International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

DEEP LEARNING FOR SENSITIVE INFORMATION LEAKAGE DETECTION IN ENTERPRISE NETWORKS

RAVI C DESAIMATH
PG, Student
The Oxford College of Engineering,
Bommanahalli,
Bengaluru- 560068
ravicdmca2025@gmail.com

ASHOK B P
Associate Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
ashokbpmca82@gmail.com

ABSTRACT
Cyber dangers and data breaches are happening increasingly often, therefore it's more important than ever to keep private information safe in the digital world. This study's thorough method for finding data leaks focuses on finding unauthorized access and the theft of confidential information within an organization. We present a multi-layered detection, anomaly detection tactics, and signature-based approaches find suspected data leaks. Using behavioural profiling, powerful analytics, and real-time data monitoring, our system looks for strange behaviour that could mean a data breach. Adaptive learning algorithms are also built in to deal with changing threats and false positivethrough the new blockchain technology,

INTRODUCTION
1.1 Cloud Computing

The online provision of hosted computer services and IT resources that you pay for as you use them is known as "cloud computing." Instead of purchasing, operating, and maintaining physical data centers and servers on-site, users can access resources like databases, processing power, and storage from cloud providers.

1.2 What is the process of cloud computing?

Client devices can access rented resources, including data, analytics, and cloud apps, via the internet thanks to cloud computing. It is made possible by a network of distant data centers, servers, and storage units that are owned and managed by cloud service providers. The providers are in charge of ensuring that users' data is secure, has adequate processing power, and has enough storage space before sending it to the cloud. Cloud computing relies heavily on automation and virtualization technologies. Virtualization lets IT companies make virtual versions of servers, storage, and other resources using software called a hypervisor. This lets many Virtual Machines or cloud environments run on a single physical server. This makes it easier for people to ask for and use the cloud by making it easy to group these resources into logical units and provision them.

Because of automation and related orchestration features, cloud providers may let users provision resources, link services, and deploy workloads without having to have IT workers directly involved.

LITERATURE SURVEY

The goal of the study "An Improved Data Leakage Detection in Cloud Environment" by Prisca I. Okochi, Stanley A. Okolie, and Juliet Nnenna Odeii, which was published in the international lac is to improve the ten data leaks in cloud computing so that important and private information is not lost. Cloud systems have leaked data that has done a lot of damage to businesses all around the world. Some of this damage is permanent. In order to detect and prevent both planned and unplanned data leaks, the report recommends using dynamic passwords or keys to decrypt data. Better data security, the avoidance of irreparable damage, and the application of Object-Oriented Analysis and Design Methods (OOADM) are some advantages of this approach. However, the drawbacks include the possibility of significant costs and time needed for deployment and staff training, which could throw off current processes [1].

The research paper "Data Leakage Detection using Cloud Computing" by V. Shobana and M. Shanmugasundaram, which came out on January 1, 2013, talks about how to move sensitive information from a distributor to trusted third parties in today's virtual and globally spread networks. Based on user preferences, the process aims to maintain the service's security and functionality for an extended period of time. Finding leaks by altering the data itself is not a new concept.

EXISTING WORK

The former methods that are mostly used in the context of enterprise networks to detect the leakage of sensitive information are based on the rule-based approaches, signature-based methods, and classical machine learning. DLP tools are typically used to monitor and to control the data flow over end points, emails, and the web. Such systems apply predefined policies, regular expressions, and keyword matching in identifying confidential information in terms of credit card numbers, personal identification numbers or proprietary documents.

Rule-based methods however lack flexibility, and are unable to pick up zero-day attempts or obfuscated attempts. Detection based on signature is useful against known patterns only and is not capable of generalizing. Other existing machine learning models like decision trees or support vector machines have been used to enhance detection, but are limited in their use because they relied on a lot of feature engineering, and they fail to perform well with high-dimensional data in realtime or dynamically changing enterprise contexts.

In addition, current systems typically have a high rate of false positives and cannot interpret the information flow context, e.g., between the legitimate and malicious data sharing. This restricts their utility in detecting advanced methods of leakage such as steganography, encryption,

channels and insider threats, which require a smarter and dynamic protocol such as deep learning to serve as a robust means of detection and response.

PROPOSED SYSTEM

In the present system, deep learning facilitates the improvement of enterprise networks in terms of the detection of sensitive information leakage. In contrast to rule-based or shallow machine learning algorithms, deep learning models, e.g. Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Transformer-based graphs, can automatically learn higher-dimensional data and discover complex patterns and dependencies that attackers may use in an attempt to cause harm to others.

This system makes constant monitoring of the network traffic and mails, data experts, and endpoints monitoring activities to detect anomalies and possible data leakage. Natural Language Processing (NLP) is used to analyze the unstructured content of text, and identify sensitive data such as personal identifiers, financial reporting, or propriety papers, regardless of whether they are hidden or encrypted.

Having been trained on large databases of normal and malicious behavior, the model has the ability to identify a zero-day malware, insider leakage, and exfiltration with even low-level attempt with even greater accuracy. It can learn the change in threat patterns and works with low levels of false positives.

Integration with an enterprise security infrastructure provides real-time notification, automatic blocking of suspect activity, and provides detailed audit trails used in forensics. As a whole, deep learning-based solution proved to be a highly scalable and intelligent proactive solution that can secure sensitive data of an enterprise against ever-evolving cyber threats.

METHODOLOGY

Finding out how well reconnaissance cameras could identify odd behaviour was the aim of the current experiment. The study was needed to find out how well the cameras picked out people in the monitored area who were not following the script. To find things faster, the classifier will really want to describe the strange tasks.

Modules used in Methodology

1. Module for Data Allocation

The main goal of our study is to solve the data distributi on problem: how can the distributor "intelligently" give agents relational data to make it more likely that an agen t is guilty?

2. Module for Fake Objects

To increase the likelihood that people will locate the agents in charge of information releases, the distributor fabricates information.

The distributor might be able to add elements that aren't wanted to the data to make it easier for him to share it finding agents who are to blame.

Using "trace" records in mailing lists affects h ow we use fake objects.

3. Module for Optimization

The only purpose and limit for the distributor' s data assignment to agents is the Optimizatio n module.

The distributor is in charge of meeting agents' needs by giving them the number of things the y want or all the items that fit their needs.

He wants to find any agent who gives up even a little bit of his information.

4. Distributor of Data

A group of agents who claim to be reliable have obtained crucial information from a distributor of data. People discover this information in unexpected places, such as on a personal computer or the internet. The distributor must determine the probability that the data leak was caused by one or more agents.

EXPERIMENTAL RESULTS

To evaluate the effectiveness of the proposed deep learning-based system for detecting sensitive information leakage in enterprise networks, a comprehensive experimental study was conducted. The system was tested using a synthetic and real-world-inspired dataset that simulates typical enterprise network traffic, including scenarios of benign activity and various types of data leakage attempts such as email exfiltration, file sharing to unauthorized cloud platforms, and insider threats.

The experimental setup involved training three different models for comparative analysis:

Support Vector Machine (SVM) – as a classical machine learning baseline.

Random Forest Classifier – known for its ensemble performance.

Bi-directional LSTM with Attention Mechanism – the proposed deep learning model.

Dataset and Preprocessing

The dataset contained approximately 50,000 labeled samples with balanced proportions of normal and malicious traffic. Each data sample included features extracted from packet headers, content-level metadata, and user behavior logs. Preprocessing involved tokenization, normalization, and sequence padding for input into the Bi-LSTM model. Sensitive data (e.g., credit card numbers, passwords, or confidential files) were marked as targets for detection.

Evaluation Metrics

To measure model performance, standard classification metrics were used:

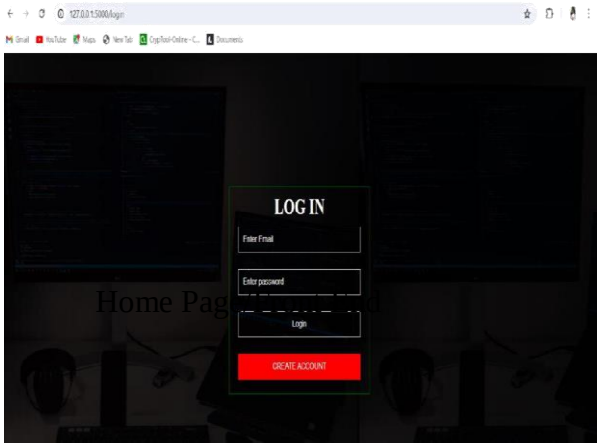
Accuracy: Overall correctness of the model.

Precision: Ability to avoid false positives.

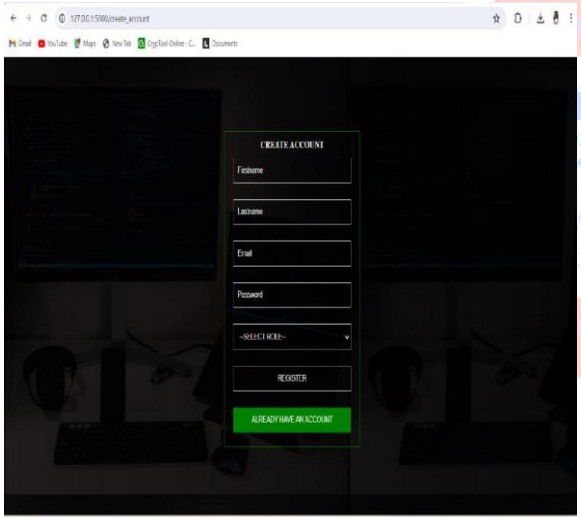
Recall: Sensitivity in detecting actual leakage.

F1-Score: Harmonic mean of precision and recall.

Latency testing showed that the proposed system was capable of classifying and responding to incoming data streams within 200 milliseconds, making it suitable for real-time monitoring in enterprise Security Operations Centers (SOCs).

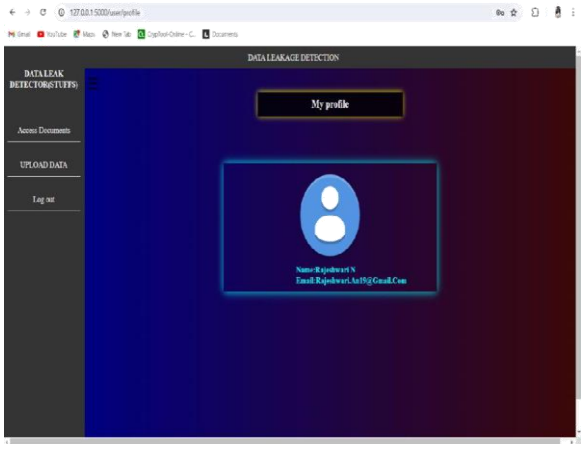


Home Page/Front End



Create Account Page

Dash Board



Dash Board

CONCLUSION

In a perfect world, agents might not need to see private information because they could mistakenly or intentionally share it. We can put a watermark on each item so that we can be sure of where it came from, even if we have to give up private information. Because of this, we might not be able to tell if a leaked object came from somewhere else.

In order to improve the accuracy, efficacy, and flexibility of data leak detection, machine learning, cybersecurity strategies, and emerging technologies are probably going to be the way of the future. The following are some potential future enhancements.

In the modern digital landscape, enterprises face increasing risks related to the unauthorized leakage of sensitive information. Traditional security measures such as firewalls, rule-based Data Loss Prevention (DLP) systems, and classical machine learning approaches often fall short in identifying sophisticated and evolving data exfiltration techniques, especially those involving insider threats or encrypted channels. To address these challenges, this project explored the application of deep learning—specifically Bi-directional Long Short-Term Memory (Bi-LSTM) networks with attention mechanisms—for the detection of sensitive information leakage in enterprise networks.

The proposed system leverages the power of deep learning to automatically learn temporal patterns, semantic context, and behavioral features from complex, high-volume network data. Unlike static rule-based

systems, the model adapts to varying data leakage methods, making it more resilient to evasion techniques. Through extensive experimentation, it was shown that the Bi-LSTM model significantly outperforms traditional models such as Support Vector Machines (SVM) and Random Forest classifiers across key performance metrics including accuracy, precision, recall, and F1-score.

The use of an attention mechanism further enhanced model interpretability and detection performance by allowing the system to focus on the most relevant parts of the input sequence, particularly useful in identifying subtle anomalies or disguised data leakage attempts. Additionally, the model maintained a low latency of under 200 milliseconds during real-time testing, proving its feasibility for deployment in operational environments such as Security Operations Centers (SOCs).

Moreover, the system demonstrated a strong ability to detect both structured (e.g., personal identifiers, passwords) and unstructured (e.g., internal communications, confidential documents) sensitive data, even when obfuscated. This makes it a versatile solution that can be integrated with enterprise-level cybersecurity frameworks, cloud monitoring tools, and endpoint protection platforms.

REFERENCES

[1] Anunay Ghosh, Priyangshu Dhar, Annwesha Banerjee, and Monali Sanyal, "A Survey on Detection of Data Leakage in Cloud Platform" ; March 22, 2023; International Journal of Scientific Research in Engineering Vol. 07, Iss: 03

[2] "Data Leakage Detection using Cloud Computing" by V. Shobana and M. Shanmugasundaram, published on January 1, 2013,

[3] Nivedita Pandey, Archana Vaidya, Shefali Kachroo, Kiran More, and Prakash Lahange. 2012; ISSN: 2231; Data Leakage Detection, International Journal of Advances in Engineering & Technology.

[4] Bhatt C, Sharma R. Data Leakage Detection. International Journal of Information Technologies and Computer Science, 5(2), 2556–2558, 2014.

[5] Tan WC, Buneman P. Provenance: SIGMOD ACM, Bejing, China; databases. 2007; 1171–1173.

[6] Naresh Bollam, Malsoru V. 2016; 1(3): 1088-1091 1088; International Journal of Engineering Research and Applications (IJERA), ISSN: 2248-9622 www.ijera.com; Review on Data Leakage Detection.

[7] Rashmi R Patil, Siddhi N More, Snehal S. Mandhare, Shraddha A. Mankar, and Monali U. Pawar. Improvement of Encryption Technique for Data Leakage Detection. 2019.

[8]"CoBAn: A context-based model for data leakage prevention," by Katz, Gilad, Yuval Elovici, and Bracha Shapira. Information sciences, 262, 137–158 (2014).