Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 14 Issue 03s, 2025

CogniLock : Bridging Cognitive Threat Insights and AI Sentinel Defence

[1]Prof. Bhakti Thakre, [2]Mahek Sheikh, [3]Rutuj Charde, [4]Akansha Bhajipale

[1,2,3,4] Department of Computer Science and Engineering (Cyber Security), St. Vincent Pallotti College of Engineering and Technology, Nagpur , Maharashtra , India – 441108

Emails: [1]bthakre@stvincentngp.edu.in , [2]iamahek.sheikh.786@gmail.com , [3]rutuj28charde@gmail.com , [4]akanshabhajipale@gmail.com

Peer Review Information

Submission: 05 Nov 2025

Revision: 25 Nov 2025

Acceptance: 17 Dec 2025

Keywords

Cognitive Security, Artificial Intelligence, Threat Intelligence, Digital Firewall, Identity Protection, Email Breach Detection, Password Strength Analysis, LinkedIn Impersonation Detection, Cyber Threat Intelligence (CTI), Machine Learning, SaaS Cybersecurity Platform, Personal Data Protection, AI Sentinel Defence, Cyber Awareness, Automated Threat Mitigation.

Abstract

In the rapidly evolving digital landscape, individuals and organizations face an increasing range of identity-based and cognitive cyber threats such as credential leaks, impersonation, and social media exploitation. Traditional cybersecurity solutions primarily focus on enterprise network defence, leaving a critical gap in personalized, intelligent protection mechanisms. This paper presents CogniLock, a SaaS-based cybersecurity framework that bridges cognitive threat intelligence with an AI-driven sentinel defines system. CogniLock operates through two primary phases: a Threat Intelligence Dashboard and a Digital Firewall. The dashboard aggregates and visualizes real-time malicious Indicators of Compromise (IOC) include IP addresses, URLs, domain names, and file hashes from reliable sources such as Alien Vault OTX, Abuse IPDB, and URL Haus. The Digital Firewall, on the other hand, offers proactive personal security modules such as email breach detection, password strength and exposure assessment, LinkedIn impersonation monitoring through cognitive similarity matching, and integrated reporting tools for social media abuse via official cyber complaint portals. By combining cognitive analytics with automated AI defences, CogniLock improves situational awareness and enables users to identify, address, and react to identity-threats cyber threats efficiently. The proposed framework contributes toward establishing an intelligent, adaptive, and user-centric model for modern digital protection.

Introduction

The exponential growth of digitalization has led to a corresponding rise in cyber threats that target both organizations and individuals. As the modern world increasingly relies on online identities, cloud-based services, and social platforms, adversaries have shifted their focus from traditional network exploitation to more sophisticated identity-centric attacks. These threats, including credential breaches, impersonation, phishing, and social media exploitation, pose significant risks to personal privacy and organizational integrity. Conventional cybersecurity solutions primarily focus on enterprise infrastructure and perimeter defines, leaving individual users vulnerable to targeted digital identity misuse.

To address this emerging challenge, there is a pressing need for intelligent and adaptive security systems that not only detect malicious activities but also understand their cognitive and behavioural context. CogniLock has been

conceptualized and developed as a comprehensive cybersecurity framework that bridges cognitive threat insights with AI-driven sentinel defence. It introduces a dual-layered approach comprising a Threat Intelligence Dashboard and a Digital Firewall.

The Threat Intelligence Dashboard collects, aggregates, and visualizes malicious Indicators of Compromise (IOC) like IP addresses, domain names, URLs, and file hashes from reliable sources including AlienVault, AbuseIPDB, and URLHaus. This module enables analysts and users to gain real-time situational awareness of the evolving threat landscape.

The Digital Firewall, in contrast, focuses on personal cybersecurity. It integrates multiple protective modules—such as email breach detection, password strength analysis, and LinkedIn impersonation monitoring—to safeguard users from credential theft and identity fraud. Additionally, the platform provides an integrated reporting interface that connects users with official cyber complaint portals like the CEIR and Sanchar Sathi, streamlining the process of reporting and mitigating digital abuse incidents.

By combining artificial intelligence, machine learning, and cognitive analytics, CogniLock aims to provide proactive, context-aware defense mechanisms that empower users to detect and eliminate dangers prior to inflicting damage. The system's user-centric design bridges the gap between enterprise-grade threat intelligence and individual digital safety, marking a step toward the realization of an intelligent, autonomous, and adaptive cybersecurity ecosystem.

Objectives

The main aim of this research is to create and implement a smart cybersecurity structure that merges cognitive threat understanding with AI-powered protection systems to protect individuals from identity-related and digital threats. The specific objectives of the CogniLock system are as follows:

- To develop a centralized Threat Intelligence Dashboard that aggregates and visualizes real-time malicious Indicators of Compromise (IOC) like IP addresses, domain names, URLs, and file hashes from trusted cybersecurity data sources including Alien Vault OTX, Abuse IPDB, and URL Haus.
- To implement a Digital Firewall that provides user-oriented security services focused on identity and data protection.
- To design an Email Breach Detection module that verifies whether a user's email address has been exposed in any known data breach and provides appropriate security recommendations.
- To build a Password Strength and Breach Analysis system capable of evaluating password robustness, detecting previously compromised credentials, and suggesting strong alternatives for enhanced account protection.
- To create a LinkedIn Vault feature that identifies potential impersonation attempts by comparing user-submitted profile information with publicly available data, ensuring protection against fraudulent social media accounts.
- To integrate a Secure Reporting Mechanism that enables users to file official complaints regarding social media misuse or identity theft through verified portals such as CEIR, Sanchar Sathi, and other government-linked cybercrime platforms.
- To utilize Artificial Intelligence and Machine Learning techniques for cognitive analysis, pattern recognition, and automated threat detection thus improving the system's flexibility and accuracy.
- To encourage user awareness and proactive defence by providing personalized security insights, encouraging safer digital practices, and bridging the gap between enterprise-grade cybersecurity and individual digital safety.

Literature Review

The idea of CTI and the dissemination of Indicators of Compromise (IOC) has become increasingly prominent in recent years. Studies highlight that while structured threat intelligence enhances situational awareness, it also faces challenges such as data redundancy, false positives, and lack of automation [1]. These challenges emphasize the importance of efficient aggregation and normalization mechanisms, forming the foundation for CogniLock's Threat Intelligence Dashboard.

Improving IOC quality and contextual relevance has become a central research focus. Several works have proposed enrichment and scoring techniques to assess the reliability and source credibility of threat indicators, reducing false positives and improving actionable insights [2]. Such quality enhancement directly supports CogniLock's design approach, which relies on contextual enrichment of IOCs gathered from multiple intelligence sources like AlienVault and AbuseIPDB.

The limitations of static indicators have led to proposals for machine learning–based cognitive threat detection, where model outputs and learned patterns are treated as higher-level indicators of compromise [3]. This approach inspired CogniLock's use of ML-driven contextual analysis to supplement conventional IOC-based threat visualization.

Credential compromise remains a major cybersecurity concern, leading to the development of privacy-preserving breach detection protocols [4]. These protocols allow users to verify if their credentials have been leaked without exposing sensitive information. CogniLock implements a similar principle for its email breach detection feature, ensuring privacy and user trust.

The practical use of k-anonymity-based password verification models, such as those used by HaveIBeenPwned, has proven to be an efficient method to check for password breaches while maintaining anonymity [5]. However, studies also note potential attack surfaces and privacy trade-offs when implementing deterministic query models [6]. CogniLock mitigates such limitations by combining breach detection with strong password recommendations and client-side strength analysis.

Machine learning techniques have also been applied to account takeover (ATO) and identity fraud detection, showing significant promise in detecting anomalies in login patterns, IP reputations, and behavioural features [7]. These insights form the foundation for CogniLock's AI Sentinel Defence, which proactively identifies potential account misuse or impersonation attempts.

Recent research on fake social media account detection has proposed ensemble and deep learning models that analyze user metadata, posting patterns, and image similarity to detect fraudulent profiles [8]. Similarly, studies on profile cloning and impersonation have explored NLP-based semantic similarity and hybrid matching algorithms for identifying cloned professional profiles, particularly on platforms like LinkedIn [9], [10]. CogniLock's LinkedIn Vault module draws inspiration from these works, employing machine learning to detect public profile similarities that may indicate impersonation.

Overall, existing research establishes the technical foundation for CogniLock's twofold architecture. By integrating threat intelligence aggregation with AI-based digital identity protection, CogniLock bridges enterprise-grade cybersecurity principles with user-centric cognitive defence mechanisms—providing a proactive, automated shield against modern cyber threats.

Methodology

The methodology of CogniLock is designed to integrate real-time threat intelligence aggregation with a user-centric AI-driven digital firewall. The system architecture follows a modular approach, allowing secure, scalable, and adaptive threat detection and identity protection. The methodology can be divided into two primary phases: the Threat Intelligence Dashboard and the Digital Firewall, each comprising several submodules.

Phase 1: Threat Intelligence Aggregator (Dashboard)

Data Collection:

CogniLock collects Indicators of Compromise (IOC) from multiple reputable threat intelligence sources including Alien Vault OTX, Abuse IPDB, URL Haus, and other open-source feeds. These sources provide real-time IP addresses, domains, URLs, and file hashes associated with malicious activities.

Data Normalization and Enrichment:

Collected raw IOCs are pre-processed using a normalization pipeline. Redundant or duplicate entries are removed, and each IOC is enriched with metadata such as:

- Geolocation and Autonomous System Number (ASN) of IPs.
- Threat classification tags (malware family, botnet, phishing).
- Source reliability score and first-seen timestamp.

Storage and Indexing:

Normalized IOCs are stored in a MongoDB database with indexing for efficient search, filtering, and correlation. The system supports real-time querying and batch updates, enabling analysts and users to retrieve threat information quickly.

Visualization and Alerting :

A React + MUI frontend provides a dynamic dashboard for visualizing threat data. Features include:

- IOC filtering by type, source, or risk score.
- Timeline and geographic visualization of threats.
- Watch list-based alerts: users can register their IPs, domains, or assets to receive notifications of suspicious activity.

Phase 2: Digital Firewall

The Digital Firewall is a user-facing module that provides identity and credential protection. It consists of four submodules:

Email Breach Detection:

- Users input their email address into the system.
- The system queries local and third-party breach databases to identify whether the email has been exposed in any known breach.
- Results include breach details (data types exposed, breach date) and remediation suggestions.

Password Strength and Breach Assessment:

- Passwords are evaluated against a strength metric considering entropy, common patterns, and length.
- The system checks for previously compromised passwords using privacy-preserving k-anonymity techniques.
- Weak or breached passwords trigger suggestions for strong, unique passwords.

LinkedIn Vault (Impersonation Detection):

- Users fill a consent-based form that mirrors LinkedIn profile fields (name, headline, bio, profile photo).
- An ML-powered similarity engine compares the submitted profile against publicly available LinkedIn profiles using:
  - Textual similarity (NLP embeddings of name, bio, headline).
  - Image similarity (face-matching algorithms).
- The system calculates a confidence score indicating potential impersonation. If high-risk matches are found, the user receives notifications with recommended actions.

Social Media & Portal Reporting:

- Users can report misuse of social media accounts or identity fraud via a two-step workflow:
  1. Submission of reporter details with a live photo for verification.
  2. Automated routing or pre-filling of official complaint portals (e.g., CERI, Sanchar Sathi).
- Reports are logged with a tracking ID, enabling users to monitor status and actions taken.

Integration of AI and Cognitive Analysis

CogniLock leverages AI and machine learning to enhance detection and decision-making:

- Behavioral analytics and cognitive matching are applied in the LinkedIn Vault and alerting modules.
- Anomaly detection techniques monitor unusual account activity, correlating it with IOC feeds for enhanced risk assessment.
- ML models are retrained periodically to adapt to emerging threats and concept drift.

Security, Privacy, and Compliance Measures

- All user data is encrypted in transit and at rest.
- Explicit user consent is obtained for profile scanning and social media reporting.
- Rate-limiting and CAPTCHA mechanisms are implemented to prevent abuse of the platform.
- Data minimization principles are followed; user-submitted data can be deleted upon request.

System Architecture

The complete architecture of CogniLock system is depicted in Fig.1. Which demonstrates the data flow, module interaction, and core processing logic that enables cognitive threat intelligence and AI-driven digital defence. The system is divided into five major functional components:

1. Data Sources and Injection:

This layer gathers data from multiple external threat intelligence sources such as AlienVault OTX, AbuseIPDB, and URLHaus, along with user-submitted information like email addresses, LinkedIn profiles, and social media abuse reports. Data is securely transmitted through an encrypted pipeline.

2. Core Processing and Intelligence Modules:

The collected data is normalized, pre-processed, and enriched with metadata. The Threat Intelligence Dashboard visualizes indicators of compromise (IOC), while the AI/ML Cognitive Engine performs pattern recognition, cognitive similarity analysis, and behavioural anomaly detection.

3. Digital Firewall – Personal Security Modules:

This module includes the Email Breach Detection, Password Strength and Exposure Assessment, and LinkedIn Vault for impersonation detection. A secure reporting mechanism allows users to escalate incidents related to identity misuse or account compromise.

4. User Interface and Interaction:

The frontend is built using React + MUI, enabling IOC filtering, timeline tracking, and alert notifications. Users can engage with the system via user-friendly dashboards, monitor real-time alerts, and file abuse reports.

5. Actionable Insights and Reporting:

This layer consolidates threat intelligence insights and generates actionable reports. The output integrates with national reporting portals such as CEIR and Sanchar Sathi for further cybercrime escalation.

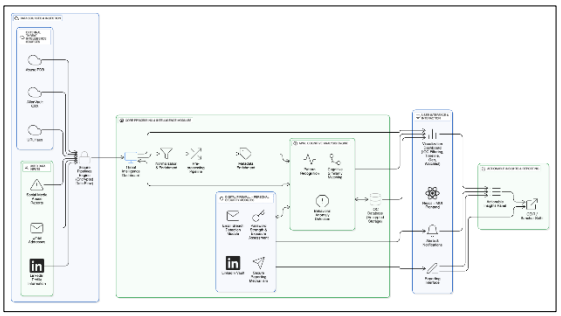

Fig.1. CogniLock System architecture

Result

The CogniLock system was evaluated across its functional modules to assess usability, interface design, and effectiveness in detecting digital threats and identity misuse. The results demonstrate the system's capability to integrate multiple cybersecurity layers into a single, intelligent SaaS platform.

A. System Interface and Dashboard

The main interface of CogniLock, as shown in Fig. 2 & Fig.3, represents the home dashboard that bridges enterprise threat intelligence and personal identity protection. It displays real-time metrics, such as processed IOCs per day, protection uptime, and threat detection accuracy, which highlight the platform's analytical efficiency and scalability.

Fig.2. System Interface

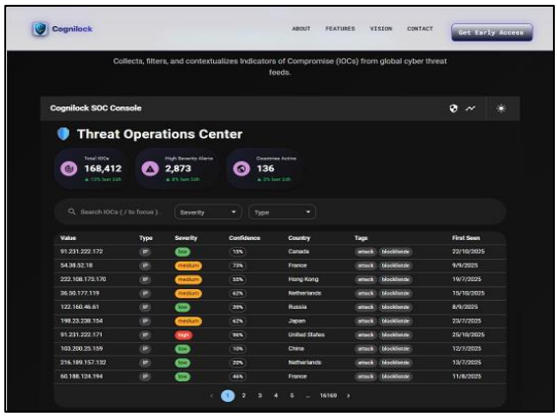

Fig.3. Threat Intelligence Dashboard

B. Email Breach Detection Module

The Email Breach Detector is a vital component of the Digital Firewall module. As shown in Fig. 4, the user can input their email address to verify whether it has been exposed in any known data breach, leveraging the CogniLock API for validation. This functionality enhances user trust and supports proactive cyber hygiene.

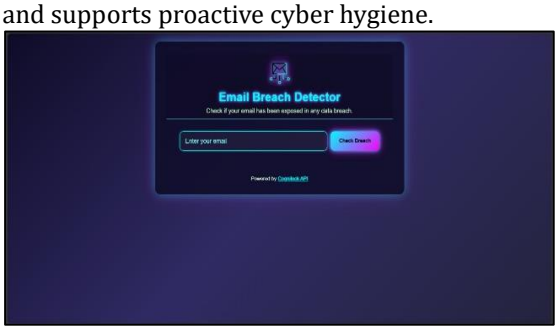

Fig.4. Email Breach Detection

C. Password Strength and Breach Detection Module

The CogniLock Password Meter is an interactive feature designed to assess password strength and validate breach exposure through real-time analysis. It utilizes the integrated API and local hashing techniques to verify whether the entered password has been found in any known data leaks and to measure its entropy-based strength. As shown in Fig. 5, a weak password triggers a red indicator, warning the user about poor strength and potential vulnerability. The system also confirms that the password has not been found in any breach, ensuring data integrity through API verification

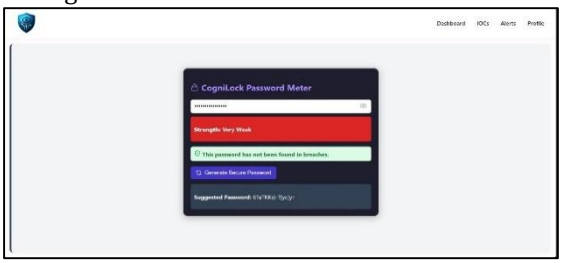

Fig. 5. Password Meter showing weak password

In contrast, Fig. 6 illustrates a strong password example. The module provides constructive feedback, recommending best practices such as avoiding certain special characters and offering an auto-generated secure alternative. This illustrates the system's ability to improve user security awareness by providing actionable recommendations.

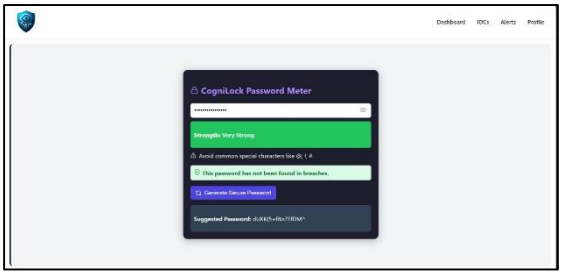

Fig. 6. Password Meter showing strong password

D. Social Media & Portal Reporting:

The Social Media Reporting Portal shown in Figure 7 displays CogniLock's unified interface for cyber-incident reporting. It integrates official platforms such as TAFCOP, Sanchar Saathi, CEIR, WhatsApp Support, and StopNCII.org into a single dashboard.

This feature enables users to quickly report issues like SIM misuse, impersonation, hacked accounts, online fraud, and non-consensual content. The results confirm that CogniLock enhances user safety by simplifying the reporting process and providing direct access to trusted cyber-safety services.

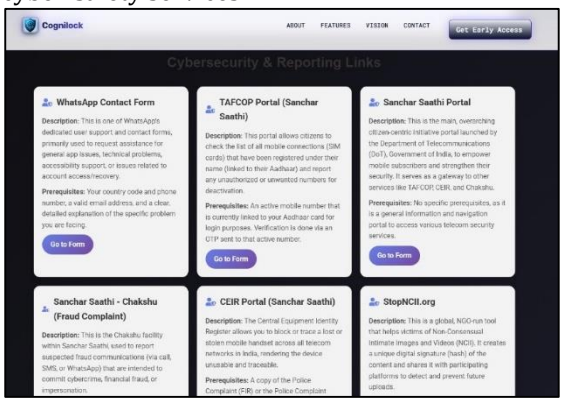

Fig.7. Social Media Reporting Portal

Conclusion

In this paper, we presented CogniLock, a comprehensive SaaS-based cybersecurity framework that integrates cognitive threat intelligence with AI-driven sentinel defence mechanisms. By combining a Threat Intelligence Dashboard with a Digital Firewall, CogniLock offers a dual-layered approach that addresses both enterprise-grade threat analysis and individual user protection. The system effectively aggregates real-time Indicators of Compromise (IOCs) from trusted sources, normalizes and enriches the data, and provides actionable insights through an intuitive dashboard.

On the user-centric side, CogniLock enhances digital safety by offering email breach detection, password strength assessment, LinkedIn impersonation monitoring, and social media reporting tools. The combination of machine learning and cognitive analysis allows for the early identification of identity theft, impersonation, and credential leakage, equipping users to respond promptly with corrective measures.

Overall, CogniLock bridges the gap between traditional threat intelligence systems and personal digital defence, offering a scalable, adaptive, and privacy-conscious solution for modern cyber threats. Future enhancements may include real-time deepfake and synthetic voice detection, continuous AI-driven alert triage, and expanded integration with additional social and professional platforms, further strengthening the platform's ability to safeguard users' digital identities in an evolving threat landscape.

Acknowledgment

The successful execution of this research project would not have been possible without the support, guidance, and encouragement from many individuals and organization. We would like to express our sincere gratitude to our mentor whose expertise and valuable insights guided us throughout the development of the CogniLock system.

We also extend our appreciation to the various open-source threat intelligence platforms and API providers, including AlienVault, AbuseIPDB, URLHaus, and HaveIBeenPwned, whose data and services were instrumental in implementing the Threat Intelligence Dashboard and Digital Firewall modules.

Finally, we are grateful to our colleagues, friends for their continuous motivation, constructive feedback, and unwavering support during the research and development process. Their encouragement has been invaluable in bringing CogniLock from concept to a functional, real-world cybersecurity solution.

References

B. Jin, A. Rashid, and M. S. G. H. A. Alazab, "Does Sharing Cyber Threat Intelligence Provide Real Benefits?," in the Proceedings of the Network and Distributed System Security Symposium (NDSS), 2022.

S. S. Chen, "Enhancing the Quality of Indicators of Compromise Through STIX and Confidence Scoring Mechanisms," Computers & Security, vol. 125, pp. 103011–103025, 2024.

D. Preuveneers, W. Joosen, and S. Latré, "Utilizing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence," MDPI Cybersecurity and Privacy, vol. 3, no. 2, pp. 85–101, 2021.

L. Li, A. K. Dutta, and K. R. Choo, "Credentials Compromise Checking Protocols," arXiv preprint, arXiv:1905.12029, 2019.

T. Hunt and Cloudflare Team, "Using k-Anonymity to Validate Leaked Passwords," Cloudflare Technical Report, 2018.

S. Alrubaian, M. Al-Qurishi, and A. Alamri, "The Cost of Having Been Pwned: Security Risks of Breached Password Lookup Services," Journal of

Information Security and Applications, vol. 78, pp. 103561–103575, 2023.

M. Raj and P. Thomas, "Detecting Account Takeover (ATO) in Fintech Companies Using Machine Learning," International Journal of Scientific and Applied Technologies, vol. 9, no. 3, pp. 112–118, 2022.

W. Dracewicz and M. Leszczuk, "Detecting Fake Accounts on Social Media Portals Using AI-Based Behavioral Analysis," MDPI Electronics, vol. 13, no. 7, pp. 1542–1557, 2024.

Sunkara, S. P. (2025). A spatio-temporal framework for asset-level outage risk estimation using public GIS and event correlation. *International Journal of Computer Engineering and Technology (IJCET), 16*(1), 4211–4227. https://doi.org/10.34218/IJCET_16_01_286

I. Mohiuddin, A. Hussain, and R. Akram, "Ensemble Techniques for Detecting Profile Cloning Attacks on Social Media," *PeerJ Computer Science*, vol. 8, e1209, 2025.

Hazarika, I., Saoji, S., Bhandari, R. B., Jorvekar, G., Rao, P. H., & Porwal, T. (2025). Mapping resilience pathways: A conceptual framework for portfolio risk management in microenterprise lending during economic shocks. Enterprise Development and Microfinance, 35(1), 1–20. https://doi.org/10.3362/edm.v35i1.5

A. Bhardwaj and R. Verma, "Detecting and Understanding the Impact of Profile Cloning on Social Media Platforms: A Case Study of LinkedIn," *International Journal of Cyber Forensics and Advanced Threat Analysis*, vol. 4, no. 1, pp. 45–56, 2025.

M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Deep learning for cybersecurity: A comprehensive survey," *Computers & Security*, vol. 106, pp. 102–115, 2021.

A. Ali, M. Z. Khan, and S. Anwar, "Intelligent phishing detection using machine learning," *IEEE Access*, vol. 8, pp. 213670–213682, 2020.

N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, "Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset," *Future Generation Computer Systems*, vol. 109, pp. 176–189, 2021.