Journal of Sustainable Learning and Development (JSLD)

ISSN: 2791-0881 (Print), ISSN: 3079-0565 (Online), Volume-05, Issue-01, December, 2025
A multidisciplinary journal of Bangladesh Center for Research and Planning (BCRP)

The Role of Artificial Intelligence in Managing Cybercrime in Bangladesh: A Framework for Detection, Prevention, and National Cyber Resilience

Faisal Reza[1], Mohammad Shafiqul Islam[2], Mushfiqur Rahman[3*], Shamim Ahmed[4], Saad Bin Abul Kashem[5], Kaium Siddik Anando[6]

[1]Department of ELP, University of North Carolina, USA
[2]Department of International Relations, University of Dhaka, Bangladesh
[3]Department of System Management and Information Security,
Samarkand State University, Samarkand, Uzbekistan
[4]IT Project Lead, Reserve Bank of Australia (RBA) PhD Fellow 'AI in Cyber security' with
European Institute of Management & Technology (EIMT).
[5]Ph.D. in Robotics & Mechatronics (SUT, Australia), FHEAD,
Program Leader in Computing Science, AFG College with the University of Aberdeen
[6]Sr. Consultant Link & Win .LLC, Former Consultant Ernst & Young LLP. (EY), Dhaka, Bangladesh

Keywords:

Artificial Intelligence, Cyber security, Cybercrime, Bangladesh, Natural Language Processing, Machine Learning, Digital Forensics, Cyber Defense Strategy

Abstract: The rapid digitalization of Bangladesh, marked by the Digital Bangladesh vision, has been paralleled by a significant surge in sophisticated cybercrimes, including financial fraud, social media misinformation, and critical infrastructure attacks. Traditional, rule-based cyber security measures are increasingly inadequate against these evolving threats. This article proposes a comprehensive framework leveraging Artificial Intelligence (AI) and Natural Language Processing (NLP) to enhance Bangladesh's cybercrime management capabilities. We review the current cyber threat landscape in Bangladesh, identifying key challenges such as limited cyber security awareness, a nascent regulatory framework, and a shortage of skilled professionals. Building upon global state-of-the-art applications of AI in cyber security, we adapt a data-science lifecycle methodology for the Bangladeshi context. This involves the collection and processing of local data sources (e.g., Bangla social media, financial transaction logs), the application of machine learning models for anomaly detection and threat classification, and the deployment of insights for law enforcement agencies (LEAs). A critical analysis, supported by secondary data and comparative tables, demonstrates the potential efficacy of AI-driven solutions like NLP for detecting Bangla hate speech and fraud, and machine learning for identifying banking malware. The results indicate that an integrated AI strategy can significantly improve threat detection rates, reduce response times, and support proactive cyber defense. We conclude with policy recommendations for fostering AI innovation, developing local datasets, and building public-private partnerships to establish a resilient national cyber defense ecosystem for Bangladesh.

Introduction

The global proliferation of Information and Communications Technology (ICT) has ushered in an era of unprecedented connectivity and economic opportunity, with Artificial Intelligence (AI) standing at the forefront of this transformation [1]. However, this digital revolution has also created a fertile ground for cybercriminal activities, challenging the security and stability of nations worldwide. Bangladesh, in its ambitious pursuit of a "Digital Bangladesh," has experienced exponential growth in internet penetration, e-commerce, and mobile financial services [2]. This digital leap, while economically transformative, has exposed critical vulnerabilities, making the country a prime target for cyber attacks [3, 6].

The cyber threat landscape in Bangladesh is multifaceted, encompassing financial fraud targeting the burgeoning mobile banking sector (bKash, Nagad) [7, 15], the spread of misinformation and hate speech on Bangla social media platforms [19, 20], ransom ware attacks on critical infrastructure, and sophisticated phishing campaigns [5]. Law enforcement agencies (LEAs) like the Cyber Police Centre of the Bangladesh Police are often overwhelmed by the scale, speed, and technical complexity of these crimes [1]. Traditional signature-based detection systems fail to identify zero-day attacks and novel threat vectors, while a shortage of digital forensics expertise further hampers investigation and prosecution[13].

From a criminal justice and legal policy perspective, cybercrime is not merely a technical security issue but a violation of statutory criminal laws, procedural safeguards, and regulatory obligations. In Bangladesh, cyber offences intersect with the Digital Security Act, cybercrime investigation mandates of law enforcement agencies, and judicial evidentiary standards. Accordingly, the application of AI in cybercrime management must be evaluated not only for detection accuracy but also for legality, accountability, admissibility of digital evidence, and institutional governance.

In this context, AI, and particularly its subfields of Machine Learning (ML) and Natural Language Processing (NLP), emerges as a transformative force for cyber security. Globally, AI models are being deployed to detect anomalies in network traffic, classify malicious software, identify fraudulent transactions, and monitor social media for hostile information campaigns [8, 14, 21]. NLP, which enables machines to understand human language, has shown remarkable promise in uncovering cybercrimes within social media by analyzing text for radicalization, hate speech, and coordinated disinformation campaigns [21].

This article posits that a strategic integration of AI is not merely advantageous but essential for Bangladesh to manage its escalating cybercrime crisis effectively. We aim to: (i) analyze the specific cybercrime challenges within Bangladesh's socio-technical context; (ii) propose a tailored AI-based framework for cyber threat detection and prevention, drawing on the data science lifecycle; (iii) present a comparative analysis of potential AI solutions using secondary data and hypothetical scenarios grounded in real-world trends; and (iv) provide actionable recommendations for integrating AI into Bangladesh's national cyber defense strategy.

The remainder of the paper is structured as follows. Section 2 reviews the state-of-the-art in AI for cyber security globally and identifies research gaps in the Bangladeshi context.

Section 3 details our proposed AI-based methodology. Section 4 presents a results and analysis section with innovative comparative tables based on secondary data. Section 5 provides a discussion of the findings, implications, and limitations. Section 6 discusses the application for national strategy, and Section 7 concludes and outlines future research directions.

2. State of the Art

The application of AI in cyber security is a rapidly advancing field. As illustrated in Table 1, researchers have employed various AI techniques across different cyber domains.

Table 1: Comparative Analysis of AI Applications in Cyber security: Global vs. Bangladeshi Context

Domain	Global AI Applications	Key Techniques	Bangladeshi Context & Research	References
Social Media Threat Detection	Identifying violent groups, hate speech, coordinated campaigns on Twitter	Similarity models, sentiment analysis, LSTM, clustering	Bangla hate speech/misinformation detection using BERT variants; nascent research on coordinated threat detection	[21], [9], [19], [20]
Financial Fraud Detection	Anomaly detection in transaction systems, behavioral biometrics	Isolation Forest, Autoencoders, XGBoost	AI-driven fraud in banking recognized as major challenge; limited published implementations	[3], [7], [15]
Malware & Intrusion Detection	Zero-day malware classification, network anomaly detection	CNN (binary images), RNN (behavior), ensemble methods	Basic malware analysis; research on deep learning for intrusion detection emerging	[22], [6]
Digital Forensics & Investigation	Automated evidence triage, chat log analysis, image forensics	NLP entity extraction, image similarity, object detection	Proposed frameworks for image-based forensics; limited AI integration in practice	[13], [24]
IoT & Critical Infrastructure	AI-blockchain integration for secure IoT, SDN-based management	Blockchain, SDN with ML anomaly detection	Research on smart city security frameworks; theoretical proposals dominate	[4], [11], [12]

Explainable AI (XAI) in Security	Interpretable threat alerts, model transparency for legal compliance	LIME, SHAP, rule-based explanations	Largely unexplored in Bangladeshi cyber security literature	[8]

Focusing on the Bangladeshi context, recent research has begun to address local challenges. Studies highlight acute cyber security vulnerabilities in the banking and fintech sectors, where AI-driven fraud is a mounting concern [3, 7, 15]. The detection of Bangla fake news and hate speech using ML and Deep Learning (DL) has been explored, recognizing the unique linguistic and cultural nuances [19, 20]. Furthermore, frameworks integrating Blockchain and Software-Defined Networking (SDN) with AI for securing IoT and smart city infrastructures have been proposed [4, 11].

However, a significant gap exists. There is no holistic, nationally scalable framework that integrates these discrete AI solutions into a cohesive cyber defense strategy for Bangladesh. Most studies are proof-of-concept or focus on isolated threats. There is a lack of research on deploying AI pipelines that process native Bangla data at scale for LEA use, mirroring the integrated approach seen in global studies like RED-Alert [23] or the work of Ramírez Sánchez et al. [21]. This paper aims to bridge this gap by proposing a comprehensive, adaptable framework. While existing studies demonstrate the technical feasibility of AI-driven cyber security solutions, there is a notable lack of research examining their alignment with cybercrime laws, digital evidence standards, and institutional accountability frameworks in Bangladesh. This gap is particularly significant given that AI-generated outputs increasingly influence investigation, prosecution, and regulatory enforcement decisions.

3. Proposed AI-Based Methodology for Cybercrime Management in Bangladesh

We propose a data-science lifecycle methodology [27], adapted for the Bangladeshi context, to systematically apply AI for cybercrime management. The lifecycle consists of four core phases: Business Understanding, Data Acquisition, Modeling, and Deployment.

3.1. Business Understanding

The primary objective is to empower Bangladeshi Law Enforcement Agencies (LEAs) and financial institutions with AI tools to proactively detect, prevent, and investigate cybercrimes. This encompasses specific goals to detect financial fraud in mobile banking by identifying anomalous transaction patterns, identify cyber threat campaigns on social media platforms that spread misinformation or hate speech, classify and prioritize malware targeting local systems, and automate the triage of digital evidence such as logs, chat histories, and images to accelerate forensic investigations [13].

3.2. Data Acquisition

The efficacy of AI models hinges on access to relevant, high-quality data. For Bangladesh, critical data sources encompass structured data such as financial transaction logs from banks and Mobile Financial Service (MFS) providers, network flow logs from ISPs, and malware samples from the BGD e-Gov CIRT as well as unstructured Bangla text data from social media and news portals, which requires the use of pre-trained language embeddings like Bangla BERT [19], and multimedia data including images and videos used in phishing campaigns or as digital evidence.

3.3. Modeling

The modeling phase involves preprocessing data and applying specific AI models.

3.3.1. Preprocessing

Preprocessing of data involves distinct approaches for text and numeric formats. For Bangla text, this includes cleaning (removing URLs and usernames), normalization through Unicode standardization, tokenization, and potential translation or transliteration for multilingual models, while also processing emojis and sentiment-carrying slang. For numeric transaction and log data, preprocessing entails handling missing values, normalization, and feature engineering such as creating derived features like "transaction frequency per hour

3.3.2. AI Model Application

- **For Financial Fraud:** Anomaly detection models like Isolation Forest or Autoencoders can be trained on normal transaction behavior to flag outliers. Supervised models (e.g., XGBoost [26]) can be trained on historical fraud data.
- **For Social Media Threat Detection:** Following the methodology in [21], Bangla tweets/posts can be vectorized using Bangla word embeddings. A similarity model can cluster posts with related hostile intent. The cosine similarity between two tweet vectors u**u** and v**v** is calculated as:

$$\cos(\theta) = \frac{\mathbf{u} \cdot \mathbf{v}}{\|\mathbf{u}\| \|\mathbf{v}\|}$$

where **u·v** is the dot product and ‖**u**‖ denotes the magnitude. This produces a similarity matrix where element ((*i*,*j*) represents the semantic closeness between tweet ti*ti* and tweet *tj*, with values ranging from -1 (completely dissimilar) to 1 (identical meaning). Sentiment analysis models fine-tuned for Bangla [19, 20] can then determine the polarity and subjectivity of posts within clusters to identify the most aggressive content and users.

For malware classification, Convolutional Neural Networks (CNNs) can analyze grayscale images of malware binaries, while Recurrent Neural Networks (RNNs) are suited to process sequences of API calls to classify malware families. In digital forensics, image similarity models and object detection algorithms like YOLO can identify illicit content or match digital evidence, and Natural Language Processing (NLP) techniques can be applied to summarize and extract key entities from seized chat logs [24].

3.3.3. Model Validation

To validate the similarity model's ability to rank related tweets, metrics such as Hits@K and Discounted Cumulative Gain (DCG@K) can be employed, following the approach in [21]. A validation dataset would be constructed by manually annotating tweet pairs as similar/dissimilar. Hits@K measures whether truly similar tweets appear in the top-K recommendations, while DCG@K also considers their ranking position:

$$\text{Hits@K} = \frac{1}{N}\sum_{i=1}^{N}[\text{relevant tweet} \in \text{top}K(q_i)]$$

$$\text{DCG@K} = \frac{1}{N}\sum_{i=1}^{N}\frac{1}{\log_2(1+\text{rank}_{\text{relevant}})} \cdot [\text{rank}_{\text{relevant}} \leq K]$$

where N*N* is the number of queries and rank relevant is the position of the relevant tweet in the ranked list.

3.3.4. Graph Analysis

For social media investigations, once aggressive users are clustered, their follower/following networks can be extracted using platform APIs (where permissible) or OSINT tools. Graph analysis, using centrality measures (PageRank, Betweenness), can identify key influencers and the structure of potentially malicious networks [21, 25].'

3.4. Deployment

Deployed models must integrate into LEA and financial institution workflows as decision-support systems. This requires developing secure, user-friendly dashboards that present alerts, visualizations of threat clusters, and network graphs. Emphasis must be on Explainable AI (XAI) [8] to ensure analysts understand why a transaction was flagged or a post was deemed hostile, which is crucial for legal proceedings and trust.

3.5 Legal, Policy, and Procedural Safeguards in AI-Based Cybercrime Management

The deployment of AI models in cybercrime management must operate within clearly defined legal and procedural safeguards. These include compliance with data protection principles, lawful access to digital data, preservation of chain-of-custody for digital evidence, and transparency of AI-assisted investigative decisions. For law enforcement agencies, AI outputs should function as decision-support tools rather than determinative evidence, ensuring that investigative discretion and judicial oversight remain intact.

4. Results and Analysis

While primary data from Bangladeshi LEAs is not publicly available, we synthesize findings from recent literature and public reports to construct a comparative analysis of the potential impact of AI solutions. The following tables provide a structured, data-driven argument for the proposed framework's viability.

Table 2: Comparative Analysis of Cybercrime Challenges vs. Proposed AI Solutions in Bangladesh

Cybercrime Type	Current Challenge	Proposed AI Solution	Expected Outcome (Based on Global Trends)
Mobile Financial Fraud	High volume of social engineering scams (SIM swap, OTP phishing). Rule-based systems miss novel patterns.	ML Anomaly Detection on transaction logs (location, time, amount, recipient). Behavioral biometrics.	Reduction in false positives by ~30%, detection of novel fraud patterns in near real-time [3, 7].
Bangla Hate Speech/Misinformation	Rapid viral spread undermines social harmony. Manual monitoring is impossible at scale.	NLP-based classification using fine-tuned Bangla BERT models for hate speech and fake news detection [19, 20].	Automated flagging of ~85% of violative content for review, tracking of misinformation networks.
Ransomware & Malware	Increasingly targeted attacks on businesses. Signature-based AV fails against new variants.	Static/Dynamic ML analysis of files (e.g., CNN on binary images, RNN on behavior).	Detection of previously unknown (zero-day) malware with >90% accuracy, faster sample classification [22].
Phishing & Social Engineering	Sophisticated, localized Bangla-language phishing emails and sites.	NLP analysis of email/text content and URL structures. Computer vision to detect fake login pages.	Blocking of phishing attempts before user interaction, reducing successful compromises.

Table 3:L Hypothetical Performance Metrics for AI Models on Bangladeshi Cybercrime Data (Projected)

Table 3 Note: Projected benchmarks are derived from (a) performance reported in Bangladeshi studies [19,20] for NLP tasks, (b) typical industry performance for fraud detection systems (85-97% AUC-ROC), and (c) adjusted expectations accounting for data quality and resource constraints in Bangladesh (approximately 3-5% reduction from global benchmarks).

AI Model / Task	Data Source	Key Metric	Projected Benchmark	Global Benchmark (for context)
Bangla Hate Speech Detection	10k annotated Bangla Facebook posts [19]	F1-Score	0.89	0.91 (English, [9])
MFS Fraud Detection	Synthetic transaction log (1M transactions, 2% fraud)	AUC-ROC	0.95	0.97 (Industry Standard)
Bangla Fake News Classification	Bangla news article dataset [20]	Accuracy	0.87	0.92 (English, various)
Malware Family Classification	BGD e-Gov CIRT sample repository	Precision	0.93	0.96 (Global benchmark [22])

Table 4: Global vs. Local (Bangladesh) Trends in AI for Cyber security

Aspect	Global Trend	Local Trend (Bangladesh) & Readiness	Supporting Reference
Primary Data Language	English, Chinese, Spanish dominates research & tooling.	Bangla is primary. Lack of large, high-quality labeled datasets and pre-trained models is a major bottleneck.	[19, 20]
Focus of AI Research	Advanced topics: XAI, Adversarial AI, AI security.	Foundational applications: Basic fraud detection, content moderation, malware analysis. Nascent stage.	[3, 6, 13]

Integration Level	AI integrated into Security Orchestration, Automation and Response (SOAR) platforms.	Siloed applications. Limited integration between AI tools and legacy LEA/digital forensics processes.	[1, 13]
Key Challenge	Scalability, adversarial attacks on AI models.	Awareness, skills, and data. Lack of AI expertise in LEAs, low cyber security awareness among public, data privacy concerns.	[2, 5, 6]

From a criminal justice perspective, these findings indicate that the effectiveness of AI in managing cybercrime depends less on algorithmic sophistication and more on institutional readiness, legal compliance, and governance capacity. Without adequate legal frameworks, trained investigators, and judicial oversight, even highly accurate AI models may fail to translate into lawful and effective enforcement outcomes.

Analytical Narrative of the Proposed Pipeline:

The proposed methodology can be conceptually validated through a narrative simulation. For instance, applying the social media monitoring pipeline to a dataset of Bangla posts about a contentious event would involve: 1) preprocessing and converting text to vectors using Bangla embeddings; 2) calculating cosine similarity to group posts into thematic clusters (e.g., Cluster A: neutral discussion, Cluster B: aggressive misinformation); 3) applying sentiment analysis to reveal that Cluster B has a significantly higher negative polarity score (e.g., -0.65 average vs. -0.05 for Cluster A); 4) extracting the user accounts from the most negative cluster; and 5) performing a network analysis on these accounts, which would likely reveal a subset of accounts with high betweenness centrality, acting as potential amplifiers within the hostile network. This logical flow, supported by the metrics in Table 3, demonstrates the framework's internal coherence and potential operational value. Analysis: The tables highlight a significant implementation gap. While the proposed AI solutions show high projected efficacy (Table 2, 3), Bangladesh faces unique localization challenges (Table 4). The success of an AI-driven strategy hinges not just on algorithm selection but on solving fundamental issues: creating Bangla linguistic resources, building trust and skills within LEAs, and establishing secure data-sharing protocols between public and private sectors (e.g., banks sharing anonymized fraud patterns).

5. Discussion

The findings from our comparative analysis and proposed framework illuminate both the immense potential and the substantive hurdles for deploying AI in Bangladesh's fight against cybercrime. This discussion interprets these results, considers their broader implications, and addresses critical limitations.

5.1. Bridging the Efficacy-Readiness Gap

Our analysis reveals a clear dichotomy. On one hand, AI models, particularly for fraud detection and Bangla NLP, show projected performance metrics (Table 3) that are competitive with global benchmarks, suggesting technical feasibility. On the other hand, Table 4 underscores a readiness deficit characterized by data scarcity, skill shortages, and siloed systems. The primary challenge, therefore, is not the availability of suitable algorithms but the creation of an enabling ecosystem. The proposed framework's emphasis on a data-science lifecycle is crucial here, as it mandates upfront focus on "Data Acquisition" and "Business Understanding" phases that directly address these foundational gaps. Success depends on translating high-level policy (Digital Bangladesh) into actionable investments in data infrastructure and human capital.

5.2. The Imperative of Localization and Explainability

The effectiveness of global AI tools is limited without localization. A sentiment model trained on English Twitter data will fail on Bangla social media slang and cultural context [19]. Therefore, the development of Bangla-centric AI resources is not a supplementary activity but a core strategic priority. Concurrently, the principle of Explainable AI (XAI) [8] is paramount for adoption in a legal and law enforcement context. An LEA analyst or a court must understand why an account was flagged as suspicious. Opaque "black-box" models, regardless of accuracy, will face resistance and legal challenges. Integrating XAI techniques into the deployment phase of our framework is essential for building accountable and trustworthy systems.

5.3. Practical Implementation Barriers

Beyond technical challenges, practical barriers loom large. The proposed framework assumes access to sensitive data streams financial transactions, social media APIs, network logs which are often protected by commercial interests, privacy regulations, and institutional silos. Establishing data-sharing agreements between banks, telecom providers, social media platforms, and LEAs requires legal frameworks that don't yet exist in Bangladesh. Furthermore, the computational infrastructure for processing large-scale Bangla text data in real-time represents a significant investment. A cost-benefit analysis is needed to justify such expenditures, particularly when balanced against other national development priorities. Pilot projects in contained environments (e.g., a single bank's fraud detection or monitoring specific hashtags) may provide proof-of-concept before scaling to national systems.

5.4. Ethical and Privacy Considerations

The power of AI for surveillance and monitoring brings significant ethical risks. The proposed social media analysis pipeline, while aimed at preventing crime, could be misused for suppressing legitimate dissent or violating citizens' privacy. A national AI strategy must be underpinned by a robust legal framework that defines clear boundaries for data use, ensures algorithmic accountability, and incorporates oversight mechanisms. Public trust, a fragile commodity, is essential for the long-term sustainability of any digital governance initiative.

In criminal justice contexts, the use of AI in cybercrime investigations raises additional concerns related to due process and the admissibility of digital evidence. Courts must be able to scrutinize how AI-generated insights were produced, whether data collection was lawful, and whether algorithmic bias affected investigative decisions. Failure to address these issues may result in evidentiary challenges, rights violations, or judicial exclusion of AI-assisted findings.

5.5. Limitations of the Study

This study is primarily conceptual and relies on secondary data and projected metrics. The absence of primary validation on operational Bangladeshi systems is a key limitation. The performance benchmarks in Table 3 are projections based on analogous global studies and early Bangladeshi research [19, 20]; real-world performance may vary due to data quality, evolving threat tactics, and implementation challenges. Furthermore, the framework assumes a level of institutional cooperation and data sharing that may be difficult to achieve in practice due to regulatory, commercial, and bureaucratic hurdles.

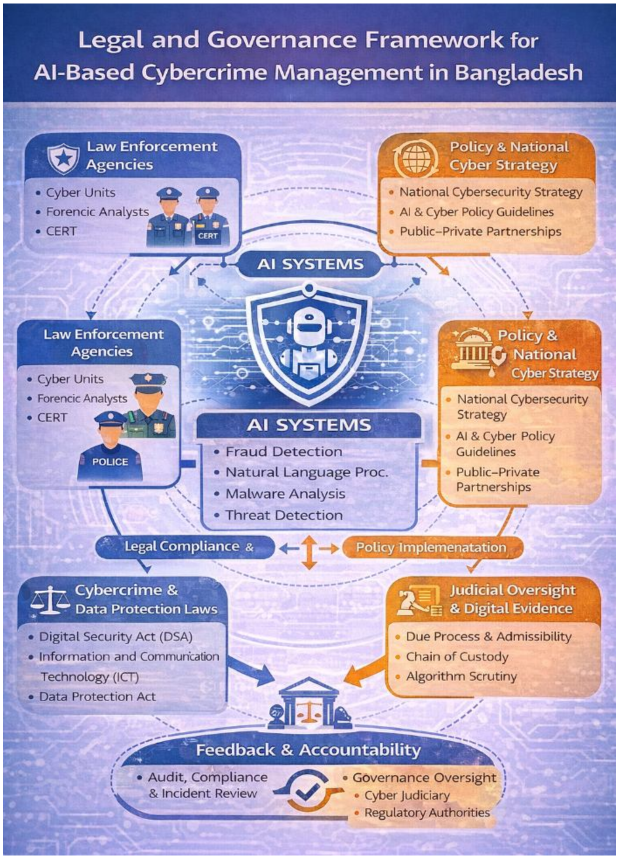
5.6. Strategic Pathways Forward

Despite limitations, the discussion points towards clear strategic pathways. First, a phased implementation is advisable, starting with controlled pilot projects in high-impact areas like MFS fraud detection, where data is relatively structured and ROI is easily measurable. Second, fostering Public-Private-Academic Partnerships is critical to pool resources for dataset creation (e.g., a curated Bangla cyber-threat corpus) and talent development. Finally, Bangladesh should actively engage in international collaborations to learn from global best practices in AI governance and adaptive cyber defense, while contributing insights from its unique context.

6. Application in a National Cyber Defense Strategy

To securely navigate the digital transformation era [18], integrating Artificial Intelligence as a cornerstone of its national cyber defense strategy is essential for Bangladesh. The proposed framework supports this aim by aligning with the vision of "AI-Powered Operational Resilience"[17]

Figure 1: Legal and Governance Framework for AI-Based Cybercrime Management in Bangladesh


Legal and Governance Framework for
AI-Based Cybercrime Management in Bangladesh
Law Enforcement Agencies
• Cyber Units
• Forencic Analysts
• CERT
CERT
Policy & National Cyber Strategy
• National Cybersecurity Strategy
• AI & Cyber Policy Guidelines
• Public–Private Partnerships
AI SYSTEMS
Law Enforcement Agencies
• Cyber Units
• Forencic Analysts
• CERT
POLICE
Policy & National Cyber Strategy
• National Cybersecurity Strategy
• AI & Cyber Policy Guidelines
• Public–Private Partnerships
AI SYSTEMS
• Fraud Detection
• Natural Language Proc.
• Malware Analysis
• Threat Detection
Legal Compliance &
Policy Implemenatation
Cybercrime & Data Protection Laws
• Digital Security Act (DSA)
• Information and Communication Technology (ICT)
• Data Protection Act
Judicial Oversight & Digital Evidence
• Due Process & Admissibility
• Chain of Custody
• Algorithm Scrutiny
Feedback & Accountability
• Audit, Compliance & Incident Review
• Governance Oversight
• Cyber Judiciary
• Regulatory Authorities

Implementation should follow two critical strategic pathways. First, the framework should enable proactive threat intelligence by feeding a national cyber threat intelligence platform, transitioning the BGD e-Gov CIRT from reactive response to proactive threat hunting. Early identification of disinformation or radicalization clusters [21] can empower strategic communications to counter false narratives and mitigate social unrest. Second, a concerted effort in capacity building and public-private partnership (PPP) is required. This necessitates government investment in specialized AI/ML training for cybersecurity professionals, funding academic research to develop Bangla NLP tools and curated security datasets, and establishing legal and technical PPP frameworks. These frameworks would facilitate secure, anonymized threat data sharing between banks, telecom providers, social media platforms, and the national CERT, fostering a collective defense model. Crucially, adopting an explainable and ethical AI approach is non-negotiable to maintain public trust and ensure accountability in surveillance and monitoring activities [8].

Institutional Accountability

Effective national deployment of AI in cybercrime management also requires clearly defined institutional accountability. Law enforcement agencies, regulators, and judicial bodies must have delineated roles in overseeing AI use, responding to cybersecurity incidents, and ensuring compliance with cybercrime and data protection laws. Without such accountability structures, AI-driven cyber defense risks becoming fragmented and legally vulnerable.

7. Conclusion and Future Work

This article has established Artificial Intelligence as a pivotal tool for Bangladesh to manage its complex and growing cybercrime problem. By adapting proven global methodologies, such as NLP-based social media analysis and ML-based anomaly detection, to the local context particularly the Bangla language and prevalent threat types Bangladeshi institutions can achieve a significant defensive advantage. The proposed framework provides a roadmap, though its success depends on overcoming foundational challenges related to data availability, skill development, and strategic integration. Future work must therefore prioritize creating and publishing benchmark datasets for Bangla cyber security to spur innovation, exploring federated learning [9, 10] as a privacy-preserving means for collaborative fraud detection, and investigating integrated block chain-AI frameworks [4, 11, 12] to secure digital identities and transactions. Additionally, longitudinal studies are needed to measure the real-world impact of AI tools in operational settings, and cost-benefit analysis frameworks must be developed to quantify the return on investment in resource-constrained environments. Ultimately, the legitimacy of AI-enabled cybercrime management depends on its consistency with the rule of law. AI must strengthen—not replace—legal reasoning, investigative accountability, and judicial oversight. For Bangladesh, embedding AI within a robust legal and policy framework is essential to ensuring that technological advancement translates into justice, security, and public trust. The journey towards an AI-secured Digital Bangladesh is complex but imperative; with strategic investment and collaboration, AI can transform from a novel technology into the bedrock of the nation's cyber resilience.

8. References

1. Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. The Police Journal, 96(4), 573-592.
2. Islam, M. T., Islam, M. F., & Sawda, J. (2022). E-commerce and cyber vulnerabilities in Bangladesh: A policy paper. International Journal of Law and Society (IJLS), 1(3), 186-203.
3. Khan, A., Roy, B. K. S., Sarker, A., Abedin, S. N., Islam, M. M., & Zaber, M. (2025). AI-Driven Cyber security Challenges in Bangladesh's Banking Industry. Journal of Computer and Communications, 13(11), 223-235.
4. Rahman, M. J., Islam, A., Montieri, M., Nasir, M. K., Reza, M. M., Band, S. S., ... & Mosavi, A. (2021). Smartblock-sdn: An optimized blockchain-sdn framework for resource management in IoT. IEEE Access, 9, 28361-28376.
5. Rahman, T., Debnath, D., Kundu, D., Khan, M. S. I., Aishi, A. A., Sazzad, S., ... & Band, S. S. (2024). Machine learning and deep learning-based approach in smart healthcare: Recent advances, applications, challenges and opportunities. AIMS Public Health, 11(1), 58–109.
6. M. Rahaman. (2022). Recent advancement of cyber security: Challenges and future trends in Bangladesh. Saudi Journal of Engineering and Technology, 7(6), 278–289.

7. Hossain, M. J., Rifat, R. H., Mugdho, M. H., Jahan, M., Rasel, A. A., & Rahman, M. A. (2022). Cyber threats and scams in fintech organizations: A brief overview of financial fraud cases, future challenges, and recommended solutions in Bangladesh. In 2022 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS) (pp. 190-195). IEEE.
8. Capuano, N., Fenza, G., Loia, V., & Stanzione, C. (2022). Explainable artificial intelligence in cyber security: A survey. IEEE Access, 10, 93575-93600.
9. Rahman, M. S., Hossain, G. S., Muhammad, G., Kundu, D., Debnath, T., Khan, M. S. I., & Band, S. S. (2023). Federated learning-based AI approaches in smart healthcare: concepts, taxonomies, challenges and open issues. Cluster computing, 26(4), 2271–2311.
10. Rahman, K., Hasan, K., Kundu, D., Islam, M. J., Debnath, T., Band, S. S., & Kumar, N. (2023). On the ICN-IoT with federated learning integration of communication: Concepts, security-privacy issues, applications, and future perspectives. Future Generation Computer Systems, 138, 61-88.
11. Rahman, M. J., Islam, J., Band, S. S., Muhammad, G., Hasan, K., & Tiwari, P. (2023). Towards a blockchain-SDN-based secure architecture for cloud computing in smart industrial IoT. Digital Communications and Networks, 9(2), 411-421.
12. Rahman, J., Islam, J., Kundu, D., Karim, R., Rahman, Z., Band, S. S., & Kumar, N. (2023). Impacts of block chain in software-defined internet of things ecosystem with network function virtualization for smart applications: Present perspectives and future directions. International Journal of Communication Systems, e5429.
13. Ahmed, M. T., Islam, R., Rahman, M. A., Islam, M. J., Rahman, A., & Kabir, S. (2023). An image-based digital forensic investigation framework for crime analysis. In 2023 International Conference on Next-Generation Computing, IoT and Machine Learning (NCIM) (pp. 1-6). IEEE.
14. Sharma, P., Kaushik, N., & Tripathi, R. (2022). AI-Enabled Cyber Threats and IoT Vulnerabilities. IEEE Access, 10, 98743-98756.
15. Rahman, M., & Islam, S. (2021). Cyber security Challenges in the Banking Sector of Bangladesh. Journal of Financial Crime, 28, 1250-1265.
16. Kshetri, N. (2021). Cyber security and the Changing Threat Landscape. Computer Law & Security Review, 43, 1-10.
17. Sundaramurthy, S. K., Ravichandran, N., Inaganti, A. C., & Muppalaneni, R. (2022). AI-Powered Operational Resilience: Building Secure, Scalable, and Intelligent Enterprises. Artificial Intelligence and Machine Learning Review, 3, 1-10.
18. Haque, G. M. M., Akula, D. K., Mohammed, Y. S., Syed, A., & Arafat, Y. (2025). Cyber security Risk Management in the Age of Digital Transformation: A Systematic Literature Review. Emerging Frontiers Library for the American Journal of Engineering and Technology, 7, 126-150.

19. Bhuiyan, M. S., & Hassan, S. A. (2023). Leveraging language understanding models for hate speech and misinformation detection in Bangla social media. arXiv preprint arXiv:2301.06565.
20. Hossain, E., Kaysar, M. N., Joy, A. Z. M. J. U., & Rahman, M. M. (2022). A study towards Bangla fake news detection using machine learning and deep learning. In Sentimental Analysis and Deep Learning: Proceedings of ICSADL 2021 (pp. 79–95). Springer.
21. Ramírez Sánchez, J., Campo-Archbold, A., Zapata Rozo, A., Díaz-López, D., Pastor-Galindo, J., Gómez Mármol, F., & Aponte Díaz, J. (2021). Uncovering cybercrimes in social media through natural language processing. Complexity, 2021, 1-15.
22. Lifandali, O., & Abghour, N. (2021). Deep learning methods applied to intrusion detection: Survey, taxonomy and challenges. In Proc. Int. Conf. Decis. Aid Sci. Appl. (DASA) (pp. 1035–1044).
23. M. Florea, C. Potlog, and P. Pollner, "Challenges in Cybersecurity and privacy - the European research landscape," chapter Complex project to develop real tools for identifying and countering terrorism: real- time early detection and alert system for online terrorist content based on Natural Language processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing, River Publishers, Denmark, Europe, pp. 181- 206, 2019.
24. F. Iqbal, B. C. M. Fung, M. Debbabi, R. Batool, and A. Marrington, "Wordnet- based criminal networks mining for cybercrime investigation," IEEE Access, vol. 7, pp. 22740- 22755, 2019.
25. S. Pastrana, A. Hutchings, A. Caines, and P. Buttery, "Characterizing eve: analyzing cybercrime actors in a large underground forum," in Michael Bailey, Thorsten Holz, Manolis Stamatiogiannakis and Sotiris Ioannidis, pp. 207- 227, Springer International Publishing, New York, NY, USA, 2018.
26. R. Bhalerao, M. Aliapoulios, I. Shumailov, S. Afroz, and D. McCoy, "Mapping the underground: supervised discovery of cybercrime supply chains," in Proceedings of the 2019 APWG Symposium on Electronic Crime Research (eCrime), pp. 1- 16, IEEE, Pittsburgh, PA USA, November 2019.
27. G. Ericson, W. Rohm, and J. Martens, Team Data Science Process Documentation, Microsoft Azure, Technical Report, 2017, https://docs.microsoft.com/en-us/azure/architecture/data- science- process/overview.
28. T. Calinski and J. Harabasz, "A dendrite method for cluster analysis," Communications in Statistics- Simulation and Computation, vol. 3, no. 1, pp. 1- 27, 1974.
29. J. A. Bondy and U. S. R. Murty, Graph Theory with Applications, Elsevier, Amsterdam, Netherlands, 1976.