IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

A CRITICAL STUDY ON AI FOR CYBERSECURITY AND MOBILE BIOMETRICS: A DUAL-DOMAIN FRAMEWORK FOR THREAT DETECTION

Rajendrakumar Ranchhodbhai Patel[1]
Research Scholar
Faculty of IT and Computer Science
Swaminarayan University, Kalol

Prof. (Dr.) Geetanjali Amarawat[2]
Dean and Professor
Faculty of IT and Computer Science
Swaminarayan University, Kalol

Prof. (Dr.) Jigar Patel[3]
Director MCA/MBA
Kalol Institute of Technology & Research Center, Kalol

Abstract: In today's digitally interconnected world, the convergence of cybersecurity and mobile security presents both opportunities and urgent challenges. Rapid digital transformation, fuelled by cloud computing, mobile devices, and the Internet of Things (IoT), has created vast and dynamic attack surfaces. The increasing complexity of digital ecosystems and the proliferation of mobile connectivity have heightened vulnerabilities in both network infrastructures and personal authentication systems. Traditional cybersecurity defences and mobile security mechanisms often fail to adapt to the evolving nature of threats, leading to gaps in real-time protection, identity verification, and trust. Artificial Intelligence (AI) offers promising solutions through adaptive learning, predictive analytics, and biometric pattern recognition. However, current implementations suffer from critical limitations, including poor generalizability, adversarial susceptibility, demographic bias, and ethical opacity, particularly within regional and resource-constrained contexts like India.

Keywords: AI, Cybersecurity, Mobile Biometrics, Threat Detection

1.Introduction

This research proposes a dual-domain investigation into the effectiveness, robustness, and ethical implications of AI applications in two interrelated areas: (i) threat detection in cybersecurity via intelligent Intrusion Detection Systems (IDS), and (ii) biometric-based mobile authentication using facial, fingerprint, and voice recognition models. The study adopts a convergent parallel mixed-method design, combining quantitative experimentation with qualitative user perception studies. Deep learning and hybrid models will be trained and validated on both benchmark and demographically diverse Indian datasets. Adversarial testing and explainability techniques will be employed to assess model resilience and transparency.

Alongside technical evaluation, the research includes an ethical audit covering data privacy, algorithmic fairness, and user trust. The final deliverables will include an integrated AI evaluation framework, optimized for deployment in Indian cybersecurity infrastructure and mobile identity systems. The expected outcomes aim to contribute to academic scholarship, practical system design, and public policy formulation by enabling secure, inclusive, and ethically grounded AI deployments in national digital ecosystems.

2.Background and Context

Cyberattacks ranging from data breaches to ransomware and distributed denial-of-service (DDoS) attacks have become increasingly sophisticated and damaging. Simultaneously, the growth of mobile authentication technologies introduces new vulnerabilities in biometric data handling and user privacy. Artificial Intelligence (AI) has emerged as a promising technology to address both domains by providing intelligent threat detection, biometric verification, and behaviour analysis capabilities [1].

Modern security development paradigms such as DevSecOps (Development Security and Operations) emphasize the proactive integration of security measures across the software lifecycle. This model, an evolution of DevOps, ensures that development, security, and operations teams collaborate continuously to embed automated, scalable protections within Continuous Integration/Continuous Deployment (CI/CD) workflows. Frameworks like OWASP SAMM and the NIST Secure Software Development Framework (SSDF) provide formalized practices to secure software pipelines and detect vulnerabilities early [2].

Despite these global advances, the Indian landscape presents distinctive challenges: infrastructural inequality, edge-device constraints, linguistic diversity, and regulatory transition. Moreover, existing security models often treat cybersecurity and mobile authentication separately, leading to fragmentation and inefficiencies. This thesis addresses this critical need through a dual-domain investigation that integrates AI in cybersecurity threat detection and biometric mobile authentication, emphasizing fairness, contextual robustness, and ethical compliance [3].

3.Emergence of AI in Cybersecurity

AI has revolutionized the cybersecurity domain by enabling systems to learn from dynamic data and detect previously unknown threats. Traditional rule-based Intrusion Detection Systems (IDS) are inadequate against modern, stealthy attacks such as Advanced Persistent Threats (APT), zero-day exploits, and polymorphic malware. Machine learning (ML) and deep learning (DL) models like Support Vector Machines (SVM), Convolutional Neural Networks (CNNs) [4].

Nevertheless, these systems pose challenges. Deep models are often opaque, leading to concerns over explainability and accountability, especially in critical sectors like banking and defense [5]. Lipton [6] emphasize that AI's lack of transparency hinders stakeholder trust and regulatory compliance. Additionally, most AI-based Intrusion Detection Systems solutions rely on benchmark datasets such as NSL-KDD, CICIDS, and UNSW-NB15, which were developed in Western infrastructure contexts. Their applicability to Indian network environments is limited by differences in topology, traffic behaviour, and attack patterns.

A pertinent case study is the Colonial Pipeline ransomware attack (2021), which shut down a major U.S. fuel pipeline for several days. Had real-time anomaly detection and predictive AI models been in place, early signs of lateral movement could have been detected and contained. This underscores the growing necessity for AI-based, context-sensitive cybersecurity frameworks.

4.AI in Biometric Mobile Security

The shift from password-based to biometric authentication systems on mobile platforms has enabled more convenient and secure access to services. AI-driven biometric modalities, including facial recognition, fingerprint matching, and voice authentication, leverage deep learning to improve accuracy and response time. CNN-based systems such as FaceNet and ResNet are widely used for facial feature extraction; fingerprint recognition uses autoencoders for minutiae detection; and voice authentication benefits from LSTM networks analyzing spectral patterns .

However, biometric systems are vulnerable to spoofing attacks. For example, adversaries may use high-resolution images or 3D models to deceive facial recognition, synthetic audio clips for voice spoofing, or gel overlays for fingerprint bypass. To counter these, AI-based anti-spoofing techniques employ liveness detection and adversarial training.

5.Convergence of Cybersecurity and Mobile Security

In real-world scenarios, mobile and network-level threats increasingly overlap. A compromised mobile device can act as a bridge for launching enterprise-level attacks; likewise, malware detected in network flows may originate from mobile endpoints. This operational overlap necessitates integrated AI frameworks.

Patel and Shah [7] demonstrated that behavioural signals from mobile devices, such as app-switching patterns, keystroke dynamics, and location anomalies, can improve IDS accuracy when fused with network telemetry. Such cross-domain analytics provide early warning capabilities and reduce false positives.

This research proposes a unified AI security architecture that treats mobile behaviour and network threats as co-dependent signals. By consolidating data sources and evaluation metrics, the study seeks to maximize detection efficacy while minimizing computational redundancy.

AI architectures in cybersecurity. Their perspective reinforces the need for collaboration between AI scientists, security engineers, and policymakers to ensure ethical and effective model deployment.

Table 1: Comparative Analysis Table

Citation	Domain	AI Technique	Context (India/Global)	Deployment Focus	Key Strength	Limitation / Research Gap
ElSayed et al. (2021) [15]	Cybersecurity (SDN IDS)	CNN + Parametric Dropout	Global	Cloud/SDN	Generalization in SDN environments	No explainability or fairness audit
Shtayat et al. (2023) [16]	IIoT Intrusion Detection	CNN + BiLSTM + DNN (Ensemble)	Global	IIoT edge/cloud	High accuracy with XAI	No fairness or edge profiling
Siddiqui et al. (2024) [17]	UTM for Home Networks	UTM architectures (review)	Global	Consumer networks	Comprehensive UTM taxonomy	No implementation or fairness analysis
Sharma et al. (2024) [18]	IoT Intrusion Detection	CNN + LSTM	Global	Edge devices	Explainable DL for IoT IDS	Uses LSTM (less edge-efficient), lacks fairness insights
Naeem et al. (2021) [19]	IoT Malware Detection	Transfer Learning (CNN)	Global	Low-end IoT	Image-based malware detection	Lacks fairness, dataset generalizability
Kotwal & Marcel (2024) [20]	Face Recognition	Score Calibration + Softmax	Global	Biometric systems	Demographic bias mitigation	Limited to face recognition fairness only
Kaur et al. (2023) [21]	Cybersecurity (Survey)	CNN, RNN, Autoencoders	Global	General	Identifies trends and gaps	No empirical model, lacks India-specific insights
Michael et al. (2023) [22]	Ethical AI in Cybersecurity	Conceptual critique	Global	Policy and ethics	Highlights sociotechnical risks of AI	No technical model or testable solution

Buriro & Luccio (2025) [23]	Mobile Biometrics	Multimodal, On-device AI	Global	Edge/mobile	Comprehensive review on mobile biometrics	No dataset or model evaluation
Wali et al. (2025) [24]	IDS (Cloud/Enterprise)	RF + SHAP	Global	Cloud / on-prem	Lightweight interpretable IDS	Not evaluated on Indian network logs
Lai et al. (2023) [25]	Biometric Decision Systems	Trust Framework (conceptual)	Global	Institutional / Governance	Fairness + trust architecture	Lacks empirical validation
Valdivia et al. (2023) [26]	Biometric Fairness	Critical philosophical analysis	Global	Ethical critique	Framework for structural fairness	No algorithm or model tested
Bergadano & Giacinto (2023) [27]	Cybersecurity (Editorial)	Robust AI models (overview)	Global	Broad (Auth/Anomaly/Threat)	Next-gen cybersecurity roadmap	No specific technical experiments

6.Challenges in the Indian Context

India's expanding digital infrastructure, including initiatives like Digital India and increasing mobile penetration, presents a unique environment for AI-driven cybersecurity and mobile authentication systems. However, several India-specific challenges must be addressed to ensure that AI-based solutions are effective, inclusive, and ethically compliant.

- Data Representativeness
- Device Constraints
- Biometric Diversity
- Awareness and Consent
- Regulatory Uncertainty

In summary, these challenges highlight the need for designing AI-based cybersecurity and biometric authentication systems that are lightweight, culturally aware, and aligned with India’s evolving legal frameworks. The proposed research explicitly addresses these through contextual dataset development, edge-optimized AI deployment, fairness evaluation, user trust assessment, and policy compliance mapping.

7.Conclusion

Artificial Intelligence (AI) continues to play a transformative role in reshaping digital security architectures, particularly within the domains of intrusion detection and biometric authentication. While significant research has explored each domain independently, there remains a gap in the literature addressing their integration in regional and resource-constrained contexts. This chapter critically reviews developments in AI-based intrusion detection systems (IDS), CNN-powered biometric models, explainability frameworks, and demographic fairness, with a focus on studies published in recent years.

The paper systematically categorizes UTM architectures based on key functional components such as firewall integration, intrusion prevention systems (IPS), content filtering, and antivirus modules. A critical review of commercial and open-source UTM platforms is presented, highlighting deployment challenges such as latency overhead, privacy concerns, and limited firmware scalability on consumer-grade routers. The authors also emphasize the role of AI and deep packet inspection in enhancing detection accuracy in modern UTMs.

One of the major contributions of the study is the articulation of future research directions, particularly the potential for edge-AI-enabled UTMs, secure firmware update pipelines, and policy-based parental control frameworks. By addressing the convergence of security, usability, and performance, this survey serves as a foundational resource for researchers and developers seeking to design next-generation UTM systems optimized for smart home ecosystems.

Equally notable is their treatment of sociotechnical challenges: demographic bias, spoofing susceptibility, and lack of standardization across mobile operating systems. The paper highlights how adversarial attacks and deepfake technologies pose new threats to biometric robustness, necessitating liveness detection and explainability as core system features. Future directions proposed include decentralized biometric storage using blockchain and federated learning models.

This work is particularly valuable in contexts such as e-governance or law enforcement, where biometric automation must reconcile technical efficacy with societal equity, transparency, and institutional accountability.

8.References

[1] Ring, M., Wunderlich, S., Scheuring, D., Landes, D., & Hotho, A. (2019). A survey of network-based intrusion detection data sets. *Computers & Security*, *86*, 147-167. https://doi.org/10.1016/j.cose.2019.06.005

[2] OWASP Foundation, “DevSecOps Guidelines: Integrating Security into DevOps,” OWASP, 2021. [Online]. Available: https://owasp.org/www-project-devsecops-guideline/. [Accessed: 01-Jul-2025].

[3] National Institute of Standards and Technology, “Secure Software Development Framework (SSDF) Version 1.1,” NIST Special Publication 800-218, Feb. 2022. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-218/final. [Accessed: 01-Jul-2025].

[4] Shrestha, R., Mohammadi, M., Sinaei, S., Salcines, A., Pampliega, D., Clemente, R., Sanz, A. L., Nowroozi, E., & Lindgren, A. (2024). Anomaly detection based on LSTM and autoencoders using federated learning in smart electric grid. Journal of Parallel and Distributed Computing, 193, 104951. https://doi.org/10.1016/j.jpdc.2024.104951

[5] F. Doshi-Velez and B. Kim, “Towards a rigorous science of interpretable machine learning,” arXiv preprint arXiv:1702.08608, 2017.

[6] Lipton, Z. C. (2018). The mythos of model interpretability: In machine learning, the concept of interpretability is both important and slippery. Queue, 16(3), 31-57.

[7] Ullah, F., Ullah, S., Srivastava, G., & Lin, J. C. W. (2024). IDS-INT: Intrusion detection system using transformer-based transfer learning for imbalanced network traffic. Digital Communications and Networks, 10(1), 190-204. https://doi.org/10.1016/j.dcan.2023.03.008