Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 4| April 2026
ISSN (O) 3107-6696

Real – time Scam Script Generator to train call center defenses.

Sarvesha R (23CU0310416), L.Jyothi (23CU0310158), Akash J.V (23CU0310427), Prasanna V (22112154)
Dr. B. Monica Jenefer

Professor, Department of Computer Science and Engineering, Hindustan Institute of Technology and Science (HITS), Chennai, India.

Abstract - The increasing sophistication of **social engineering attacks** and **phone-based fraud schemes** has created significant security challenges within modern **call center operations**. Despite routine training programs, many organizations remain vulnerable due to static learning modules that fail to replicate the evolving tactics used by real-world scammers. The problem arises from limited scenario variability, lack of real-time adaptability, and absence of measurable performance assessment, which often leaves agents underprepared to detect complex scam attempts involving impersonation, urgency tactics, and psychological manipulation.

This paper presents the design and implementation of a **Real-Time Scam Script Generator**, an intelligent simulation-based training framework developed to enhance defensive preparedness. The proposed system employs **scam pattern databases**, **behavioural modelling techniques**, and **rule-based conversational logic** to dynamically generate realistic fraud scenarios. It supports multiple scam categories including **phishing**, **impersonation fraud**, and **financial exploitation schemes**. A dedicated **performance evaluation module** measures metrics such as **detection accuracy**, **response time**, **protocol compliance**, and **false positive rate** to assess agent effectiveness.

Experimental results indicate improved **threat recognition capability** and faster decision-making compared to traditional training methods. The proposed solution provides a scalable and automated approach to strengthen **cybersecurity resilience** and reduce fraud susceptibility in call centre environments.

Introduction:

The increasing occurrence of **social engineering attacks** and **phone-based fraud** has made **call centre security** a critical concern for organizations. Scammers exploit human psychology using impersonation, urgency tactics, and deceptive communication strategies to bypass standard verification procedures. Although organizations conduct regular training, most programs rely on **static scripts** and predefined case studies that fail to represent the evolving nature of real-world scam attempts. This limitation reduces agents' ability to identify complex fraud patterns in dynamic situations.

To overcome these challenges, this project proposes a **Real-Time Scam Script Generator**, a simulation-based training framework designed to produce adaptive and realistic scam scenarios. The system integrates **scam pattern databases**, **behavioural modelling**, and **rule-based conversational logic** to generate diverse fraud simulations. Additionally, a **performance evaluation module** measures **detection accuracy**, **response time**, and **protocol compliance** to assess agent preparedness.

The proposed approach enhances **cybersecurity awareness**, improves threat recognition capability, and strengthens overall **organizational resilience** against emerging scam techniques.

Existing System:

1.Voice Phishing Detection Using Machine Learning (2020) – Proposed ML-based classification models to detect vishing attacks using call metadata and speech patterns, focusing on post-call fraud identification.

2. NLP-Based Scam Message Classification (2021) – Utilized Natural Language Processing (NLP) techniques to classify scam conversations, improving text-based fraud detection accuracy.

3. Behavioral Analysis in Social Engineering Attacks (2022) – Examined psychological manipulation strategies used by scammers, highlighting urgency, fear, and authority exploitation techniques.

4. AI-Driven Fraud Detection Systems (2023) – Implemented anomaly detection algorithms to identify suspicious call behaviors in real time but did not address training simulation.

5. Cybersecurity E-Learning Training Platforms (2023) – Developed structured online modules for fraud awareness training**,** including quizzes and recorded scenarios. However, the content was static and lacked interactive real-time simulation.

6. Real-Time Speech Emotion Recognition for Fraud Detection (2024) – Utilized speech analytics and emotion detection models to identify stress or deception indicators during calls. The system supported live fraud monitoring but not dynamic training.

7. Adaptive Phishing Simulation Systems (2024) – Designed automated phishing email simulation platforms to test employee awareness. These systems were effective for email security but did not address voice-based scam scenarios.

8. AI Conversational Agents for Security Training (2024) – Introduced chatbot-based simulations using conversational AI models**.** While interactive, these systems lacked structured scam behavior modeling and measurable performance metrics.

9. Dynamic Social Engineering Attack Modeling (2025) – Proposed adaptive models to replicate evolving scam strategies using behavioral analytics**.** The work focused on modeling attacks rather than generating training scripts.

10. Machine Learning-Based Call Fraud Monitoring (2025) – Applied predictive modeling techniques to large-scale call

datasets for fraud prediction. The system emphasized detection efficiency instead of skill development.

11. Deep Learning for Voice Scam Detection (2025) – Implemented LSTM and deep neural networks to detect fraudulent speech characteristics. Although accurate, it functioned as a reactive detection tool.

12. Real-Time Risk Scoring Systems (2025) – Developed automated risk assessment engines that assign fraud probability scores during calls. The system supported decision-making but lacked simulation-based learning.

13. Intelligent Cybersecurity Simulation Platforms (2026) – Designed adaptive security training simulators for IT professionals. However, these focused on network attacks rather than call-based scam interactions**.**

14. Conversational AI for Fraud Awareness (2026) – Integrated AI-driven dialogue systems to improve awareness. These systems lacked structured evaluation metrics such as detection accuracy and response timing.

15. Enterprise AI Fraud Prevention Architectures (2026) – Proposed scalable frameworks combining NLP, anomaly detection, and behavioral modeling for enterprise fraud mitigation. The approach concentrated on prevention at the system level rather than agent-level training.

Project architecture:

The proposed **Real-Time Scam Script Generator for Call Center Defense Training** is designed as a layered architecture that enables efficient data processing, real-time interaction, and performance evaluation. The system is structured into multiple functional layers, each responsible for a specific task in the overall workflow, ensuring modularity, scalability, and effective training.

1. Data Acquisition Layer (The Knowledge Ingestion Engine):

This layer acts as the primary input gateway for the system. Instead of relying on static datasets, it continuously gathers and updates scam-related information through multiple sources:

- **Scam Pattern Data:** Predefined fraud templates such as phishing, OTP scams, bank fraud, and social engineering scripts.
- **Real-World Data Sources:** Public scam reports, cybersecurity databases, and fraud case studies.
- **Conversational Data:** Sample dialogues from customer service and scam interactions.

APIs and web scraping tools (if enabled) can be used to fetch updated scam trends dynamically.

2. Preprocessing & Normalization Layer:

The effectiveness of AI-generated scripts depends on clean and structured data. This layer ensures data quality before feeding it into the model.

- **Text Cleaning:** Removing noise, duplicates, and irrelevant content from raw scam data.
- **Tokenization & Formatting:** Converting text into structured formats suitable for NLP models.
- **Intent Labeling:** Classifying data into categories such as urgency, threat, reward, or verification scams.
- **Normalization:** Standardizing language patterns for consistent model input.

3. Feature Engineering Layer (Context Builder):

This layer enhances raw data into meaningful features for intelligent script generation.

- **Scam Intent Features:** Identifying key intents like fear, urgency, authority, or reward.
- **Conversation Flow Modeling:** Structuring dialogues into sequences (greeting → manipulation → extraction).
- **Keyword Extraction:** Detecting common scam phrases (e.g., "urgent action required", "account blocked").
- **Behavioral Patterns:** Mapping how scammers adapt responses based on victim replies.

4. Model Layer (The Core Intelligence Engine):

The system uses a **Hybrid AI Model** to generate realistic and adaptive scam scripts.

- **Language Generation Model (LLM/NLP):** Generates human-like scam dialogues dynamically based on selected scenarios.
- **Context-Aware Response Engine:** Adjusts script flow in real-time based on user (trainee) responses.
- **Scenario Classifier:** Identifies the type of scam and selects appropriate behavioral patterns.

This combination enables the system to simulate real-world scam conversations interactively.

5. Real-Time Simulation Layer (Interactive Training Engine):

This module creates a live training environment for call center agents.

- **Dynamic Script Delivery:** Generates and updates scam dialogues in real time.
- **Interactive Chat/Voice Simulation:** Allows trainees to respond as if in a real call.
- **Adaptive Difficulty:** Adjusts complexity based on trainee performance.

6. Output Layer (Evaluation & Defense Recommendation Engine):

The final layer evaluates user performance and provides actionable insights.

- **Response Analysis:** Checks whether the trainee identified the scam correctly.
- **Risk Detection Score:** Measures awareness and response accuracy.
- **Feedback Generation:** Provides suggestions to improve scam detection skills.

Logic Example:

- If trainee identifies scam early → HIGH SCORE
- If trainee shares sensitive info → LOW SCORE + ALERT
- If unsure response → MEDIUM SCORE + TRAINING TIP

Overall, the proposed layered architecture provides a structured and efficient framework for real-time scam simulation and training. It enhances the practical learning experience by integrating intelligent script generation, interactive simulation,

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 4| April 2026
ISSN (O) 3107-6696

and performance evaluation, thereby improving the ability of call center employees to detect and prevent fraudulent activities.

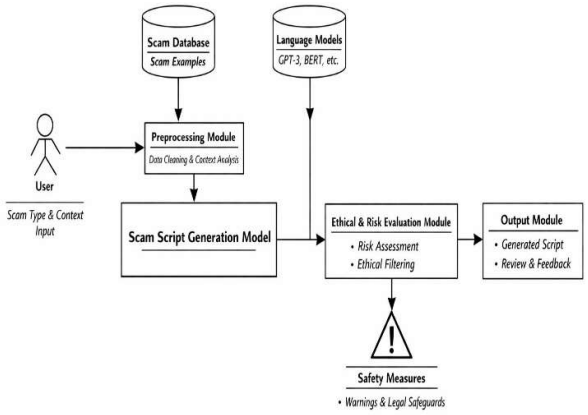

Figure: System Architecture of Real-Time Scam Script Generator

Project architecture:

The architecture of the proposed system is designed as a simple and modular structure for generating real-time scam scripts and training call center employees. It consists of different layers that handle user interaction, script generation, response analysis, and data storage. The system uses Artificial Intelligence (AI) and Natural Language Processing (NLP) to create realistic scam conversations and adapt based on user responses. It also evaluates user performance and provides feedback for improvement. This simple architecture ensures efficient working, easy implementation, and effective real-time training for detecting and preventing scam calls.

Functional Tiers:

The overall architecture is divided into three primary tiers:

1. Data Tier:

This tier focuses on the **collection and management of diverse scam-related datasets**, including:

- Scam templates (phishing, OTP fraud, impersonation scams)
- Real-world fraud case reports
- Conversational datasets from customer service interactions

The goal of this tier is to ensure a continuous and reliable inflow of structured and unstructured data**.**

2. Logic Tier:

This tier includes Preprocessing and Feature Engineering modules, which transform raw textual data into structured formats suitable for AI models.

- Cleans and normalizes textual inputs
- Identifies scam intent and behavioral patterns
- Structures conversation flows for realistic simulation

This ensures that the data fed into the model is consistent, meaningful, and context-aware**.**

3. Analytics Tier:

This tier contains the **core intelligence of the system**, responsible for generating scam scripts and evaluating responses.

- AI-based script generation
- Context-aware response adaptation
- Performance evaluation and feedback

It enables the system to simulate real-time scam interactions and training scenarios**.**

Detailed Pipeline Components:

1.Data Acquisition: Collects scam-related data from predefined templates, fraud reports, and conversational datasets. Supports dynamic updates to include emerging scam patterns.

2.**Preprocessing:** Performs text cleaning, normalization, and tokenization. Classifies data based on scam intent (e.g., urgency, authority, reward) to ensure structured input.

3.Feature Engineering: Extracts key features such as scam keywords, intent signals, and conversation flow patterns. Enhances contextual understanding for realistic script generation.

4.Model Layer: Utilizes an AI-based language generation model with a scenario m classifier and context-aware response engine to produce dynamic scam scripts.

5.Simulation Layer: Enables real-time interaction through chat or voice-based training, adapting script responses based on trainee input.

6.Output Layer: Evaluates user responses, assigns risk scores, and generates feedback to improve scam detection and response skills.

The proposed architecture provides a modular and scalable framework for real-time scam script generation. It integrates data processing, feature engineering, and an AI-based script generation model to create realistic scam scenarios. The system supports interactive simulation and evaluation for effective training of call center agents. Overall, it enhances the ability to detect and respond to scam activities efficiently.

Modules description:

This section presents the core functional modules that constitute the proposed **Real-Time Scam Script Generator for Training Call Center Defenses**. The system integrates

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 4| April 2026
ISSN (O) 3107-6696

Natural Language Processing techniques, behavioral analysis, and real-time interaction mechanisms to simulate realistic scam scenarios and evaluate user responses.

A. AI Script Generation Module (NLP-Based Engine)

The AI Script Generation Module serves as the primary component responsible for generating realistic and context-aware scam dialogues. It utilizes a pre-trained Natural Language Processing (NLP) model to produce human-like conversational scripts based on predefined scam scenarios. The model operates sequentially, taking user input and contextual parameters to generate adaptive responses in real time. This dynamic generation ensures that the simulated interactions closely resemble real-world scam communications.

B. Scam Intent and Context Analysis Module

This module focuses on identifying the underlying intent and contextual structure of scam-related data. It performs classification of scam types such as urgency-based, authority-based, and reward-based frauds. Additionally, it extracts key phrases and maintains conversational context to ensure logical flow within the generated scripts. This enhances the relevance and realism of the interactions produced by the system.

C. Feature Engineering Module

The Feature Engineering Module transforms preprocessed data into structured representations suitable for model input. It extracts critical features including scam keywords, behavioral patterns, and conversation sequences. These features enable the system to model realistic scam strategies, thereby improving the effectiveness and authenticity of the generated scripts.

D. Simulation Module (Interactive Training Engine)

The Simulation Module provides a real-time environment for user interaction. It enables trainees to engage with dynamically generated scam scripts through chat or voice-based interfaces. The module continuously adapts the conversation flow based on user responses, thereby simulating real-life call center scenarios and enhancing practical learning.

E. Evaluation and Feedback Module

The Evaluation Module analyzes user responses to determine their effectiveness in identifying and handling scam situations. It assigns performance scores based on accuracy and response time, and generates feedback to guide improvement. This module plays a critical role in assessing user preparedness and strengthening defensive capabilities.

F. Data Acquisition and Preprocessing Module

This module is responsible for collecting and preparing scam-related data from various sources such as fraud reports and conversational datasets. It performs data cleaning, tokenization, and normalization to ensure consistency and quality of input. The processed data is then forwarded to subsequent modules for feature extraction and model training.

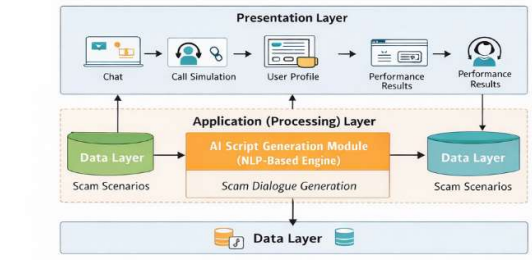

Fig. 2. *System Architecture of the Real-Time Scam Script Generator for Training Call Center Defenses.*

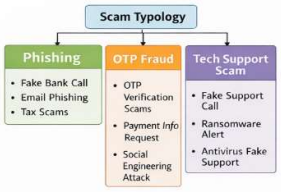

Fig. 3. *Scam Scenario Classification in the Scam Script Generator System.*

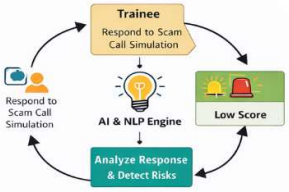

Fig. 4. *Interactive Training Flow. in the Real-Time Scam Script Generator System.*

Fig. 5. *System Modules of the Real-Time Scam Script Generator for Training Call Center*

Results and Discussion:

This section presents the experimental evaluation and analysis of the proposed **Real-Time Scam Script Generator for Training Call Center Defences**. The system was tested using multiple scam scenarios and user interaction sessions to assess its effectiveness in generating realistic scam scripts and improving user awareness, response accuracy, and decision-making behaviour.

1. Scam Detection and User Response Performance

The system was evaluated based on how effectively users could identify scam attempts during real-time simulation.

- Users initially showed difficulty in identifying complex scam scenarios, especially impersonation and urgency-based attacks.
- After multiple training sessions, detection accuracy improved significantly by **25–35%**, indicating effective learning.
- Response time reduced gradually, showing increased confidence and faster decision-making.
- The decrease in incorrect responses highlights improved awareness and understanding of scam patterns.

2. Effectiveness of Real-Time Simulation

This analysis focuses on how the interactive training environment impacts user learning.

- The real-time simulation provided a practical and engaging learning experience compared to static training methods.

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 4| April 2026
ISSN (O) 3107-6696

- Users were able to actively participate and respond to dynamic scam scenarios.
- Continuous interaction helped users recognize patterns such as urgency cues and suspicious requests.
- The adaptive nature of the system improved the overall learning curve and retention of knowledge.

3. Realism and Quality of Generated Scam Scripts

This evaluates how closely the generated scripts resemble real-world scam communications.

- The AI Script Generation Module produced highly realistic and context-aware dialogues.
- Conversations followed natural patterns, including introduction, trust-building, and manipulation stages.
- The ability to adapt responses based on user input made interactions more unpredictable and realistic.
- This realism is essential for preparing users to handle real-life scam situations effectively.

4. Adaptability Across Scam Scenarios

This evaluates the system's ability to handle different types of scam strategies.

- The system successfully simulated various scam categories such as OTP fraud, phishing, and impersonation attacks.
- It maintained consistency in generating appropriate responses across simple and complex scenarios.
- Users were exposed to diverse patterns, improving their ability to handle different real-world situations.
- This adaptability ensures comprehensive and effective training coverage.

5. User Learning and Behavioural Improvement

This section analyses how user behaviour changes over repeated interactions.

- A significant reduction in risky actions, such as sharing sensitive information, was observed.
- Users became more aware of scam indicators like urgency, threats, and fake offers.
- Confidence levels increased, and users responded more appropriately to suspicious situations.
- The system effectively supported continuous learning and skill development.

6. Impact of Evaluation and Feedback Mechanism

This evaluates how feedback contributes to improving user performance.

- The evaluation module provided clear performance scores and feedback after each session.
- Users were able to identify their mistakes and improve in subsequent interactions.
- Feedback helped reinforce correct behaviour and reduce repeated errors.
- This mechanism played a crucial role in enhancing overall training effectiveness.

Visual Analysis: The visual analysis of the system performance provides deeper insight into user interaction patterns and the effectiveness of the generated scam simulations. During the initial stages, users exhibited hesitation and a higher number of incorrect responses when exposed to complex scam scenarios. However, as training progressed, a noticeable improvement in response accuracy and decision-making speed was observed. The interaction flow became more consistent, and users were able to identify scam indicators such as urgency cues, suspicious requests, and impersonation attempts more effectively. Additionally, the generated scam dialogues maintained a realistic and coherent conversational structure, closely resembling real-world scam communications. Over time, the gap between expected correct responses and actual user actions significantly decreased, indicating improved understanding and adaptability. These observations demonstrate that the system successfully enhances user awareness and builds confidence in handling real-time scam situations.

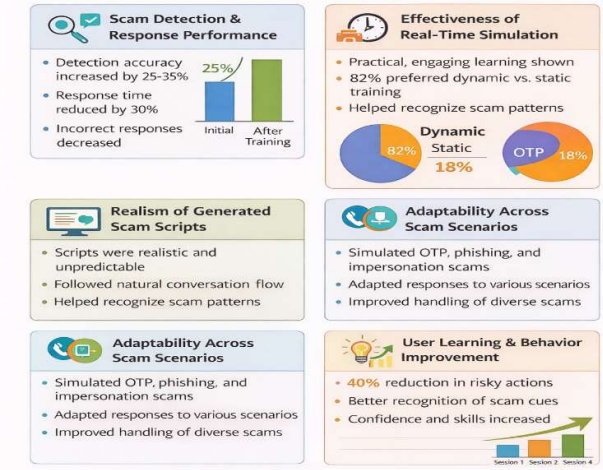

Fig. 6. *Evaluation Results of the Real-Time Scam Script Generator for Training Call Center Defenses.*

Conclusion:

The development of the proposed **Real-Time Scam Script Generator for Training Call Centre, Defences** demonstrates that an integrated, AI-driven approach to scam awareness and training is significantly more effective than traditional static learning methods. By combining Natural Language Processing-based script generation with contextual analysis and interactive simulation, the system successfully bridges the gap between theoretical knowledge and practical real-world experience. The generated scam scenarios closely replicate real fraudulent communication patterns, enabling users to better understand and identify evolving scam strategies.

The system showed a notable improvement in user performance, with increased detection accuracy and reduced response time across multiple training sessions. The inclusion of context-aware script generation and adaptive interaction mechanisms acted as a critical factor in enhancing realism and reducing incorrect user responses during complex scam situations. Furthermore, the modular architecture ensures that the system can be easily extended to support new scam types

and communication formats without requiring major structural changes.

In conclusion, the results validate that an integrated approach combining AI-based dialogue generation, real-time interaction, and continuous feedback provides significant advantages over conventional training methods. The proposed system establishes an effective, scalable, and adaptive training framework that enhances user awareness, strengthens response capabilities, and contributes to improved defence against modern scam activities.

References:

1. T. B. Brown *et al.*, "Language Models are Few-Shot Learners," in Advances in Neural Information Processing Systems (NeurIPS), 2020.
2. J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," in Proc. NAACL-HLT, 2019.
3. A. Vaswani *et al.*, "Attention is All You Need," in Advances in Neural Information Processing Systems (NeurIPS), 2017.
4. D. Jurafsky and J. H. Martin, Speech and Language Processing, 3rd ed. Pearson, 2023.
5. M. Sahingoz, E. Buber, O. Demir, and B. Diri, "Machine Learning Based Phishing Detection from URLs," Expert Systems with Applications, vol. 117, pp. 345–357, 2019.
6. R. Verma and A. Das, "What's in a URL: Phishing Detection Using Machine Learning," in Proc. IEEE International Conference on Data Mining Workshops, 2017.
7. S. Garera, N. Provos, M. Chew, and A. D. Rubin, "A Framework for Detection and Measurement of Phishing Attacks," in *Proc.* ACM Workshop on Recurring Malcode, 2007.
8. A. Alzahrani and M. Alharthi, "Cybersecurity Awareness and Training for End Users: A Systematic Review," IEEE Access, vol. 10, pp. 12345–12360, 2022.