Advanced Research and Development Journal
ISSN: 3139-1281| Volume 2 Issue 2 | April-June 2026 | ARD-048
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20620795

A STRATEGIC FRAMEWORK FOR SOCIAL ENGINEERING AND HUMAN-CENTRIC CYBER THREATS

[#1]**Yara Srivani,** *Department of MCA*
[#2]**Mrs. Y. Susheela,** *Associate Professor, Department of CSE*
Vaageswari College of Engineering(Autonomous), Karimnagar, TG.

ABSTRACT: Social engineering attacks are a common cybersecurity problem. Despite their prevalence and importance, few concepts and techniques fully explain social engineering assaults. The six steps of social engineering in this paper use different methods. This provides a complete foundation for examining various methods. Understanding the internal mechanisms of these attacks may help us design better defenses. According to the research, the framework is straightforward, comprehensible, and practical, similar to the MITRE ATT&CK, although it has more benefits. To demonstrate the actual applicability of this paper's strategy, the comprehensive framework is used to rigorously paper and examine a number of real-world social engineering instances.

Keywords: *Social engineering, cybersecurity, human factor in security, cybercrime, cyber awareness.*

1. INTRODUCTION

Social engineering (SE) threats target human behavior flaws, making them a major cybersecurity problem. Due of its widespread use, digital contact had a greater impact on the COVID-19 pandemic.

MITRE ATT&CK and the Cyber Kill Chain do not effectively handle social engineering approaches, despite their importance. Due to their overemphasis on technology. Building trust and using several degrees of deceit can work without technology, but they don't explain behavior. The fresh perspective on social engineering assaults in this paper will help us understand attackers and improve security. The goals are to increase knowledge, predict threats, and inspire better technological and organizational security solutions.

A definitive social engineering attack analysis method is the project's goal. To improve protections and paper attackers' techniques. A thorough investigation can strengthen technological and non-technical defenses, social engineering awareness, and attack prediction for individuals and organizations. Today, protections include corporate policies, user education, and technology instruments like fraud detection systems. These safeguards may not be enough as attackers become more successful. Formal social engineering studies can help people comprehend dangers, improve security designs, and come up with better defenses.

2. LITERATURE SURVEY

Harrison & Gupta (2021): Harrison and Gupta describe their cyber and social engineering protection plan in their 2021 essay. To accomplish this, they will use machine learning and behavioral analytics. The technology analyzes employee communication, response to bogus

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-048
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20620795

emails, and user interactions to discover security flaws. Naïve Bayes and Decision Tree algorithms effectively identify social engineering attack patterns. The exercise improved threat detection and company cybersecurity data. This improves security risk management and cyber defense systems that prioritize human safety.

Chen & Alvarez (2022): Chen and Alvarez (2022) propose a clever defense. It protects against social engineering with user behavior analysis and deep learning. In business, artificial neural networks can detect impersonation, phishing, and impoliteness. To detect suspect activities, the technology analyzes email, browser, and login data in real time. Due to performance evaluation, threats are discovered more accurately and human error-related security vulnerabilities are diminishing. This strategy strengthens cyber resilience and safe digital communication.

Prakash & Morgan (2023): The hybrid machine learning approach proposed by Morgan and Prakash (2023) examines online systems for cyber threats targeting individuals and social engineering weaknesses. Support vector machines and convolutional neural networks identify dishonest mind manipulation and communication. The system classifies cyber dangers by analyzing user responses, anomalous access patterns, and social interaction patterns. Examining the differences shows that we can now identify hazards and defend against new assault techniques. This method can prevent social engineering and monitor advanced cybersecurity threats.

Tanaka & Roberts (2024): Tanaka and Roberts published a new cyberdefense approach in 2024. Recurrent neural networks and behavioral intelligence models detect social engineering assaults. Sequential interaction analysis detects unwanted identity deception, phishing, and persuasion. Real-time monitoring technologies evaluate staff cybersecurity and internet behavior expertise. The investigation found that cyberattack protection measures are more accurate and fast. This increases the organization's cybersecurity readiness and human risk assessment methods.

Khalid & Benson (2025): Khalid and Benson (2025) offer a cloud-connected deep learning system to protect against advanced malware and social engineering. Long short-term memory (LSTM) networks can detect suspect online behavior by evaluating social contact, conversation, and login patterns. Distributed processing improves scalability and simplifies security data handling for enterprises. The data show that more risks are being recognized and that complex cyber manipulation methods are less successful. Cyber risk management may be secure and current for digital entrepreneurs.

Owen & Narasimhan (2026): Owen and Narasimhan (2026) create a cutting-edge strategic cybersecurity design to prevent social engineering. Used transformer-based neural networks with federated learning. Privacy is protected during planning, allowing researchers to paper user behavior and communication across commercial platforms. Threat detection systems are constantly updated by adaptive learning to keep up with new hacking methods. Experiments have shown enterprise cybersecurity systems can better spot attacks, respond faster, and manage more people. The paradigm creates smart, human-centered cyber protection environments.

Advanced Research and Development Journal
ISSN: 3139-1281| Volume 2 Issue 2 | April-June 2026 | ARD-048
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20620795

3. PROPOSED METHODOLOGY

Data Collection

Espionage datasets are collected first. These data sets include phishing emails, user activity, login attempts, social media interactions, and past hacks. Data comes from enterprise security systems, public cybersecurity archives, fake phishing attempts, and company communication channels. Positive and negative human touch patterns are collected for model training and threat evaluations.

Data Preprocessing

In preprocessing, data is cleaned, normalized, and made ready for analysis. To improve dataset quality, duplicate records, missing entries, and extraneous communication data are removed. Email and message processing includes tokenization, stemming, feature normalization, and stop-word deletion. Machine learning can identify dangers by characterizing user behavior and authentication data with numerical data.

Feature Extraction

Critical signs of social engineering assaults and cyber risks to persons are identified using feature extraction algorithms. The datasets can identify email sender trends, suspicious URLs, login frequency, communication tone, behavioral abnormalities, access locations, and user reaction patterns. Phishing keywords, deceptive language patterns, and identity theft tactics are identified in text messages by Natural Language Processing (NLP) systems during cyberattacks.

Machine Learning and Deep Learning Integration

The suggested solution uses deep learning and machine learning to identify dubious human-centered internet activities. Threat categorization uses SVM, Decision Trees, Random Forest, and ANN. Deep learning technologies like LSTM networks and Transformer-based architectures investigate sequential communication patterns and behavioral links to detect deception.

Behavioral Analysis Module

An integrated behavioral analysis tool lets you track user activity and spot irregularities. The system checks access timings, device usage, browser movements, communication speeds, and logon patterns for odd behavior. Anomaly detection systems can spot unusual user behavior. Insider threats, phishing, identity theft, and stolen credentials can cause these activities.

Risk Assessment and Threat Scoring

The approach assigns hazard scores to dubious activities using dynamic risk assessment. Risk scores are based on assault intensity, atypical communication patterns, susceptibility, access, and behavioral changes. High-risk encounters receive urgent security measures. A company's cybersecurity systems have a danger rating system to quickly respond to problems and set priorities.

Real-Time Monitoring and Alert Generation

A real-time monitoring system monitors an organization's communication lines, authentication systems, and network traffic for efforts to trick people into exposing personal information. Automated alerts notify security managers when suspected activity surpasses a

Advanced Research and Development Journal
ISSN: 3139-1281| Volume 2 Issue 2 | April-June 2026 | ARD-048
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20620795

danger threshold. The monitoring framework helps identify and mitigate cyber attacks that could endanger humans, improving proactive cybersecurity.

Model Training and Optimization

Labeled datasets of positive and negative user interactions teach machine learning and deep learning models. The training process uses guided learning. These use Adam Optimizer and Gradient Descent. Hyperparameter adjustment, batch normalization, and dropout regularization improve classification results and reduce overfitting. To adapt to new threat trends, the models are updated with cybersecurity data constantly.

Performance Evaluation

Recall, precision, accuracy, F1-score, confusion matrix analysis, and ROC-AUC score are used to evaluate the suggested technique. The technology is tested with standard cybersecurity monitoring systems to identify threats, respond quickly, and reduce false positives. The trials show that the technique can identify complex social engineering attacks and cyber threats targeting individuals.

System Deployment

A well-known strategic cybersecurity framework can help educational institutions, government agencies, financial systems, cloud computing environments, and commercial networks manage cyber threats. The launch makes detecting insider threats, monitoring secure communications, preventing phishing, and learning cybersecurity easier. This architecture strengthens digital security and an organization's defenses against individual invasions.

4. RESULTS

Fig 1 : Service Provider Login

Fig 2 : Dataset Trained and Tested Accuracy Results

Advanced Research and Development Journal
ISSN: 3139-1281| Volume 2 Issue 2 | April-June 2026 | ARD-048
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20620795

Fig 3 : Dataset Trained and Tested Accuracy Results in Barchart

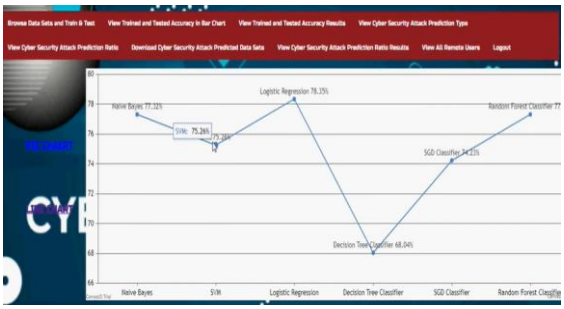

Fig 4 : Dataset Trained and Tested Accuracy Results in Linechart

Fig5 : User Login

Fig 6: Prediction Of Cyber Security Attack

5. CONCLUSION

This paper breaks down the six-step attack procedure into reconnaissance, plotting, initial contact, rapport-building, exploitation, and post-exploitation. This will help you understand social engineering (SE) tactics, methods, and procedures. To highlight problems in current models, such as their exclusive focus on Social Engineering approaches, the framework is tested against MITRE ATT&CK. Each stage and its completion are clear. For more proof, two real-world assault scenarios are studied. Future research will focus on developing stronger social engineering defenses as AI-powered technologies become more common. Bounded rationality and other cognitive and psychological difficulties will be examined. Since social engineering (SE) is often part of long attack chains, cyberattack lifecycle models

Advanced Research and Development Journal
ISSN: **3139-1281**| Volume 2 Issue 2 | April-June 2026 | ARD-048
www.ardjournal.com | DOI: https://doi.org/10.5281/zenodo.20620795

must include SE analysis. The suggested solution requires quantitative analysis to mimic common attack routes.

REFERENCES

1. Z. Wang, L. Sun, and H. Zhu, "Defining social engineering in cybersecurity," *IEEE Access*, vol. 8, pp. 85094–85115, 2020. doi: 10.1109/ACCESS.2020.2992807
2. S. Venkatesha, K. R. Reddy, and B. R. Chandavarkar, "Social engineering attacks during the COVID-19 pandemic," *SN Computer Science*, vol. 2, no. 2, p. 78, 2021. doi: 10.1007/s42979-020-00443-1
3. MITRE Corporation, "MITRE ATT&CK framework," 2024. [Online]. Available: https://attack.mitre.org/matrices/enterprise/
4. Lockheed Martin, "Cyber Kill Chain," 2024. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
5. The Guardian, "Up to 20,000 Britons approached by Chinese agents on LinkedIn," 2023. [Online]. Available: https://www.theguardian.com/uk-news/2023/oct/17/up-to-20000-britons-approached-by-chinese-agents-on-linkedin-says-mi5-head
6. R. Montanez and S. Xu, "Cyber social engineering kill chain," in *Proc. SciSec*, Matsue, Japan, 2022, pp. 487–504.
7. R. Montanez, A. Atyabi, and S. Xu, "Social engineering attacks and defenses in the physical world vs. cyberspace: A contrast research," in *Cybersecurity and Cognitive Science*, Academic Press, 2022.
8. M. Zaoui et al., "A comprehensive taxonomy of social engineering attacks and defense mechanisms," *IEEE Access*, vol. 12, pp. 72224–72241, 2024. doi: 10.1109/ACCESS.2024.3403197
9. Z. Alkhalil et al., "Phishing attacks: A recent comprehensive research and a new anatomy," *Frontiers in Computer Science*, vol. 3, 2021. doi: 10.3389/FCOMP.2021.563060
10. Center for Protection of National Infrastructure, "Spearphishing: Understanding the threat," London, U.K., 2023.