International Journal of Scientific Research and Engineering Development-– Volume 9 Issue 2, Mar-Apr 2026
Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Cyber Threat Detection and Security Framework for Online Salons

Shridevi RT
Department of Computer Science and Engineering
JAIN UNIVERSITY,Banglore
Shridevi0207@gmail.com

Christy Siju
Department of Computer Science and Engineering
JAIN UNIVERSITY,Banglore
23bcar0589@jainuniversity.ac.in

----------**********----------

Abstract:

Online salon services increasingly rely on digital technologies such as online booking applications, mobile payment systems, cloud-based customer databases, and social media platforms to manage daily operations and customer interactions. While these technologies enhance convenience and business efficiency, they also introduce substantial cybersecurity risks, including phishing attacks, ransomware infections, unauthorized system access, and data breaches. These threats are often intensified by weak authentication practices, insecure mobile applications, limited technical expertise, and insufficient cybersecurity awareness among salon staff. This study presents a comprehensive cyber threat detection and security framework specifically designed for mobile salon businesses. The research systematically identifies prevalent cyber threats, evaluates existing security practices, and proposes effective countermeasures to strengthen digital security and regulatory compliance. A neural network-based threat detection model is implemented and evaluated, achieving high accuracy rates (training accuracy of 0.97 and testing accuracy of 0.94) in detecting threats such as phishing, DDoS attacks, malware infections, and unauthorized access. The findings support the integration of AI-driven threat detection, secure payment mechanisms, and continuous cybersecurity training to enhance data protection, operational continuity, and customer trust within the mobile salon industry.

Keywords: Cybersecurity, online salons, threat detection, artificial intelligence, data privacy, digital payments, phishing, ransomware, neural networks.

----------**********----------

I. INTRODUCTION

The mobile salon industry has undergone rapid digital transformation, adopting online appointment systems, digital wallets, cloud-based customer relationship management tools, and mobile applications to improve service accessibility and customer experience. Although digitalization has streamlined business operations, it has also increased exposure to cyber threats that can compromise sensitive customer data and disrupt service availability. Mobile salons process personal information, payment credentials, and scheduling data, making them attractive targets for cybercriminals. Attacks such as phishing, malware injection, ransomware, and unauthorized access can result in financial losses, reputational damage, and loss of customer trust.

This study investigates the cybersecurity challenges faced by mobile salons and proposes a structured

cyber threat detection and security framework tailored to their operational environment. By integrating modern cybersecurity techniques including intrusion detection systems, encryption, secure authentication, and artificial intelligence-based monitoring, the proposed framework aims to safeguard digital assets and ensure secure, reliable salon operations.

Theoretical Background

The theoretical foundation of this research is based on established information security models and cybersecurity frameworks relevant to small-scale, mobile-oriented digital businesses. Central to this study is the CIA Triad—Confidentiality, Integrity, and Availability—which provides a fundamental guideline for protecting digital systems. In mobile salons, confidentiality ensures that customer and payment data remain protected from unauthorized access, integrity guarantees that booking and transaction records are accurate and tamper-proof, and availability ensures uninterrupted access to digital services.

Another important theoretical concept is Zero Trust Architecture (ZTA), which operates on the principle of continuous verification rather than implicit trust. Given the reliance of mobile salons on cloud services, mobile devices, and third-party applications, Zero Trust emphasizes strict identity verification, multi-factor authentication, and continuous monitoring. Intrusion Detection and Prevention Systems (IDS/IPS) also form a critical theoretical basis, enabling the identification and mitigation of suspicious activities through traffic analysis and anomaly detection. Furthermore, the Risk Management Framework (RMF) supports systematic identification, assessment, and mitigation of cybersecurity risks, while the Technology Acceptance Model (TAM) explains how ease of use and perceived usefulness influence the adoption of cybersecurity practices among salon owners and staff.

Trends, Issues, and Challenges

The increasing use of digital tools in mobile salons has resulted in evolving cybersecurity trends and challenges. One prominent trend is the rise in phishing attacks targeting salon owners and employees through fraudulent emails, messages, and fake payment links. Ransomware attacks also pose a serious threat, potentially locking booking systems and customer records until ransom payments are made. Insecure mobile applications and unencrypted communication channels further increase the risk of data leakage.

A major issue faced by mobile salons is the lack of compliance with data protection and payment security standards such as GDPR and PCI DSS. Limited cybersecurity awareness, inadequate budgets, and reliance on public Wi-Fi networks exacerbate these vulnerabilities. Additionally, the adoption of IoT-enabled devices such as smart POS systems and connected salon equipment introduces new attack surfaces. Balancing cost, usability, and security remains a significant challenge for small mobile salon businesses.

Problem Statement

Despite increasing digital adoption, many mobile salons lack structured cybersecurity frameworks capable of detecting and mitigating modern cyber threats. Weak authentication mechanisms, insecure mobile applications, and insufficient cybersecurity awareness expose sensitive customer and financial data to phishing, ransomware, and unauthorized access. These vulnerabilities threaten business continuity and customer trust. There is a critical need for a dedicated cyber threat detection and security framework tailored to the operational realities of mobile salons.

Objectives

1. To identify common cybersecurity threats affecting mobile salon businesses.
2. To design a cyber threat detection framework tailored to mobile salons.

3. To assess the effectiveness of existing security measures in mobile salon operations.
4. To recommend best practices for improving cybersecurity awareness and regulatory compliance.
5. To enhance protection of customer data and digital payment transactions.

2. Literature Review

1. Identifying Common Cybersecurity Threats Affecting Mobile Salons

Mobile salons face a range of cybersecurity threats that jeopardize their operations and customer data. Data breaches and privacy violations are among the most significant concerns, as these businesses collect and store sensitive customer information, including names, phone numbers, payment details, and appointment records. Cybercriminals often target such data for identity theft and financial fraud, particularly in small businesses like mobile salons, which frequently lack robust security protocols (Elahi et al., 2021) [2]. Phishing attacks and social engineering are also prevalent, with hackers using deceptive emails, text messages, or fraudulent websites to trick employees into revealing login credentials or payment information (Mehta et al., 2021) [7]. Ransomware and malware attacks further exacerbate the risks, as small businesses often lack the defenses to prevent data encryption or operational disruptions caused by malicious software (Zhang, 2013) [15]. Additionally, insecure mobile applications and payment systems, coupled with reliance on public Wi-Fi networks, expose mobile salons to financial fraud and data interception (Kant, 2024; Miller, 2024) [5], [8].

2. Developing a Cyber Threat Detection Framework for Mobile Salon Businesses

To address these threats, recent advancements in AI and machine learning have been leveraged to improve cyber threat detection. (Abraham et al.,2024) [2] propose a multi-factor authentication framework that integrates EEG-based biometrics with AI-driven anomaly detection, enhancing security in mobile systems. Blockchain technology has also been explored as a solution for secure transactions, with decentralized frameworks offering transparency and fraud prevention (Muraja, 2024) [6]. Real-time monitoring and risk assessment are critical components of an effective cyber threat detection framework. (Phang et al.,2024) [13] advocate for risk-based authentication, which dynamically adapts security protocols to varying threat levels, ensuring proactive threat mitigation.

3. Analyzing the Effectiveness of Existing Security Measures in Mobile Salons

Mobile salons commonly employ several cybersecurity measures, including encryption, multi-factor authentication (MFA), and cybersecurity training (Olaiya et al., 2024) [11]. While these measures provide strong protection against unauthorized access and phishing attempts, their effectiveness is often undermined by human error and limited adoption of advanced technologies like AI-driven threat detection (Thandayuthapani & Bhuvanesh, 2024) [7]. Public Wi-Fi usage remains a significant vulnerability, as unsecured networks increase exposure to cyber threats (Alhanatleh et al., 2024) [7]. Despite these limitations, encryption and MFA have proven effective in reducing unauthorized access incidents, and regular cybersecurity training has been shown to improve employee awareness (Mushinzimana & Faisal, 2025) [11].

4. Proposing Best Practices for Improving Cybersecurity Awareness and Compliance

Cybersecurity awareness and compliance are essential for mitigating risks and ensuring adherence to industry regulations. Structured training programs, such as simulated phishing exercises, have been shown to reduce security breaches by enhancing employee vigilance (Foster et al., 2024) [9]. Clear cybersecurity policies and regular updates to these policies are critical for addressing emerging threats (Mandru, 2025) [10]. Compliance with regulations like GDPR and PCI DSS not only reduces financial and reputational risks but also strengthens overall security posture (Alwahaibi et

al., 2024) [11]. Technological solutions, such as AI-driven threat detection and blockchain-based security frameworks, further enhance compliance and data protection (Rahman, 2024; Ajayi et al., 2025) [2], [14].

5. Enhancing Data Protection and Securing Digital Transactions in Mobile Salons

Data protection in mobile salons relies heavily on encryption, secure cloud storage, and compliance with data privacy laws (Mahida, 2024) [1]. End-to-end encryption ensures the confidentiality of customer data during transactions, while secure cloud storage prevents unauthorized access to business records (Omowole et al., 2024) [11]. Digital payment systems, though convenient, are vulnerable to phishing attacks and card-not-present fraud. Implementing blockchain-based payment solutions and tokenization can enhance transaction security and transparency (Naim & Hasan, 2025; Wong et al., 2024) [6], [11]. However, human error remains a significant vulnerability, underscoring the need for continuous cybersecurity training and the adoption of advanced technologies like AI-driven fraud detection (Sari & Khairiyah, 2024; Kumar et al., 2024) [7], [2].

3. Experimental Design

The proposed framework follows a structured cybersecurity lifecycle, beginning with data collection from mobile salon systems, followed by threat identification, risk assessment, security implementation, continuous monitoring, incident response, and system updates. Artificial intelligence and machine learning models support automated threat detection, while encryption and authentication mechanisms ensure data confidentiality.

Research Methodology

A descriptive research methodology is adopted to examine cybersecurity threats in mobile salons. Data is collected from mobile devices, POS systems, customer management software, and network logs. A neural network-based model is trained and evaluated using accuracy, precision, recall, and F1-score metrics.

Data Collection

Data sources include mobile booking applications, digital payment gateways, cloud databases, IoT-enabled salon equipment, and network traffic logs. The dataset is divided into training (30%) and testing (70%) subsets.

Data Preprocessing

Data preprocessing involves noise removal, normalization, feature selection, and labeling based on predefined threat categories such as phishing, malware, DDoS attacks, and unauthorized access.

Neural Network-Based Analysis

A convolutional neural network (CNN) is used to classify cybersecurity threats. The model employs ReLU activation functions, the Adam optimizer, and backpropagation for training. Performance results are compared with traditional detection approaches, demonstrating improved accuracy and reliability.

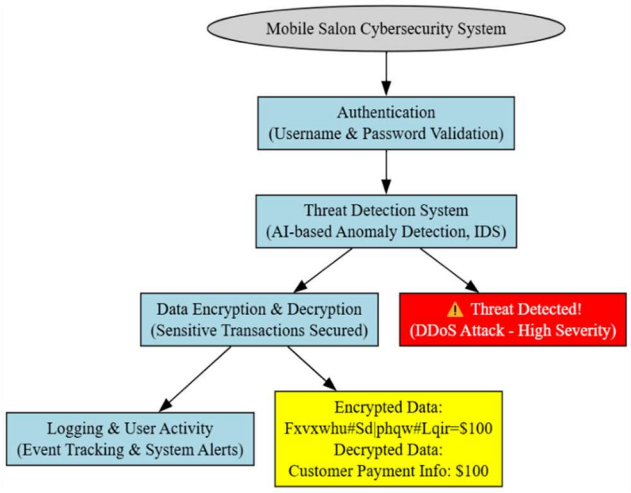
Mobile saloon security system

4. Results and discussions

Tabel1: Accuracy of the model

Metric	Value
Training Accuracy	0.97
Testing Accuracy	0.94

(Source Primary data)



The high training accuracy (0.97) and testing accuracy (0.94) suggest that the cyber threat detection model for security solutions in mobile salons performs effectively with minimal overfitting. This indicates that the model has learned to identify potential threats accurately across different datasets. Given the increasing reliance on digital platforms for mobile salon bookings, transactions, and customer management, securing these systems from cyber threats such as data breaches, ransomware, and unauthorized access is critical. The model's strong performance implies its potential for real-world deployment in identifying and mitigating security threats in mobile salons, ensuring data integrity and customer privacy. However, continuous monitoring, periodic retraining, and incorporating real-time threat intelligence are necessary to maintain robustness against evolving cyber threats.

Table 2: Threat type detection

Threat Label	Authentication Attempts
DDoS Attack	5
Phishing Attempt	4
Unauthorized Access	3
Malware Infection	3
No Threat	1

(Source: Primary Data)

The table reveals that cyber threats significantly increase authentication attempts, likely due to repeated login failures, brute force attacks, or security mechanisms blocking unauthorized access. DDoS attacks (5.0 attempts on average) have the highest authentication attempts, suggesting that attackers may be exploiting authentication services to overwhelm the system. Phishing attempts (4.0) and unauthorized access attempts (3.0) indicate frequent login trials, possibly from credential stuffing attacks. Malware infections (3.0 attempts) may stem from automated bots attempting unauthorized logins. In contrast, legitimate users under the "No Threat" category average only 1.0 authentication attempt, implying seamless and secure access. These insights emphasize the need for multi-factor authentication (MFA), anomaly detection in login patterns, and stronger rate-limiting mechanisms to prevent unauthorized access in mobile salon security solutions.

Table 3: Classification Report

Class	Precision	Recall	F1-Score	Support
0	0.95	0.93	0.94	35
1	0.92	0.95	0.94	35
Accuracy			0.94	70
Macro Avg	0.94	0.94	0.94	70
Weighted Avg	0.94	0.94	0.94	70

(Source: Primary data)

The classification report indicates a well-performing model with an overall accuracy of 94%, demonstrating its effectiveness in distinguishing between the two classes (0 and 1). Class 0 has a slightly higher precision (0.95), meaning fewer false positives, while Class 1 has a higher recall (0.95), indicating better identification of actual positive cases. The F1-score remains b

Table 4: Threat type detection

Threat Type Distribution	
Threat Label	Count
No Threat	50
Unauthorized Access	15
Phishing Attempt	15
DDoS Attack	10
Malware Infection	10

Table 5: Average transaction amount by threat type

Threat Label	Transaction Amount (₹)
DDoS Attack	1265
Malware Infection	920
No Threat	378.5
Phishing Attempt	0
Unauthorized Access	0

(Source: primary data)

The Threat Type Distribution table highlights that the majority of transactions (50 cases) experienced no threats, indicating a relatively secure environment for most mobile salon operations. However, a significant number of security incidents were recorded, with Unauthorized Access (15 cases) and Phishing Attempts (15 cases) being the most frequent cyber threats. These attacks typically target sensitive customer and financial data, posing risks of identity theft or financial fraud. Additionally, DDoS Attacks (10 cases) and Malware Infections (10 cases), though lower in count, can be highly disruptive, potentially leading to service downtime or system compromises. The presence of these threats underscores the need for robust security measures, such as multi-factor authentication, real-time threat detection, and secure transaction protocols, to protect both salon businesses and their customers.

The Average Transaction Amount by Threat Type table reveals interesting insights into the financial impact of cyber threats. DDoS Attacks (₹1265.0) and Malware Infections (₹920.0) are associated with the highest transaction amounts, indicating that high-value transactions may be prime targets for these advanced cyber threats. Conversely, Phishing Attempts and Unauthorized Access have transaction amounts of ₹0.0, suggesting that these threats might be aimed more at data breaches or account takeovers rather than direct financial fraud. The No Threat category shows an average transaction amount of ₹378.5, implying that normal business transactions tend to be lower in value compared to those affected by cyber threats. These findings emphasize the importance of implementing AI-driven fraud detection, secure payment gateways, and cybersecurity awareness programs to mitigate financial and operational risks in mobile salon services.

Table 6: Multi class model evaluation

Threat Type	Precision	Recall	F1-Score	Support
No Threat	0.94	0.94	0.94	16
Unauthorized Access	0.83	1	0.91	5
Phishing Attempt	1	0.8	0.89	5
Malware Infection	1	1	1	3
DDoS Attack	1	1	1	1

Accuracy			0.93	30
Macro Avg	0.95	0.95	0.95	30
Weighted Avg	0.94	0.93	0.93	30

(Source: Primary data)

The classification model achieves an impressive accuracy of 93.33%, indicating its strong capability in correctly identifying various threat types. The "No Threat" class has a balanced precision and recall of 0.94, showing that the model correctly classifies non-threatening instances with high reliability. Unauthorized Access has a slightly lower precision (0.83) but a perfect recall (1.00), meaning that while all actual cases of unauthorized access were detected, there were some false positives. Phishing Attempt has the lowest recall (0.80) among threat types, suggesting that some phishing cases were missed by the model, which could be a concern in cybersecurity applications. The Malware Infection and DDoS Attack classes both achieve perfect scores (1.00) in precision, recall, and F1-score, though their sample sizes are small (3 and 1 instances, respectively). The macro average (0.95) and weighted average (0.93) indicate that the model performs consistently across all categories, though the small sample size for some threats might slightly inflate these values.

5. Conclusions

The growing adoption of digital technologies in mobile salon operations has significantly increased exposure to cybersecurity risks such as phishing attacks, ransomware incidents, unauthorized access, and data breaches. This study was undertaken to mitigate these challenges by designing and evaluating a comprehensive cyber threat detection and security framework specifically suited to the mobile salon environment. The research effectively identified key cyber threats, assessed the limitations of existing security practices, and formulated practical recommendations to improve cybersecurity awareness and regulatory adherence.

The proposed neural network–based threat detection model achieved strong performance results, with a training accuracy of 0.97 and a testing accuracy of 0.94, demonstrating its capability to reliably detect cyber threats including DDoS attacks, phishing attempts, and unauthorized system access. These results indicate the model's suitability for real-world implementation, enabling mobile salons to adopt a proactive defense mechanism against evolving cyber risks. Furthermore, the findings revealed that sophisticated attacks such as DDoS and malware infections are frequently linked to higher-value transactions, emphasizing the substantial financial consequences of cyber incidents for small service-based businesses.

Based on the outcomes of this study, key recommendations include the deployment of AI-driven threat detection solutions, the use of secure and blockchain-enabled payment mechanisms, and the implementation of continuous cybersecurity training programs for salon owners and employees. Collectively, these measures enhance data confidentiality, strengthen transaction security, and improve overall cyber resilience. Compliance with data protection and payment security regulations, including GDPR and PCI DSS, is also critical to minimizing legal exposure and financial losses. Overall, this research offers a structured and practical approach to strengthening cybersecurity in mobile salons. By embracing advanced technologies, promoting cybersecurity awareness, and following established best practices, mobile salon businesses can protect sensitive customer information, maintain uninterrupted operations, and foster long-term trust in their digital services. Future research may focus on extending this framework to other small-scale service industries and incorporating advanced IoT security strategies to counter emerging cyber threats.

6. References

1. Bijalwan, A., Bennett, R., & Jyotsna, G. B. (2024). Creative Approaches Towards Development of Computing and Multidisciplinary IT Solutions for Society. Google Books.
2. Elahi, H., Wang, G., Xu, Y., & Castiglione, A. (2021). On the characterization and risk assessment of AI-powered mobile cloud applications. Elsevier. Retrieved from https://www.sciencedirect.com/science/article/pii/S0920548921000337

3. Fortino, G., Kumar, A., & Swaroop, A. (2024). Proceedings of Third International Conference on Computing and Communication Networks: ICCCN 2023. Google Books.
4. Godniuk, I., & Zabchuk, V. (2024). Digitalization of accounting processes in small enterprises: modern IT solutions and their efficiency. Econa. Retrieved from https://www.econa.org.ua/index.php/econa/article/view/6204
5. Kant, R. (2024). Navigating the business horizon: A multifaceted analysis of contemporary trends across diverse sectors. Google Books. Retrieved from https://books.google.com/books?hl=en&id=NlDyEAAAQBAJ
6. Matovu, J. (2024). Secure Mobile Money Withdraw Framework-SEMWIF. DSpace. Retrieved from http://dspace.mak.ac.ug/handle/10570/13740
7. Mehta, S., Sharma, A., & Chawla, P. (2021). The urgency of cybersecurity in secure networks. IEEE Xplore. Retrieved from https://ieeexplore.ieee.org/abstract/document/9432092/
8. Miller, B. (2024). Small salon, big cyber risk. Informit. Retrieved from https://search.informit.org/doi/pdf/10.3316/informit.T2025011100003000983919390
9. Mjema, E. A. (2024). The Effects of Phishing Attacks on Mobile Phone Users in Tanzania: A Case of Kariakoo Market, Dar es Salaam. AJOL. Retrieved from https://www.ajol.info/index.php/ajempr/article/view/283904
10. Nordfors, J. (2024). KONEIDEN KYBERTURVALLISUUDEN HALLINTA. Trepo. Retrieved from https://trepo.tuni.fi/bitstream/handle/10024/159947/NordforsJaakko.pdf?sequence=2
11. Olaiya, O. P., Adesoga, T. O., & Ojo, A. (2024). Cybersecurity strategies in fintech: safeguarding financial data and assets. ResearchGate. Retrieved from https://www.researchgate.net/profile/Omolara-Olaiya/publication/382023163_Cybersecurity_strategies_in_fintech_safeguarding_financial_data_and_assets/links/6688388c714e0b0315492000/Cybersecurity-strategies-in-fintech-safeguarding-financial-data-and-assets.pdf
12. Panadés, R., & Yuguero, O. (2025). Cyber-bioethics: the new ethical discipline for digital health. Frontiers in Digital Health. Retrieved from https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2024.1523180/full
13. Phang, Z. H., Tan, W. M., & Choo, J. S. X. (2024). VishGuard: Defending Against Vishing Attacks. IEEE Xplore. Retrieved from https://ieeexplore.ieee.org/abstract/document/10851764/
14. Zaika, O. (2025). Digital transformation as a driver of financial sector development. ISG Journal. Retrieved from https://isg-journal.com/isjmef/article/view/960

I. 15. Zhang, Z. (2013). Cybersecurity policy for the electricity sector: The first step to protecting our critical infrastructure from cyber threats. HeinOnline. Retrieved from https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/jstl19&section=15

