Secure Persona Prediction and Data Leakage Prevention: A Comprehensive Review

Vishakha Rathod[1], Shifa Shaikh[2], Dhiraj Ahire[3], Purushottam Thombre[4], Prof. P.B. Palve[5]
Department of Computer Engineering, Adsul's Technical Campus, Ahilyanagar Savitribai Phule Pune University

***Abstract*—In the era of rapid digitalization, safeguarding user identity and preventing unauthorized data access have become critical challenges. This paper presents an overview of Secure Persona Detection and Data Leakage Prevention System, designed to enhance cybersecurity through behaviour-based identity verification and proactive threat mitigation. The proposed framework utilizes machine learning models to analyse user activity patterns, detect anomalies, and prevent potential data breaches in real time. It further integrates encryption, role-based access control, and keyword-based leakage monitoring to ensure confidentiality and integrity of sensitive information. The system's user-friendly dashboard enables administrators to visualize data flow, monitor alerts, and manage access permissions efficiently. This study highlights the growing importance of intelligent, adaptive security systems capable of balancing usability and protection in modern networked environments.**

***Index Terms*—secure persona detection, data leakage prevention, machine learning, behavioral analysis, data security, encryption**

I. INTRODUCTION

In the era of rapid digital transformation, the protection of personal identities and sensitive information has become one of the most critical aspects of cybersecurity. With the widespread use of online platforms, social media, and cloud-based services, enormous amounts of user-generated data are exchanged every second, increasing the risk of data breaches and identity theft [1]. *Secure persona detection* aims to authenticate and verify legitimate users based on behavioural and contextual data, while *data leakage prevention (DLP)* focuses on identifying, monitoring, and protecting sensitive data from unauthorized disclosure [2].

The integration of artificial intelligence (AI), machine learning (ML), and natural language processing (NLP) has led to the development of intelligent security models capable of identifying unusual patterns and detecting impersonation or fraudulent behaviour [3]. These models leverage supervised and unsupervised learning techniques to classify user activities, detect anomalies, and prevent potential data misuse in real time [4]. Furthermore, cryptographic algorithms, blockchain-based identity management systems, and cloud access security brokers (CASB) are being utilized to strengthen the confidentiality and integrity of data transactions [5].

Despite these advancements, challenges such as evolving cyberattack strategies, privacy preservation, model interpretability, and the trade-off between security and usability persist [6]. Therefore, this paper presents a comprehensive review of current methods, frameworks, and technologies for secure persona detection and data leakage prevention. It further highlights research gaps and proposes future directions for building more robust and privacy-aware digital security architectures [7]

II. BACKGROUND AND KEY CONCEPTS

In the era of digital transformation, the exponential growth of online interactions has created a pressing need for systems that can ensure user authenticity and prevent information misuse. *Persona detection* refers to the process of identifying and validating the authenticity of a user's digital identity using behavioural, biometric, or contextual data. It plays a crucial role in minimizing fraudulent activities, fake accounts, and cyber impersonation. The ability to verify whether a user's actions align with their

established profile enables platforms to maintain trust and accountability.

On the other hand, *data leakage prevention (DLP)* focuses on protecting sensitive information from unauthorized access, transmission, or disclosure. With the increased integration of cloud computing and interconnected networks, unintentional data leaks have become a major threat to organizations and individuals. DLP systems use advanced encryption techniques, content inspection, and access control mechanisms to detect and block the transfer of confidential information through unsafe channels.

Integrating persona detection with data leakage prevention enables a dual-layered security model — one that not only authenticates users but also monitors data flow for potential risks. Machine learning algorithms, anomaly detection systems, and rule-based filters play a vital role in this integration by continuously learning user patterns and identifying deviations that might indicate malicious intent. This holistic approach enhances digital trust, mitigates insider threats, and ensures compliance with data protection regulations.

Such intelligent frameworks have broad applications in sectors like e-banking, healthcare, government systems, and corporate data management, where both identity verification and data confidentiality are critical.

Kim et al. (2019) proposed user behaviour modelling and anomaly detection for insider threat detection using daily activity summaries. Nasir et al. (2021) implemented a deep-learning model (LSTM + CNN) achieving high accuracy. Bertrand et al. (2022) used Bayesian Gaussian Mixture Models for unsupervised user detection. These studies demonstrate progress but also reveal usability and data availability challenges.

III. LITERATURE REVIEW

The rapid growth of digital communication has amplified the significance of ensuring privacy, authenticity, and data security across multiple domains. Several researchers have contributed toward developing robust frameworks for secure persona detection and mitigating risks associated with data leakage in online environments. This section summarizes key studies, identifies research gaps, and establishes the foundation for developing an integrated system addressing both security and privacy concerns.

Persona detection focuses on identifying genuine and fraudulent users based on behavioural, textual, or biometric patterns. Early research in this area primarily relied on statistical and linguistic analysis to detect impersonation or fake profiles [1]. These traditional models were limited by their inability to handle large-scale, unstructured social media data. With the evolution of artificial intelligence (AI) and machine learning (ML), more sophisticated methods such as deep neural networks (DNNs), convolutional neural networks (CNNs), and transformers have significantly improved accuracy in identity recognition and anomaly detection [2]. For example, hybrid models integrating textual and image-based features have shown remarkable performance in identifying malicious entities on social networking platforms [3].

In parallel, researchers have explored the domain of data leakage prevention (DLP) to ensure that sensitive information is not exposed, intentionally or accidentally. Traditional rule-based DLP systems focused on pattern matching and policy enforcement [4]; however, they often produced high false-positive rates and lacked adaptability to dynamic data patterns. Machine learning-driven DLP solutions have since emerged, leveraging anomaly detection, content inspection, and context-aware analysis to predict potential breaches before data is exfiltrated [5]. These adaptive models are capable of analysing multi-channel communication—such as emails, chat logs, and cloud storage—offering a proactive approach to security.

Recent literature emphasizes the integration of behavioural analytics and deep learning architectures for both persona detection and data leakage prevention. By analysing user behaviour, typing dynamics, and access patterns, systems can learn typical user profiles and identify deviations in real-time [6]. Techniques such as recurrent neural networks (RNNs) and graph-based analysis further enhance the contextual understanding of interactions, enabling the system to distinguish between legitimate and fraudulent access attempts [7]. These developments mark a transition from reactive defence mechanisms to predictive intelligence frameworks.

Moreover, steganography and cryptography have been widely employed to secure communication channels and conceal sensitive data from unauthorized users [8]. Steganographic techniques, when combined with

encryption algorithms, provide multi-layered protection by embedding information within images, audio, or text data, ensuring confidentiality and integrity [9]. Some studies also propose blockchain-based models to maintain immutable audit trails and ensure transparency in data transactions [10]. These integrated solutions contribute to stronger data governance and traceability across digital ecosystems. Despite these advancements, challenges remain in achieving a balance between detection accuracy and system performance. High computational costs, data imbalance issues, and adversarial attacks on ML models limit large-scale deployment [11]. Furthermore, privacy-preserving mechanisms such as federated learning and differential privacy are gaining attention to protect user data while maintaining model efficiency [12]. These approaches enable collaborative model training without exposing raw data, a critical feature for organizations managing sensitive user information.

The convergence of persona detection and data leakage prevention represents a promising direction for holistic cybersecurity frameworks. Integrating these domains through AI-driven solutions can offer adaptive, self-learning systems capable of identifying insider threats, preventing identity misuse, and safeguarding digital assets in real-time [13]. However, continuous research is needed to develop explainable AI models, improve scalability, and ensure compliance with global data protection standards such as GDPR and HIPAA [14].

In summary, existing literature highlights the progress in individual domains—persona detection and data leakage prevention—but limited studies have effectively merged the two into a unified security model. This research aims to bridge that gap by designing a framework that ensures both authenticity verification and secure information handling, thereby contributing to a safer digital environment.

IV. METHODOLOGY

The review methodology adopted for this paper involves a comprehensive analysis of existing research studies related to persona detection, user identity verification, and data leakage prevention techniques. Various peer-reviewed papers, IEEE conference proceedings, and UGC CARE indexed journals were referred to understand the evolution of secure systems. The selection criteria focused on studies employing artificial intelligence, machine learning, and encryption models for identity recognition and secure data handling. A comparative assessment was carried out based on the accuracy, scalability, and robustness of each approach. The reviewed works were categorized under behavioural analysis, biometric verification, and secure data transmission frameworks to identify the key patterns and limitations within current research trends.

V. DISCUSSION

From the literature reviewed, it is evident that traditional security frameworks are no longer sufficient to address modern cyber threats and identity theft. Deep learning-based persona detection methods have significantly improved accuracy and adaptability by learning from complex behavioural data. However, a critical challenge remains in balancing security and user convenience. Some models offer strong protection but increase computational cost, making real-time deployment difficult. Data leakage prevention systems often rely on encryption, but poor key management and insider threats continue to pose risks. The integration of multi-factor authentication, user profiling, and anomaly detection has shown promise in mitigating unauthorized access. However, a unified and adaptive system that ensures privacy, speed, and scalability is still needed.

VI. FUTURE SCOPE

Future research in secure persona detection and data leakage prevention should focus on designing lightweight, adaptive, and privacy-preserving models suitable for large-scale enterprise environments. Integration of blockchain technology for decentralized identity management and enhanced data integrity could further strengthen such systems. Additionally, incorporating federated learning and homomorphic encryption may allow secure training of models without compromising user data. The development of standardized benchmarks for evaluating security algorithms is another key direction. A human-centric approach, emphasizing ethical AI and user transparency, will ensure that emerging systems are both secure and socially responsible.

VII. CONCLUSION

In conclusion, the integration of secure persona detection and data leakage prevention mechanisms represents a crucial step toward ensuring privacy and trust in digital ecosystems. As modern networks handle vast amounts of sensitive data, the fusion of artificial intelligence, behavioural analytics, and encryption-based security frameworks has become essential to detect malicious activities and unauthorized access in real time. This review highlights how machine learning models, identity verification techniques, and multi-layered security approaches can significantly enhance user authenticity and reduce data breaches. Despite notable advancements, the field still faces challenges related to scalability, adaptive threat detection, and user transparency. Future developments should emphasize explainable AI, secure federated learning, and improved policy frameworks to balance user privacy with proactive data protection. Overall, the reviewed studies indicate that combining detection intelligence with robust preventive architectures can create a more secure and privacy-aware digital environment.

REFERENCES

[1] S. K. Singh and R. K. Dwivedi, "Machine learning-based anomaly detection for data leakage prevention systems," IEEE Access, vol. 9, pp. 13124–13135, 2021.

[2] P. Gupta and M. S. Khan, "Enhancing data privacy through intelligent access control mechanisms in cloud environments," Journal of Information Security and Applications, vol. 68, pp. 102–115, 2023.

[3] A. K. Sahu, S. Sinha, and D. Kumar, "Deep learning approaches for behavioural biometrics and persona identification," IEEE Transactions on Information Forensics and Security, vol. 17, no. 4, pp. 2456–2469, 2022.

[4] T. Banerjee, R. Singh, and A. Shukla, "Privacy-preserving identity verification using hybrid encryption and steganography," Computers & Security, vol. 120, 2022.

[5] N. Sharma and P. Bansal, "Role-based access control models for secure enterprise systems," International Journal of Computer Applications, vol. 182, no. 36, pp. 20–25, 2021.

[6] R. Patel and K. Jain, "AI-driven frameworks for insider threat detection in organizational networks," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9783–9795, 2021.

[7] J. Thomas and A. Bose, "Secure data sharing and leakage prevention using federated learning," Future Generation Computer Systems, vol. 145, pp. 85–98, 2024.

[8] L. Zhang, Y. Wang, and J. Zhao, "Blockchain-enabled data protection and traceability in distributed systems," IEEE Transactions on Industrial Informatics, vol. 18, no. 8, pp. 5431–5443, 2022.

[9] H. Patel, S. Rao, and K. Verma, "Design of hybrid frameworks for real-time intrusion and leakage detection," International Journal of Advanced Computer Science and Applications, vol. 13, no. 11, pp. 76–84, 2022.

[10] D. Roy and S. Banerjee, "A comprehensive review of data leakage prevention techniques in cyber-physical systems," IEEE Access, vol. 10, pp. 89156–89172, 2022.

[11] R. Mehta and V. Naik, "An adaptive framework for secure persona profiling using behaviour analytics," Journal of Network and Computer Applications, vol. 210, 2023.

[12] M. Ahmed, Z. Ullah, and J. Qadir, "Artificial intelligence in data security: A review of opportunities and challenges," IEEE Communications Surveys & Tutorials, vol. 24, no. 3, pp. 1450–1478, 2022.

[13] P. Verma and N. Kaur, "Explainable Artificial Intelligence for Identity Verification and Access Control," IEEE Transactions on Artificial Intelligence, vol. 5, no. 2, pp. 187–198, 2024.

[14] S. Das and R. Iyer, "Enhancing Data Privacy using Differential Privacy and Federated Learning Techniques," Journal of Information Security and Privacy, vol. 15, no. 1, pp. 56–70, 2023.