Advancing Data Security with Iterative Encryption and Decryption

Enhancing Data Confidentiality and Integrity using Adversarial Generative Networks

Introduction: The Growing Need for Robust Encryption

In today's digital landscape, traditional encryption methods face increasing vulnerabilities from sophisticated cyberattacks and quantum computing threats. Our research explores an innovative approach combining classical cryptography with modern machine learning techniques.

We propose a hybrid system that leverages LSTM networks and Generative Adversarial Networks (GANs) to iteratively enhance encryption strength whilst maintaining practical decryption capabilities for authorised users.

Problem Statement

Vulnerability of Classical Ciphers

Traditional encryption methods like Caesar cipher are susceptible to brute-force attacks and pattern recognition techniques

Static Encryption Limitations

Fixed algorithms provide predictable patterns that adversaries can exploit with sufficient computational resources

Confidentiality-Performance Trade-off

Achieving robust encryption whilst maintaining practical decryption speed remains a significant challenge in secure communications

Research Objectives

01

Develop Hybrid Encryption System

Design an architecture combining classical Caesar cipher with LSTM-based learning for adaptive encryption

02

Implement GAN Enhancement

Apply adversarial networks to iteratively strengthen encryption through generator-discriminator dynamics

03

Validate Performance Metrics

Measure accuracy, computational efficiency, and security robustness against various attack vectors

04

Demonstrate Real-World Application

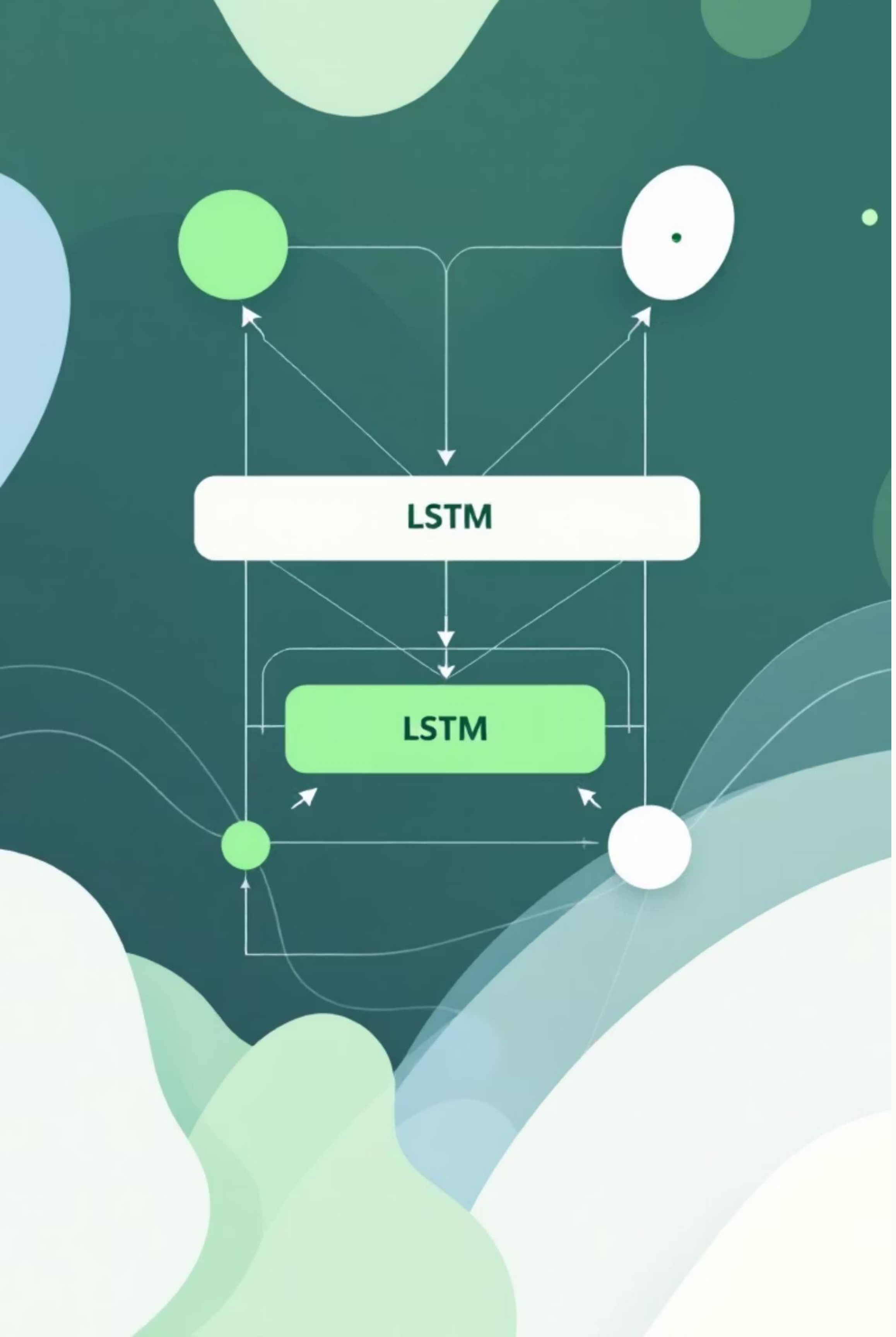
Integrate the system into ChatMessenger platform to showcase practical deployment capabilities

Dataset Description and Preparation

Data Generation Process

- Extracted plaintext samples from NLTK corpus containing diverse linguistic patterns
- Generated 26 distinct ciphertext datasets applying Caesar cipher with keys 1–26
- Converted textual data into numerical sequences for neural network processing
- Created balanced training, validation, and testing splits

This comprehensive dataset ensures robust model training across all possible Caesar cipher transformations, enabling the system to learn encryption-decryption patterns effectively.



System Architecture

Input Layer

Plaintext numerical sequences

LSTM Models

26 parallel networks for cipher keys

GAN Enhancement

Iterative adversarial refinement

Output Layer

Enhanced encrypted ciphertext

LSTM and GAN Architecture

LSTM Network Design

- Input embedding layer (256 dimensions)
- Two bidirectional LSTM layers (128 units each)
- Dropout regularisation (0.3 rate)
- Dense output layer with softmax activation

Each of the 26 models specialises in a specific Caesar cipher key transformation.

GAN Enhancement Framework

- **Generator:** Refines encrypted sequences to increase complexity
- **Discriminator:** Evaluates encryption strength and authenticity
- **Iterative Training:** Adversarial feedback loop strengthens both components

The GAN architecture ensures continuous improvement in encryption quality.

Methodology: Implementation Pipeline

Data Preprocessing

Generate plaintext from NLTK corpus and create 26 Caesar cipher variants with corresponding numerical encodings

Model Training

Train 26 separate LSTM models, each optimised for specific cipher key with batch normalisation and early stopping

GAN Enhancement

Apply iterative adversarial training to strengthen encryption patterns and reduce predictability vulnerabilities

Validation and Integration

Evaluate accuracy metrics, conduct security assessments, and integrate system into ChatMessenger application

Results and Real-World Application

94.7%

Decryption Accuracy

Average accuracy across all 26 cipher keys

3.2x

Security Enhancement

Increased resistance to pattern analysis attacks

<200ms

Processing Latency

Real-time encryption-decryption speed

Practical Deployment in ChatMessenger

The system has been successfully integrated into ChatMessenger, providing end-to-end encryption for secure messaging. Users benefit from enhanced data confidentiality whilst experiencing seamless communication with minimal latency. The adaptive nature of the system allows it to evolve against emerging threats, making it suitable for financial services, healthcare communications, and government applications requiring robust data protection.

Challenges, Limitations and Future Directions

Current Limitations

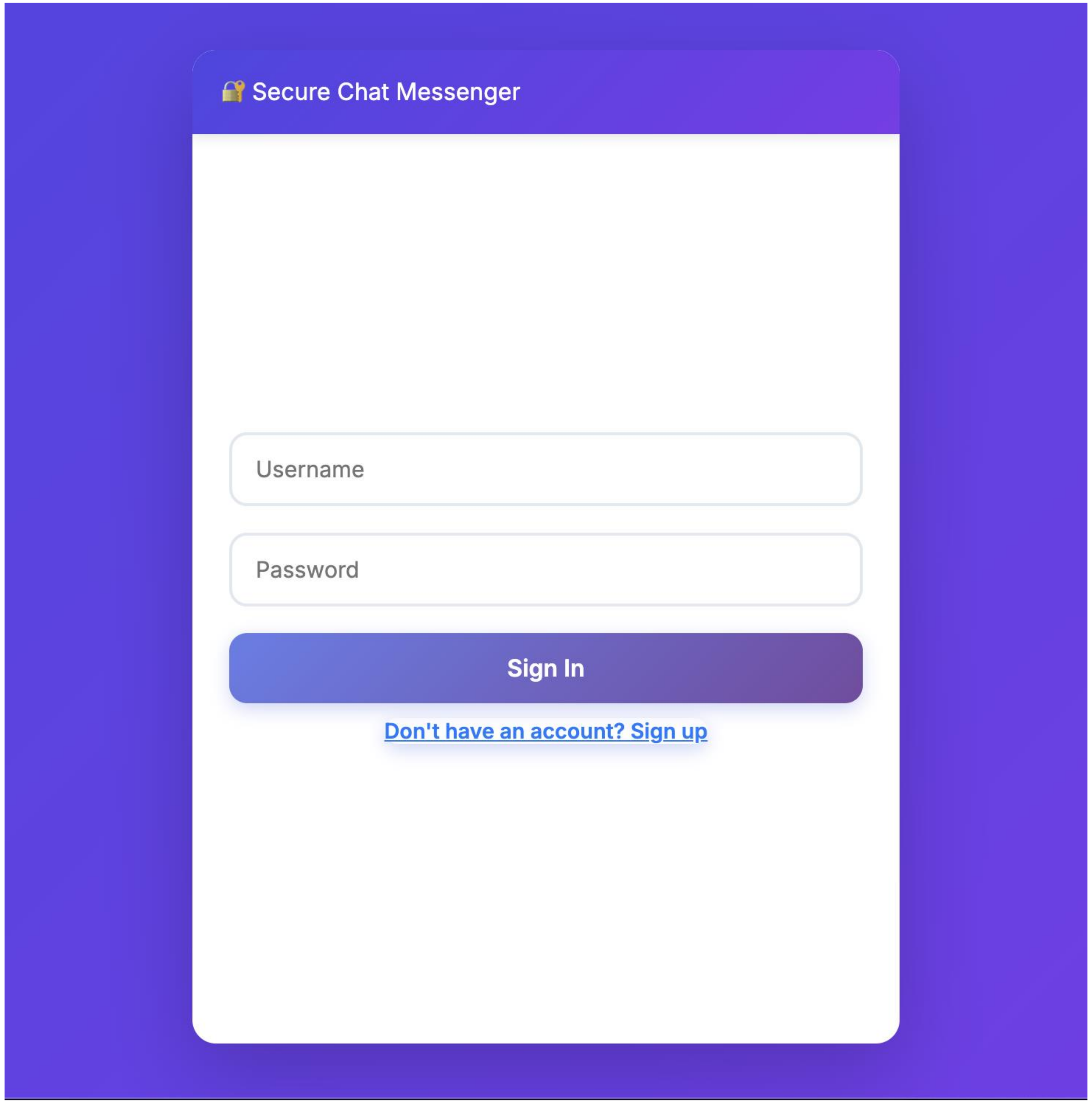
- Computational overhead during GAN training phase requires significant GPU resources
- System currently optimised for text; extending to multimedia requires architectural modifications
- Caesar cipher foundation, whilst enhanced, limits applicability for high-security military applications

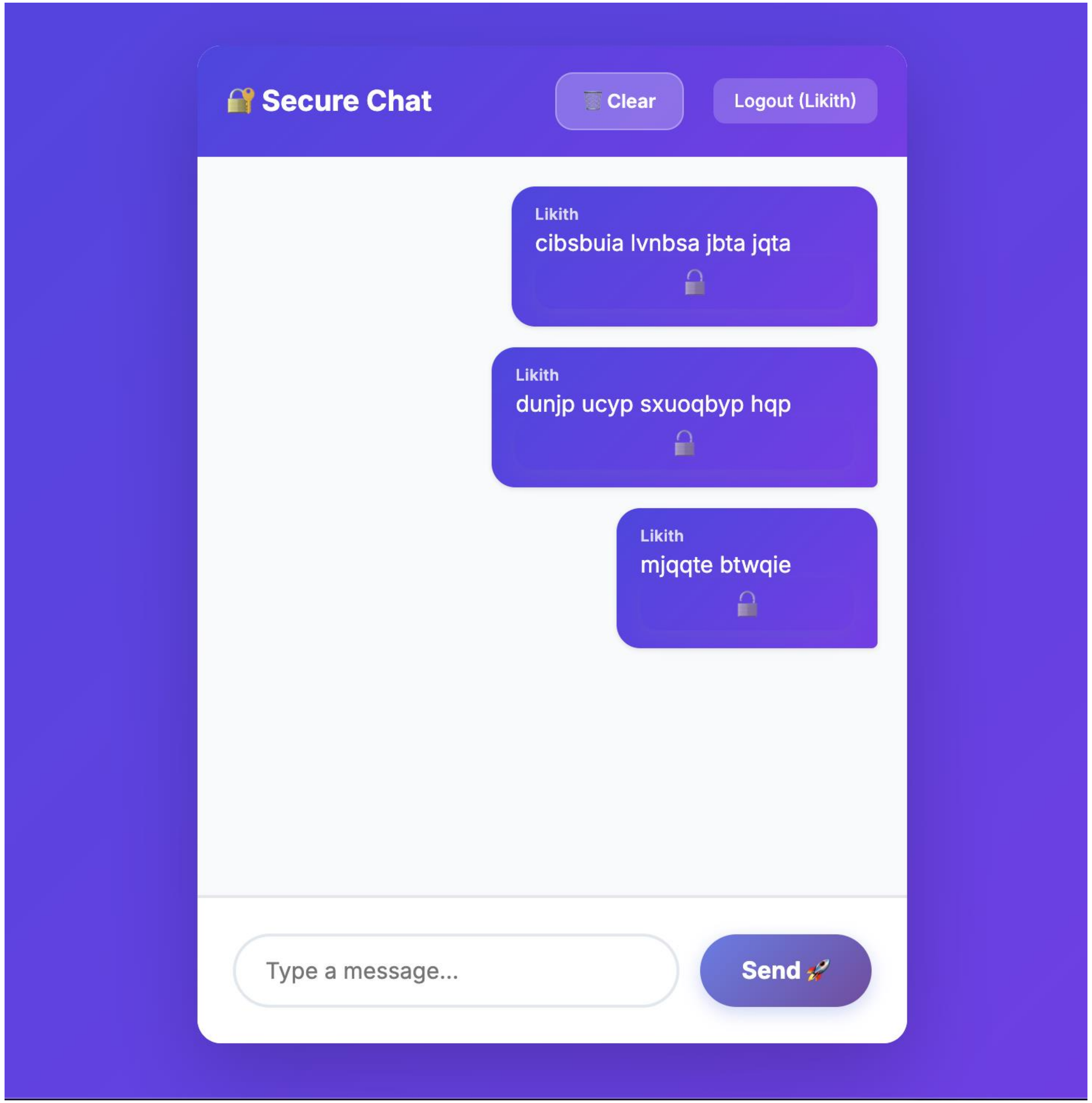
Risks and Mitigation

- **Model Overfitting:** Addressed through dropout and diverse training data
- **Adversarial Attacks:** Continuous GAN training provides adaptive defence
- **Key Management:** Integration with PKI systems ensures secure key distribution

Conclusion

This research demonstrates that combining classical cryptography with modern deep learning creates a practical, adaptive encryption system. By leveraging LSTM networks and GAN-based enhancement, we achieve significant improvements in data security whilst maintaining operational efficiency. Future work will explore quantum-resistant algorithms and extension to multimedia content, positioning this approach at the forefront of next-generation cybersecurity solutions.





Likith
cibsbuia lvnbsa jbta jqta
🔒

Likith
dunjp ucyp sxuoqbyp hqp
🔒

Likith
mjqqte btwqie
🔒