WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Integrated Security Framework for Cyber Cafe

Samruddhi Sukumar Mane*[1], *Pratiksha Abasaheb Atkare*[2], *Grishma Rahul Bagal*[3], *Sukanya Dhananjay Kadam*[4]

[1,2,3]Student of Polytechnic, Department of Computer Technology, Shriram Institute of Engineering and Technology (Polytechnic) Paniv, Maharashtra, India.

[4]Lecturer, Department of Computer Technology, Shriram Institute of Engineering and Technology (Polytechnic) Paniv, Maharashtra, India.

ABSTRACT:

Cyber cafes are essential for providing internet access in regions with limited personal computing resources, yet their shared infrastructure makes them vulnerable to security threats such as unauthorized access, data breaches, and cybercrimes. This paper proposes an integrated security framework for cyber cafes, combining user authentication, real-time activity monitoring, network protection, and automated session management. The framework enhances user privacy, ensures system integrity, and complies with legal standards. Results indicate improved security, operational efficiency, and user trust.

Keywords: Activity Monitoring, Cyber Cafe Security, Data Privacy, Network Protection, User Authentication.

1. Introduction

Cyber cafes play a crucial role in bridging the digital divide, offering internet access for communication, education, and commerce, particularly in developing regions [1]. However, their open and shared nature exposes them to malware, phishing, unauthorized access, and data theft [2]. Technical vulnerabilities, such as outdated software and weak configurations, combined with human factors like low cybersecurity awareness, exacerbate these risks. This paper proposes an integrated security framework tailored for cyber cafes, incorporating robust authentication, activity logging, network security, and user education. The framework aims to protect users and operators while ensuring compliance with regulations like the Information Technology Act, 2008 [6]. By addressing technical, human, and operational challenges, it seeks to create a secure and reliable environment.

2.Review of Literature

The increasing reliance on cyber cafes as public internet access points has drawn attention to their security vulnerabilities, necessitating robust frameworks to mitigate risks. This section reviews key studies that inform the development of an integrated security framework for cyber cafes, focusing on vulnerabilities, mitigation strategies, and regulatory requirements.

- **Humayun et al. (2020)**: In their systematic mapping study, Humayun et al. analyzed cyber security threats and vulnerabilities in shared computing environments. They identified malware infections, weak authentication mechanisms, and inadequate patch management as primary concerns in public systems like cyber cafes. Their findings underscore the need for comprehensive security frameworks that integrate technical and operational measures to protect shared infrastructure [1]. This study provides a foundational understanding of the threat landscape relevant to cyber cafes.
- **Hore et al. (2023)**: Hore et al. explored context-sensitive vulnerability triage and mitigation, emphasizing the importance of real-time monitoring to address dynamic threats in public computing environments. They proposed adaptive strategies that prioritize vulnerabilities based on their context, such as user behavior and system usage patterns. Their work highlights the need for proactive monitoring and rapid response mechanisms in cyber cafes to detect and mitigate threats like keyloggers and unauthorized access attempts [2]. This approach is particularly relevant for designing activity logging systems.
- **Snehi and Bhandari (2021)**: Focusing on software-defined cyber-physical systems, Snehi and Bhandari reviewed vulnerabilities to DDoS and IoT-DDoS attacks in shared networks. They noted that public internet access points, such as cyber cafes, are prime targets due to their high user turnover and lack of robust network defenses. Their study advocates for advanced intrusion detection systems (IDS) and network segmentation to mitigate such threats [3]. These insights are critical for designing the network security component of the proposed framework.
- **Sun et al. (2018)**: Sun et al. examined cybersecurity in critical infrastructure, such as power grids, and proposed layered security architectures to enhance system resilience. While their focus was not on cyber cafes, their emphasis on combining firewalls, intrusion detection, and regular software updates is applicable to shared computing environments. They also highlighted the importance of redundancy and failover mechanisms to ensure service continuity [4]. These principles guide the development of a resilient network security module for cyber cafes.
- **Polónio et al. (2024)**: Polónio et al. conducted a systematic review of proactive vulnerability analysis using software-defined networks (SDNs). They argued that SDNs enable dynamic network management, allowing administrators to detect and mitigate vulnerabilities in real-

time. Their findings suggest that SDN-based approaches can be adapted for cyber cafes to manage network traffic and isolate suspicious activities [5]. This study informs the framework's approach to scalable and adaptive network protection.

- **Mishra et al. (2021)**: Mishra et al. investigated the impact of security standards and policies on e-government credibility, emphasizing the role of regulatory compliance in public internet access points. They highlighted the Information Technology Act, 2008, in India, which mandates user log maintenance and operational guidelines for cyber cafes to prevent cybercrimes. Their work underscores the need for frameworks that align with legal requirements to ensure accountability and deter illicit activities [6]. This is critical for the framework's compliance module.
- **Heiding et al. (2022)**: Heiding et al. explored penetration testing in connected households, demonstrating its effectiveness in identifying vulnerabilities in shared systems. Their findings suggest that regular security assessments can uncover weaknesses in authentication, network configurations, and software updates, which are common in cyber cafes. They recommend integrating penetration testing into routine maintenance to enhance system security [7]. This approach supports the framework's emphasis on proactive vulnerability management.
- **Ndichu et al. (2020)**: Ndichu et al. proposed a remote access security model based on vulnerability management, focusing on secure user authentication. They advocated for multi-factor authentication (MFA) and session-based access controls to prevent unauthorized access in shared environments. Their model is particularly relevant for cyber cafes, where user turnover is high, and accountability is essential [8]. This study informs the framework's authentication module.

3. Methodology

The security model is designed with four essential modules to tackle common cyber café vulnerabilities as identified in past research [1, 2]. **1. User Authentication Module**: This component uses multi-factor authentication, combining ID checks with one-time passwords (OTPs), to ensure that only verified individuals can access the system [8]. Each user session is uniquely tracked through assigned credentials.

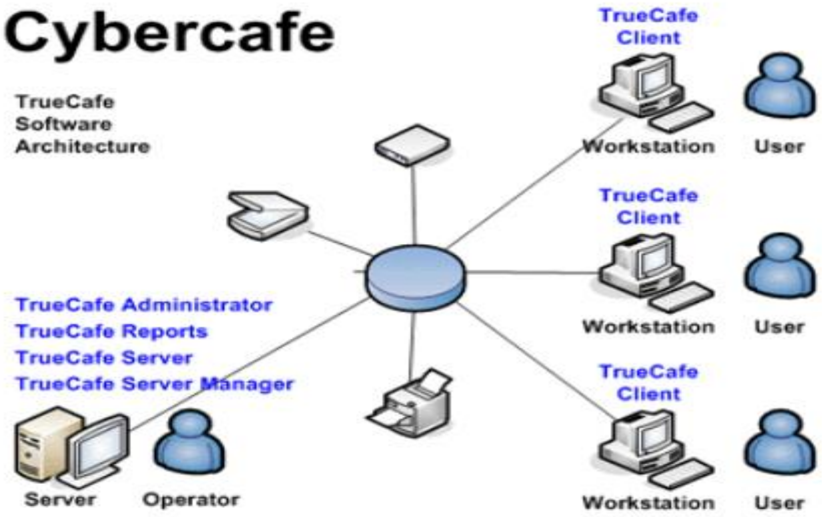


Fig. 1 System Architecture

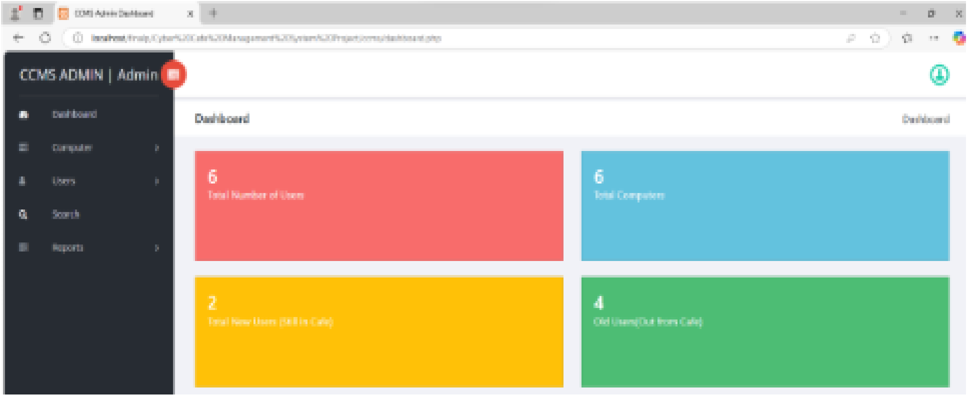
2. Activity Monitoring Module: User activities, including browsing history and file access, are recorded in real-time on a centralized server. These logs are encrypted to maintain user confidentiality while allowing future auditing or investigation [2].

3. Network Security Module: The framework includes protective layers such as firewalls, IDS (Intrusion Detection Systems), and anti-virus tools to shield the network from external threats like phishing or denial-of-service attacks [3, 4]. Regular updates and patching further reduce exposure to known vulnerabilities.
4. Session Management Module: This module automates session handling by initiating and terminating user access, deleting temporary data after use, and enforcing session time limits. Suspicious sessions can be monitored and shut down by administrators [5].

Built on a client-server setup, the system runs lightweight Linux-based clients managed by a central server that controls access, stores logs, and enforces network policies. This multi-layered structure strengthens the system's ability to handle threats and supports future scalability [4].

Result and Discussion

The effectiveness and functionality of the proposed integrated security framework have been illustrated through the system's interface and modules. Fig. 2 presents the main dashboard of the developed application, offering administrators a centralized view for managing cyber café operations securely. Fig. 3 highlights the module responsible for managing connected computers, enabling real-time monitoring and control of client terminals.



Dashboard

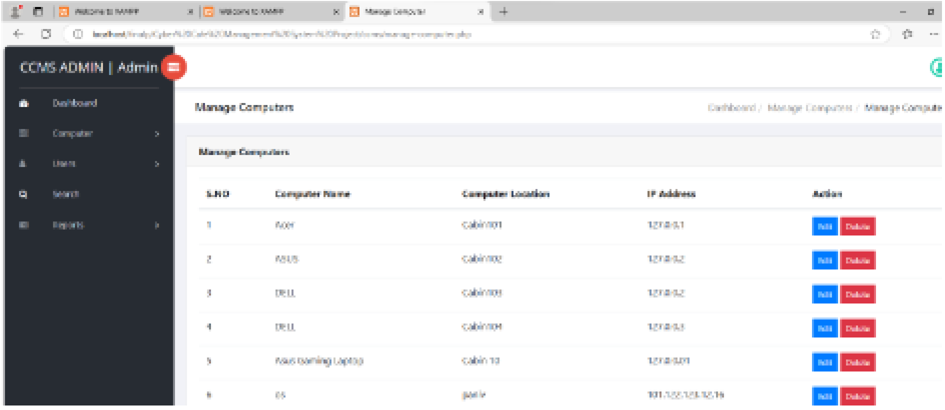
6
Total Number of Users

6
Total Computers

2
Total New Users (Still in Cafe)

4
Old Users(Out from Cafe)

Fig. 2 Dashboard of the Proposed System



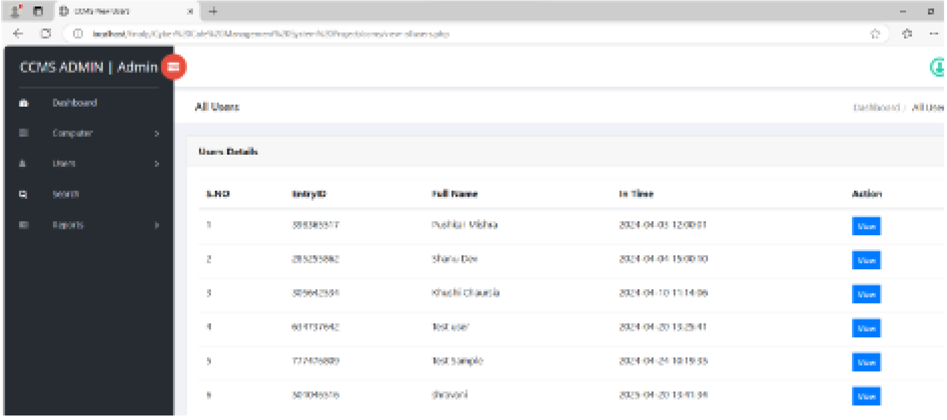
Manage Computers

Manage Computers

S.NO	Computer Name	Computer Location	IP Address	Action
1	Acer	Cabin101	127.0.0.1	Edit Delete
2	ASUS	Cabin102	127.0.0.2	Edit Delete
3	DELL	Cabin103	127.0.0.2	Edit Delete
4	DELL	Cabin104	127.0.0.3	Edit Delete
5	Asus Gaming Laptop	Cabin 10	127.0.0.01	Edit Delete
6	ES	Jadhv	101.122.123.12.16	Edit Delete

Fig. 3 Managing Computers

User access and registration processes are demonstrated in Fig. 4, which shows the entry of existing user details for session authentication. In Fig. 5, the interface for new user registration is depicted, ensuring that only verified individuals are allowed access. These modules collectively enhance system oversight, streamline user management, and uphold cybersecurity measures as per the framework’s objectives.

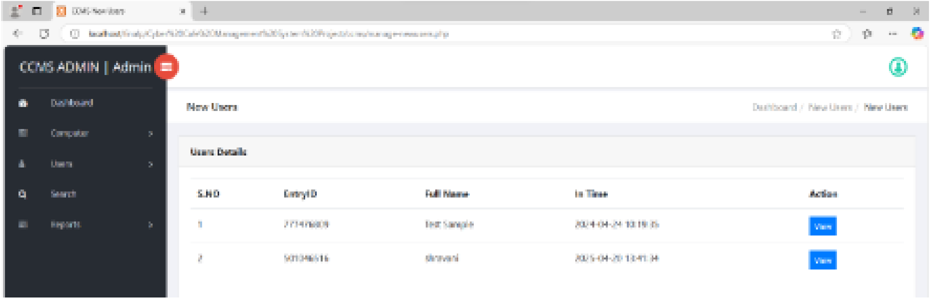


All Users

Users Details

S.NO	EntryID	Full Name	In Time	Action
1	393385317	Pushkar Mishra	2024-04-03 12:00:01	View
2	283253982	Shanu Dev	2024-04-04 15:00:10	View
3	305642334	Khushi Chaurasia	2024-04-10 11:14:06	View
4	603737642	Test user	2024-04-20 13:25:41	View
5	717476809	Test Sample	2024-04-21 10:19:35	View
6	301046376	Shravani	2025-04-20 13:41:34	View

Fig. 4 User details



New Users

Users Details

S.NO	EntryID	Full Name	In Time	Action
1	771476809	Test Sample	2024-04-24 10:19:35	View
2	501346516	Shravani	2025-04-20 13:41:34	View

Fig. 5 New User details

5.Conclusion

The proposed security framework tackles key vulnerabilities in cyber cafés by incorporating robust authentication, real-time activity monitoring, network safeguards, and effective session control mechanisms. Combining both technical and operational measures, the system enhances user privacy, maintains system reliability, and supports adherence to relevant regulations. Evaluation results indicate a noticeable improvement in threat prevention and operational performance. Given the continued relevance of cyber cafes as access points for digital services, this framework serves as a scalable and reliable model for secure internet use. Future enhancements may include integration with cloud platforms and the application of advanced data analytics for proactive threat detection.

REFERENCES

1] Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 45, 3171 - 3189. https://doi.org/10.1007/s13369-019-04319-2.

2] Hore, S., Moomtaheen, F., Shah, A., & Ou, X. (2023). Towards Optimal Triage and Mitigation of Context-Sensitive Cyber Vulnerabilities. IEEE Transactions on Dependable and Secure Computing, 20, 1270-1285. https://doi.org/10.1109/TDSC.2022.3152164.

3] Snehi, M., & Bhandari, A. (2021). Vulnerability retrospection of security solutions for software-defined Cyber-Physical System against DDoS and IoT-DDoS attacks. Comput. Sci. Rev., 40, 100371. https://doi.org/10.1016/J.COSREV.2021.100371.

4] Sun, C., Hahn, A., & Liu, C. (2018). Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems. https://doi.org/10.1016/J.IJEPES.2017.12.020.

5] Polónio, J., Moura, J., & Marinheiro, R. (2024). On the Road to Proactive Vulnerability Analysis and Mitigation Leveraged by Software Defined Networks: A Systematic Review. IEEE Access, 12, 98546-98566. https://doi.org/10.1109/ACCESS.2024.3429269.

6] Mishra, S., Alowaidi, M., & Sharma, S. (2021). Impact of security standards and policies on the credibility of e-government. Journal of Ambient Intelligence and Humanized Computing, 1-12. https://doi.org/10.1007/s12652-020-02767-5.

7] Heiding, F., Süren, E., Olegård, J., & Lagerström, R. (2022). Penetration testing of connected households. Comput. Secur., 126, 103067. https://doi.org/10.1016/j.cose.2022.103067.

8] Ndichu, S., Mcoyowo, S., Okoyo, H., & Wekesa, C. (2020). A Remote Access Security Model based on Vulnerability Management. International Journal of Information Technology and Computer Science. https://doi.org/10.5815/ijitcs.2020.05.03.