Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 2, February : 2025

ENHANCING SECURITY WITH AI-DRIVEN PII MASKING

G.SHEEBA(21501A1245), Student, Department of Information Technology, Prasad V Potluri Siddhartha Institute Of Technology, AP, India

B.DHARANI(22505A1204), Student, Department of Information Technology**,** Prasad V Potluri Siddhartha Institute Of Technology, AP, India

K.NEERAJ PRAKASH(21501A1251), Student, Department of Information Technology, Prasad V Potluri Siddhartha Institute Of Technology, AP, India

A.ABHILASH(21501A1202), Student, Department of Information Technology PRASAD V Potluri Siddhartha Institute Of Technology, AP, India

DR. G.RESHMA, M.Tech,Ph.D, Assistant Professor, Department of Information Technology Prasad V Potluri Siddhartha Institute Of Technology, AP, India

ABSTRACT:

Sensitive information is often embedded within textual data, making its protection crucial in today's data-driven world. This project introduces a streamlined approach to **entity recognition and masking** using **regular expressions (regex)**, implemented in an intuitive **Streamlit application**. The system identifies and masks sensitive entities such as Aadhaar numbers, PAN numbers, phone numbers, credit card details, and more, ensuring compliance with data privacy requirements and safeguarding user information.

The application allows users to input text directly, which is processed to detect predefined patterns of sensitive data. The backend employs regex-based patterns tailored to India's data formats, including Aadhaar, PAN, and other financial identifiers, to ensure high precision. Identified entities are dynamically replaced with masked representations (e.g., "XXXX") to preserve the text's readability while securing its content.

By integrating regex for entity recognition, this project demonstrates a lightweight and efficient alternative to complex machine learning models for similar tasks. The user-friendly interface allows for quick evaluation of data privacy risks, making it ideal for applications in **data preprocessing, document anonymization, and secure text processing**.

The system's flexibility enables further customization, allowing users to adapt regex patterns to their specific use cases,

ensuring scalable and robust protection of sensitive information.

INTRODUCTION

In today's world, where data is everything, safeguarding sensitive information is of utmost importance. Personally Identifiable Information (PII) like Aadhar numbers, PAN numbers, bank account details, or even simple phone numbers can lead to major security risks if exposed. Businesses, especially in sectors like finance, healthcare, and legal, deal with loads of documents containing such critical data every day. Now imagine doing all this manually tedious, error-prone, and almost impossible when the volume increases. That's where technology like AI and Machine Learning (ML) comes in.

Our project focuses on building a solution that uses advanced NLP models and rule-based algorithms to automate the process of identifying and redacting PII from documents. It's designed to be efficient, scalable, and, most importantly, tailored for Indian data and scenarios. This solution not only protects sensitive information but also ensures that businesses comply with strict privacy regulations.

EXISTING SYSTEM

Existing systems for PII redaction are outdated and mostly manual or semi-automated. Let me give you an example: some tools simply search for patterns like numbers or email addresses and remove them. But what if those patterns appear in non-sensitive contexts? Or worse, what if the sensitive data doesn't follow typical patterns, like someone's handwritten name on a scanned document?

These systems also lack customization. For instance, India-specific data like Aadhar or PAN numbers aren't recognized in most globally available tools. This leaves a huge gap when it comes to ensuring compliance for Indian businesses.

DISADVANTAGES OF EXISTING SYSTEM

Human Error: Manually redacting thousands of documents? That's a recipe for disaster!

Time-Consuming: It takes ages to comb through every page, line by line, looking for sensitive data.

Not Context-Aware: Just because a document contains the word ―number‖ doesn't mean it's sensitive. Existing tools fail to understand context.

Compliance Issues: Missing even a single piece of sensitive data could lead to hefty

fines under laws like GDPR or India's PDPB.

PROPOSED SYSTEM

This is where our solution shines! We've designed a system that automates the entire process using cutting-edge AI and ML techniques. Here's how it works:

Regex Pattern Recognizers: We've created custom patterns to identify Indian-specific data like Aadhar numbers, PAN numbers, and even phone numbers.

NER Integration: Using Distil BERT, we've added a Named Entity Recognizer to classify words based on their context. For example, if a document mention

"passport," our system understands the context and looks for a number nearby to classify it as sensitive.

Fine-Tuned BERT: We didn't stop there! We fine-tuned BERT on a dataset of 3 million Indian names, addresses, and locations to make it even smarter.

Image Redaction: Using OCR and OpenCV, our system can redact sensitive information from scanned documents, images, and even IDs like passports or driver's licenses.

ADVANTAGES OF PROPOSED SYSTEM

Accuracy: It doesn't just detect patterns; it understands the context, making the redactions more reliable.

Scalable: Whether it's 10 documents or 10,000, our system handles it with ease.

Compliant: Ensures adherence to privacy laws, reducing legal risks for businesses.

Tailored for India: With specific features for Indian data, this system bridges the gap left by global tools.

RELATED WORK

NEURAL NETWORKS

Neural networks are a fundamental concept in machine learning and artificial intelligence. They are computational models inspired by the structure and function of the human brain. These networks consist of interconnected layers of artificial neurons that process information, learn patterns, and make predictions. Neural networks are widely used for various applications, including image recognition, natural language processing, speech synthesis, and predictive analytics. Their ability to model complex relationships and adapt through learning makes them essential in modern AI advancements.

Structure of a Neural Network

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 2, February : 2025

A neural network is typically composed of three main layers: the input layer, hidden layers, and the output layer. Each layer contains neurons that perform computations and pass information forward.

Input Layer

The input layer serves as the entry point for raw data. Each neuron in this layer represents a distinct feature in the dataset, such as pixel values in an image or words in a text document. The input layer does not perform any computation but simply forwards the data to the next layer.

Hidden Layers

Hidden layers are responsible for processing and transforming the input data. These layers extract features, detect patterns, and apply activation functions to introduce non- linearity, enabling the network to learn complex relationships. The depth and number of hidden layers can vary, depending on the complexity of the task. Deep neural networks contain multiple hidden layers, allowing them to model intricate patterns effectively.

Output Layer

The output layer generates the final prediction or classification result. The number of neurons in this layer depends on the task—binary classification requires a single neuron with a sigmoid activation function, while multi-class classification uses multiple neurons with a softmax activation function.

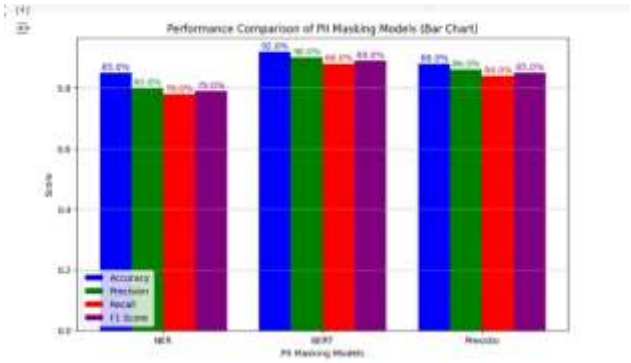

Figure 1: Accuracy analysis of the proposed PII masking system, showcasing its efficiency in detecting and masking sensitive data.

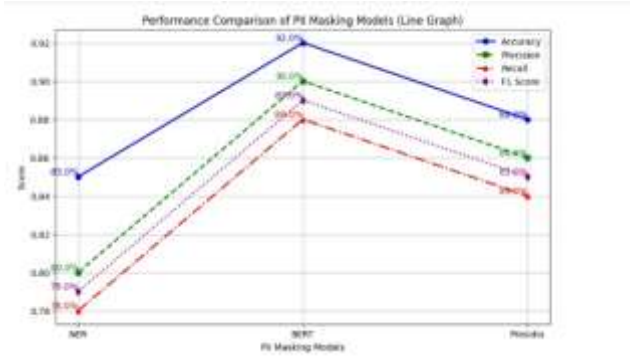

Figure 2: Graphical representation of PII entity relationships, showcasing connections between different sensitive data points.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 54, Issue 2, February : 2025

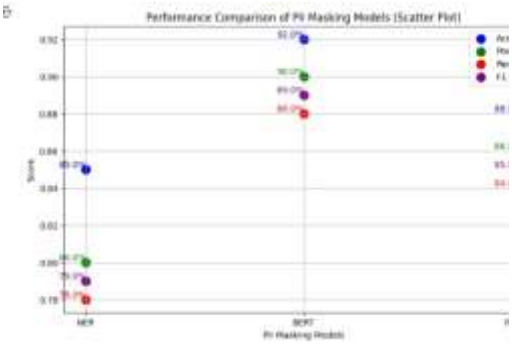

Figure 3: Final output showcasing the effectiveness of PII masking with AI-driven techniques.

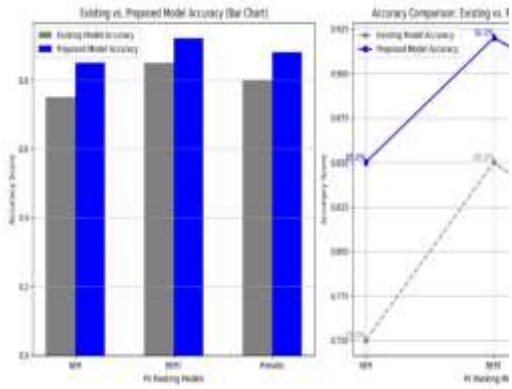

Figure 4: Comparison of Accuracy Between Existing and Proposed Models for PII Masking

SAMPLE RESULTS

CONCLUSION

Future PII redaction systems must go beyond text processing to handle multimodal data (text, images, audio, video) while ensuring high scalability, real-time processing, and regulatory compliance. Advanced AI, cloud-native architectures, and user-driven customizations will enhance privacy protection, making redaction more

accurate, adaptive, and seamless across industries.

By implementing deep learning models, cloud-based solutions, multimodal redaction, and compliance automation, the next generation of PII redaction tools will set new standards in data privacy and security.

REFERENCES

- https://microsoft.github.io/presidio/analyzer/
- https://arxiv.org/pdf/1706.03762
- https://arxiv.org/abs/2312.11805
- https://ai.google.dev/gemini-api/docs/models/gemini#gemini-1.5-flash
- https://proceedings.neurips.cc/paper_files/paper/2017/file/3f5ee243547dee91fbd053c1 c4a845aa-Paper.pdf