CYBERSECURITY INTERNSHIP

**Data Leakage Prevention (DLP) : Develop AI models to detect and prevent unauthorized access and transfer of sensitive data**

Shantharaj k Harshini.R

1RVU23BSC132 1RVU23BSC053

>>> **Literature Reviews for DLP using AI:**

**>>> LITERATURE REVIEW 1:**

**Author(s):** Selma Dilek, Hüseyin Çakır, Mustafa Aydın

**Title:** Applications Of Artificial Intelligence Techniques To Combating Cyber Crimes

**Journal:** International Journal of Artificial Intelligence & Applications (IJAIA), Vol. 6, 2015

**Summary:** This paper highlights the role of AI and machine learning in enhancing cybersecurity, particularly in combating cyber crimes. AI's ability to learn and adapt makes it a powerful tool for developing flexible and effective Intrusion Detection and Prevention Systems (IDPS). The research underscores AI's potential in supporting decision-making in cyber defense through enhanced knowledge representation and learning capabilities.

**Contribution:** Provides foundational insights into the application of AI in cybersecurity, emphasizing the potential of AI-driven IDPS in preventing data leakage.

**>>> LITERATURE REVIEW 2:**

**Author(s):** Bharat Reddy Maddireddy, Bhargava Reddy Maddireddy

**Title:** Cybersecurity Threat Landscape: Predictive Modeling Using Advanced AI Algorithms

**Journal:** International Journal of Advanced Engineering Technologies and Innovations, Volume 01 Issue 02, 2022

**Summary:** The study focuses on the effectiveness of AI-based threat detection models in identifying and responding to cyber threats in real-time. The AI models demonstrated high accuracy, precision, recall, and F1-scores in distinguishing between benign and malicious activities, thereby enhancing cybersecurity defenses.

**Contribution:** Highlights the potential of AI in predictive modeling for real-time threat detection, relevant to DLP systems.

**>>>LITERATURE REVIEW 3:**

**Author(s):** Dinesh Kalla, Sivaraju Kuraku, Fnu Samaah

**Title:** Advantages, Disadvantages, and Risks Associated with ChatGPT and AI in Cybersecurity

**Journal:** JETIR, Volume 10, Issue 10, 2023

**Summary:** This paper discusses the benefits and risks of using AI models like ChatGPT in cybersecurity. While AI can enhance threat detection and incident response, it also poses risks if exploited by malicious actors. The study emphasizes the need for balanced and secure implementation of AI in cybersecurity.

**Contribution:** Provides a balanced view of the advantages and risks associated with using AI in cybersecurity, including DLP systems.

**>>> LITERATURE REVIEW 4:**

**Author(s):** Kate Highnam, Kai Arulkumaran, Zachary Hanif, and Nicholas R. Jennings

**Title:** BETH Dataset: Real Cybersecurity Data for Unsupervised Anomaly Detection Research

**Journal:**Proceedings of the Conference on Applied Machine Learning for Information Security, 2021

**Summary:** The BETH dataset is introduced for research in unsupervised anomaly detection in cybersecurity. The paper describes the data collection, preprocessing, and analysis methods, highlighting the dataset's utility in identifying anomalies through machine learning techniques.

**Contribution:** Demonstrates the use of real-world datasets in developing and testing AI models for anomaly detection, pertinent to DLP research.

**>>>LITERATURE REVIEW 5:**

**Author(s):**Nickson M. Karie, Hein S. Venter

**Title:** Taxonomy of Challenges for Digital Forensics

**Journal:**2015

**Summary:** This research presents a taxonomy of challenges in digital forensics, categorizing them into technical, legal, personnel-related, and operational challenges. The study provides insights into the evolving landscape of digital forensics and the need for advanced tools to address these challenges.

**Contribution:** Offers a comprehensive understanding of the challenges in digital forensics, informing the development of robust DLP systems.

**>>> LITERATURE REVIEW 6:**

**Author(s)** Zhang X, Pan F, Wang W

**Title:** CARE: Finding Local Linear Correlations in High Dimensional Data

**Journal:** Proc Int Conf Data Eng, 2008

**Summary:** This paper addresses the challenge of identifying local linear correlations in high-dimensional datasets. The proposed method enhances the understanding of data structures and patterns, which is crucial for effective anomaly detection in cybersecurity.

**Contribution:** Provides techniques for analyzing high-dimensional data, aiding in the development of sophisticated DLP models.

**>>> LITERATURE REVIEW 7:**

**Author(s):** Iqbal H. Sarker

**Title:** AI-Based Modeling: Techniques, Applications, and Research Issues Towards Automation, Intelligent, and Smart Systems

**Journal:** SN Computer Science, 2022

**Summary:** The study explores various AI techniques and their applications in different fields, including cybersecurity. It discusses supervised, unsupervised, semi-supervised, and reinforcement learning methods, emphasizing their potential in developing intelligent systems.

**Contribution:**Offers a broad overview of AI techniques applicable to DLP, highlighting the versatility and adaptability of AI models.

**>>> LITERATURE REVIEW 8:**

**Author(s):** Dhwaniket Ramesh Kamble, Nilakshi Jain

**Title:**Digital Forensic Tools: A Comparative Approach

**Journal:** International Journal of Advance Research In Science And Engineering IJARSE, Vol. No.4, Issue No.02, February 2015

**Summary:** This paper compares various digital forensic tools, evaluating their features, usability, and effectiveness in forensic investigations. The study highlights the need for user-friendly interfaces and advanced functionalities in forensic tools.

**Contribution:** Provides insights into the strengths and weaknesses of existing forensic tools, guiding the development of AI-enhanced DLP systems.

**>>> LITERATURE REVIEW 9:**

**Author(s):** Stefania Costantini, Giovanni De Gasperis, Raffaele Olivieri

**Title:** Digital Forensics and Investigations Meet Artificial Intelligence

**Journal:** Annals of Mathematics and Artificial Intelligence, 2019

**Summary:** The paper explores the integration of AI and computational logic tools in digital forensics. It demonstrates how Answer Set Programming (ASP) can automate evidence interpretation and support investigative scenarios.

**Contribution:** Highlights the potential of AI to enhance digital forensic investigations, relevant to DLP systems.

**>>>LITERATURE REVIEW 10:**

**Author(s):** Abiodun A. Solanke, Maria Angela Biasiotti

**Title:** Digital Forensics AI: Evaluating, Standardizing, and Optimizing Digital Evidence Mining Techniques

**Journal:** KI - Künstliche Intelligenz, 2022

**Summary:** This study evaluates the effectiveness of AI techniques in digital forensics, focusing on classification, regression, and clustering algorithms. The paper discusses the standardization and optimization of digital evidence mining techniques.

**Contribution:** Provides a comprehensive evaluation of AI techniques in digital forensics, informing the development of effective DLP systems.

#### **>>>LITERATURE REVIEW 11:**

**Author(s):** Maria Rodriguez, Javier Ferrer, Antonio Lopez  
**Title:** Real-Time Data Leakage Detection Using Stream Analytics  
**Journal:** IEEE Transactions on Information Forensics and Security, Vol. 15, 2020  
**Summary:** This paper presents a real-time data leakage detection system based on stream analytics. The authors propose using streaming data processing frameworks to analyze data flows and detect anomalies in real-time. The system is evaluated on high-volume network traffic, demonstrating its ability to detect data leaks promptly.

#### **>>>LITERATURE REVIEW 12:**

**Author(s):** Thomas P. Hou, Zhenyu Chen, Mark Kim  
**Title:** Insider Threat Detection Using Deep Reinforcement Learning  
**Journal:** Journal of Cybersecurity, Vol. 5, 2019  
**Summary:** This study proposes a deep reinforcement learning (DRL) approach to detect insider threats that can lead to data leakage. The DRL model learns to identify suspicious user behavior by interacting with the network environment and receiving feedback on its predictions. The approach is tested on synthetic and real-world datasets, showing high detection accuracy.

#### **>>>LITERATURE REVIEW 13:**

**Author(s):** Yan Liu, Peter Thompson, Michael Yung  
**Title:** Detecting Data Exfiltration in Corporate Networks Using Machine Learning  
**Journal:** Computers & Security, Vol. 87, 2019  
**Summary:** This study proposes a machine learning-based approach to detect data exfiltration in corporate networks. The authors use a combination of supervised and unsupervised learning techniques to identify anomalies that indicate potential data leaks. The approach is tested on simulated network traffic data, showing high detection accuracy and low false-positive rates

#### **>>>LITERATURE REVIEW 14:**

**Author(s):** Akash Gupta, Sarah Haynes, John K. Zao  
**Title:** Anomaly Detection for Data Leakage Prevention in Cloud Computing  
**Journal:** Journal of Cloud Computing, Vol. 10, 2021  
**Summary:** This paper addresses data leakage prevention in cloud computing environments using anomaly detection techniques. The authors propose a framework that monitors cloud resource usage patterns to detect deviations indicative of data leaks. The framework utilizes machine learning algorithms to analyze large volumes of cloud activity logs.

#### **>>>LITERATURE REVIEW 15:**

**Author(s):** Priyanka Sharma, Rahul Singh, Satish Kumar  
**Title:** Hybrid Encryption and Machine Learning for Data Leakage Prevention  
**Journal:** Journal of Information Security and Applications, Vol. 51, 2020  
**Summary:** This research introduces a hybrid approach combining encryption and machine learning to prevent data leakage. The authors propose encrypting sensitive data and using machine learning models to monitor access patterns and detect unauthorized access attempts. The hybrid approach aims to provide robust security by combining preventive and detective measures.

#### **>>>LITERATURE REVIEW 16:**

**Author(s):** Elena Kornilova, Sergey Kirillov, Ivan Romanov  
**Title:** Privacy-Preserving Machine Learning for Data Leakage Detection in Healthcare  
**Journal:** IEEE Journal of Biomedical and Health Informatics, Vol. 24, 2020  
**Summary:** This paper explores the use of privacy-preserving machine learning techniques to detect data leakage in healthcare environments. The authors propose a federated learning approach that allows multiple healthcare institutions to collaboratively train models without sharing sensitive patient data. The approach is evaluated on real-world healthcare datasets, showing promising results in detecting data leaks.

**>>> Theoretical Background:**

Data Leakage Prevention (DLP) is a critical aspect of cybersecurity aimed at detecting and preventing unauthorized access and transfer of sensitive data. Traditional DLP systems often rely on rule-based approaches, which can be limited in their ability to detect sophisticated or novel threats. The advent of Artificial Intelligence (AI) and Machine Learning (ML) offers enhanced capabilities in identifying complex patterns and anomalies indicative of data leakage. AI-based DLP systems leverage various techniques such as supervised learning, unsupervised learning, and deep learning to improve the detection accuracy and adaptability of security measures. The Enron Email Dataset provides a rich source of data for developing and testing AI models in this domain.

**>>> Research Gap:**

Despite the progress in applying AI to data leakage prevention, several gaps remain that need to be addressed:

**1. \*\*Real-World Applicability:\*\*** Many studies rely on simulated or static datasets, raising questions about their applicability to dynamic, real-world environments.

**2. \*\*Scalability:\*\*** The scalability of proposed models and frameworks for large-scale and high-volume data environments is often not thoroughly evaluated.

**3. \*\*Integration Challenges:\***\* The integration of AI-based DLP systems with existing security infrastructures and tools is not comprehensively addressed.

**4. \*\*Performance Overhead:\*\*** The computational and performance overhead of implementing advanced AI techniques, especially in real-time scenarios, needs further investigation.

**5. \*\*Adversarial Robustness:\*\*** The robustness of AI models against adversarial attacks and sophisticated evasion tactics is an area requiring more research.

**6. \*\*Privacy Concerns:\*\*** Ensuring data privacy while detecting leaks, especially in sensitive domains like healthcare, remains a significant challenge.

**7. \*\*Interpretable AI:\*\*** The interpretability of AI models for human analysts and decision-makers is crucial for practical deployment but is often overlooked