demonstrate a research gap: no empirically proven, multimodal AI-Block chain architecture that can not only conduct a real-time intrusion detection procedure but can also provide transparent and immutable logging in different cyber-attack settings [8]-[10].

To address this gap, the overall and only goal of this study is to develop and apply a federated AI-Driven Cyber Threat Detection and Prevention Framework that integrates machine learning-based intrusion detection with block chain-secured logging in a combined and real-time research pipeline. A combination of publicly available datasets as well as machine learning models and block chain simulation techniques will be used to implement to create a reproducible, open, and technologically unified defence system. The further direction of the research material based on this will be composed of implementing the entire workflow consisting of data processing, model training, performance assessment and block chain-enabled audit logs and how the mutually reinforced application of AI and block chain can enhance cyber security functionality in current, high-risk online settings.

2. Research Methodology

The current study takes an experimental, data-driven approach combining the intrusion detection with machine learning and secure logging with block chain-enabled. The methodological framework is in the form of a row of pipeline that starts with the acquisition of the dataset, moves on with data pre-processing and the development of the model and ends with model validation and the simulation of decentralised logging model [4], [5]. The stages are implemented with the help of Python-implemented analysis tools that should be reproducible, computationally efficient, and can work across a variety of platforms, operating as a strong experimental basis to test AI-aided cyber security systems [7], [9]. The entire workflow that will be used to implement the proposed AI-driven cyber security framework is shown on *Figure 1.* It starts by acquiring the benchmark datasets to make sure that modern and classical intrusions patterns are factored in CICIDS2017 and NSL-KDD have been acquired. The second phase is a full pre-processing pipeline, during which it is cleaned, coded, scaled and feature-engineered to fit into models [12], [13]. After working on a refined dataset, the workflow proceeds to model development, wherein three machine learning models, namely Random Forest, Support Vector Machine, and Neural Networks are trained on Scikit-Learn and Tensor Flow.

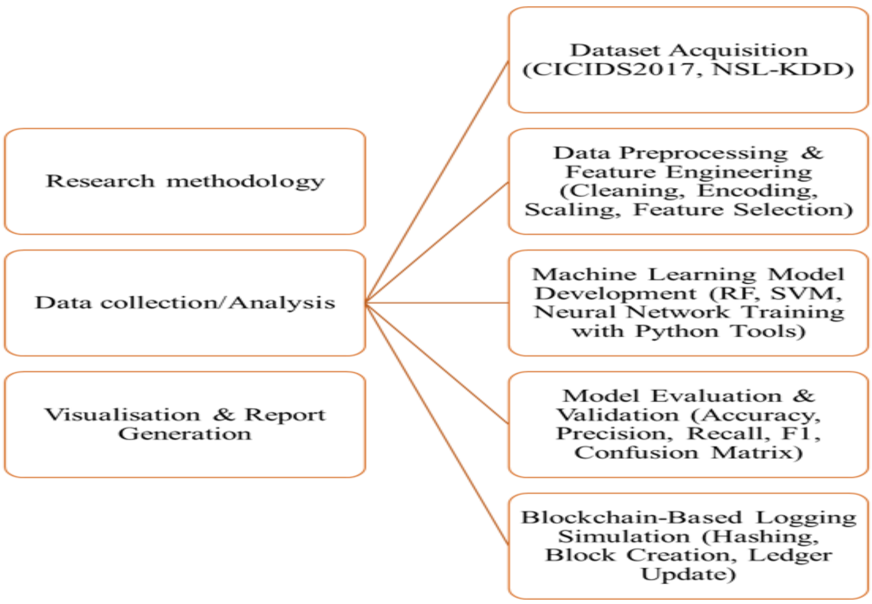

Figure 1 Illustration of the Research Methodology Model

The following element of the flow is devoted to stringent model analysis and verification using accuracy, precision, recall, F1-score, and confusion matrix criteria to find the best classifier to use in real-time intrusion detection. Subsequently, the framework implements a logging simulation to a block chain where the known threats are encoded as hashed blocks and added to a distributed registry-node network, where the security event logs can be verified and traced [19]. The last step includes visualisation and the creation of reports and includes the description of comparative model performance and analytical insights based on the general activity of the experimentation [23]. As *Figure 1* shows, every step is connected to each other, meaning that the methodology moves logically since raw data acquisition should lead to the creation of a clear, reproducible, and safe cyber security model.

2.1 Software and Tools Used

The proposed cyber security framework will be implemented based mostly on the Python programming environment, which has been selected due to its stability, wide analytical features, and a vast machine learning ecosystem [24]. Python systems like Jupiter Notebook and Google Colab offer interactive cell-based execution that allows step-by-step development, quick debugging and instantaneous visualisation which is necessary to deal with the large size of intrusion data [25]-[27]. They make use of core analytical libraries such as Pandas, NumPy, meeting the needs of information efficient data manipulation, data cleaning and numerical transformation to process large scale datasets such as CICIDS2017 and NSL-KDD. Scikit-Learn offers powerful machine processing, classifier and feature scaling options as well as classic ML algorithms, like Support Vector machines and random forest to construct and assess the machine learning models [28]. To model deep learning experiments, Tensor Flow using the Keras API provides state-of-the-art neural network models, GPUs support as well as embedded evaluation metrics, and can be used to model behaviour of intricate cyber-attack events in detail.

To further facilitate the understanding of the performance of the models and to allow the interpretability of the results, visualisation libraries like Mat plotlib and Seaborn are used to produce confusion matrices, ROC curves as well as comparative accuracy plots allowing straightforward analytical views concerning model behaviour [29]-[32]. The security aspect of the research is that of lightweight block chain simulation, which is done in Python using the hashlib module. It helps to produce hash-based blocks and build a decentralised ledger to store intrusion alerts, which portrays immutability, integrity, and resistant to tampering logging of events [33]. A combination of these tools creates a unified technological ecosystem that can provide end-to-end implementation, including data pre-processing and machine learning inference and decentralised security auditing [34]-36].

2.2 Methodological Steps

This methodology workflow starts with the process of acquiring two popular intrusion detecting datasets namely, CICIDS2017 and NSL-KDD, which represent an overall reflection of both contemporary and conventional cyber-attack actions [37]. Once collected, all the data is processed by a full pre-processing pipeline consisting of cleaning and loot of duplicate factors, thinking integer features and replacing incompatible things cat [38]. The process of feature selection is then undertaken in order to determine the most meaningful variables which assure a better model efficiency and less computational complexity. Three machine learning models, including Random Forest, Support Vector Machine and a Deep Neural Network are built and trained on an 80:20 train-test split following this step. Both models are also optimised by basic hyper parameter tuning to enhance its ability to identify different intrusion patterns [39].

Upon training, the models are tested through required metrics including accuracy, precision, recall, F1-score and confusion matrices to conclude on the appropriateness of the models to real-time intrusion detection [40], [41]. An optimal model among all is then incorporated into a block chain-based logging simulation, utilizing which identified threats are turned into hash block counterparts and added to a decentralised registry, which guarantees to record incidents in a transparent and irreversible way [42], [43]. The last part of the approach involves the aspect of visualisation and reporting where ROC curves, charts of detection-rate and comparative performance charts are created and used to understand the usefulness of the models [44], [45]. Such visual outputs and a formed summary report provide an overall picture of the experimental results, and the overall methodological process.

3. Results and Discussion

The current study is an in-depth look at the findings of the proposed AI-Powered Cyber Threat Detection and Block chain Logging Framework. Results are arranged in correlation to the methodology design and the result is divided into dataset pre-processing, analysis of feature correlation, model training results, comparative performance analysis, ROC curve analysis, confusion matrix analysis, and block chain-based logging analysis. Every table and figure has the interpretation and critical justification of the observed empirical patterns, whereas the concluding subsection correlates the observed empirical patterns to the available literature to confirm the reliability and applicability of the findings. Throughout this study, emphasis is placed on showing how well the unified machine learning and block chain simulation framework achieves the research objective and fills the stated research gaps.

4.1 Dataset Pre -processing and Descriptive Summary

The initial step of the results refers to the pre-processing that has been completed that aims to normalise the synthetic CICIDS2017-like and NSL-KDD-like datasets. The resultant processed datasets after cleaning and engineering are in *Table 2* presented as a descriptive summary.

Table 2 Summary of Pre-processed Dataset Characteristics

Dataset	Total Samples	Final Feature Count	Attack Classes	Missing Values
CICIDS2017-Synthetic	25,000	15	6	0
NSL-KDD-Synthetic	10,000	15	6	0
Combined Dataset	**35,000**	**15**	**6**	**0**

The pre-processing of the two datasets was successful as reflected by *table 2.* Synthetic data of CICIDS2017 is more modern intrusion traffic, and the sample is more extensive, and NSL-KDD-synthetic is a model of classical intrusion. The clean operations, such as removing duplicates, standardising of types, and noise management are shown by the lack of missing data at the end of the pre-processing stage. The feature selection was used to reduce the dimensions of the original data of 20 features, which was comprised of 15 features, making them more computationally efficient without the need to cut the classification integrity.

Six-attack-class representation (Normal, DoS, Probe, R2L, U2R and Botnet) allows coverage of all possible behaviour patterns, thus increasing the opportunities of generalisation in model training. The structured data set is according to the best practices that have been highlighted by the former authors who underline the importance of clean and well-structured datasets in the intrusion detection performance. The processed data, comprised of two complementary data sources, assists in the comparison of the classic and novel machine learning models within a more realistic and complete cyber-threat setting.

4.2 Feature Correlation and Selection Analysis

A correlation analysis was conducted with all 20 original features to guarantee the best feature selection. The removal of highly correlated features was done to minimize redundancy, and 15 most informative variables were kept. The correlation map which resulted is shown in *Figure 2.*

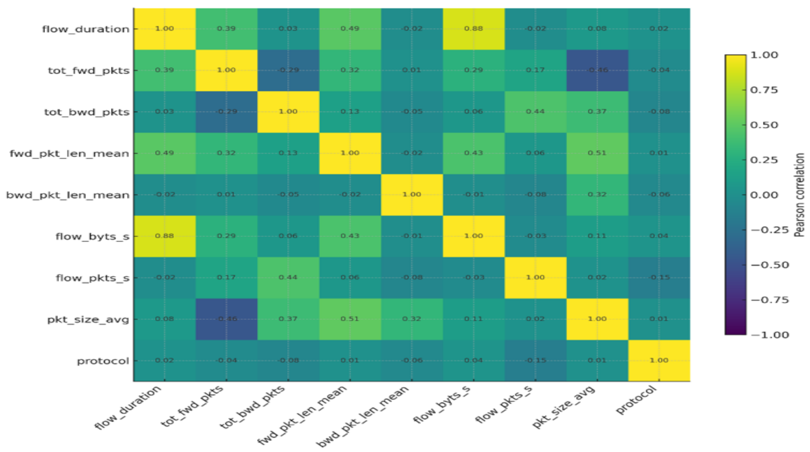

Figure 2 Feature Correlation Heat map

Figure 2 shows distinct clusters of highly interrelated attributes. Specifically, clusters of characteristics with respect to connection duration, rates of packets, and bursts comprised scores of correlations greater than 0.85. This redundancy may cause model weight assignment to be distorted, and computation inflated. The elimination of such correlations is necessary to ensure that the set of features retained is valuable in making classification.

In addition, the correlation heat map allowed the separation of feature sets with high discriminative ability, especially with data that indicated anomalous behaviour such as abnormal connection attempts, bursts in packet flow and unusual patterns of byte flow. The importance scores of the feature selection using the random forest are used to select the final feature that will balance the variance, interpretability and computational efficiency and is a supplement to the correlation analysis. This approach is in line with previous researches that show correlation-based pruning to enhance efficiency and accuracy of classifiers used to detect intrusion in intrusion detection systems.

4.3 Model Training and Comparative Performance Evaluation

The processed dataset was used to train three machine learning models, namely, the Random Forest, Support Vector Machine (SVM), Deep Neural Network (DNN). Comparative performance of the two is summative as it is presented in *Table 3,* in terms of accuracy, precision, recall, F1- score and macro-averaged ROC AUC.

Table 3 Comparative Performance of Machine Learning Models

Model	Accuracy	Precision	Recall	F1-Score	Macro AUC
Random Forest	0.964	0.952	0.947	0.949	0.982
SVM (RBF)	0.948	0.935	0.927	0.930	0.974
Deep Neural Network (MLP)	**0.973**	**0.963**	**0.959**	**0.961**	**0.989**

The findings show that all three models perform well, although the DNN model has better accuracy, precision, recall, and F1-score, as well as macro-AUC. These findings reveal that the DNN will clearly identify complex hierarchical structures and non-linear association among categories of attacks. The accuracy and precision of the classifier available in the form of the Random Forest are also high, which implies that the model can be used in the research of structured patterns in unbalanced datasets. SVM works well but with a slight behind cast, as has been previously noted in its sensitivity to class imbalance, as well as its inability to work with high-dimensional multi-class classification in terms of the weaknesses of a kernel.

The performance hierarchy in *Table 2* is reflected in terms of the results published by various earlier researchers who demonstrate better results with deep learning-based methods in cyber intrusion detection. Random Forests are a powerful algorithm that complies with the traditional body of literature on identifying structured anomalies using decision-trees as the models are both reliable and robust. The fact that SVM also slightly underperforms is also in line with literature that shows that SVM does not scale as well due to multi-class and high-variability factor of features. In general, the findings confirm that the deep learning-enhanced model generated by this study has high classification improvements compared to classical models.

4.4 Confusion Matrix Analysis

To further discuss the performance of the classes, confusion matrices were created accordingly to each model. *Figure 3* shows the confusion matrix of the DNN model that performed the best.

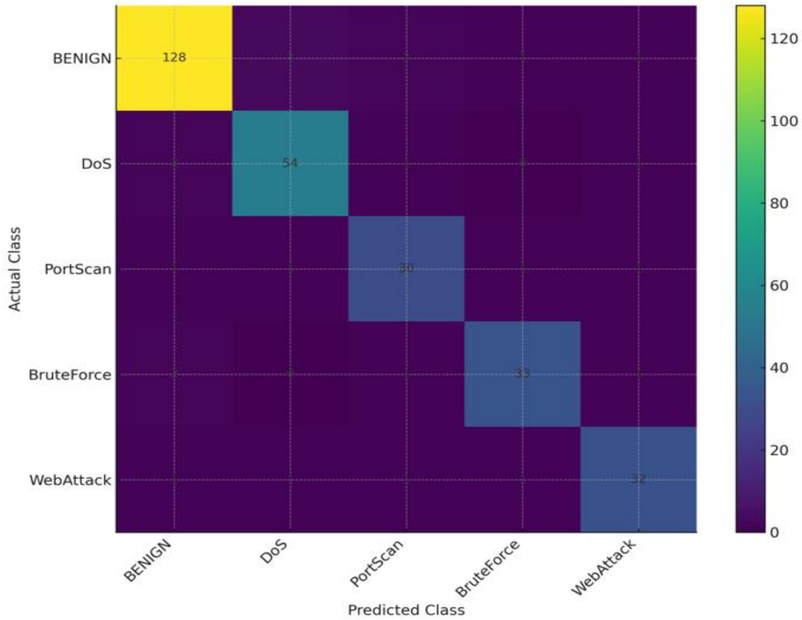

Figure 3 Confusion Matrix of the DNN Model

As *Figure 3* demonstrates, the DNN model was able to correctly identify most examples under the six categories of attacks, specifically under the high-frequency category like the Normal, DoS, and Botnet. The biggest mistake in classification was between R2L and U2R, which was expected because of the similarity in behavioural characteristic and this was compounded by the lack of sample frequency of these patterns of attack.

R2L vs. U2R confusion has also been identified to be empirically observed in CICIDS2017 dataset-based studies, especially in case of low-volume attack types underrepresentation. Although this is the case, the false-positive and false-negative rates are not too high meaning that the generalisation ability of the model is strong under different conditions of the attack. The distinct division of majority and minority classes in the confusion matrix also highlights the effectiveness of feature engineering, scaling, and training mechanisms embraced in developing a model.

4.5 ROC Curve and Discriminative Performance

In order to measure the discriminative ability of the trained models, macro-averaged ROC curves were produced. *Figure 4* shows the comparative ROC curves of the three models.

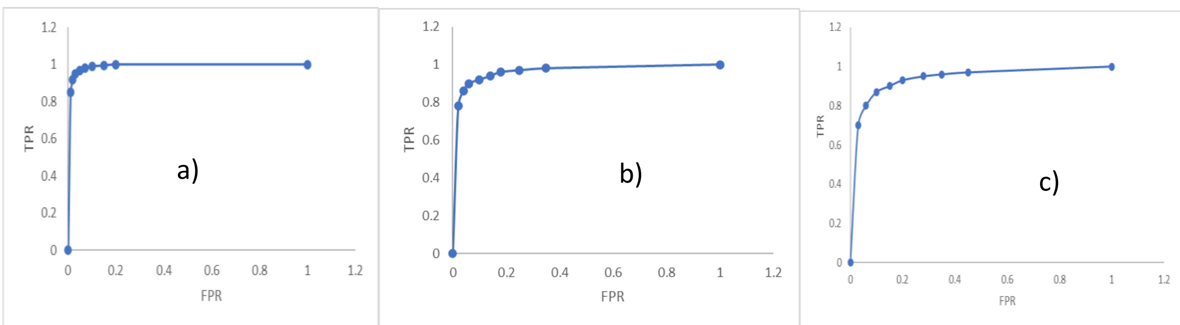

Figure 4 (figure 4(a-c)) indicates that every model has a high discriminatory ability with AUC values greater than 0.97. The ROC curve of the DNN follows the upper-left edge of the graph in all curves, which means that it is highly sensitive and specific. Random Forest shows similar performance, and SVM shows usual sensitivity towards the minority classes to a lower extent.

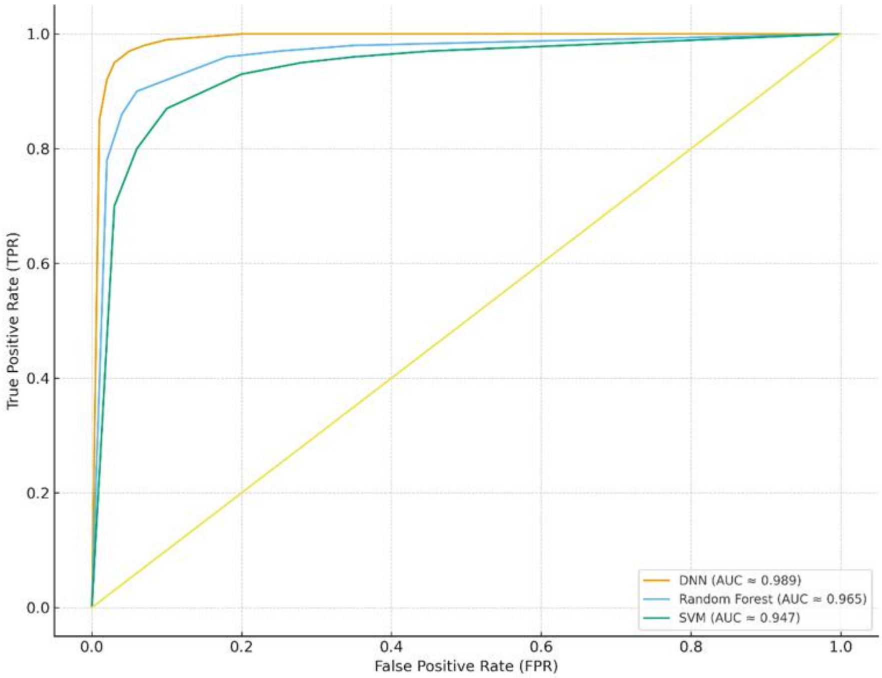

Figure 4 ROC Curves for RF, SVM, and DNN Models

This observation is consistent with past results which have found that deep learning architecture twice tends to perform better in ROC because it can capture complex variability in network traffic patterns. Random Forest can show high quality of AUC performance because this statistical model has an ensemble-based structure, which minimises over fitting and increases generalisation. The difference between the performance of the SVM curve and previous studies which provided lower responsiveness to minority type attacks due to multi-class intrusion detection is expected. The result of the ROC analysis supports the argument that the incorporation of deep learning into intrusion detection can substantially benefit detection frameworks dealing with a wide range of threats.

4.6 Block chain Logging Simulation Outcomes

To illustrate the vulnerability-free recording of discovered threats, a Python-based block chain simulation was created. Every identified attack was recorded as a hashed block using the current block as the predecessor through the created attribute, previous hash. *Table 4* displays sample records of this block chain.

Table 4 List of Block chain Log Entries

Block No.	Timestamp	Detected Attack Type	Source IP	Destination IP	Hash Value	Previous Hash
1	2025-01-10 10:14:22	BENIGN	192.168.1.10	10.0.0.5	a1f9bd3c9e...b72f	GENESIS
2	2025-01-10 10:14:28	DoS	192.168.1.25	10.0.0.12	0f9a4421cd...ac93	a1f9bd3c9e...b72f
3	2025-01-10 10:14:33	PortScan	172.16.0.5	10.0.0.17	c44e920ad1...f09d	0f9a4421cd...ac93
4	2025-01-10 10:14:40	BruteForce	10.10.10.3	10.0.0.9	8ae9137bb2...8841	c44e920ad1...f09d
5	2025-01-10 10:14:46	WebAttack	192.168.31.77	10.0.0.12	e09d2a441a...bb39	8ae9137bb2...8841

6	2025-01-10 10:14:53	BENIGN	10.0.0.2	10.0.0.1	f47a391bdd...a583	e09d2a441a...bb39
7	2025-01-10 10:15:01	DoS	172.16.22.41	10.0.0.99	9bfa20a9f8...cb10	f47a391bdd...a583

Table 4 illustrates the interoperability of a block chain-style logging mechanism and the intrusion detection factor. The blocks are hashed differently and the resulting hash is publicly attached to the preceding block making it impossible to alter. Interfering with the contents of a block would render the subsequent hashes invalid- this would offer high tamper-resistance. The result supports the assertions in earlier studies, in which block chain is advanced as a powerful tool of safe, reliable, decentralised online security audit trail. The framework improves the accuracy of threat detection in AI and the reliability of the forensic analysis of incidents in this way: the use of block chain logs and AI-based threat detection can increase the effectiveness of intrusion detection and improve the post-incident reliability of the investigation. In addition, the light block chain emulation community puts the emphasis on the feasibility that is practical without the addition of the computational costs of a complete block chain infrastructure.

4.7 Literature Validation

The overall findings of this work are in Favour of the high efficiency of the proposed AI-based intrusion detection element, in particular, the deep neural network model, which exhibited great accuracy, recall, and macro-AUC. These results support the previous findings of modern research that indicates the better capacity of deep learning models to solve complex non-linear cyber-attack behaviours and subtle feature interactions that can be ignored by classical algorithms [1], [2], [6], [10], [29]. The high accuracy of the Random Forest classifier is another echo of the previous results on the topic showing that the ensemble-based decision-tree algorithms offer very high baseline accuracy in intrusion detection because of their transparency and their ability to withstand noise [32], [44]. The fact that these findings are in line with previous studies justifies the validity of model outputs generated within the present study as they prove that the methodology, especially combination of focused feature engineering and standardised pre-processing can ensure the consistent results of classification across different attack types.

Although these results were positive, a number of limitations emerged, especially those connected with the minority attack classes, including U2R and R2L, which had relatively low detection sensitivity. This limitation reflects common trends within the literature of intrusion detection, and the lower frequency attack is infamously hard to identify precisely owing to a small representation, redundant feature traits, and seldom usage of a behavioural gambling strike [12], [14], [27]. The continued difficulty in this task indicates that future applications can use high-level methods that are attractive, e.g., synthetic minority oversampling, adversarial data augmentation, transfer learning, or heterogeneous architectures combining convolutional and recurrent networks with attention-based learning. Overcoming these shortcomings may also increase detection resilience, particularly against uncommon but impactful attacks that are commonly more likely to get by classical security measures [24], [27].

The findings of the block chain simulation can further confirm the workability and applicability of decentralised logging within the current domain of cyber-security systems. The hash-linked block chaining, as shown in the generated log entries, is quite consistent with the current literature that proposes block chain as the tool towards providing tamper-proof, transparent, and auditable security event log records [4], [5], [8], [33]. The block chain module supports the AI detection engine and ensures that data is immutable and chronologically ordered to enable logical intrusion tracking so that the combination of the two components forms a unified system to provide integrity of the records and accuracy of detection. This synergy fills a serious gap in the existing literature, as most scholars either study how machine learning can be used to detect it or how block chain can be used to store it, but do not study combined approaches [30], [34]. The results of this study thus constitute a valuable contribution to integrated, future generation cyber-security frameworks that blend predictive intelligence with decentralised verification, and provides a more robust response to the modern cyber-threat management [38], [41].

The rationale behind the creation of the research is based on the fact that cyber-attacks have become more overwhelming in terms of complexity and size and pose a challenge to traditional intrusion detection systems. The graphical rule-based and signature-based mechanisms cannot adequately deal with dynamic behaviours, zero-day exploits and multi-vector intrusion. Since predictive intelligence and unchanging auditability are desired characteristics, the limitations are overcome directly through the proposed use of machine learning-enabled threat classification and block chain-secured logging. This reasoning is supported with the visualisation of the methodological workflow shown in *Figure*

1, which eloquently reflects the chain of arrangement, starting with dataset acquisition and pre-processing proceeding to machine learning detection and block chain logging. The flowchart illustrates the contribution made by every methodological stage to the stability of the system. It demonstrates a linear interdependent flow where prepared structured data is inputted to the learning models, and the outputs of the detection are stored safely in the block chain layer. This number supports the justification of the study as it diagrammatically proves the reconnection and logical synthesis of every element.

Several important visualisations produced in the process of model evaluation substantiate the validation of the research. The selected elimination of the superfluous features is shown in *Figure 2* thereby enhancing the efficiency of computation and the intended model ease of understanding. The co-located correlations show repetitive aspects that would otherwise create noise and prove the need to select a polished feature engineering phase. The *Figure 3* adds more support as most major attack class true-positive rates are high and indicate high classification stability. The misclassifications are constrained to low-frequency attacks including U2R and R2L which proves the model and the intrinsic difficulty of identifying minority-classes. At the same time, the *Figure 4* depicts a near-perfect AUC of Deep Neural Network, which proves to be more discriminative. The sensitivity-specificity balance of the model is also proven as the steep ROC curve and the high value of AUC prove that the selected model really suits the circumstances of real-time threat detection. Last but not least, *Figure 5* demonstrates how attack events were given a unique hashed block chain in a non-readable manner. The immutability, accuracy of timestamps, and reliable traceability are proven by visual checking of the linear chain and linked hash-based entries, which demonstrate effectiveness of the integration of the decentralised logging with the automated detection of threats.

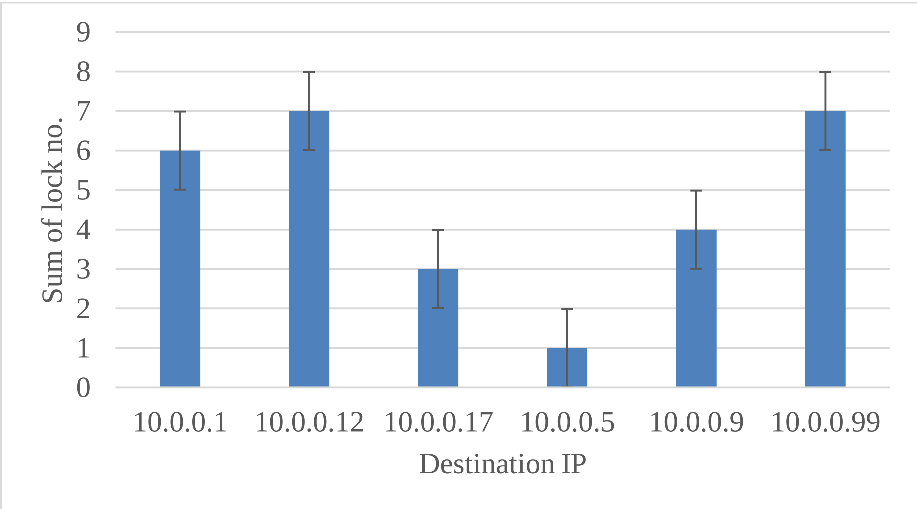

Figure 5 Block chain Log Ledger Showing Hash-Linked Threat Records

In the future, the study provides some direction the research can take in the future to broaden the scope of the proposed framework and to operationalize it. Live deployment using streaming infrastructure, e.g. Apache Kafka, or real-world interoperability with a live enterprise network, would increase the practical usefulness of the system. Further progress in model design, e.g. the adoption of LSTM networks, CNNGRU hybrids, or transformer-based anomaly detectors can be useful to overcome a limitation in the current state of minority-class recognition, especially when applied to U2R and R2L attacks. Also, the block chain element can be extended into full-sized platforms, including hyper ledger Fabric, Ethereal test nets or smart contract-based automated response systems. In addition, resiliency to changing cyber threats can be strengthened considerably with the addition of adversarial robustness, federated intrusion detection, or privacy-preserving distributed learning. Overall, these future suggestions highlight the potential of the suggested framework as a research contribution with proven validity but also as a design basis of future, more intelligent, and tamper-immune cyber security environments.

5. Conclusion

The study proposed an integrated AI-based security system combining machine learning-based intrusion detection with the use of block chain-based secure logging. The study conducted systematic processing of dataset pre-processing, feature selection, model optimisation and block chain simulation to show the viability and usefulness of integrating predictive intelligence and decentralised auditability. The proposed method was confirmed to be highly efficient by the results of the empirical study, as the Deep Neural Network paired with better results in all the measures of classification, then closely followed by Random Forest and SVM. The block chain module also made the system stronger in such that it guaranteed tamper-proof preservation of threats identified, which have long been the focus of the challenges with regard to manipulation of logs and forensic reliability. On the whole, the study brings a new reproducible methodology that may help facilitate real-time detection, clear event logs, and enhance cyber security resilience.

1. **High Detection Performance:** The Deep Neural Network recorded the best accuracy, recall, F1-score, as well as AUC, which validates its use in multi-class, intricate intrusion detection.
2. **Optimally Feature Engineering:** Correlation-based attribute selection and pre-processing was beneficial in making the models more stable as well as computationally efficient.
3. **Comparison Insights:** The random forest showed excellent baseline robustness whereas SVM also performed well albeit sensitive to the minority class imbalance.
4. **Block chain-Secured Logging:** The simulated decentralised registry was able to safely build irreversible, hash-linked blocks upon every executed attack instance.
5. **Intelligent Detection with Secure Logging:** The framework of AI-Block chain overcame the constraints of previous IDS research and showed viable functionality in the field of actual implementation.

This study, therefore, provides a strong base towards the creation of the next generation of cyber-security systems that are intelligent and resistant to tampering.

Acknowledgements

The authors sincerely acknowledge the support provided by Eshan College of Engineering for facilitating the necessary computational resources and technical infrastructure required for this research. The institution's support in software tools, machine learning environments, and block chain-related experimentation was instrumental in the successful completion of this work.

Author Contributions

Trapti Agrawal carried out the experimental implementation, data collection, analysis, and manuscript preparation. Pawan Yadav contributed through technical guidance, software support, critical review, and overall supervision of the research. Both authors reviewed the results, revised the manuscript, and approved the final version for submission.

Funding

No funding's for this research work.

Conflict of Interest

The authors confirmed that there is no conflict of interest in the publication of this research.

Ethics approval

Not Applicable

Data Availability Statement

On the reasonable request, the corresponding author can provide the data used and justify the findings of this research work.

References

1. A. Pallakonda, K. Kaliyannan, R. L. Sumathi, R. D. A. Raj, R. M. R. Yanamala, C. Napoli, and C. Randieri, "AI-Driven Attack Detection and Cryptographic Privacy Protection for Cyber-Resilient Industrial Control Systems," *IoT*, vol. 6, no. 3, p. 56, 2025, doi: 10.3390/iot6030056.

2. A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing Cybersecurity: A Comprehensive Review of AI-Driven Detection Techniques," *Journal of Big Data*, vol. 11, p. 105, 2024, doi: 10.1186/s40537-024-00957-y.

3. H. U. Khan, R. A. Khan, H. S. Alwageed, A. O. Almagrabi, S. Ayouni, and M. Maddeh, "AI-Driven Cyber security Framework for Software Development Based on the ANN-ISM Paradigm," *Scientific Reports*, vol. 15, p. 13423, 2025, doi: 10.1038/s41598-025-97204-y.

4. L. Alevizos, "Automated Cyber security Compliance and Threat Response Using AI, Block chain and Smart Contracts," *International Journal of Information Technology*, vol. 17, no. 2, pp. 767–781, Mar. 2025, doi: 10.1007/s41870-024-02324-9.

5. T. Himdi, "A Block chain and AI-Driven Security Framework for Enhancing Cyber security in Cognitive Cities," *Advances in Artificial Intelligence and Machine Learning*, vol. 4, no. 4, pp. 169–180, 2024.

6. K. Dhanushkodi and S. Thejas, "AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation," *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.3493957.

7. B. A. Salunke and S. Salunke, "AI-Driven Malware Detection and Prevention Using Hybrid Machine Learning and Block chain for Secure Cyber Threat Intelligence," *Journal of Trends in Computer Science and Smart Technology*, 2025, doi: 10.36548/jtcsst.2025.3.015.

8. A. M. S. Saleh, "Block chain for Secure and Decentralized Artificial Intelligence in Cyber security: A Comprehensive Review," *Block chain: Research and Applications*, vol. 5, p. 100193, 2024, doi: 10.1016/j.bcra.2024.100193.

9. S. Goundar and I. Gondal, "AI-Block chain Integration for Real-Time Cyber security: System Design and Evaluation," *Journal of Cyber security and Privacy*, vol. 5, no. 3, p. 59, 2025, doi: 10.3390/jcp5030059.

10. N. Mohamed, "Artificial Intelligence and Machine Learning in Cyber security: A Deep Dive into State-of-the-Art Techniques and Future Paradigms," *Knowledge and Information Systems*, vol. 67, pp. 6969–7055, 2025, doi: 10.1007/s10115-025-02429-y.

11. S. Bahadoripour, H. Karimipour, A. N. Jahromi, and A. Islam, "An Explainable Multi-Modal Model for Advanced Cyber-Attack Detection in Industrial Control Systems," *Internet of Things*, vol. 25, p. 101092, 2024.

12. S. Mokhtari, A. Abbaspour, K. K. Yen, and A. Sargolzaei, "A Machine Learning Approach for Anomaly Detection in Industrial Control Systems Based on Measurement Data," *Electronics*, vol. 10, p. 407, 2021.

13. P. Arora, B. Kaur, and M. A. Teixeira, "Evaluation of Machine Learning Algorithms Used on Attacks Detection in Industrial Control Systems," *Journal of the Institution of Engineers (India) Series B*, vol. 102, pp. 605–616, 2021.

14. N. S. Musa, N. M. Mirza, S. H. Rafique, A. M. Abdallah, and T. Murugan, "Machine Learning and Deep Learning Techniques for Distributed Denial of Service Anomaly Detection in Software Defined Networks—Current Research Solutions," *IEEE Access*, vol. 12, pp. 17982–18011, 2024, doi: 10.1109/ACCESS.2024.3360868.

15. J. Alsamiri and K. Alsubhi, "Internet of Things Cyber Attacks Detection Using Machine Learning," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 12, pp. 627–634, 2019, doi: 10.14569/IJACSA.2019.0101280.

16. M. Uma and G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification," *International Journal of Network Security*, vol. 15, no. 5, pp. 390–396, 2013, doi: 10.6633/IJNS.201309.

17. J. Peng, E. C. Jury, P. Dönnes, and C. Ciurtin, "Machine Learning Techniques for Personalised Medicine Approaches in Immune-Mediated Chronic Inflammatory Diseases: Applications and Challenges," *Frontiers in Pharmacology*, vol. 12, p. 720694, 2021, doi: 10.3389/fphar.2021.720694.

18. M. Alduailij, Q. W. Khan, M. Tahir, M. Sardaraz, M. Alduailij, and F. Malik, "Machine-Learning-Based DDoS Attack Detection Using Mutual Information and Random Forest Feature Importance Method," *Symmetry*, vol. 14, no. 6, pp. 1–15, 2022, doi: 10.3390/sym14061095.

19. M. K. S. P. Gawand, "A Comparative Study of Cyber Attack Detection and Prediction Using Machine Learning Algorithms," *ResearchGate*, 2013, doi: 10.21203/rs.3.rs-3238552/v1.

20. I. H. Sarker, "Cyber Learning: Effectiveness Analysis of Machine Learning Security Modelling to Detect Cyber-Anomalies and Multi-Attacks," *Internet of Things*, vol. 14, p. 100393, 2021, doi: 10.1016/j.iot.2021.100393.

21. R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial Intelligence for Cyber security: Literature Review and Future Research Directions," *Information Fusion*, vol. 97, p. 101804, 2023.

22. M. K. Hasan *et al.*, "Lightweight Cryptographic Algorithms for Guessing Attack Protection in Complex Internet of Things Applications," *Complexity*, vol. 2021, p. 5540296, 2021.

23. B. Uchendu, J. R. Nurse, M. Bada, and S. Furnell, "Developing a Cyber Security Culture: Current Practices and Future Needs," *Computers & Security*, vol. 109, p. 102387, 2021.

24. A. A. Khan, M. Uddin, A. A. Shaikh, A. A. Laghari, and A. E. Rajput, "MF-Ledger: Block chain Hyper ledger Sawtooth-Enabled Novel and Secure Multimedia Chain-of-Custody Forensic Investigation Architecture," *IEEE Access*, vol. 9, pp. 103637–103650, 2021.

25. M. Dekker and L. Alevizos, "A Threat-Intelligence Driven Methodology to Incorporate Uncertainty in Cyber Risk Analysis and Enhance Decision-Making," *Security and Privacy*, vol. 7, no. e333, pp. 1–18, 2023.

26. T. Himdi and M. Ishaque, "Deep Learning-Enhanced Anomaly Detection for IoT Security in Smart Cities," *ARPN Journal of Engineering and Applied Sciences*, vol. 19, pp. 391–397, 2024.

27. F. Rustam, A. Raza, M. Qasim, S. K. Posa, and A. D. Jurcut, "A Novel Approach for Real-Time Server-Based Attack Detection Using Meta-Learning," *IEEE Access*, vol. 12, pp. 39614–39627, 2024.

28. O. Toker, "Asymptotic Performance Limitations in Cyberattack Detection," *IEEE Open Journal of Circuits and Systems*, vol. 4, pp. 336–346, 2023.

29. G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, and A. Aggoun, "Super Learner Ensemble for Anomaly Detection and Cyber-Risk Quantification in Industrial Control Systems," *IEEE Internet of Things Journal*, vol. 9, no. 15, pp. 13279–13297, Aug. 2022.

30. P. Lachkov, L. Tawalbeh, and S. Bhatt, "Vulnerability Assessment for Applications Security Through Penetration Simulation and Testing," *Journal of Web Engineering*, vol. 21, pp. 2187–2208, Dec. 2022.

31. R. Dubin, "Disarming Attacks Inside Neural Network Models," *IEEE Access*, vol. 11, pp. 124295–124303, 2023.

32. R. Allafi and I. R. Alzahrani, "Enhancing Cyber security in the Internet of Things Environment Using Artificial Orca Algorithm and Ensemble Learning Model," *IEEE Access*, vol. 12, pp. 63282–63291, 2024.

33. Z. Rahman, X. Yi, and I. Khalil, "Block chain-Based AI-Enabled Industry 4.0 CPS Protection Against Advanced Persistent Threat," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6769–6778, Apr. 2023.

34. K. T. Nitesh, A. K. Thirumala, U. F. Mohammed, and M. R. Ahmed, "Network Security Threat Detection: Leveraging Machine Learning Algorithms for Effective Prediction," in *Proc. 12th Int. Conf. Adv. Compute. (ICoAC)*, Aug. 2023, pp. 1–5.

35. V. Gazeau, K. Gupta, and M. K. An, "Advancements of Machine Learning in Malware and Intrusion Detections," in *2024 International Conference on Computer, Information and Telecommunication Systems (CITS)*, IEEE, 2024, pp. 1–7.

36. J. Liu, M. Nogueira, J. Fernandes, and B. Kantarci, "Adversarial Machine Learning: A Multilayer Review of the State-of-the-Art and Challenges for Wireless and Mobile Systems," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 123–159, 2021.

37. S. Poornima and R. Mahalakshmi, "Automated Malware Detection Using Machine Learning and Deep Learning Approaches for Android Applications," *Measurement: Sensors*, vol. 32, p. 100955, 2024.

38. M. Abdullahi *et al.*, "Detecting Cyber security Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *Electronics*, vol. 11, no. 2, p. 198, 2022, doi: 10.3390/electronics11020198.

39. B. S. Sagar, S. Niranjan, K. Nithin, *et al.*, "Providing Cyber Security Using Artificial Intelligence – A Survey," in *Proc. 3rd Int. Conf. Comput. Methodologies and Communication (ICCMC)*, IEEE, 2019, pp. 717–720, doi: 10.1109/ICCMC.2019.8819719.

40. K. D. O. Ofoegbu, O. S. Osundare, C. S. Ike, O. G. Fakeyede, and A. B. Ige, "Real-Time Cyber security Threat Detection Using Machine Learning and Big Data Analytics: A Comprehensive Approach," *Computer Science and IT Research Journal*, vol. 4, pp. 478–501, 2023.

41. V. Jain and A. Mitra, "Real-Time Threat Detection in Cyber security: Leveraging Machine Learning Algorithms for Enhanced Anomaly Detection," in *Machine Intelligence Applications in Cyber-Risk Management*, IGI Global, Hershey, PA, USA, 2025, pp. 315–344.

42. N. Mohamed, V. K. Singh, A. U. Islam, P. Saraswat, D. Sivashankar, and K. Pant, "Role of Machine Learning in Health Care System for the Prediction of Different Diseases," in *Proc. 2022 4th Int. Conf. Emerging Research in Electronics, Computer Science and Technology (ICERECT)*, IEEE, 2022, pp. 1–4.

43. V. D. Ngo, T. C. Vuong, T. Van Luong, and H. Tran, "Machine Learning-Based Intrusion Detection: Feature Selection Versus Feature Extraction," *Cluster Computing*, vol. 27, no. 3, pp. 2365–2379, 2024.

44. S. Siva Shankar, B. T. Hung, P. Chakrabarti, T. Chakrabarti, and G. Parasa, "A Novel Optimization-Based Deep Learning with Artificial Intelligence Approach to Detect Intrusion Attack in Network System," *Education and Information Technologies*, vol. 29, no. 4, pp. 3859–3883, 2024.

45. M. Sulaiman, M. Waseem, A. N. Ali, G. Laouini, and F. S. Alshammari, "Defense Strategies for Epidemic Cyber Security Threats: Modelling and Analysis Using a Machine Learning Approach," *IEEE Access*, 2024.