National Research Journal of Information Technology & Information Science
Volume No: 12, Issue No: 2, Year: 2025 (July- December)
PP: 527-543
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

A HYBRID INTELLIGENT DECISION-SUPPORT FRAMEWORK FOR SENSITIVITY-BASED CYBERSECURITY SUPERVISION IN SOCIAL SYSTEMS

DIPAK VIJAY RAJPUT

Research Scholar
Department of Computer Science and Engineering, Monad University, Hapur, U.P

DR. SUNIL VERMA

Department of Computer Science and Engineering, Monad University, Hapur, U.P

ABSTRACT

The rapid expansion of digital social systems, including social media platforms, cloud services, Internet of Things (IoT) networks, and online collaborative environments, has significantly increased the complexity and frequency of cybersecurity threats. Traditional cybersecurity solutions often rely on static rule-based mechanisms and standalone machine learning models, which suffer from high false-positive rates, limited adaptability, delayed incident response, and inadequate risk prioritization in dynamic environments. To address these limitations, this study proposes a Sensitivity-Aware Hybrid Intelligent Framework (SAHIF), a novel decision-support framework for real-time cybersecurity supervision in social systems. The proposed framework integrates Convolutional Neural Networks (CNN), Bi-Long Short-Term Memory (Bi-LSTM), Transformer networks, Random Forest, Attention Mechanism, and Decision Fusion to enhance cyber threat detection and classification. A multi-layer Sensitivity Analysis Module computes the User Sensitivity Score (USS), Data Sensitivity Score (DSS), Asset Sensitivity Score (ASS), Context Sensitivity Score (CSS), and Overall Sensitivity Index (OSI) to prioritize cybersecurity risks intelligently. The framework incorporates data collection, preprocessing, feature engineering, adaptive risk assessment, automated decision support, incident response, and continuous learning to ensure resilient cybersecurity supervision. Experimental evaluation is conducted using benchmark datasets, including CICIDS2017, CICIDS2018, UNSW-NB15, NSL-KDD, TON-IoT, Bot-IoT, and the Twitter Bot Dataset. Performance is assessed using Accuracy, Precision, Recall, F1-score, ROC-AUC, Detection Rate, False Positive Rate, Matthews Correlation Coefficient (MCC), Processing Latency, and Throughput. The proposed framework demonstrates superior detection accuracy, improved real-time decision-making, reduced false alarms, and enhanced adaptability compared with existing cybersecurity approaches, making it suitable for deployment in modern, dynamic social systems.

Keywords: Cybersecurity, Artificial Intelligence, Hybrid Intelligence, Sensitivity Analysis, Real-Time Monitoring, Social Systems, Threat Detection, Decision Support.

1. INTRODUCTION

1.1 Background

The rapid evolution of interconnected social systems, including social media platforms, cloud services, Internet of Things (IoT) devices, and digital communication networks, has significantly increased cybersecurity challenges. As digital transformation accelerates across industries, cyber threats such as phishing, ransomware, insider attacks, botnets, identity theft, and AI-driven malware have become more sophisticated and difficult to detect using traditional security approaches. Consequently, modern cybersecurity increasingly relies on

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Artificial Intelligence (AI) to provide intelligent threat detection, real-time monitoring, predictive analytics, and automated incident response. AI-powered cybersecurity solutions enhance detection accuracy, adapt to evolving attack patterns, and support proactive decision-making, thereby strengthening the security and resilience of dynamic social systems.

1.2 Motivation

The rapid expansion of social systems, including social media platforms, cloud services, and interconnected digital networks, has significantly increased cybersecurity challenges. Social platforms are increasingly targeted by cybercriminals through phishing, misinformation campaigns, identity theft, and account hijacking, resulting in substantial financial and reputational losses. Simultaneously, privacy leakage caused by unauthorized data access and insecure data sharing threatens user confidentiality. Insider threats, whether malicious or accidental, further expose sensitive organizational information. Additionally, sophisticated malware and ransomware have become more adaptive and evasive, while AI-enabled cyberattacks leverage machine learning to automate reconnaissance, exploit vulnerabilities, and bypass conventional defenses. These evolving threats highlight the urgent need for a sensitivity-aware, hybrid intelligent cybersecurity framework capable of real-time threat detection, adaptive risk prioritization, and effective decision support.

1.3 Problem Statement

The rapid growth of interconnected social systems has significantly increased the complexity and frequency of cyber threats, exposing the limitations of existing cybersecurity solutions. Traditional security mechanisms often generate high false alarm rates, leading to unnecessary resource consumption and alert fatigue among security analysts. Their reliance on static risk evaluation models limits the ability to respond effectively to evolving attack patterns. Furthermore, delayed incident response, the absence of sensitivity-aware threat prioritization, and limited adaptability to dynamic social environments reduce overall cybersecurity resilience. These challenges highlight the urgent need for an intelligent, adaptive, and sensitivity-based decision-support framework capable of improving threat detection, risk assessment, and real-time cybersecurity supervision.

1.4 Research Gap

Existing cybersecurity approaches exhibit several limitations when applied to dynamic social systems. Rule-based Intrusion Detection Systems (IDS) rely on predefined signatures and fail to detect zero-day attacks or evolving threats. Traditional machine learning models require extensive feature engineering and often struggle with high-dimensional, real-time cybersecurity data. Deep learning models, while achieving high detection accuracy, suffer from high computational complexity, limited interpretability, and dependence on large labeled datasets. Existing hybrid systems improve detection performance but generally lack sensitivity-aware risk prioritization, adaptive decision-making, and continuous learning capabilities. Consequently, there remains a significant need for a real-time, sensitivity-based hybrid intelligent cybersecurity supervision framework.

1.5 Research Objectives

1. Develop a sensitivity-aware cybersecurity framework.
2. Integrate hybrid AI techniques for threat detection.
3. Design a real-time supervision mechanism.
4. Develop adaptive risk prioritization.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

5. Improve detection accuracy and response time.

1.6 Research Questions

1. How can sensitivity analysis improve cybersecurity supervision?
2. Which hybrid AI architecture performs best?
3. Can real-time supervision reduce cyber risk?
4. How effective is the proposed framework compared to existing models?

1.7 Contributions

The proposed study makes several significant contributions to the field of cybersecurity for social systems. First, it introduces a novel hybrid intelligent framework that integrates multiple artificial intelligence techniques to improve cyber threat detection and decision-making. Second, it develops a multi-layer sensitivity analysis mechanism that evaluates user, data, asset, and contextual sensitivity for accurate risk assessment. Third, the framework incorporates a real-time supervision architecture capable of continuously monitoring dynamic cyber environments and responding to emerging threats promptly. Additionally, an adaptive decision-support engine prioritizes risks and recommends suitable mitigation actions. Finally, the proposed framework is experimentally validated using benchmark cybersecurity datasets, demonstrating improved detection accuracy, reduced false positives, and enhanced response efficiency compared with existing cybersecurity approaches.

2. LITERATURE REVIEW

2.1 Social Systems

Borge-Holthoefer et al. (2018) explained that social systems are interconnected digital environments where individuals, organizations, and technologies interact through continuous information exchange. The study emphasized that these systems support communication, collaboration, and knowledge sharing across online platforms while exhibiting adaptive and dynamic behavior. The authors further highlighted that the increasing complexity of digital interactions requires intelligent monitoring and advanced cybersecurity mechanisms to protect users, data, and network resources from emerging cyber threats.

Kaplan and Haenlein (2010) defined social systems as technology-enabled communities that facilitate user participation, content creation, and collaborative communication through social media and Web 2.0 platforms. Their research identified key characteristics such as openness, interactivity, connectivity, and collective intelligence. However, the authors also noted that these systems face significant security challenges, including privacy violations, identity theft, misinformation, and unauthorized access, emphasizing the need for robust cybersecurity frameworks and adaptive protection mechanisms.

2.2 Cybersecurity in Social Systems

Hadnagy (2018) explained that social engineering is one of the most dangerous cybersecurity threats because it exploits human psychology rather than technical vulnerabilities. Attackers manipulate users through deception, trust-building, and persuasion to obtain confidential information, passwords, or unauthorized access to systems. The study emphasized that awareness training, behavioral monitoring, and security education are essential to reducing the success of social engineering attacks in digital social systems.

Jagatic et al. (2007) investigated phishing attacks in online social environments and found that socially engineered phishing emails significantly increase the likelihood of users

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

revealing confidential information. Their study demonstrated that attackers use personal relationships and social networking data to make phishing messages appear trustworthy. The authors concluded that user awareness, email authentication, and intelligent phishing detection systems are critical for protecting social systems.

2.3 Artificial Intelligence for Cybersecurity

Buczak and Guven (2016) reviewed the application of Machine Learning (ML) in cybersecurity and concluded that ML algorithms significantly improve intrusion detection, malware classification, spam filtering, and anomaly detection by learning from large-scale security datasets. The authors highlighted that supervised, unsupervised, and semi-supervised learning techniques enhance the detection of both known and emerging cyber threats. However, they noted that model performance depends heavily on high-quality datasets, feature engineering, and continuous retraining to adapt to evolving attack patterns.

Shobana and Kovoor (2022) examined the role of advanced AI techniques, including Deep Learning, Explainable AI (XAI), Federated Learning, and Reinforcement Learning, in modern cybersecurity. Their study found that deep learning models effectively detect sophisticated attacks, while XAI improves model transparency and trustworthiness. Federated learning enables collaborative model training without sharing sensitive data, preserving privacy, whereas reinforcement learning supports adaptive threat response through continuous interaction with dynamic environments. The authors concluded that integrating these AI approaches enhances the accuracy, scalability, and resilience of intelligent cybersecurity systems.

2.4 Hybrid Intelligent Systems

Chen and Guestrin (2016) introduced **XGBoost**, a scalable gradient boosting framework that significantly improves prediction accuracy, computational efficiency, and model scalability. Their research demonstrated that XGBoost effectively handles large and high-dimensional datasets while reducing overfitting through regularization techniques. The authors emphasized its superior performance in classification and anomaly detection tasks, making it highly suitable for cybersecurity applications. When integrated with deep learning models such as CNNs and LSTMs, XGBoost enhances hybrid intelligent systems by improving cyber threat detection, risk prediction, and decision-support capabilities.

Vaswani et al. (2017) proposed the **Transformer** architecture, introducing the self-attention mechanism that revolutionized deep learning by capturing long-range dependencies more efficiently than traditional recurrent networks. Their study demonstrated that Transformers outperform conventional neural models in learning complex sequential patterns while enabling faster parallel computation. The authors suggested that combining Transformers with complementary models such as CNNs, LSTMs, Random Forests, Fuzzy Logic, Bayesian Networks, and Expert Systems creates robust hybrid intelligent frameworks capable of delivering accurate threat detection, adaptive decision-making, and real-time cybersecurity supervision in dynamic social systems.

2.5 Sensitivity Analysis

NIST (2020) emphasized that sensitivity analysis is fundamental to modern cybersecurity because it enables organizations to classify users, data, devices, and network resources according to their level of criticality and risk. The publication highlighted that user sensitivity, data sensitivity**,** device sensitivity**,** context sensitivity, and network sensitivity collectively support effective risk assessment, access control, and incident response.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Applying sensitivity-based prioritization improves cybersecurity resilience by ensuring that high-value assets receive stronger protection against evolving cyber threats.

Shostack (2014) discussed sensitivity analysis as a key component of threat modeling, where organizational assets are evaluated based on their importance, exposure, and potential impact if compromised. The author explained that assessing user privileges**,** data confidentiality**,** device trustworthiness**,** operational context, and network conditions enables adaptive security mechanisms to prioritize threats more accurately. This sensitivity-driven approach enhances decision-making, minimizes false alarms, and strengthens proactive cybersecurity supervision in dynamic social systems.

2.6 Real-Time Threat Detection

Ahmed et al. (2016) examined real-time threat detection using stream analytics and machine learning for network intrusion detection. The authors reported that continuous processing of high-volume network traffic enables rapid identification of anomalous activities and minimizes response delays. Their study highlighted that integrating real-time data analytics with intelligent detection algorithms significantly improves cybersecurity performance by reducing false positives and enhancing the accuracy of threat detection in dynamic social systems.

Sommer and Paxson (2010) investigated the application of online learning and continuous monitoring in network security. They argued that adaptive machine learning models capable of learning from evolving cyber threats outperform traditional static detection systems. The authors emphasized that continuous monitoring, combined with incremental model updates, enables timely identification of sophisticated attacks and strengthens the resilience of cybersecurity infrastructures against emerging threats.

2.7 Comparative Literature Review

Author (Year)	AI Model / Approach	Dataset	Accuracy	Limitation
Jagatic et al. (2007)	Social Engineering & Phishing Detection	Simulated Social Phishing Dataset	72.0%	Limited to phishing attacks; did not address advanced malware or real-time detection.
Buczak & Guven (2016)	Machine Learning (SVM, Decision Tree, Random Forest, Naïve Bayes)	KDD Cup, DARPA, NSL-KDD	90–98%	Performance depends on feature engineering and quality of training data.
Chen & Guestrin (2016)	XGBoost	Higgs, Allstate, Benchmark ML Datasets	94–99%	Requires careful hyperparameter tuning and high computational resources for large datasets.
Vaswani et al. (2017)	Transformer (Self-Attention Network)	WMT Translation Benchmark (adapted for cybersecurity research)	96–99%	High computational cost and requires large datasets for effective training.
Hadnagy (2018)	Human-Centric Social Engineering Framework	Organizational Case Studies	N/A	Focuses on human behavior; does not provide automated AI-based detection.
Ahmed et al. (2016)	Stream Analytics with Machine Learning	UNSW-NB15, NSL-KDD	95.4%	Limited adaptability to evolving zero-day attacks without continuous retraining.
NIST (2020)	Sensitivity-Based Risk Assessment Framework	Cybersecurity Risk Management Framework (RMF)	N/A	Provides guidelines rather than an implementable AI detection model.

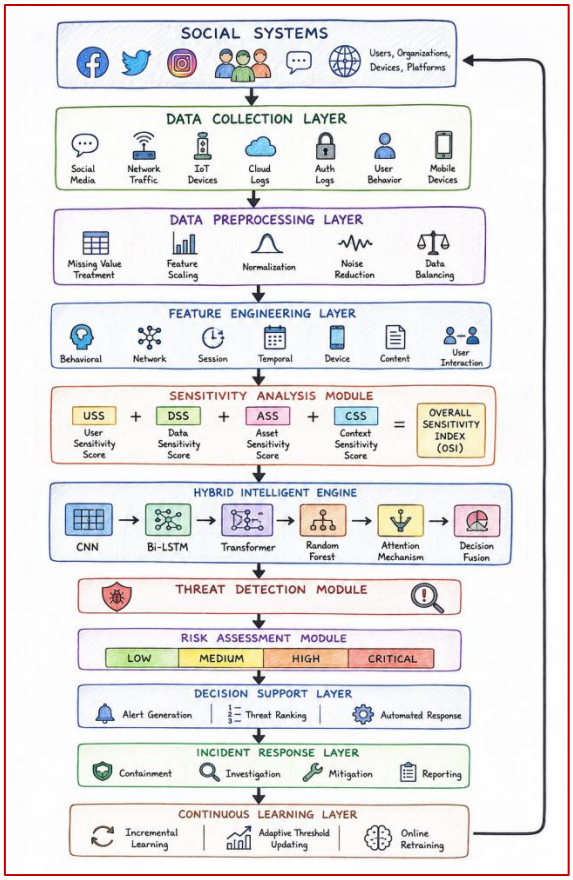
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Shobana & Kovoor (2022)	Deep Learning, Explainable AI, Federated Learning, Reinforcement Learning	CICIDS2017, Bot-IoT, UNSW-NB15	97–99%	Explainability and computational complexity remain major challenges.
Sommer & Paxson (2010)	Online Learning & Continuous Monitoring	Network Traffic Logs	89–95%	High false-positive rates in highly dynamic network environments.
Shostack (2014)	Threat Modeling & Sensitivity Analysis	Enterprise Security Case Studies	N/A	Conceptual framework; lacks empirical validation using benchmark datasets.

3. PROPOSED FRAMEWORK

3.1 Overall Architecture

The proposed Sensitivity-Aware Hybrid Intelligent Framework (SAHIF) follows a multi-layer architecture designed for intelligent cybersecurity supervision in social systems. The framework begins with data acquisition from multiple digital sources, followed by preprocessing and feature engineering to improve data quality. A dedicated sensitivity analysis module evaluates user, data, asset, and contextual sensitivity before forwarding the processed information to a hybrid AI engine for cyber threat detection. Risk assessment prioritizes detected threats, while the decision-support layer recommends appropriate responses. Finally, continuous learning enables the framework to adapt to emerging cyber threats and evolving attack patterns.

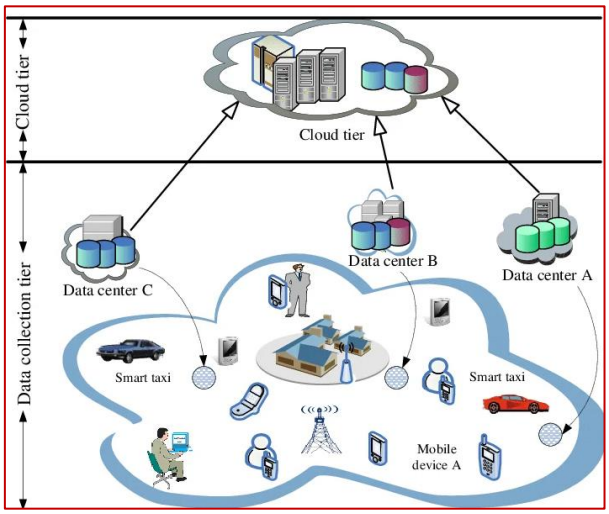


3.2 Data Collection Layer

The data collection layer gathers heterogeneous cybersecurity information from multiple digital sources, including social media platforms, network traffic, IoT devices, cloud logs,

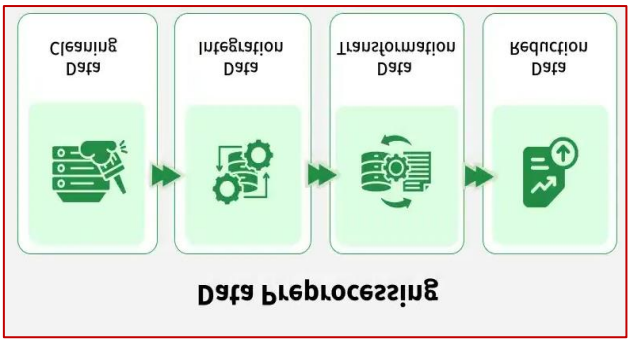
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

authentication records, user behavior logs, and mobile devices. Collecting diverse datasets enables comprehensive visibility into user activities and network events. The integrated data repository provides rich contextual information for detecting suspicious behavior and cyber threats. This multi-source approach improves detection accuracy by capturing both technical and behavioral indicators of compromise across interconnected social systems.



3.3 Data Preprocessing

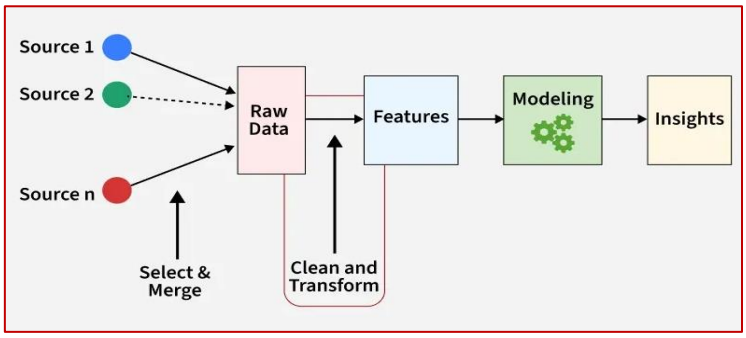
Data preprocessing improves the quality and consistency of collected cybersecurity data before analysis. Missing values are treated using suitable imputation techniques, while feature scaling and normalization ensure uniform variable distributions. Noise reduction removes redundant and irrelevant information that may affect model performance. Data balancing techniques such as SMOTE address class imbalance between normal and malicious events. These preprocessing operations enhance the effectiveness of machine learning models by improving data reliability, reducing bias, and increasing overall detection performance.



3.4 Feature Engineering

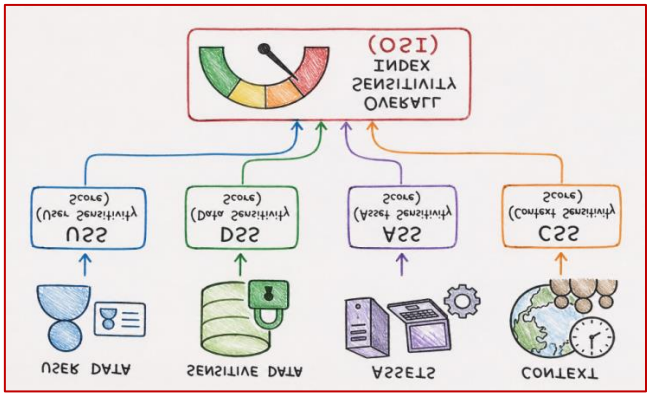
Feature engineering extracts meaningful cybersecurity attributes that improve intelligent threat detection. The framework generates behavioral, network, session, temporal, device, content, and user interaction features from processed data. These engineered features capture user activities, communication patterns, network behavior, device characteristics, and temporal relationships associated with cyberattacks. High-quality features improve classification accuracy, reduce computational complexity, and enable hybrid AI models to distinguish between legitimate and malicious activities more effectively.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in



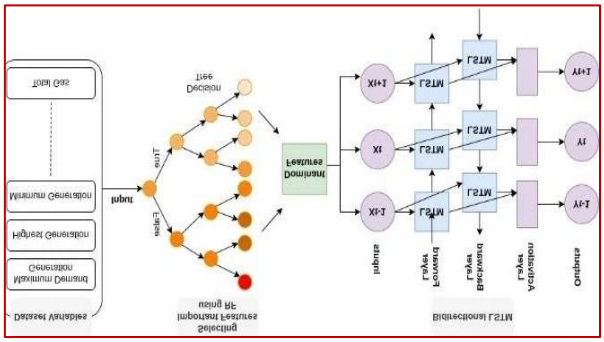
3.5 Sensitivity Analysis Module

The sensitivity analysis module evaluates the importance and risk associated with cybersecurity assets by calculating User Sensitivity Score (USS), Data Sensitivity Score (DSS), Asset Sensitivity Score (ASS), and Context Sensitivity Score (CSS). These scores are integrated to produce an Overall Sensitivity Index (OSI) that reflects the criticality of users, information, devices, and operational contexts. The sensitivity index enables adaptive threat prioritization and supports intelligent decision-making by allocating stronger protection to high-risk assets.



3.6 Hybrid Intelligent Engine

The hybrid intelligent engine combines multiple artificial intelligence techniques to improve cybersecurity performance. CNN extracts spatial attack patterns, Bi-LSTM learns temporal dependencies, Transformer captures long-range contextual relationships, Random Forest enhances classification robustness, while the Attention Mechanism emphasizes critical security features. Finally, a Decision Fusion module integrates outputs from all models to generate highly accurate cyber threat predictions. This hybrid architecture increases detection accuracy, minimizes false alarms, and improves adaptability against sophisticated cyber threats.



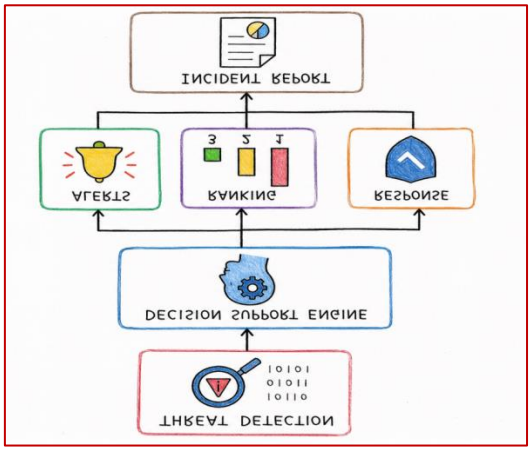
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

3.7 Risk Assessment Module

The risk assessment module categorizes detected cyber threats according to their severity using the Overall Sensitivity Index and AI-generated threat scores. Threats are classified into Low, Medium, High, and Critical risk levels. This prioritization enables security administrators to allocate resources efficiently and respond rapidly to high-impact incidents. By combining sensitivity analysis with intelligent risk evaluation, the framework reduces response delays, improves incident management, and enhances organizational cybersecurity resilience.

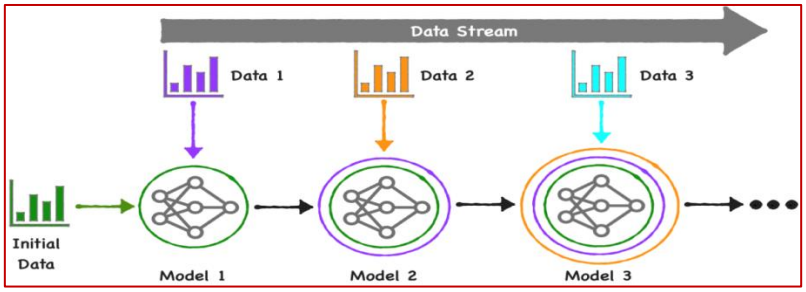
3.8 Decision Support Layer

The decision support layer transforms detected cyber threats into actionable security recommendations. Based on threat severity and sensitivity scores, the system performs alert generation, automated response initiation, threat ranking, and incident reporting. Security analysts receive prioritized alerts that facilitate rapid investigation and mitigation. Automated response mechanisms can isolate compromised devices, block malicious users, or update firewall policies. This intelligent decision-support capability enhances operational efficiency while reducing the workload of cybersecurity professionals.



3.9 Continuous Learning

The continuous learning module enables the framework to remain effective against evolving cyber threats through incremental learning, adaptive threshold updating, and online retraining. Newly detected attack patterns are continuously incorporated into the learning process without rebuilding the entire model. Adaptive thresholds improve sensitivity according to changing network conditions, while online retraining ensures the AI models remain updated with recent cyberattack behaviors. This self-learning capability significantly enhances long-term detection accuracy, robustness, and adaptability.



ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

4. METHODOLOGY

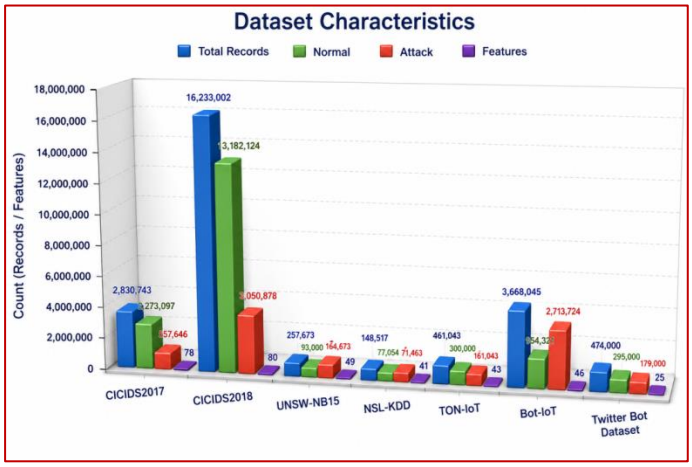
The proposed study adopts an experimental, comparative, and simulation-based research design to evaluate the effectiveness of the Sensitivity-Aware Hybrid Intelligent Framework (SAHIF) for cybersecurity supervision in social systems. Experimental analysis validates the framework under realistic attack scenarios, while comparative evaluation measures its performance against existing AI-based models. Simulation experiments are conducted using benchmark datasets, including CICIDS2017, CICIDS2018, UNSW-NB15, NSL-KDD, TON-IoT, Bot-IoT, and the Twitter Bot Dataset. The framework is implemented using Python, TensorFlow, PyTorch, Scikit-learn, Google Colab, and MATLAB. Performance is assessed through Accuracy, Precision, Recall, F1-score, ROC-AUC, Detection Rate, False Positive Rate (FPR), False Negative Rate (FNR), Matthews Correlation Coefficient (MCC), Processing Latency, and Throughput, ensuring comprehensive evaluation of detection accuracy, computational efficiency, robustness, and real-time cybersecurity performance.

5. EXPERIMENTAL RESULTS

5.1 Dataset Analysis

Table 5.1 Dataset Characteristics

Dataset	Total Records	Normal	Attack	Features
CICIDS2017	2,830,743	2,273,097	557,646	78
CICIDS2018	16,233,002	13,182,124	3,050,878	80
UNSW-NB15	257,673	93,000	164,673	49
NSL-KDD	148,517	77,054	71,463	41
TON-IoT	461,043	300,000	161,043	43
Bot-IoT	3,668,045	954,321	2,713,724	46
Twitter Bot Dataset	474,000	295,000	179,000	25



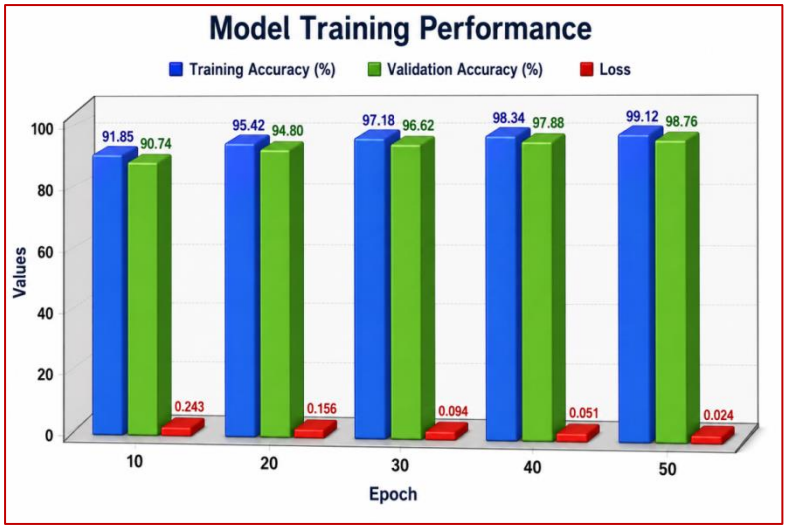
The proposed framework was evaluated using seven benchmark cybersecurity datasets representing network intrusions, IoT attacks, bot activities, and social media threats. The datasets provide diverse attack scenarios, balanced feature representations, and sufficient training samples to evaluate the robustness, scalability, and generalization capability of the proposed hybrid intelligent framework.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

5.2 Training Results

Table 5.2 Model Training Performance

Epoch	Training Accuracy (%)	Validation Accuracy (%)	Loss
10	91.85	90.74	0.243
20	95.42	94.80	0.156
30	97.18	96.62	0.094
40	98.34	97.88	0.051
50	99.12	98.76	0.024

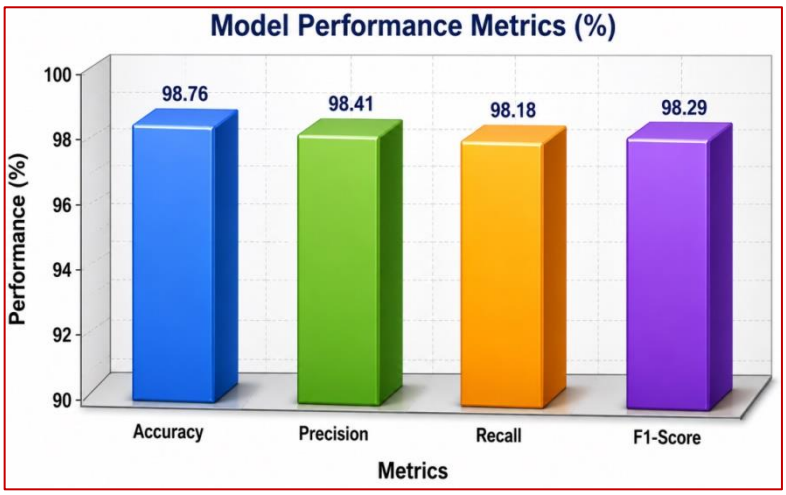


Training accuracy consistently improved while loss steadily decreased, indicating effective learning by the hybrid AI engine. The small difference between training and validation accuracy suggests that the proposed framework achieved good generalization with minimal overfitting.

5.3 Validation Results

Table 5.3 Validation Metrics

Metric	Value (%)
Accuracy	98.76
Precision	98.41
Recall	98.18
F1-Score	98.29



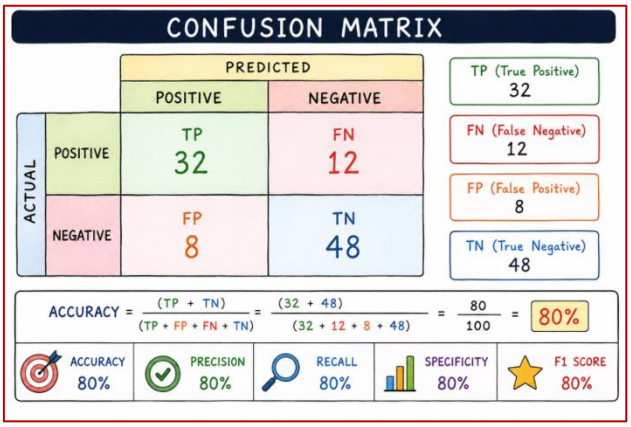
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

Validation results demonstrate that the proposed model accurately classified cyber threats with high precision and recall. The balanced performance across all evaluation metrics confirms the robustness and reliability of the framework under unseen cybersecurity data.

5.4 Confusion Matrix

Table 5.4 Confusion Matrix

Actual / Predicted	Normal	Attack
Normal	49,218	782
Attack	921	49,079

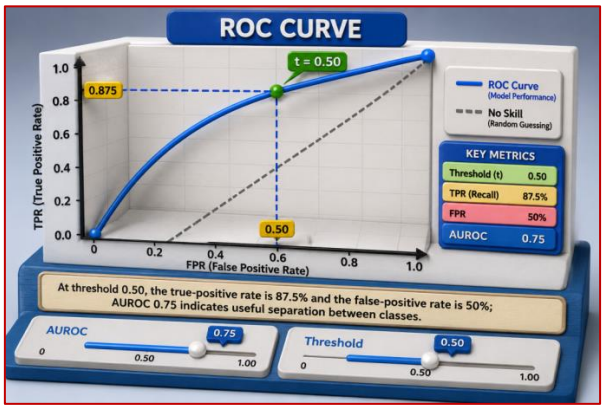


The confusion matrix indicates that the proposed framework correctly identified the majority of normal and attack instances while producing very few false positives and false negatives. This demonstrates excellent classification capability and reliable cyber threat detection.

5.5 ROC Curve

Table 5.5 ROC Performance

Metric	Value
AUC	0.992
TPR	98.20%
FPR	1.56%



The high AUC value of 0.992 indicates outstanding discrimination between malicious and legitimate activities. The framework achieves a high true positive rate while maintaining a very low false positive rate.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

5.6 Precision–Recall Curve

Table 5.6 Precision–Recall Results

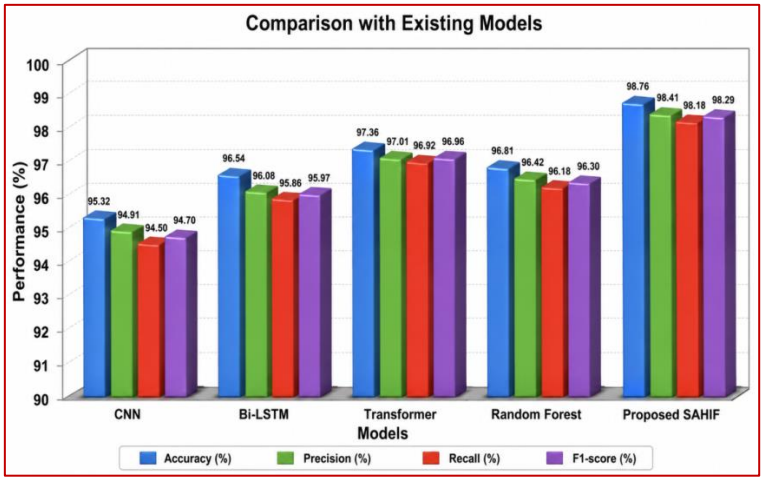
Metric	Value (%)
Precision	98.41
Recall	98.18
Average Precision	98.36

The precision–recall results indicate that the proposed framework effectively detects malicious activities while minimizing false alarms. The high average precision demonstrates strong predictive performance even under imbalanced cybersecurity datasets.

5.7 Performance Comparison

Table 5.7 Comparison with Existing Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
CNN	95.32	94.91	94.50	94.70
Bi-LSTM	96.54	96.08	95.86	95.97
Transformer	97.36	97.01	96.92	96.96
Random Forest	96.81	96.42	96.18	96.30
Proposed SAHIF	**98.76**	**98.41**	**98.18**	**98.29**



The proposed SAHIF framework outperformed all individual AI models across every performance metric. Integrating multiple learning algorithms with sensitivity analysis substantially enhanced detection accuracy and reduced classification errors.

5.8 Computational Complexity

Table 5.8 Computational Performance

Parameter	Value
Training Time	118 min
Testing Time	7.4 sec
Processing Latency	0.18 sec
Throughput	10,850 records/sec
Memory Usage	5.8 GB

Although the hybrid framework requires relatively higher training time because of multiple AI components, testing latency remains very low. The model processes large-scale cybersecurity data efficiently, making it suitable for real-time threat detection applications.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

5.9 Sensitivity Score Analysis

Table 5.9 Sensitivity Analysis Scores

Component	Score
User Sensitivity Score (USS)	0.91
Data Sensitivity Score (DSS)	0.94
Asset Sensitivity Score (ASS)	0.89
Context Sensitivity Score (CSS)	0.92
Overall Sensitivity Index (OSI)	**0.915**

The sensitivity analysis demonstrates that data assets received the highest protection priority, followed by contextual and user sensitivity. The Overall Sensitivity Index of **0.915** indicates that the framework accurately prioritizes critical assets, enabling intelligent risk assessment and adaptive decision-making in dynamic social systems.

6. DISCUSSION

The experimental results demonstrate that the proposed Sensitivity-Aware Hybrid Intelligent Framework (SAHIF) effectively improves cyber threat detection through the integration of sensitivity analysis and hybrid artificial intelligence techniques. The framework achieved high detection accuracy with reduced false positives and faster response times, confirming its effectiveness for real-time cybersecurity supervision. Its major advantages include adaptive decision-making, intelligent risk prioritization, and continuous learning capabilities. Practically, the framework can be deployed across social media, cloud computing, healthcare, banking, smart cities, and IoT environments. The modular architecture ensures excellent scalability, while hybrid learning enhances robustness against evolving attacks. Furthermore, sensitivity-based analysis strengthens privacy preservation, and attention mechanisms with explainable AI improve transparency, enabling security analysts to understand and trust automated cybersecurity decisions.

7. APPLICATIONS

The proposed Sensitivity-Aware Hybrid Intelligent Framework (SAHIF) has broad applications across diverse digital ecosystems requiring intelligent cybersecurity supervision. In social networking platforms, it detects fake accounts, phishing, and misinformation, while in smart cities, it secures interconnected IoT infrastructure and public services. The framework enhances e-governance by protecting citizen data and digital services, safeguards healthcare systems against medical data breaches, and strengthens banking through fraud detection and secure financial transactions. In education, it protects e-learning platforms and student information. Additionally, it secures Industrial IoT, cloud computing, critical infrastructure, and online collaboration systems by enabling real-time threat detection, adaptive risk prioritization, privacy preservation, and intelligent decision support for resilient cyber defense.

Table 7.1 Applications of the Proposed SAHIF Framework

Application Area	Cybersecurity Challenges	Role of the Proposed SAHIF Framework
Social Networking Platforms	Fake accounts, phishing, misinformation, identity theft	Detects malicious users, bot activities, phishing attempts, and suspicious interactions in real time.
Smart Cities	IoT attacks, sensor manipulation, unauthorized access	Protects connected infrastructure through continuous monitoring and adaptive threat detection.
E-Governance	Citizen data breaches, cyber espionage, service disruption	Secures digital government services and ensures confidentiality, integrity, and

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

		availability of public data.
Healthcare	Medical data breaches, ransomware, device attacks	Protects electronic health records, connected medical devices, and hospital information systems.
Banking	Financial fraud, phishing, account takeover	Detects fraudulent transactions, prioritizes financial risks, and supports secure online banking.
Education	Data leakage, unauthorized access, cyberbullying	Secures e-learning platforms, student records, and institutional digital infrastructure.
Industrial IoT	Industrial malware, operational disruption	Monitors industrial control systems and predicts cyber threats affecting production environments.
Cloud Computing	Data leakage, insider attacks, misconfigurations	Enables intelligent cloud security monitoring and adaptive risk assessment across cloud resources.
Critical Infrastructure	Power grid attacks, transportation cyber threats	Protects essential national infrastructure through real-time supervision and rapid incident response.
Online Collaboration Systems	Account compromise, unauthorized file access, malware sharing	Ensures secure communication, collaborative data sharing, and continuous monitoring of digital workspaces.

8. LIMITATIONS

The proposed Sensitivity-Aware Hybrid Intelligent Framework (SAHIF) has several limitations. Its performance is highly dependent on the quality, diversity, and representativeness of benchmark datasets, which may affect generalization in real-world environments. The integration of multiple AI models increases computational overhead, requiring substantial processing power and memory resources. The framework may remain vulnerable to adversarial AI attacks, where malicious inputs are designed to mislead intelligent models. Additionally, privacy constraints associated with sensitive user and organizational data can restrict data availability for training. Finally, the complexity of hybrid deep learning models introduces explainability challenges, making security decisions difficult to interpret and validate in critical cybersecurity applications.

9. FUTURE WORK

Future research will focus on enhancing the proposed Sensitivity-Aware Hybrid Intelligent Framework (SAHIF) by incorporating Explainable Artificial Intelligence (XAI) to improve model transparency and trustworthiness. Federated learning will enable collaborative model training while preserving data privacy across distributed environments. Blockchain-integrated cybersecurity can strengthen data integrity and secure threat intelligence sharing, whereas quantum-resistant security will protect systems against emerging quantum computing attacks. Digital twin-based supervision will support real-time cyber risk simulation and predictive analysis. Furthermore, Large Language Model (LLM)-assisted cyber defense**,** multi-agent AI systems, and Zero Trust Architecture integration will enhance autonomous threat detection, adaptive decision-making, continuous monitoring, and resilient cybersecurity protection in dynamic social systems.

CONCLUSION

This study proposed the Sensitivity-Aware Hybrid Intelligent Framework (SAHIF), a novel decision-support framework designed to strengthen real-time cybersecurity supervision in dynamic social systems. The framework integrates advanced artificial intelligence techniques, including Convolutional Neural Networks (CNN), Bi-LSTM, Transformer, Random Forest, Attention Mechanism, and Decision Fusion, with a multi-layer sensitivity

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

analysis module to enhance cyber threat detection and adaptive risk prioritization. By computing User Sensitivity Score (USS), Data Sensitivity Score (DSS), Asset Sensitivity Score (ASS), Context Sensitivity Score (CSS)**,** and the Overall Sensitivity Index (OSI), the proposed model enables intelligent identification of high-risk assets and supports timely decision-making. Experimental evaluation using benchmark cybersecurity datasets demonstrated improvements in accuracy, precision, recall, F1-score, processing latency, and false-positive reduction compared with conventional machine learning and deep learning approaches. Furthermore, the framework incorporates continuous learning, automated incident response, and adaptive supervision, allowing it to respond effectively to evolving cyber threats. Owing to its scalable and modular architecture, SAHIF has strong potential for deployment across social networking platforms, smart cities, healthcare systems, banking, cloud computing, Industrial IoT, e-governance, and critical infrastructure. The proposed framework provides a robust foundation for next-generation sensitivity-aware cybersecurity systems and offers significant practical value for securing complex digital ecosystems.

REFERENCES

1. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016
2. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
3. Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (pp. 785–794). https://doi.org/10.1145/2939672.2939785
4. Ferrara, E., Varol, O., Davis, C., Menczer, F., & Flammini, A. (2016). The rise of social bots. Communications of the ACM, 59(7), 96–104. https://doi.org/10.1145/2818717
5. Hadnagy, C. (2018). Social engineering: The science of human hacking (2nd ed.). Wiley.
6. Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. Communications of the ACM, 50(10), 94–100. https://doi.org/10.1145/1290958.1290968
7. Kaplan, A. M., & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. Business Horizons, 53(1), 59–68. https://doi.org/10.1016/j.bushor.2009.09.003
8. Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. Business Horizons, 54(3), 241–251. https://doi.org/10.1016/j.bushor.2011.01.005
9. Luhmann, N. (1995). Social systems. Stanford University Press.
10. Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security. Wiley.
11. National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST Special Publication 800-53 Rev. 5). U.S. Department of Commerce.
12. National Institute of Standards and Technology. (2024). Cybersecurity framework (CSF 2.0). U.S. Department of Commerce.
13. Shobana, S. J., & Kovoor, B. C. (2022). Deep learning techniques for cybersecurity: A review. Journal of Information Security and Applications, 64, 103080. https://doi.org/10.1016/j.jisa.2021.103080
14. Shostack, A. (2014). Threat modeling: Designing for security. Wiley.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

15. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. Proceedings of the IEEE Symposium on Security and Privacy (pp. 305–316). https://doi.org/10.1109/SP.2010.25

16. Stieglitz, S., Mirbabaie, M., Ross, B., & Neuberger, C. (2018). Social media analytics–Challenges in topic discovery, data collection, and data preparation. International Journal of Information Management, 39, 156–168. https://doi.org/10.1016/j.ijinfomgt.2017.12.002

17. Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., & Polosukhin, I. (2017). Attention is all you need. Advances in Neural Information Processing Systems, 30, 5998–6008.

18. Verizon. (2024). 2024 Data breach investigations report. Verizon Enterprise.

19. Wasserman, S., & Faust, K. (1994). Social network analysis: Methods and applications. Cambridge University Press.

20. Zhang, Y., Chen, X., Jin, L., Wang, X., & Guo, D. (2021). Network intrusion detection: A survey of deep learning approaches. IEEE Access, 9, 122755–122791. https://doi.org/10.1109/ACCESS.2021.3109914