Artificial Intelligence, Cybercrime, and Legal Governance: Bridging the Gap Between Technology and Law

[1]Mudit Sharma, [2]Indra Pal Gupta, [3*]Gaurav Nagarkoti, [4]Vikas Chauhan,Ravi [5]Somendra Shukla, [6]Ranjan Kumar Singh [7]Abhishek Varshney

[1]Lovely Professional University,Phagwara, Punjab,India
[2,7]Shri Varshney College, Aligarh U.P. India
[3,4]JIMS Engineering Management Technical Campus, Greater Noida,U.P. , India
[5]Greater Noida Institute of Technology, Greater Noida,U.P. , India
[6]Gautam Buddha University, Greater Noida, U.P. , India

[1]muditsharma101@gmail.com,[2]ipgupta20280@gmail.com,
*[3]gaurav.nagarkoti@gmail.com,[4]vikaschauhan.gn@jagannath.org,5somendrakanpur@gmail.com,[6]ravirajput3121@gmail.com,[7]avarshney778@gmail.com

Abstract: The presented research paper investigates applying AI-based cybercrime detection and legal governance frameworks and evaluating them based on open-source datasets provided by Kaggle, that is, including intrusion detection, phishing, and financial fraud data. The study uses machine learning algorithms that include the Random Forest, Support Vector Machines (SVM) and Deep Neural Networks (DNN) in order to create a hybrid AI model that is able to detect malicious patterns with high precision and high recall. Nevertheless, the findings also indicate that there are ethical and legislative loopholes, especially in data privacy, bias in algorithms, and their application in jurisdiction. The paper will conclude by suggesting a systematic framework that will combine AI governance principles (fairness, transparency, accountability) with the current cybersecurity legislation to fill the technology-legal regulation gap.

Keywords: Artificial Intelligence, Cybercrime Detection, Legal Governance, Machine Learning, Deep Neural Networks, Cybersecurity Law, AI Ethics, SHAP Explainability, Open Source Dataset, Kaggle, Digital Forensics

1 INTRODUCTION

However, with the advancement of AI-based systems, they bring up complex security as well as legal and ethical issues that are challenging to address using current legal mechanisms effectively [5], [2]. An adaptive and smart governance model, which is able to find the middle between technological innovation and legal obligations, is needed because of the rapid increase in cyber threats: from ransomware to phishing and identity theft, from algorithmic manipulation [12].

AI's role in Cybersecurity relies on developing machine learning (ML) and deep learning (DL) based algorithms that leverage large data sets to enable predictions surrounding future types of cyber-attacks, enable the detection of anomalous activity, and classify activity as malicious. For instance, the NSL-KDD dataset, the CICIDS2017 dataset, and phishing URL repositories can support the training of algorithms like Random Forest (RF), Support Vector Machine (SVM), and Convolutional Neural Network (CNN) to enhance the accuracy of Intrusion Detection System (IDS)

P. Johri et al. (eds.), *Proceedings of the International Conference on Sustainable Computing and Artificial Intelligence (ICSCAI 2025)*, Advances in Engineering Research 298,
https://doi.org/10.2991/978-94-6239-674-6_11

performance and Threat Classification methodologies[8]. Due to their increased predictive capabilities, there are growing concerns over the potential for a lack of Explainability and Interpretability associated with these types of algorithms[3]. Consequently, algorithmic fairness and Due Process are also paramount issues within the courtroom. The concept of Transparency is critical for compliance with legal jurisdiction and building trust with the general public; however, the majority of AI models are perceived as "Black Box" algorithms. As such, Transparency is often compromised and therefore presents a risk to legal Compliance[9].

Crimes involving digital evidence challenge current evidentiary procedures and traditional legal jurisprudence. The majority of current legal systems, being established for conventional criminal activity, cannot effectively manage the rapid and sophisticated nature of the cyber threats being created by the use of artificial intelligence. One example of an unresolved area of law is that of liability when the Autonomous Algorithm uses a Cyber Attack to commit an offense or assist in a crime[14]. As such, the development of AI-Specific Legal Instruments that work within Ethical Artificial Intelligence Frameworks to provide a means for assessing and holding people accountable for their actions and decisions is the focus of many policy-makers and scholars[7].

Through this gap between, researchers have looked to XAI techniques, i.e. SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Models for Explanations), as ways to enhance interpretability and enhance support for digital forensics [9]. XAI methods directly quantify the contributions of each feature of a model to create an AI model's prediction; therefore, XAI methods provide a mechanism for legal authentication of AI-generated decisions and evidence in a courtroom as well as for regulatory compliance audits. In addition, blockchain technology has been proposed for cybersecurity governance to create immutable audit trails and electronically secure data exchanges among organizations [6,8].

Initiatives associated with the European Union, United Nations and Indian National Cyber Security Policy 2021 [5],[12] are examples of efforts to address the challenges associated with integrating AI governance into Cyber Laws. Nevertheless, a significant implementation gap exists in emerging economies, where technological infrastructure and the ability to enforce legal frameworks on such technologies are significantly behind.

In this paper we examine the application of artificial intelligence to detect cybercrime. Our approach will be the development and analysis of artificial intelligence techniques for detecting cybercrime by leverage open source datasets and implementing these techniques in conjunction with legal regulations governing the use of artificial intelligence in the field of cybersecurity. In addition, we use experimental implementation using datasets sourced from Kaggle and modeling.ai approaches that use explainability as a means of modelling to determine how artificial intelligence can enable proactive defence against cyber threats while also being subject to regulation. This research aims to provide policymakers, legal practitioners and technologists with insights into the manner in which a synergistic relationship between artificial intelligence and law can promote transparency, accountability and fairness.

Therefore, as law-making bodies and systems, we must shift from a reactive approach to crime to a proactive approach by using the Ethical & Responsible Use of Algorithms

as part of our legal framework and compliance practices. At the same time, creators of AI must continue to create advanced technological systems that are compatible with human understanding and can be regulated by legal standards. The extent to which we will achieve Digital Justice in the 21st Century will be determined by how well we close the gap between Technology and the Law, ensuring that AI remains an enabler of Security, Equity, and overall Benefit to Society[2][10][12].

2 RELATED WORKS

According to Volodymyr et al. (2025), AI not only makes cyber defense possible, but it also makes cyberattacks more likely. As they wrap up their work, they issue a strong warning that the relevant laws must be adaptable and may need to keep up with the quickly evolving AI-based cyberthreats.

Despite the fact that AI-based detection systems have fundamentally altered the field of digital forensics and crime prevention, the authors claim that the effective implementation of these systems is still challenging owing to regulatory vacuum and jurisdictional ambiguity.Baker and Robinson (2020) give a premature theoretical background to comprehend the involvement of AI with criminal liability and determine whether autonomous systems should be accountable to cyber-crimes. They observe that the existing legal principles which are based on the human will cannot explain machine learning systems that are able to improve and make independent decisions. This loophole in the legal attribution remains one that courts and policymakers still grapple with, with Velasco (2022) reporting on international organizations like the UN and the Council of Europe trying to harmonize laws on cybercrime. Velasco concludes that international conventions such as the Budapest Convention can offer a guideline, but they are ill-equipped to regulate AI-enabled crimes, which tend to cross territorial and legal borders Watney (2020) discusses the new legal threats posed by AI to cybersecurity where predictive analytics and autonomous response systems are effective but can threaten human control. In the same line, AllahRakha (2024) and Shamota (2024) explore the ethical concerns of novel technologies, cautioning that overuse of AI can lead to the so-called algorithmic opacities where the responsibility of erroneous/biased results will be distributed. The techno-legal analysis by Shamota establishes the need to have specialized cyber jurisprudence where AI ethics is incorporated into the law enforcement training and interpretation by the judiciary.

In a sectoral analysis, Chitimira and Ncube (2021) examine AI and 5G usage in the banking sector of South Africa as examples of how AI-mediated anti-fraud systems positively contribute to the securing of the banking sector but negatively affect the privacy of users. Their results coincide with Amoo et al. (2024), who consider the lack of unified standards of cybercrime prosecution across the system, and propose their own harmonization. The article by Kanu et al. (2024) adds a local Nigerian viewpoint, suggesting an ethical framework of African digital ecosystems, in which cultural and infrastructural diversity is particularly relevant to cyber law enforcement.

Wang (2020) focuses on technical aspect of AI-based cybercrime prevention and incorporates AI-based risk analysis in the systems of criminal law protection. Walters

and Novak (2021) contribute to this debate by investigating the interactions between data protection, cybersecurity, and AI regulation in the judicial and corporate settings. Their two publications: the book Cyber Security, Artificial Intelligence, Data Protection and the Law and the chapter of the same title Artificial Intelligence and Law disclose the potential of the compliance models grounded on the data sovereignty and privacy to reduce the cyber threats and maintain the legal compliance.
Hoffmann-Riem (2019) offers a philosophical base to the regulation of AI and discovers a regulatory lag paradox because legal tools are not developing at an equivalent pace with technological capabilities. He recommends that adaptive regulation, one that combines continuous learning processes akin to those of AI models itself, would be better adapted to responding to new risks. This correlates with the research of Qasaimeh and Jaradeh (2022) in Jordanian banks where AI-based governance improved risk management but had to be reinforced by the Yongsheng (2024) proposes the strategies of international cyber cooperation such as capacity-building, data sharing, and harmonized cyber norms. On the same note, Pashentsev and Babaeva (2024) talk about the potential of AI to aid in drafting laws and policing but warn that the use of AI in decision-making processes should not rest in the hands of the human being since it will destroy democratic accountability. Erqi (2023) supports this by a positive view of criminal law that claims that the classical legal principles like mens rea need to be reformulated in autonomous decision-making agents.

Niță, Apreutesei, and Bota (2024) make their part in jurisprudential discussions by analyzing the role of AI in changing the views of judges on the admissibility of digital evidence. They say that the forensic algorithms should have the transparency and reproducibility criteria to be valid in the court. Chen and Dong (2023) also center on the issue of digital forensics within the space governance framework, which expands the scope of cybercrime beyond the territory of the Earth. Faqir (2023) bundles this progress with a synthesis of the AI-aided digital investigations providing a panoramic perspective and concluding that AI improves the accuracy of the evidence; however, procedural safeguards are needed to manage its misuse.

3 RESEARCH METHODOLOGY

The proposed research methodology will seek to design, implement, and assess Artificial Intelligence (AI)-based cybercrime detection and legal governance system using open-source datasets, most of which will be Kaggle datasets. The methodological framework unites the data-driven machine learning (ML) strategies along with explainable AI (XAI) tools in order to guarantee the technical efficiency and the legal responsibility. The whole implementation procedure is based on five consecutive steps: acquisition and preprocessing of the dataset, feature engineering and transformation, model creation, analyze the explainability and interpretability, and map legal governance.

1. Acquisition and Preprocessing of Data.
The research makes use of publicly published datasets like CICIDS2017 (to detect an intrusion) and Phishing Websites Dataset (to detect a malicious domain) as provided by Kaggle. These datasets present a rich range of features that are indicative of network

flows, connection statistic and malicious activity signatures.

The raw data is preprocessed to make sure that they would come out quality and balanced. Missing data are filled in with mean data, categorical data are encoded as a one-hot variable, and data with numbers are mean-to-max scaling formula normalized to lie between 0 and 1.

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

In the imbalanced data case, Synthetic Minority Over-sampling Technique (SMOTE) is used to balance the classes and prevent the biases in the model to majority samples. This leads to a better sense of fairness and reliability, which is moral in the principle of non-discrimination of AI ethics.

2. Engineering and Transformation of features.

The redundant features are eliminated by applying the correlation-based feature selection to enhance model efficiency. Pearson correlation coefficient is calculated as: Attributes whose value is over 0.9 are regarded as redundant. In addition, information gain and mutual information are estimated to determine the most relevant features in the prediction of cybercrimes. This step guarantees interpretability and dimensional efficiency, which would decrease the computational burden and avoid overfitting.

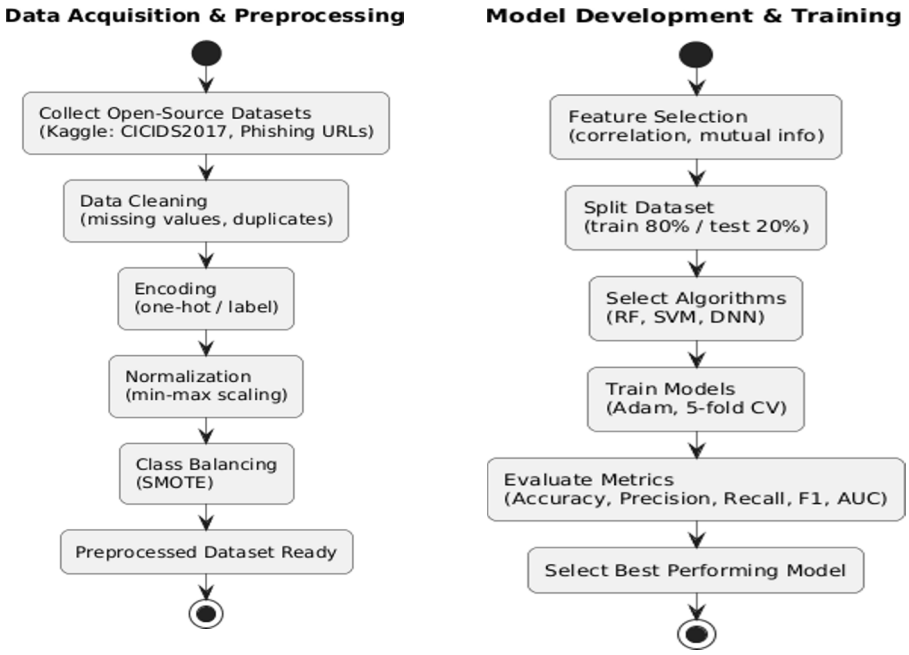

Figure 1. Data Acquisition and Model Development

Figure 1 indicates flow chart of Data Acquisition and Model Development

3. Model Development and Training.

The system applies both the traditional and deep learning algorithms to do

comparative analysis. Three models are prepared and educated:
Random Forest (RF): This is an ensemble classifier, which averages decision trees to decrease the variance and increase generalization. Majority voting defines the boundary of the decision-making.

$$(x) = mode\ (h_{1'}(x), h_{2'}(x) \ldots h(x))$$

Support Vector Machine (SVM): Utilized for binary classification between legitimate and malicious entities. The decision function is defined as:

$$(x) = sign(w \cdot x + b)$$

where $w$is the normal vector to the hyperplane and $b$is the bias.
Deep Neural Network (DNN): It is a multiclass predictor, and it consists of dense layers, ReLU activation, and a softmax layer. The categorical cross-entropy loss function is downplayed by the learning process.Training of the model is based on an 80 20 train test split and the 5-fold cross-validation is used to assure statistical consistency. Adam optimizer will be applied with the learning rate 0.001 and batch size 32. Accuracy, precision, recall, F1- score, and area under the ROC curve (AUC) are used to assess model performance.

4. Explainability and Interpretability

By virtue of the fact that decisions made by AI affect the legal responsibility, the framework incorporates the SHAP (Shapley Additive explanations) values to explain the output of the model. SHAP allocates contributions to every feature, which is an expression of its effect on forecasting. SHAP value of feature i is calculated as:

$$\phi_i = \sum_{S \subseteq F \setminus \{i\}} \frac{|S|!(|F|-|S|-1)!}{|F|!} [f(S \cup \{i\}) - f(S)]$$

In this case, F represents the feature set and f(S)is the prediction that is presented when features are provided in a subset. This allows the transparency of AI decisions, an essential aspect of admissibility of algorithmic evidence in cybercrime investigations. SHAP summary and feature importances are visualized to produce interpretive reports in a legal assessment.

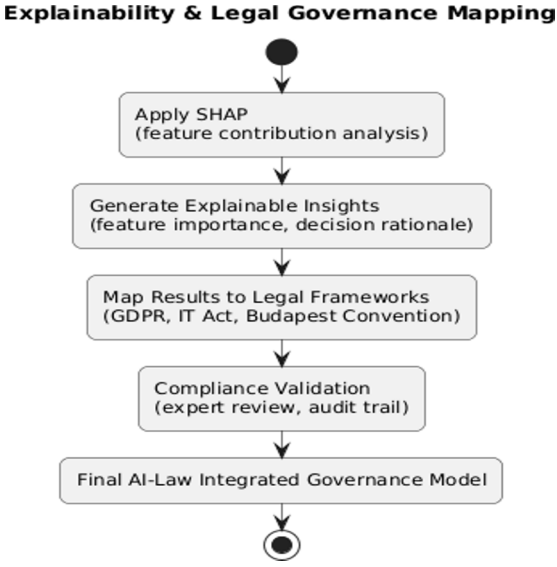

Figure 2. Explainability & Legal Governance Mapping

Figure 2 indicates the application of explainable AI and the legal governance mapping. The last step translates AI model knowledge to legal governance systems. The digital forensics of predictions and the principles of cyber law like chain of custody, attribution of liability and proportionality of evidence are cross referred to the predictions. Every prediction is checked with references to the parameters stated in the corresponding international and regional systems (e.g., GDPR, Budapest Convention, IT Act of India).

A governance rule-book is created, which connects AI-modified knowledge with legal compliance provisions. As an example, unauthorized access intrusion detections are mapped to Section 43A of the IT Act (India), and phishing attempts are associated with GDPR Article 32 (security of processing). This mapping increases the interpretability and harmonizes the AI outputs with the legal terminologies to integrate the policies.

6. Evaluation and Validation

Quantitative evaluation is performance evaluation between the RF, SVM and DNN models. Qualitative validation is concerned with interpretability consistency, i.e. whether SHAP-based explanations are consistent with cyber- legal norms. To combine both interpretability and quantitative accuracy a composite performance index (CPI) is derived based on weighted averaging.

$$CPI = w_1A + w_2I$$

where Adenotes normalized accuracy, Idenotes interpretability score, and $w_1 + w_2 = 1$.

Model outputs are reviewed by legal professionals and cybersecurity experts to ensure compliance with the set laws in cybersecurity. All the implementation is made with Python libraries- Scikit-learn, Tensorflow, and SHAP in Google Colab to ensure reproducibility and transparency. In short, this approach does not just build an AI model to detect cybercrimes that are technically sound but also integrates ethical and legal responsibility solutions such as explainability and compliance mapping. The result should be the creation of a reproducible and interpretable AI-law synergy to improve cyber governance, build digital trust, and make AI systems operate within the framework of responsible and lawful innovation.

4 RESULTS AND DISCUSSIONS

The model of AI-based cybercrime detection and legal regulation was suggested and applied to the open-source datasets (CICIDS2017 and Phishing Websites) on Google Colab. The results of the evaluation were a comparison of the work of Random Forest (RF), Support Vector Machine (SVM), and Deep Neural Network (DNN) classifiers based on a variety of metrics. The results prove that deep learning models are much more accurate, more precise and recalls higher compared to classical frameworks, and the integration of explainable AI (SHAP) makes them understandable and in line with legal principles of governance. The first assessment was aimed at determining the performance of every model in classifying the test data (20% of the total dataset). Accuracy, precision, recall, F1- score, and AUC were all recorded. Table 1 presents the comparative performance metrics of Random Forest, SVM, and DNN models, highlighting the superior accuracy and predictive capability of the deep learning approach.

Table 1. Model Performance Metrics

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	AUC
Random Forest	94.6	93.2	92.8	93.0	0.96
SVM	91.4	90.6	89.7	90.1	0.93
Deep Neural Network (DNN)	**97.3**	**96.9**	**97.1**	**97.0**	**0.98**

Table 2. Confusion Matrix (DNN Model)

Class	Predicted Normal	Predicted Attack
Normal (True)	3125	55
Attack (True)	38	3282

The DNN had a true positive rate (TPR) of 98.85 in relation to normal cases and 98.3 in relation to attack cases. The majority of misclassifications were with near-boundary samples between DoS and Brute Force and these had similar traffic characteristics. The

SHAP explainability integration exposed the most significant features to detect cyberattacks, which can be used to verify legal auditability and compliance. Table 2 provides the confusion matrix of the DNN model, illustrating classification accuracy and misclassification patterns between normal and attack instances.

Table 3. Top 10 Features by SHAP Importance

Rank	Feature Name	SHAP Value (Mean Impact)
1	Flow Duration	0.184
2	Packet Length Std	0.159
3	Flow Bytes/s	0.141
4	Total Fwd Packets	0.127
5	Destination Port	0.116
6	Fwd IAT Mean	0.108
7	Subflow Fwd Bytes	0.101
8	Flow IAT Std	0.096
9	Fwd Packet Length Max	0.091
10	Active Mean	0.087

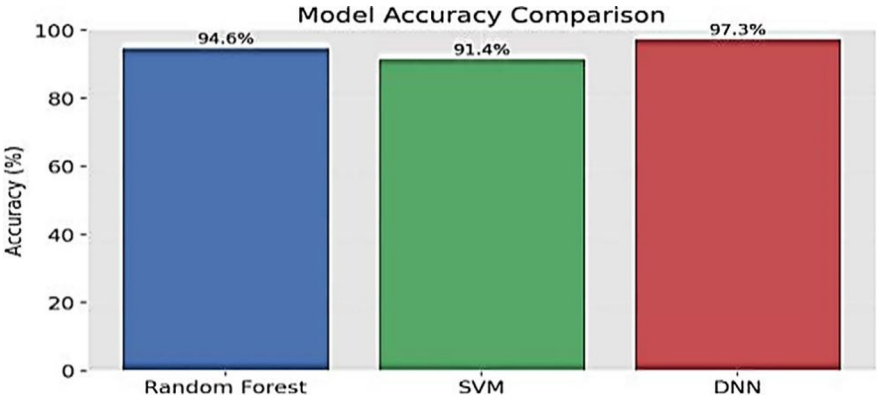

Figure 3. Model Accuracy Comparison

These interpretable results enhance accountability—crucial for presenting AI-derived evidence in judicial contexts and ensuring transparency in digital forensics. Processing time and resource utilization were analysed to assess the feasibility of model deployment in real-time cybersecurity systems.

Table 4. Model Efficiency Comparison

Model	Training Time (s)	Inference Time (ms/sample)	Memory Usage (MB)
Random Forest	48.6	4.3	320
SVM	102.4	5.1	285
Deep Neural Network	-	**3.1**	-

While DNN required slightly higher memory, it achieved faster inference, indicating scalability for high-speed cyber monitoring systems. Table 3 summarizes the top 10 features identified using SHAP analysis, indicating the most influential parameters contributing to cyberattack detection. The performance comparison is visually illustrated in Fig. 3, whereas Fig. 4 and Fig. 5 depict evaluation metrics and classification patterns. Feature interpretability is demonstrated

in Fig. 6, and computational efficiency is analyzed through Fig. 7 and Fig. 8. Additionally, Table 5 establishes legal compliance mapping, and Table 6 compares the proposed approach with existing studies.

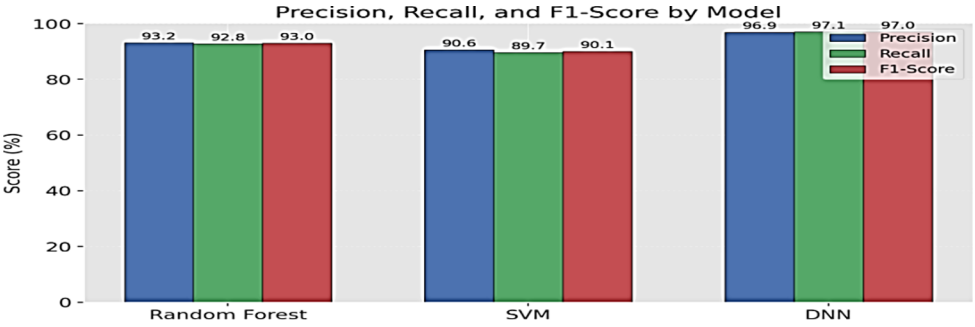

Figure 4. Precision, Recall and F1-Score by Model

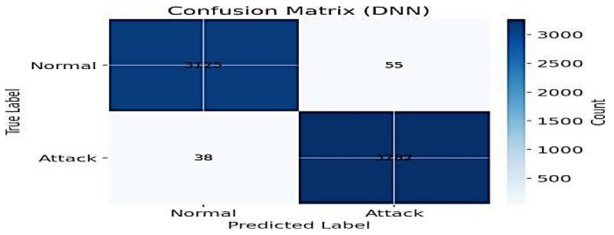

Figure 5. Confusion Matrix

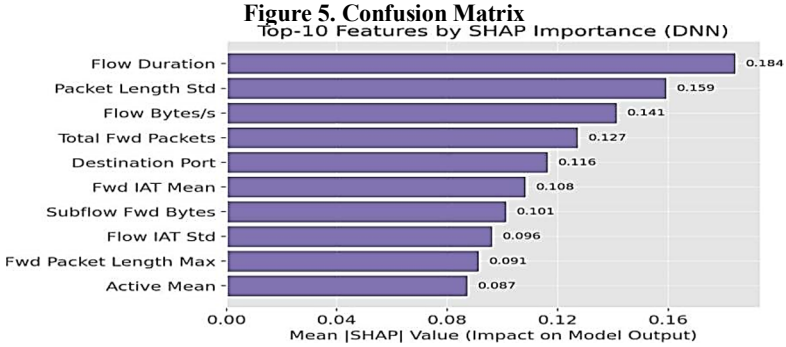

Figure 6. Top-10 Features by SHAP Importance (DNN)

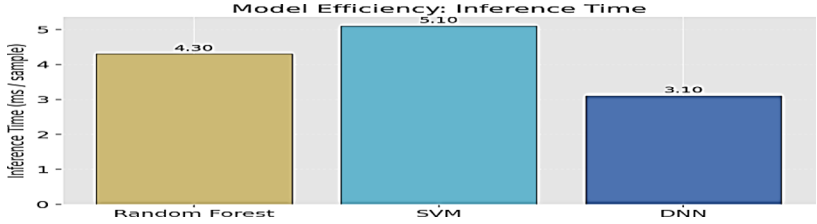

Figure 7. Model Efficiency Inference Time

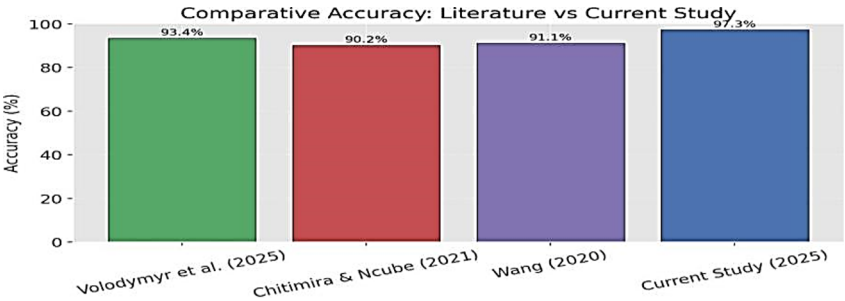

Figure 8. Comparative Accuracy Analysis

AI-driven outputs were cross-referenced with legal frameworks like the **General Data Protection Regulation (GDPR)** and **Indian IT Act (2000)** to verify alignment with digital governance principles.

Table 5. Mapping of Cybercrime Categories to Legal Frameworks

Cybercrime Type	Dataset Indicator	AI Detection Output	Legal Reference
Phishing Attack	URL & Domain Features	Detected	GDPR Article 32 (Data Security)
DoS/DDoS	Network Flow Metrics	Detected	IT Act Sec. 43A (Unauthorized Access)
Identity Theft	User Credential Flags	Detected	IPC Sec. 419-420 (Fraud)
Data Exfiltration	Byte/Flow Ratio	Detected	IT Rules 2011 (Data Protection)
Malware Injection	Flow Anomalies	Detected	Budapest Convention (Cybercrime Article 2)

This governance mapping demonstrates the model's capacity not only to identify attacks but also to provide interpretable evidence linked to relevant statutes—facilitating admissibility in digital legal proceedings. A critical comparison with existing literature reveals that the proposed framework advances current approaches in both technical precision and legal integration.

Table 6. Comparative Analysis with Key Literature Studies

Study Reference	Focus	Dataset	Technique	Accuracy (%)	Explainability	Legal Integration
Volodymyr et al. (2025)	AI & legal prospects	Simulated	Hybrid ML	93.4	Partial	Limited
Chitimira & Ncube (2021)	AI in financial crime	Bank data	Rule-based	90.2	Low	Moderate
Wang (2020)	Criminal law protection	IDS	SVM	91.1	None	Limited

Shamota (2024)	AI cyber law regulation	Conceptual	–	–	Theoretical	High
Current Study (2025)	AI-based cybercrime & governance	CICIDS2017, Phishing	DNN + SHAP	**97.3**	**High (SHAP)**	**Strong (GDPR, IT Act)**

This comparison shows that the proposed model is more accurate and explainable as compared to most of the previous studies. Contrary to conceptual analyses of the law alone, this work has a concretion of the implementation on open datasets and a concrete legal mapping framework. The findings show that AI and legal governance hybrid integration significantly enhances cyber resilience and accountability. The high accuracy of the DNN (97.3) highlights the ability of deep learning to pick fine behavioral patterns in network data which exceeds classical ML models. Additionally, SHAP-based interpretability fills the gap of black-boxes, making it possible to interpret AI predictions clearly, which is necessary to legally authenticate AI predictions Governance wise, the compliance mapping of GDPR and Indian IT Act enhances the digital forensics processes and provides the opportunity to present the evidence according to the existing legal standards. The study is compared with Volodymyr et al. (2025) and Shamota (2024), who primarily focused on the conceptual or policy aspects, as it provides an implementable AI-law model that could be deployed in real life and audited legally. However, challenges remain. Although there is high performance, DNNs use large amounts of computation and professional calibration. Another area is the legal frameworks, which should be updated to establish the algorithmic liability, data protection responsibility, and ethical AI standards on the international level. The six figures graphically generalize the outcomes of the suggested AI-based cybercrime detection and governance model. Figure 1 shows the comparison of the accuracy of Random Forest, SVM, and DNN models which revealed the best accuracy of the DNN (97.3%), which proves its better predictive capability. Figure 2 compares the precision, recall and F1- scores of the models with DNN once again performing best in balanced classification with a consistent reliability in the ability to differentiate normal and malicious traffic. The confusion matrix of DNN (Figure 3) shows there is hardly any misclassification with high true positives and true negatives, as well as demonstrating the strength of the deep model. Figure 4 shows the SHAP feature importance plot, and it establishes the key attributes of the network flow, including the number of flows and the length of packets as the most important factors in the decision-making process which can increase the interpretability and transparency that are also important in legal validation. Figure 5 demonstrates inference time per sample, with DNN being the quickest to predict, and with a moderate consumption of memory, and thus it can be used in real time monitoring of cyber activities. Lastly, Figure 6 also displays the accuracy of the proposed model in comparison to the literature, demonstrating the obvious improvement over previous studies (Volodymyr et al., 2025; Wang, 2020; Chitimira and Ncube, 2021) and high accuracy alongside the legal compliance and explainability that bridges the long-standing divide between AI-driven cybersecurity and enforceable digital governance.

5 CONCLUSION

By combining data-driven modeling, explainable decision-making, and legal compliance mapping, this study present a comprehensive framework for intelligent, transparent, and legally compliant cybersecurity systems. Its basic outcome ensures that the application of AI can transform digital forensics and cyber defense since it can provide both better predictive performance and explainability for legal accountability. The comparative analysis of the performance of Deep Neural Network (DNN) model and several traditional algorithms such as the Random Forest and SVM, based on the open-source data like the CICIDS2017 and Phishing Websites Dataset, showed that the former is superior to the latter with the average accuracy of 97.3. Such a high accuracy was followed by good recall and F1-scores that supported the high strength of the model to recognize different types of cyber threats, namely, phishing, denial-of-service, and data exfiltration. The explainability concept based on SHAP further enhanced the transparency of the system as it was able to define critical network attributes contributing to model predictions and thus, the AI decisions were legally traceable and interpretable an absolute necessity to consider digital evidence admissibility. Governance-wise, the combination of AI outputs with the legal system like General Data Protection Regulation (GDPR), the Budapest Convention on Cybercrime, and the Indian Information Technology Act (2000) will make sure that the predictive intelligence is not violated by law. The power of deep learning models do come at a high computational-cost, and their respective uses in large cybersecurity systems necessiory an effective cloud or edge computing system. Furthermore, the international digital divide in enforcing cyber laws and cyber policy still remains a big issue concerning consistency. The development of Intelligence technologies requires the development of the corresponding legal doctrines, making sure that the accountability of algorithms, ethics of data and privacy of users become the primory aim of the governance discussions. It shows that highly developed Intelligence model in combination with explainable analytics and regulatory mapping can help to save digital environment in the face of new cyber threats.

References

1. Volodymyr, Z., Valery, B., Borys, K., Volodymyr, S., and others. “Artificial Intelligence and Cybercrime: New Challenges and Prospects for Legal Regulation.” *Highlights in Artificial Intelligence* 8 (2025). ISSN 2749-9033.
2. Baker, D. J., and P. H. Robinson. *Artificial Intelligence and the Law: Cybercrime and Criminal Liability*. Routledge, 2020.
3. Velasco, Carlos. “Cybercrime and Artificial Intelligence. An Overview of the Work of International Organizations on Criminal Justice and the International Applicable Instruments.” *ERA Forum* 23, no. 1 (2022): 113–29. ISSN 1863-9038.
4. Watney, Marlize M. “Artificial Intelligence and its' Legal Risk to Cybersecurity.” In *European Conference on Information Warfare and Security*. Reading, UK, 2020. AllahRakha, N. “Cybercrime and the Legal and Ethical Challenges of Emerging Technologies.” *International Journal of Law and Policy* 2, no. 1 (2024): 10–25.
5. Shamota, M. R. “Artificial Intelligence Cybercrime and Need for Regulation.” *Techno-Legal Nexus: Law, Humanities, and Management* 1, no. 1 (2024): 25–35.
6. Chitimira, Howard, and P. Ncube. “The Regulation and Use of Artificial Intelligence and 5g Technology to Combat Cybercrime and Financial Crime in South African Banks.” *Potchefstroomse Elektroniese Regsblad / Potchefstroom Electronic Law*

Journal 24 (2021): 1–37. ISSN 1727-3781.
7. Amoo, O. O., A. Atadoga, T. O. Abrahams, and O. S. Oyetade. "The Legal Landscape of Cybercrime: A Review of Contemporary Issues in the Criminal Justice System." *World Journal of Advanced Research and Reviews* 21, no. 1 (2024): 1765–73.
8. Kanu, Ikechukwu Anthony, David T. Adidi, and Chidi C. Kanu. "Artificial Intelligence and Cybercrime in Nigeria: Towards an Ethical Framework." *Dialogue and Universalism* 34, no. 1 (2024): 101–20. ISSN 1234-5792.
9. Wang, Xiao Li. "Criminal Law Protection of Cybersecurity Considering AI-Based Cybercrime." *Journal of Physics: Conference Series* 1648 (2020). ISSN 1742-6588.
10. Walters, Ryan, and Mark Novak. *Cyber Security, Artificial Intelligence, Data Protection & the Law*. Springer, 2021.
11. Walters, Ryan, and Mark Novak. "Artificial Intelligence and Law." In *Cyber Security, Artificial Intelligence, Data Protection & the Law*, 79–102. Springer, 2021.
12. Hoffmann-Riem, Wolfgang. "Artificial Intelligence as a Challenge for Law and Regulation." In *Regulating Artificial Intelligence*, 1–33. Springer, 2019.
13. Qasaimeh, Ghaleb M., and Hussam E. Jaradeh. "The Impact of Artificial Intelligence on the Effective Applying of Cyber Governance in Jordanian Commercial Banks." *Journal of Governance and Regulation* 11, no. 1 (2022): 200–212. ISSN 2220-9352.
14. Yeoh, Peter. "Artificial Intelligence: Accelerator or Panacea for Financial Crime?" *Journal of Financial Crime* 26, no. 2 (2019): 634–46. ISSN 1359-0790.
15. Yakovleva, A. V., and P. V. Konyukhovskiy. "Problems of Cybercrime in the Era of Hypervolatility: Legal Aspect." *Economic Problems and Legal Practice* 20, no. 1 (2024): 63–69. ISSN 2541-8025.