International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: http://ijwos.com
Vol.02 No.10.
OPEN ACCESS
E-ISSN : 3049-2424
DOI: doi.org/10.71366/ijwos

A User-Centric Machine Learning Framework for Enhancing Decision-Making and Automation in Cybersecurity Operations Centers

Mrs. N. Shilpa[1], K. Bhargav[2], P. Manoj Reddy[3], M. Sairam[4], P. Sai Kiran[5]
[*1] *Assistant Professor, Department of CSE(Cyber Security), Sri Indu Institute of Engineering and Technology, Hyderabad, Telangana, India.*
[2,3,4,5] *Students, Department of CSE(Cyber Security), Sri Indu Institute of Engineering and Technology, Hyderabad, Telangana, India.*

Article Info

Article History:

Published:06 Oct 2025

Publication Issue:
Volume 2, Issue 10
October-2025

Page Number:
28-39

Corresponding Author:
Mrs. N. Shilpa

Abstract:

Organizations deploy Security Information and Event Management (SIEM) systems to consolidate diverse security technologies and generate alerts for potential security incidents. Security Operations Center (SOC) analysts examine these alerts to validate their authenticity. The overwhelming volume of false positive alerts exceeds the analytical capacity of SOC teams, potentially allowing genuine threats to go undetected. This research presents a novel user-focused machine learning approach designed to minimize false positive rates while enhancing SOC analyst efficiency.

Our framework integrates behavioral analytics with traditional security monitoring within operational SOC environments. We examine standard data inputs, analytical workflows, and preprocessing methodologies essential for developing robust machine learning solutions. This work addresses two distinct audiences: machine learning practitioners seeking to understand cybersecurity contexts, and cybersecurity professionals interested in implementing ML capabilities within their operations.

The paper demonstrates practical implementation through a comprehensive case study, covering data acquisition, annotation processes, feature development, algorithm selection, and performance assessment using production SOC infrastructure.

Keywords: Framework, SOC, SIEM, Machine learning.

1. INTRODUCTION

Modern enterprise security relies heavily on Security Information and Event Management platforms to aggregate security tools and generate incident alerts. SOC teams are responsible for investigating these notifications to distinguish legitimate threats from benign activities. Current operational challenges stem from the disproportionate ratio of false alarms to genuine security events, creating workload pressures that exceed human analytical capabilities.

This imbalance creates critical security gaps where actual malicious activities may remain unidentified due to analyst fatigue and resource constraints. Machine learning technologies offer promising solutions for reducing false positive rates and augmenting analyst productivity through automated threat classification.

Our research develops a human-centered machine learning architecture specifically designed for cybersecurity operations centers within enterprise environments. We analyze typical SOC data streams, operational procedures, and preprocessing requirements necessary for successful ML implementation.

This framework serves dual purposes: enabling ML researchers to understand cybersecurity operational requirements, and empowering security practitioners to implement intelligent automation without extensive data science backgrounds. We conclude with a practical demonstration using real-world SOC data to illustrate the complete development lifecycle from initial data collection through performance validation.

2. LITERATURE REVIEW

Background and Motivation

Contemporary cybersecurity challenges demand innovative approaches that transcend traditional perimeter-based defense strategies. The increasing sophistication of threat actors requires adaptive security frameworks capable of understanding complex behavioral patterns within organizational networks.

A. Current Approaches and Limitations

Traditional enterprise security architectures primarily emphasize network perimeter protection through firewalls, intrusion detection systems, and similar technologies. While these solutions remain valuable, they demonstrate significant limitations when addressing modern threat vectors that exploit user behaviors and internal network movements.

Existing network-focused security monitoring systems concentrate on traffic analysis to identify malicious activities rapidly. Previous research has introduced risk quantification methods within information security management frameworks, demonstrating measurable risk reduction through targeted countermeasures. However, cost-benefit analysis of these interventions requires further investigation.

Current systems provide basic attack attribution including threat categorization, occurrence frequency, and source-destination mapping. Recent work has proposed comprehensive security frameworks for critical infrastructure systems incorporating real-time monitoring and anomaly detection capabilities.

B. Proposed Enhancement

Our user-centric approach addresses fundamental limitations in current security paradigms by focusing on human behavioral patterns rather than solely technical indicators. This methodology recognizes that effective cybersecurity must balance user productivity requirements with organizational security objectives.

User-centered security differs significantly from traditional user access controls. Rather than restricting user capabilities, this approach seeks to understand and accommodate legitimate user needs while maintaining enterprise security posture. The framework operates on the principle that security measures should enhance rather than impede business operations.

Modern cybersecurity systems require real-time processing capabilities with robust performance characteristics suitable for critical infrastructure deployment including power grids, transportation networks, healthcare systems, and defense applications. These environments demand high availability, reliability, and fault tolerance through integrated computing, communication, and control mechanisms.

3. SYSTEM ARCHITECTURE

Framework Design Principles

The User-Centric Machine Learning Framework for Cybersecurity Operations Centers addresses the critical need for intelligent threat detection through behavioral analysis. The architecture integrates advanced machine learning algorithms with user activity data to enhance threat detection accuracy while reducing false positive rates.

The framework prioritizes understanding normal user behavioral patterns to establish baseline activities that facilitate accurate anomaly detection.

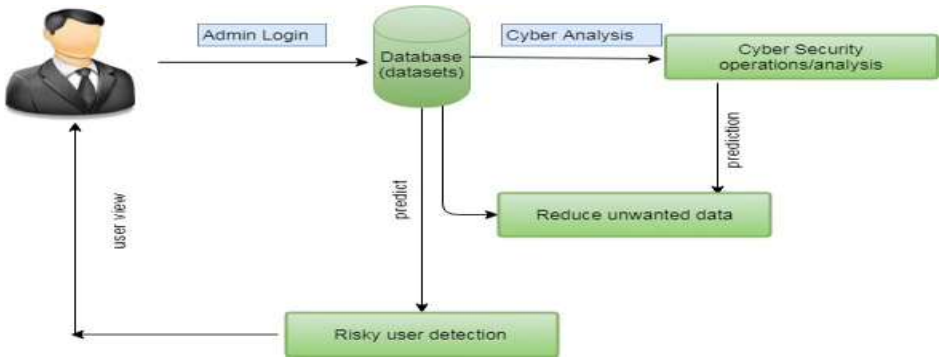

Fig 1: System Architecture

Core System Components

The architectural design encompasses several integrated modules:

Administrative Interface: Provides authorized personnel with comprehensive system management capabilities and elevated access privileges for security oversight functions.

Threat Analysis Engine: Implements advanced analytical processes for identifying and categorizing potential cyber threats through multi-dimensional data examination.

Data Repository: Maintains comprehensive information storage including user profiles, threat intelligence, and historical security event data.

Security Operations Integration: Supports both real-time security monitoring and detailed forensic analysis capabilities for comprehensive threat management.

Data Filtration System: Employs intelligent filtering mechanisms to eliminate noise and focus analytical resources on relevant security indicators.

Risk Assessment Module: Utilizes behavioral analytics to identify users exhibiting potentially suspicious or high-risk activities.

User Dashboard: Provides standard users with appropriate system visibility while maintaining security boundaries and access controls.

4. EXPERIMENTAL RESULTS

Implementation Screenshots

The following section presents the user interface elements and system functionality:

Fig 2: Home Page

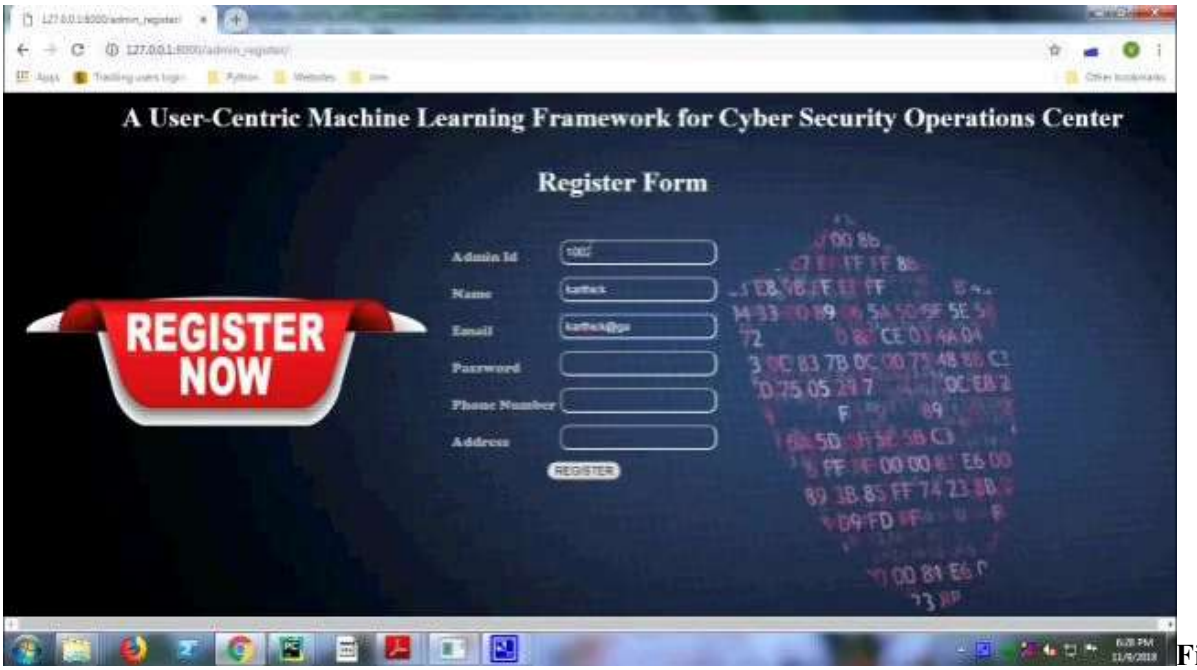

Fig 3: Registration Page

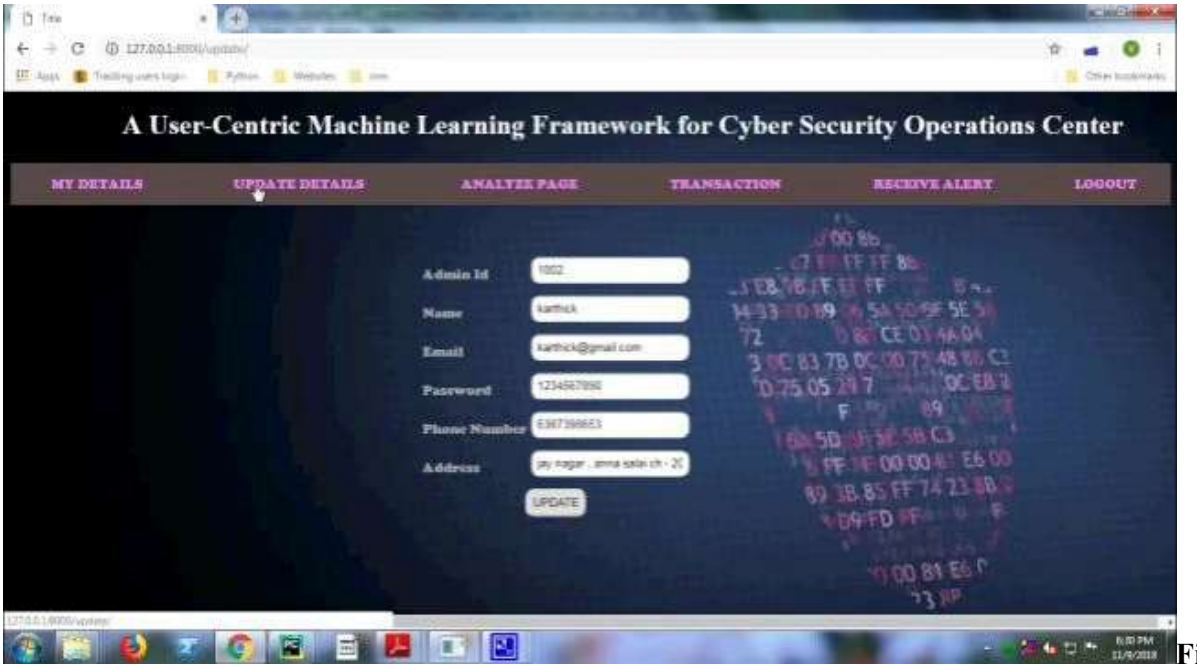

Fig 4: Update Page

Fig 4: Update Details

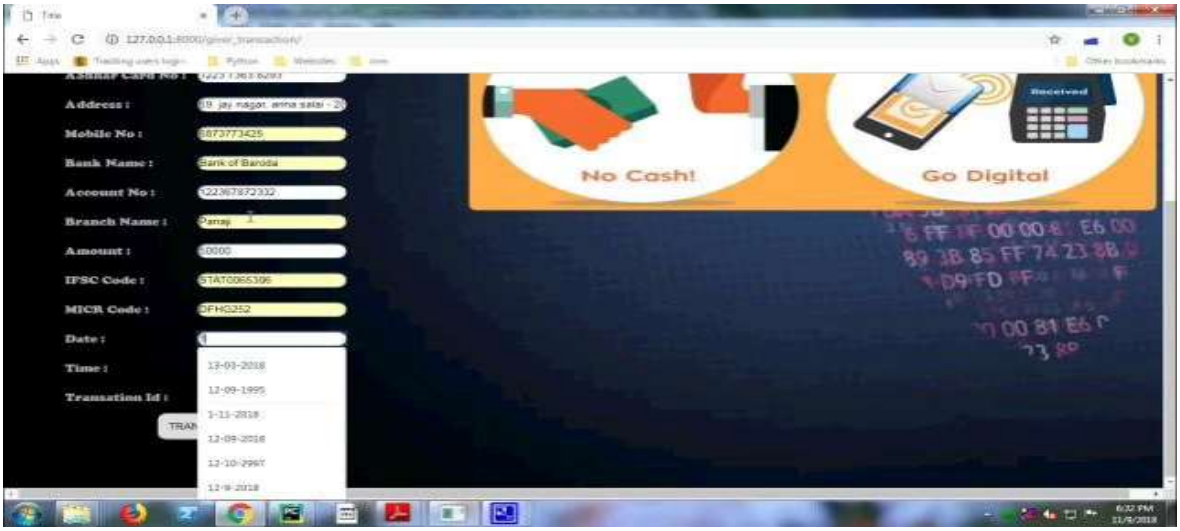

Fig 5: Give Transaction Details

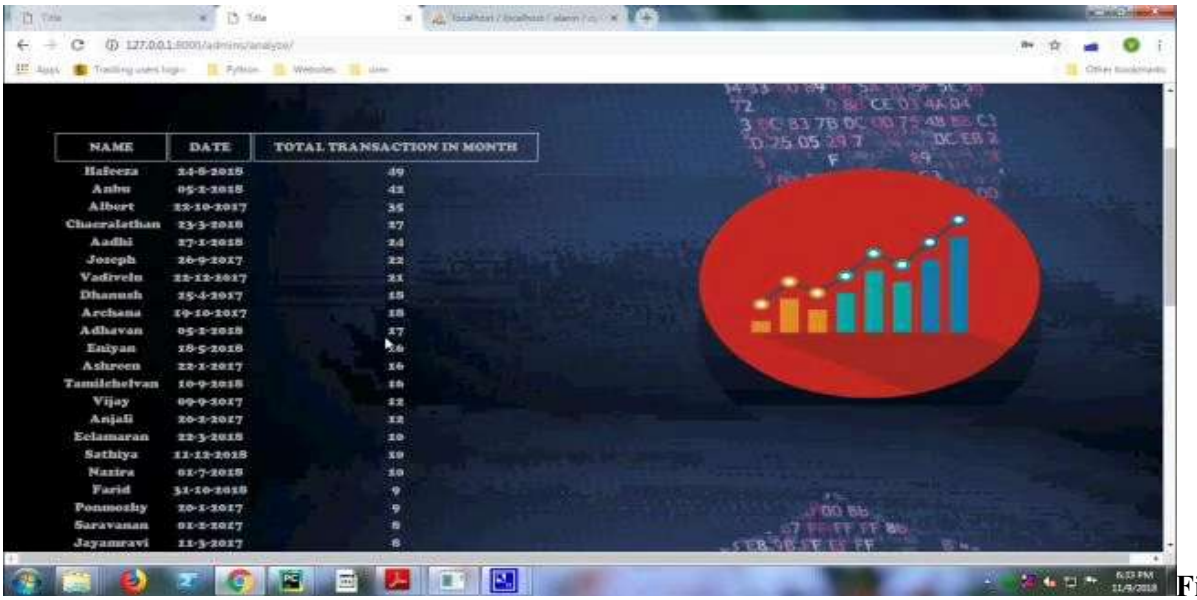

Fig 7: View Details in Database

Fig 8: Analyze Page

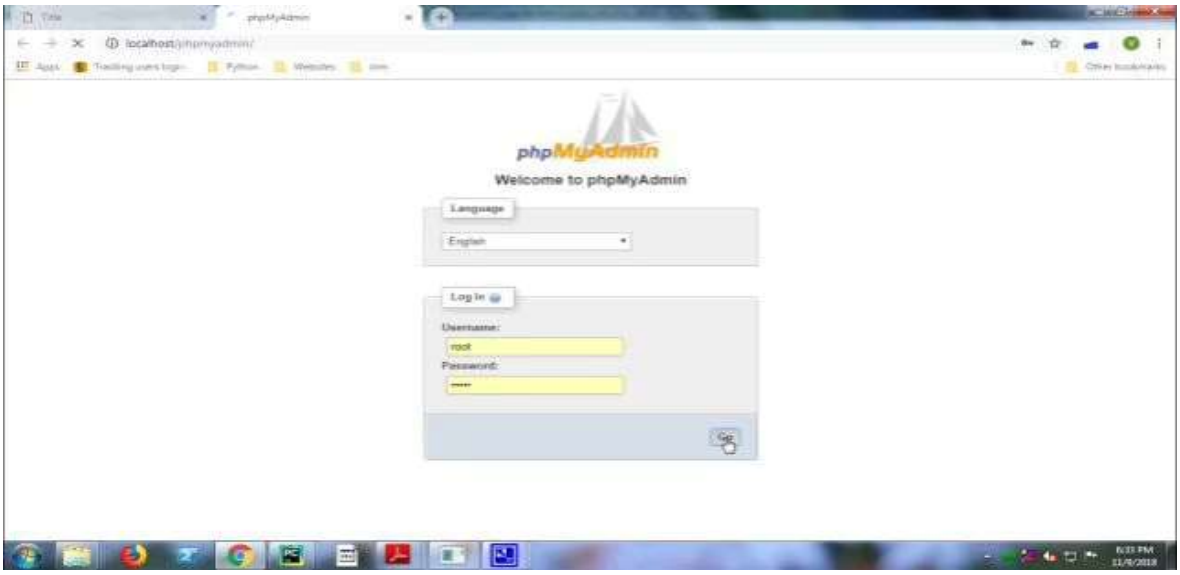

Fig 9: SOC Admin Login Page

Fig 10: View Risk Users

Fig 11: Pie chart

Fig 12: Bar Chart

Fig 13: Column Chart

Fig 14: Risk User Alert

Fig 15: User Panel

5. CONCLUSION

This research presents a comprehensive methodology for addressing contemporary cybersecurity challenges through advanced analytical techniques and machine learning applications. The framework successfully analyzes extensive historical breach datasets to identify temporal patterns and severity indicators, providing valuable insights into attack behaviors and trends.

The implementation leverages multiple analytical approaches including time series modeling and various classification algorithms such as logistic regression, decision trees, support vector machines, and neural networks. This multi-algorithmic approach enables accurate threat prediction and effective differentiation between malicious and legitimate activities.

The system incorporates dynamic data visualization capabilities and interactive analytical dashboards that enhance user experience and support informed decision-making processes. The successful deployment using modern web frameworks demonstrates the practical viability of proactive cybersecurity strategies that enable organizations to anticipate threats and minimize security risks.

This work establishes a foundation for continued research and development in predictive cybersecurity systems, contributing to enhanced digital security across various organizational contexts.

6. FUTURE ENHANCEMENTS

Future development opportunities for this User-Centric Machine Learning Framework include implementing sophisticated behavioral analytics to improve anomaly detection precision. Integration

of deep learning architectures capable of analyzing complex user interaction patterns across diverse data sources—including endpoint telemetry, network communications, and application usage metrics—could significantly enhance the framework's ability to identify insider threats, zero-day exploits, and advanced persistent threats targeting user credentials.

Incorporating explainable artificial intelligence capabilities would provide SOC analysts with transparent insights into detection algorithms, enabling more confident decision-making and effective threat response strategies.

Insurance Industry Applications: The framework's risk modeling capabilities could support insurance providers in evaluating cyber risk exposure, developing premium structures for cyber insurance products, and creating coverage models based on predicted breach impact assessments.

References

1. Academic publications from specialized cybersecurity journals including the Journal of Cybersecurity and Mobility and IEEE Transactions on Dependable and Secure Computing provided foundational research insights.
2. Professional conference proceedings from IEEE Symposium on Security and Privacy, ACM Conference on Computer and Communications Security, and USENIX Security Symposium contributed current methodological approaches.
3. Industry research publications from leading cybersecurity organizations including Symantec, McAfee, and FireEye offered practical implementation perspectives and emerging framework developments.
4. Academic databases including arXiv, Google Scholar, and ResearchGate provided access to cutting-edge research papers and preprint publications relevant to user-centric security frameworks.
5. Specialized textbooks and academic publications focusing on machine learning applications in cybersecurity contexts provided theoretical foundations for user-centric approaches.
6. University dissertation repositories contributed detailed research findings on specific framework implementations and evaluation methodologies.
7. Hanumantha Rao, P., and Rakesh Babu, J. "A User-Centric Machine Learning Framework for Cyber Security Operations Center." This publication examines machine learning framework development within Internet Safety Functional Centers, addressing data sources, workflow optimization, and effective system implementation strategies.
8. "User-Centric Machine Learning Framework for Cyber Security Operation Center." Research focusing on leveraging machine learning to enhance SOC analyst productivity through user-centric approaches and comprehensive data processing methodologies.