DATA BREACH MONITORING SYSTEM

Ms.Dhivya K

Department of Computer Science (CYBER SECURITY) Sri Shakthi Institute of Engineering and Technology Coimbatore, India

dhivyacys@siet.ac.in

Janaki R

Department of Computer Science (CYBERSECURITY) Sri Shakthi Institute of Engineering and Technology Coimbatore, India

janakir22cys@srishakthi.ac.in

Abinaya M

Department of Computer Science (CYBER SECURITY) Sri Shakthi Institute of Engineering and Technology Coimbatore, India

abinayam22cys@srishakthi.ac.in

Kavya S

Department of Computer Science (CYBER SECURITY) Sri Shakthi Institute of Engineering and Technology Coimbatore, India

kavyas22cys@srishakthi.ac.in

Sowbarnika P N

Department of Computer Science (CYBER SECURITY) Sri Shakthi Institute of Engineering and Technology Coimbatore, India

sowbarnikapn22cys@srishakthi.ac.in

## ABSTRACT

Current data breach monitoring systems provide continuous oversight of network activity and data access points, leveraging analytics and machine learning to detect unauthorized access to sensitive information. These systems generate real-time alerts for rapid response actions, such as isolating compromised devices and blocking suspicious IPs, while also supporting regulatory compliance through detailed activity logs. This project proposes enhancements in anomaly detection precision using adaptive machine learning algorithms that update behavior baselines dynamically and reduce false positives, improving threat identification accuracy. Additionally, it integrates seamlessly with automated incident response platforms for efficient containment and remediation. Future developments aim to incorporate predictive analytics to anticipate breaches by analyzing evolving behavioral trends, enhancing proactive defense capabilities and the system’s adaptability to emerging cyber threats.

## INTRODUCTION

A Data Breach Monitoring System is a sophisticated cybersecurity tool designed to protect an organization’s sensitive data by continuously monitoring network activity, user behaviors, and data flows to identify and respond to suspicious activities that may signal a potential data breach. As cyber threats grow in complexity and frequency, organizations are under increased pressure to adopt proactive solutions that not only detect breaches but also prevent them by identifying vulnerabilities before they can be exploited. Data Breach Monitoring Systems offer this capability by leveraging a combination of real- time monitoring, machine learning, and analytics, providing comprehensive visibility into network and user activity.

The primary purpose of a Data Breach Monitoring System is to detect and respond to potential breaches swiftly, minimizing damage by isolating and containing the threat early. This system continuously observes access points and data

movement across networks, flagging anomalies that deviate from established behavioral norms, such as unauthorized logins, unexpected file downloads, or sudden spikes in data access. By automating alerts and responses, these systems reduce detection time and enable security teams to act immediately, preventing small issues from escalating into significant breaches.

## OBJECTIVE

### Detect Suspicious Activity Early

Implement mechanisms to detect unauthorized access or unusual activity patterns across systems, databases, and user accounts to identify potential breaches early.

### Real-Time Alerts and Notifications

Send immediate alerts to system administrators and security teams when suspicious activity or anomalies are detected to enable swift responses.

### Monitor Data Integrity

Track changes in sensitive data (e.g., customer information, financial records) to ensure that no unauthorized modifications or deletions occur.

### Analyze User Behavior

Implement user behavior analysis to identify irregular access patterns, such as unusual login locations, times, or frequency of access to sensitive files.

### Automate Threat Detection

Utilize automation to continuously monitor for data breaches, reducing the need for manual tracking and enhancing detection accuracy.

### Generate Detailed Reports

Create comprehensive, periodic reports of all access and activity, including any anomalies detected, for internal audits and compliance purposes.

### Ensure Compliance with Security Regulations

Ensure that the system is compliant with data privacy laws and standards (e.g., GDPR, HIPAA, PCI-DSS) by logging access and incident data securely.

### Mitigate Data Exfiltration Risks

Deploy safeguards and monitoring tools to detect attempts to export or transfer sensitive data out of the system.

### Integrate with Incident Response Plans

Link detected breaches or suspicious activities to incident response protocols, facilitating swift containment and investigation.

### Maintain Historical Data for Forensic Analysis

Store historical data on access patterns, alerts, and breaches to facilitate forensic analysis in the event of a confirmed breach.

### Enhance Security Awareness

Provide insights into common data breach attempts and trends, helping the organization proactively adjust security practices and improve awareness among employees.

## LITERATURE SURVEY

### Existing Data Breach Detection Solutions

**SIEM Systems**: Security Information and Event Management (SIEM) tools, such as Splunk and IBM QRadar, are commonly used for centralized log collection, analysis, and correlation to detect anomalies. However, research has identified that SIEM systems often suffer from high false-positive rates and limited real-time detection capabilities, which necessitates further research into improving detection accuracy.

**IDS and IPS**: Intrusion Detection and Prevention Systems (IDS/IPS) are widely used to monitor network traffic for suspicious activities. Studies show that while effective at detecting known threats, traditional IDS systems struggle with unknown threats or subtle, low-and-slow attack techniques.

**DLP Solutions**: Data Loss Prevention (DLP) solutions protect sensitive data from unauthorized access and distribution. However, literature points to challenges in tuning DLP rules to balance security and usability without creating unnecessary friction for users.

### Machine Learning and AI in Breach Detection

**Anomaly Detection**: A large body of research focuses on using machine learning for anomaly detection in network and application logs. Techniques like clustering, regression, and classification are used to identify patterns that deviate from the norm, indicating potential breaches. For example, recent studies demonstrate the effectiveness of Support Vector Machines (SVM), Random Forests, and neural networks in detecting anomalies.

**Behavioral Analytics**: Behavioral analytics is an emerging area where machine learning models

analyze user behavior, such as login patterns, access frequency, and file modification activities. Deviations from established behavior profiles may indicate insider threats or compromised accounts. Studies by researchers like David et al. (2021) emphasize the potential of behavioral analytics in reducing false positives in breach detection.

**Challenges in ML-based Detection**: Despite advancements, machine learning models face challenges like data imbalance, feature selection, and high false-positive rates. Literature stresses the importance of continuously updating models to adapt to evolving threat landscapes.

### Blockchain for Enhanced Data Integrity and Security

**Decentralized Security Models**: Research has explored the use of blockchain for secure data handling and tamper-proof logs. By creating immutable audit trails, blockchain can improve breach detection by making unauthorized data modification more detectable. Studies, such as those by Zheng et al. (2022), argue that blockchain technology may address key issues in log integrity and tamper-resistance in traditional breach monitoring systems.

**Challenges in Blockchain Implementation**: Although promising, blockchain-based security models face challenges in scalability, privacy, and integration with existing systems. Literature suggests that further research is needed to make blockchain solutions more practical for enterprise- level data breach monitoring.

### Forensics and Incident Response Post-Breach

**Forensic Analysis Techniques**: In case of a detected breach, forensic analysis helps trace the source, scope, and impact. Literature reviews tools and techniques for log analysis, memory forensics, and network forensics. Tools like Volatility and

Wireshark are commonly referenced in studies for their capabilities in detailed data examination.

**Automated Forensic Tools**: Recent advancements include automated forensic analysis tools that aid in rapid incident response. Research indicates these tools can significantly shorten investigation time, enabling organizations to resume normal operations faster post-breach.

### Legal and Privacy Considerations in Data Breach Monitoring

**Data Protection Regulations**: The General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and California Consumer Privacy Act (CCPA) impose strict requirements on data protection and breach notification. Literature shows that compliance is not only legally necessary but also impacts breach detection strategies, as organizations must balance security with privacy.

**Challenges in Compliance**: Studies highlight challenges related to monitoring sensitive data without violating privacy rights. This has led to an increased focus on data anonymization techniques and secure multi-party computation methods in breach monitoring.

### Future Directions and Emerging Trends in Data Breach Monitoring

**AI-Powered Predictive Analytics**: Predictive analytics uses historical data to predict potential breach events before they occur. Literature suggests that by combining predictive models with anomaly detection, organizations can potentially prevent breaches by proactively addressing vulnerabilities.

**Use of Advanced Cryptography**: Research on encryption and advanced cryptographic methods, such as homomorphic encryption, shows promise

in securing data at rest, in transit, and in processing, making it harder for attackers to access useful information even if a breach occurs.

### Gaps and Challenges in Current Literature

**High False Positives**: A common challenge across various methods is the high rate of false positives, which can overwhelm security teams. Research highlights the need for hybrid models combining rule-based and machine-learning approaches to improve accuracy.

**Need for Real-Time Capabilities**: Many traditional solutions operate on a periodic monitoring basis rather than real-time detection, which delays breach discovery. Literature emphasizes the need for advancements in real-time data processing and analysis.

**Adaptability to Evolving Threats**: Attack patterns and techniques evolve quickly, posing challenges for breach monitoring systems that rely on static detection rules. Studies suggest implementing continuous learning mechanisms to keep detection models up-to-date with new threats.

## METHODOLOGY

The methodology for a data breach monitoring system involves a multi-step approach, beginning with **data collection** and **log aggregation** from various sources, such as network traffic, server logs, and application activities. Data is gathered continuously from these sources to ensure comprehensive coverage of potential breach points. Logs are then centralized using a Security Information and Event Management (SIEM) system, enabling real-time data processing and correlation. This aggregation provides a foundation for monitoring by consolidating data from various endpoints, applications, and network segments,

allowing the system to identify unusual patterns across different layers.

In the **detection phase**, machine learning and rule-based algorithms analyze the aggregated data for signs of anomalies or suspicious activities. Anomaly detection techniques, such as clustering, classification, and behavioral analytics, are applied to identify deviations from typical usage patterns, which may indicate a potential breach. For example, if a user's login behavior suddenly changes—such as logging in from an unusual location or accessing atypical data—behavioral analytics algorithms flag this as suspicious. Additionally, the system employs predefined rule-based alerts for known indicators of compromise (IoCs), such as unauthorized file downloads or high-volume data transfers, which are common signs of data exfiltration.

The final phase, **incident response and mitigation**, is triggered when suspicious activities are detected. Automated alerts notify security personnel, who then validate the potential breach and initiate response procedures, such as isolating affected systems, terminating suspicious sessions, or initiating a deeper forensic investigation. The system maintains a record of incidents for forensic analysis, allowing organizations to analyze breach patterns and refine detection methods for future incidents. This phase also involves regular updates to detection rules and machine learning models to adapt to evolving threat landscapes, ensuring that the breach monitoring system remains robust and effective over time.

# EXISTING SYSTEM

Data breach monitoring systems play a critical role in today’s digital security landscape, where the risk of cyberattacks is ever-increasing. These systems are designed to detect, track, and alert organizations to potential or ongoing breaches, aiming to mitigate the impact on sensitive

information. Given the significant growth in both the volume and sophistication of cyber threats, effective monitoring is essential. However, the scope of data breach monitoring is vast and presents challenges, including the need to balance detection accuracy, scalability, and response speed.

1.Overview of Existing Data Breach Monitoring

Systems

Traditional data protection systems, such as firewalls, antivirus tools, and Intrusion Detection Systems (IDS), have served as the first line of defense for many years. However, these systems are often limited in their ability to detect real-time breaches. Modern data breach monitoring solutions have evolved to incorporate advanced technologies such as Artificial Intelligence (AI) and machine learning, which enable the detection of anomalous activities based on patterns in user behavior and data access. Behavioral analytics tools monitor interactions across an organization’s systems to detect deviations from normal activity, while Data Loss Prevention (DLP) tools focus on identifying and preventing unauthorized data transfers. Additionally, Security Information and Event Management (SIEM) systems aggregate logs from various sources to facilitate real-time analysis and threat detection. With the rise of cloud computing, cloud-based monitoring tools have also emerged, tailored to handle the complexities and scale of cloud environments.

**2. Key Components of Data Breach Monitoring**

**Systems**

Effective data breach monitoring systems consist of several critical components. The data collection process relies on sensors, loggers, and monitoring agents that gather real-time data from various endpoints, such as servers, networks, and databases. Data analysis is the core of breach detection, using

statistical analysis, rule-based algorithms, or machine learning models to identify abnormal behavior that may indicate a breach. When suspicious activity is detected, the alerting and notification systems notify security teams via email, text, or through visual dashboards. Incident response integration is also essential, enabling breach monitoring systems to work in concert with an organization’s broader security framework to initiate automated responses or escalate alerts for manual intervention.

**3.** Real-Time Monitoring and Alerting Techniques

Data breach monitoring systems increasingly focus on real-time processing and alerting to minimize response times. Real-time data processing allows for continuous data analysis and immediate detection of intrusions or suspicious behavior. Threshold-based detection is a common approach, where predefined conditions—such as a high number of failed login attempts—trigger alerts. For more sophisticated breaches, anomaly detection is used to identify deviations from established behavior patterns. This machine learning-based approach is often more effective at catching unknown attack vectors. Signature and heuristic-based detection methods, on the other hand, rely on known patterns of malicious activity and provide an additional layer of detection against common threats.

4. Case Studies and Real-World Examples

Several high-profile data breaches underscore the importance of effective monitoring systems. Incidents like those experienced by Equifax, Target, and Yahoo demonstrate how the absence or inadequacy of data breach monitoring systems can lead to severe consequences, including significant financial losses and damage to reputation. Conversely, successful case studies highlight organizations that have adopted robust breach monitoring systems, effectively strengthening their security posture and enabling rapid response to

emerging threats. These cases showcase the value of proactive monitoring and real-time detection in preventing and mitigating the impact of breaches.

5. Challenges in Data Breach Monitoring

Data breach monitoring systems face multiple challenges, one of the most prominent being the issue of false positives and false negatives. Excessive alerts can overwhelm security teams, while undetected breaches may result in substantial harm. Scalability is another concern, as large organizations generate vast amounts of data, requiring monitoring systems to process and analyze data continuously without sacrificing performance. Privacy concerns also play a critical role, as monitoring tools must ensure compliance with regulations like GDPR and CCPA, which govern data collection and usage. Additionally, the constantly evolving tactics of attackers make it challenging for monitoring systems to adapt quickly enough to new threats, such as Advanced Persistent Threats (APTs).

6. Emerging Trends and Future Directions

Emerging trends in data breach monitoring systems include integration with real-time threat intelligence, which enhances detection capabilities by continuously updating the system with the latest known attack methods. As cloud computing and the Internet of Things (IoT) expand, monitoring tools are increasingly adapting to secure cloud environments and distributed systems. Decentralized monitoring solutions are also gaining traction, leveraging blockchain technology to offer secure, transparent data breach monitoring that is resistant to tampering. These advancements suggest that the future of data breach monitoring will be characterized by greater sophistication, adaptability, and integration across digital ecosystems.

# PROPOSED SYSTEM

The proposed data breach monitoring system aims to provide an advanced, real-time solution for detecting and responding to potential breaches. It leverages a combination of artificial intelligence (AI), machine learning (ML), behavioral analysis, and real-time data processing to overcome the limitations of traditional systems. Here’s a breakdown of the main components and features of the proposed system:

**1.** Architecture and Design

* **Distributed Monitoring and Data Collection**: The proposed system employs a distributed architecture with monitoring agents deployed across all critical endpoints, including servers, network devices, databases, and cloud environments. This setup allows for continuous data collection and monitoring, enabling comprehensive visibility across the entire IT infrastructure.
* **Centralized Data Lake**: A centralized data lake aggregates raw data from distributed agents. This central repository supports big data processing and provides a foundation for high-volume storage, allowing the system to analyze data trends over time.
* **AI-Driven Analytics Engine**: An AI analytics engine analyzes the aggregated data in real-time. This engine uses ML models and statistical analysis to identify unusual patterns and potential breaches.

**2.** Real-Time Anomaly Detection with Machine Learning

* **Behavioral Profiling**: The system builds behavioral profiles for users, applications, and systems. Using machine learning algorithms, it creates a baseline of "normal"

activity, making it easier to spot anomalies. For example, unusual login times, location changes, or abnormal data access patterns can trigger alerts.

* **Dynamic Thresholds and Self-Learning Models**: The ML models in the system can dynamically adjust thresholds based on user behavior and activity patterns. This minimizes false positives and ensures that detection remains accurate as system usage patterns change over time.
* **Advanced Anomaly Detection Algorithms**: Algorithms like clustering and neural networks are used to detect sophisticated attack vectors, such as insider threats or advanced persistent threats (APTs). These algorithms are designed to detect subtle patterns that traditional rule- based detection might miss.

**3.** Threat Intelligence Integration

* **Real-Time Threat Feeds**: The system incorporates real-time threat intelligence feeds from reputable sources, enabling it to detect known threats and attack signatures quickly. This integration allows the system to stay up-to-date with the latest vulnerabilities, attack techniques, and indicators of compromise (IOCs).
* **Automated Signature Updates**: The system automatically updates its database of threat signatures and indicators based on threat intelligence, allowing for rapid detection of known attack vectors.
* **Community-Driven Threat Sharing**: Through community-driven threat sharing, the system allows organizations to share anonymized threat data, strengthening overall threat detection across multiple systems by leveraging collective knowledge.

**4.** Incident Response and Automated Remediation

* + **Automated Containment and Response**: Upon detection of a confirmed breach, the system can trigger automated actions to contain the threat. Examples include isolating affected systems, revoking user access, or quarantining malicious files. This rapid response capability can prevent breaches from spreading further within the network.
	+ **Integration with Security Orchestration, Automation, and Response (SOAR)**: The system is integrated with SOAR tools to streamline incident management and automate responses based on predefined playbooks. SOAR integration allows for efficient coordination across different security tools and teams.
	+ **Customizable Response Playbooks**: Organizations can create custom response playbooks that outline specific actions for different types of breaches. This flexibility ensures that the system’s response aligns with the organization’s unique security policies and requirements.

only authorized personnel can access sensitive monitoring data, aligning with privacy regulations and organizational policies.

**6.** User Interface and Visualization

* + **Real-Time Dashboards**: The system provides a user-friendly dashboard with real-time alerts and visualizations, offering a high-level overview of security posture, detected incidents, and response actions.
	+ **Customizable Alerts and Notifications**: Users can customize alerts based on severity levels and preferred notification channels (e.g., SMS, email, mobile app notifications). The system also allows users to set up thresholds for alerts, ensuring that they only receive notifications for significant incidents.
	+ **Threat Heatmaps and Analytics**: The dashboard includes heatmaps and analytics for visualizing trends, helping security teams spot patterns or recurring threats and prioritize critical incidents for immediate action.

**5.** Privacy and Compliance Controls

**7.** Continuous Improvement and Self-Learning

* + **Data Masking and Encryption**: To ensure compliance with data protection regulations (e.g., GDPR, CCPA), sensitive data in the monitoring system is masked or encrypted. This ensures that the data remains protected during analysis and storage.
	+ **Audit Trails and Reporting**: The system generates detailed audit logs and compliance reports. These logs track all detected breaches, responses, and changes to the system, enabling transparency and accountability in incident handling.
	+ **User Privacy and Access Controls**: Role- based access controls (RBAC) ensure that
	+ **Feedback Loops for ML Model Improvement**: The system includes feedback mechanisms where analysts can tag incidents as true or false positives. This feedback improves the accuracy of the ML models over time, allowing the system to adapt to changing threat landscapes.
	+ **Periodic Model Retraining**: The system automatically retrains its ML models at regular intervals using the latest threat data, ensuring ongoing relevance and robustness of detection algorithms.
	+ **Attack Simulation and Testing**: The system can simulate various attack

scenarios to test its detection and response capabilities. Regular testing helps identify potential weaknesses and areas for improvement, enhancing the system’s effectiveness over time.

## SYSTEM REQUIREMENTS

**1.** Hardware Requirements

### Servers:

At least **2 high-performance servers** (scalable as data grows) for data aggregation, processing, and storage.

**Multi-core CPUs** (8 cores minimum) with high clock speeds (3.0 GHz or above) to support real- time data processing and analysis.

Minimum of **32 GB RAM** (recommended 64 GB) for running machine learning algorithms and data processing tasks.

### Storage:

Minimum **1 TB SSD storage** per server for fast read/write speeds (adjustable based on data retention requirements).

**Centralized Data Lake Storage**: Up to **100 TB** for large-scale organizations handling high data volumes (network-attached storage or cloud storage).

### Network Interface:

High-speed network interfaces (1 Gbps or higher) to handle continuous data flow from multiple sources.

**Load Balancers** to distribute traffic among servers for scalability and high availability.

**2.** Software Requirements

### Operating Systems:

Linux-based OS (e.g., **Ubuntu Server 20.04+, CentOS 7+, or RHEL 8+**) for server environments due to stability, security, and compatibility with open-source monitoring tools.

Windows Server OS for environments that require integration with Active Directory or Windows- specific applications.

### Database Management System:

**Relational Database (e.g., PostgreSQL, MySQL)** for structured data storage and relational queries.

**NoSQL Database (e.g., MongoDB, Elasticsearch)** for handling unstructured data, such as logs or network data, and supporting high- speed searching and indexing.

### Data Processing and Big Data Analytics Framework:

**Apache Spark** or **Apache Flink** for big data processing, as they support real-time data streaming and batch processing.

**Kafka** or **RabbitMQ** for reliable, scalable message queuing and data ingestion.

### Machine Learning Libraries:

Python-based libraries like **scikit-learn, TensorFlow, and PyTorch** for model training and anomaly detection.

**Jupyter Notebooks** for model development and testing, especially during initial setup.

### Visualization and Dashboard Tools:

**Grafana** or **Kibana** for real-time data visualization, dashboards, and custom alerting.

### Threat Intelligence Integration:

**SIEM software** such as **Splunk, LogRhythm, or IBM QRadar** to collect and correlate security events across the infrastructure.

APIs for integrating **threat intelligence feeds** .

## MODULO DESCRIPTION

A Data Breach Monitoring System is essential for organizations aiming to protect sensitive information from unauthorized exposure. This system actively scans various online sources, such as dark web forums, social media, and underground marketplaces, for signs of compromised data, including leaked credentials or personal information. By leveraging real-time monitoring, the system identifies and alerts the security team to potential breaches as soon as they emerge, enabling organizations to respond quickly before sensitive data becomes widely exposed. Through advanced algorithms, it prioritizes incidents based on risk, sending targeted notifications and recommended actions to mitigate the impact. J Additionally, this system integrates with security tools, such as Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platforms, streamlining the incident response process and allowing for a faster, coordinated reaction to threats. Beyond real-time alerts, the Data Breach Monitoring System also offers historical breach tracking and analytics, helping organizations recognize patterns in exposures and address recurring vulnerabilities. This approach not only enhances security posture but also supports regulatory compliance by documenting breach incidents and organizational responses. In an era where cyber threats are increasingly sophisticated, a Data Breach Monitoring System enables proactive defense strategies, giving

organizations the upper hand in managing and mitigating the risks associated with data breaches.

## CONCLUSION

In conclusion, a Data Breach Monitoring System represents a critical tool in modern cybersecurity efforts, enabling organizations to proactively detect and respond to data exposure incidents before they escalate. By continuously scanning for leaked or compromised data, this system provides real-time insights and prioritizes threats based on risk, allowing security teams to focus on the most critical incidents and implement swift countermeasures. Furthermore, the integration with incident response and analytics platforms strengthens the overall security infrastructure, offering organizations not only immediate alerts but also a strategic understanding of long-term vulnerabilities and patterns.

**REFERENCES** Chhabra, S., & Singh, A.K. - Dynamic Data Leakage Detection Model for Cloud Security (2016)

1. Patil, Rina - Root causes, ongoing difficulties, proactive prevention techniques, and emerging trends of enterprise data breaches (2023)
2. Wang, B., et al. - A Survey of Data Breach Detection and Prevention Techniques (2022)
3. Zhang, H., & Zhang, X. - Blockchain- Based Data Breach Detection: Approaches, Challenges, and Future Directions (2023)
4. Chouikhi, M., et al. - Anomaly-based Intrusion Detection Systems for Cybersecurity (2022)
5. Khan, Z., et al. - Managing Data Breach Risks in Cloud Computing Environments (2021)
6. Patel, N., & Patel, R. - Data Breach Prevention and Management in Enterprise Networks (2020)
7. Shu, X., et al. - Fast Detection of Transformed Data Leaks (2016)
8. Gomez-Hidalgo, J.M., et al. - Data Leak Prevention through Named Entity Recognition (2010)
9. Lu, Y., et al. - Collaborative Graph-based Mechanism for Distributed Big Data Leakage Prevention (2018)
10. Katz, G., et al. - CoBAn: A Context-Based Model for Data Leakage Prevention (2014)
11. Trieu, L.Q., et al. - Document Sensitivity Classification for Data Leakage Prevention (2017) [12]Basso, T., et al. - Challenges in Data Breach Detection: Prevention, Causes, and Mitigation Strategies (2016)
12. Cheng, L., et al. - Enterprise Data Breach: Causes, Challenges, Prevention, and Future Directions (2017)
13. Rajendran, R., & Ramaswamy, S.R. - Data Leakage Detection Using Traffic Pattern Analysis (2017)

Proposes a dynamic model for detecting data leakage in cloud environments, focusing on security in MapReduce computation

JNCET

1. Baba, S., & Singh, N. - Data Breach Detection in IoT-based Systems (2022)
2. Zhang, M., et al. - Securing Open NetBIOS Shares Against Unauthorized Access (2020)
3. Vaidya, T.N., & Prasad, R.D. - Access Control and Data Breach Prevention: A Comprehensive Approach (2016)