Reducing Organizational Vulnerabilities to Social Engineering via Risk Prediction

Md. Jamaluddin Mondal[1], Pranab Kanti Roy[2], Anirban Mitra[3*], Subrata Paul[4], Ramakant Bhardwaj[5], Pranabesh Ghosh[6]

[1]Dept. of Computer Science, Seacom Skills University, WB, India
[2]School of Engineering, Seacom Skills University, WB, India
[3]Dept. of CSE, Amity University Kolkata, Newtown, WB, India
[4]Dept. of CSE-AI, Brainware University, WB, India
[5]Department of Mathematics, Amity University Kolkata, Newtown, WB, India
[6]Dean of Doctoral Studies, Seacom Skills University, WB, India

mondaljamaluddin@gmail.com[1], roypranab549@gmail.com[2], amitra@kol.amity.edu[3*], subratapaulcse@gmail.com[4], drrkbhardwaj100@gmail.com[5], doctorpranabeshghosh@gmail.com[6]

[*]Corresponding Author

Abstract: Social Engineering attacks circumvent technological defences and jeopardise organisational security by manipulating human psychology by taking advantage of authority, urgency, and trust considerations. In order to foresee and mitigate such attacks, this study presents a behaviorally-driven approach that integrates psychological insights with Social Network Analysis (SNA). The framework's fundamental component is the BRP algorithm, which divides people into high-, medium-, and low-risk groups by calculating a Risk Index (RI) for each individual based on behavioural and network centrality measures. The findings demonstrate how the framework dramatically raises the training completion rate from 70% to 90% and lowers phishing success rates from 60% to 30%. The study actually emphasises the benefits of customised actions, updated regulations, and advanced detection technologies that raise security metrics and improve organisational resilience. This paradigm is especially pertinent to the medical and rehabilitation fields, where maintaining uninterrupted operations and protecting sensitive patient data are essential. It also offers a proactive, flexible way to combat these constantly evolving social engineering risks by addressing human vulnerabilities while taking technical defence into account.

Keywords: Social engineering, behavioral analysis, attack prediction, security framework, medical, rehabilation, organizational resilience.

1. Introduction

One of the most common and enduring cybersecurity threats is social engineering, which compromises security systems by taking advantage of human flaws rather than technical ones. While the majority of traditional cyberattacks involve compromising software or hardware, social engineering attacks take advantage of human behavior by using authority biases, urgency, and trust to obtain sensitive data or obtain unauthorized access. The strategies of phishing, baiting, pretexting, and vishing are also included. It focuses on the organization's and individual's psychological makeup to carry out the attack effectively. The expansion of the digital world with interconnected technologies and a rise in online interactions has significantly expanded attack surfaces. One of the most important fields for defense and study nowadays is social engineering (Salahdine & Kaabouch, 2019).

Even if technology security measures have advanced significantly, human vulnerabilities continue to be the biggest issue. Because social engineering uses fundamental psychological concepts that get past even the strongest security measures, it frequently succeeds. Attackers may, for example, pretend to be reliable organizations in order to obtain private information or instill a sense of urgency that leads individuals to act hastily. These deceptive strategies highlight how crucial it is to address psychological aspects in addition to technological protections. There is a significant gap in the behavioral aspects of the social engineering attack, though, as many of the frameworks currently in use focus primarily on technology-based solutions (Syafitri et al., 2022). A few social engineering strategies and countermeasures are shown in Table 1.

Tactic	Psychological Manipulation	Suggested Countermeasure	Example Application
Phishing	Trust, Urgency	Training, Email Filtering	Employee Training Program
Pretexting	Authority Bias	Verification Protocols, Role-Based Access	Strict Caller Verification
Baiting	Curiosity, Greed	Awareness Campaigns	Avoiding Suspicious Links
Social Media Exploits	Trust, Over-sharing	Privacy Settings Training	Limiting Data Sharing Online

Table 1. Summary of Social Engineering Tactics and Countermeasures

In industries like medicine and rehabilitation, where data breaches can have serious repercussions like compromised patient confidentiality and operational disruptions, social engineering assaults continue to be a major worry. Healthcare networks have become more interconnected, which has raised the attack surface and made it simpler for bad actors to take advantage of systemic and human weaknesses. It is crucial to handle social engineering challenges in these sectors since they put sensitive data, like as patient records and treatment regimens, at risk (Satpute et Al., 2021).

In order to detect and lessen social engineering risks, this study suggests a behaviorally-driven framework that integrates behavioral insights with social network analysis (SNA). The framework's foundation is an examination of network measurements like centrality measures in conjunction with human inclinations including urgency, trust, and authority biases (Paul et Al., 2024). Fundamentally, the framework revolves around the BRP algorithm, which uses network influence and manipulation susceptibility to determine a risk index for a particular person. By doing this, companies can more effectively identify high-risk personnel and implement interventions that may include real-time monitoring technologies, policy revisions, and targeted training programs.

In tackling the problem of social engineering, the framework fundamentally represents a paradigm shift, making human conduct the crucial element of security. By bridging behavioral and technical problems, it has taken a proactive, flexible stance in reducing the dangers of social engineering. Through the utilization of data-driven technologies and psychological analysis, the framework not only promotes organizational resilience but also cultivates a culture that is cognizant of security. Through theoretical modeling and empirical validation, this study will show how effective the framework is at giving organizations a road map for successfully fending off the evolution of social engineering threats. The goal of this research is also to create a defence system that is suited to these high-stakes situations, highlighting the necessity of both technical and behavioural responses.

2. Related Work

The necessity of addressing human vulnerabilities in cybersecurity is established by a comprehensive study. By interviewing responders from a range of businesses that continued socially engineered ransomware attacks, Bello & Maurushat (2020) discovered gaps in cybersecurity knowledge and training. The study suggests training strategies designed to increase users' resistance to these dangers. In 2020, Ahmed et al. presented an EmRmR technique that uses feature selection and optimized Windows API call sequences to enhance ransomware detection. To guarantee high accuracy in the scalable identification of ransomware variations, two deep learning frameworks have been developed and proposed: supervised and semi-supervised. Testing revealed that experimental results outperformed conventional methods in the early stages of ransomware detection. In their non-signature-based detection method, Ahmed et al. (2020) employed EmRmR to identify pertinent features and remove noisy ones from the Windows API call sequences. The suggested method offers high ransomware detection accuracy with low false positives while lowering computational cost and call trace size. Its superiority over the current behavioral-based detection techniques was demonstrated by experimental evaluation.

Overlaps in enforcement between the DMA and competition law are examined by Ribera Martínez (2023) in its examination of the interaction between the CJEU's decisions in Bpost and Nordzucker and the double jeopardy principle. In order to address the incoherent application, a paper identifies a narrow gap for the competition authority's enforcement activities and proposes segmenting enforcement efforts according to the sorts of services offered in digital markets. By taking into account parameters like domain age and URL length, as well as attributes in HTML/JavaScript, Baliyan & Prasath (2024) used ensemble machine learning models to detect phishing websites with 91% accuracy. In the end, the ensemble approach demonstrated its promise for improved online security by outperforming individual models like Random Forest and Logistic Regression. More

characteristics and advanced ensemble techniques should be incorporated throughout future studies in this field to combat phishing assaults. In order to improve threat detection and mitigation, Ofoegbu et al. (2024) offer an active cybersecurity framework that combines user-centric security procedures with data-driven analytics. This method incorporates user behavior, network traffic insights, and tailored security training to take into account both human and technology vulnerabilities. Case studies show improved security resilience, faster response times, and more accurate threat detection. Because individuals are the weakest link in cyber protection, Udofia (2024) emphasizes that human-centric behaviors in cyber defense put the human on center by focusing on awareness and training that will minimize risks. In order to help end users, IT specialists, and executives strengthen their cyber security, this chapter offers best practices and tactics for a range of roles. It also emphasizes the significance of workplace culture and corporate rules in fostering cyber-safe practices.

2.1 Research Gap

Even though a lot of research has been done on many cybersecurity topics, there is still a big gap in threat mitigation when it comes to combining behavioral insights with sophisticated detection systems. Although Bello & Maurushat (2020) emphasized the value of customized training methods to increase user resistance to socially engineered attacks, they did not investigate how to combine these methods with sophisticated detection systems. Machine learning-based techniques for ransomware detection, such as the Enhanced Maximum-Relevance and Minimum-Redundancy method, have been proposed by Ahmed (2020) and Ahmed et al. (2020). Technical optimization was the foundation of their work, and user behavior's contribution to strengthening these defenses was not taken into account. In the same way, Ribera Martínez (2023) noted difficulties with enforcement in digital markets but neglected to address behavioral elements that influence adherence. Although Baliyan & Prasath (2024) demonstrated the usefulness of ensemble models in identifying phishing attempts, more features and sophisticated methods are needed to boost adaptability. While Udofia (2024) highlighted the human weaknesses in cybersecurity, Ofoegbu et al. (2024) created a proactive architecture that integrated analytics and user-centric protocols. However, neither study has gone so far as to combine behavioral and network-based findings into a single prediction paradigm.

By combining behavioral assessments with social network analysis (SNA) to identify and prioritize high-risk individuals, our suggested Behavioral-Driven Framework closes the gaps that have been found. Predictive analytics and customized training programs will ensure that the technical solution is complemented by improved user awareness and behavior. BRP offers a dynamic risk assessment based on changing risks, bridging the gap between strictly technological approaches and more human-centric ones. The framework's all-encompassing strategy for fixing vulnerabilities guarantees a stronger and more thorough defense against social engineering and other online dangers.

3. Proposed Framework

A multi-layered security system is created by combining behavioral analysis and social network insights in the Behavioral-Driven Framework to prevent social engineering attacks (Montañez et al., 2020). The framework is basically made up of three interrelated modules: the Integrated Defense Mechanism, the Network Assessment Module, and the Behavioral Analysis Module. Individual psychological inclinations including trust, urgency, and authority bias—all of which are frequently targeted for manipulation in social engineering attacks—are assessed using the Behavioral Analysis Module. These variables are measured via surveys, event data from the past, and behavioral evaluations, providing a comprehensive risk profile for every person. In the meantime, the Network Assessment Module calculates the centrality measures of degree, betweenness, and proximity in order to examine the network's structural characteristics. It highlights clusters, bridging roles, and key nodes. It may also highlight organizational structure weaknesses. All things considered, the modules offer a comprehensive perspective on how the risk landscape is constructed by individual susceptibilities and their locations within a network.

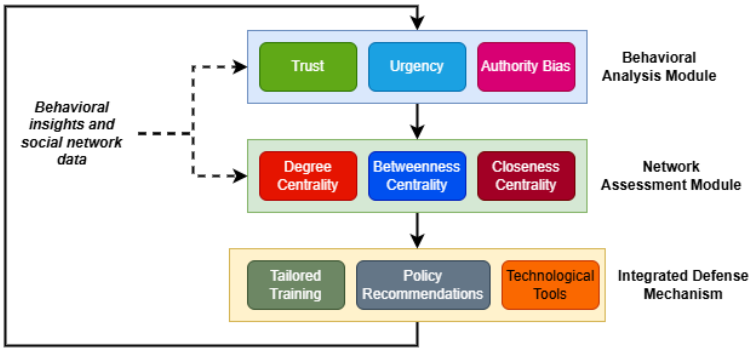

Fig 1. Proposed Framework

These insights are then used to inform the Integrated Defense Mechanism, which targets those threats with interventions. Higher risk individuals, or those with higher RI values, are involved in training programs intended to increase their awareness and fortitude in manipulative techniques. At the same time, policy suggestions regarding system vulnerabilities would be written, including stronger communication protocols, limitations on access to sensitive information, etc. In order to provide real-time defenses against such threats, sophisticated monitoring systems are also used as technological instruments to identify anomalous network behavior. This multi-layered strategy guarantees a comprehensive approach to addressing organizational and individual weaknesses. The interaction of these elements is depicted in Figure 1, which highlights the framework's adaptability and comprehensiveness by demonstrating the data flow from behavioral and network analysis to practical defense tactics.

3.1. Mathematical Formulation for Proposed Algorithm

The mathematical foundation of the suggested framework is the Behavioral Risk Prediction (BRP) algorithm, which combines behavioral insights with network metrics to measure the risk of each participant in a social network. This algorithm assesses psychological vulnerabilities including urgency bias and trust, which are frequently used in phishing attempts pertaining to healthcare. Fundamentally, the algorithm analyzes input data that includes behavioral risk variables and the social network graph. The social network is represented as $G = (V, E)$, where V denotes the set of nodes (individuals) and E represents the set of edges (relationships). Centrality metrics such as degree, betweenness, and closeness are calculated to evaluate each node's influence within the network. These metrics are normalized to ensure comparability across the network. Behavioral risk factors, including trust (T), urgency (U), and authority bias (A), are assessed through surveys or historical data. These factors are also normalized to align with the scale of centrality measures.

The Risk Index (RI) for each node is calculated by combining normalized centrality scores with behavioral risk factors using weighted coefficients. The normalized centrality scores for degree (NC_{DC}), betweenness (NC_{BC}), and closeness (NC_{CC}) are computed as follows:

$$NC(v) = \frac{C(v) - \min(C)}{\max(C) - \min(C)} \text{ for } c \in \{DC, BC, CC\}$$

Similarly, the behavioral risk factor (BRF) for each node is derived by averaging the normalized psychological scores:

$$BRF(v) = \frac{T(v) + U(v) + A(v)}{3}$$

The combined Risk Index (RI) is then calculated as:

$$RI(v) = w_1 . NC_{DC}(v) + w_2 . NC_{BC}(v) + w_3 . NC_{CC}(v) + w_4 . BRF(v)$$

where w_1, w_2, w_3, w_4 are weights assigned to reflect the relative importance of each factor. To classify nodes as high-risk, the algorithm compares each node's RI against a predefined threshold (τ):

$$V_{high-risk} = \{v \in V | RI(v) \geq \tau\}.$$

Above this point, nodes are classified as high-risk nodes and given more attention or training. The threshold's value is determined by the network's overall risk distribution and organizational risk tolerance. This mathematical modeling provides a solid foundation for reducing the danger of social engineering by taking into consideration both behavioral and structural weaknesses. The system can adapt dynamically to evolving threats by combining network data with psychological insights, which makes it applicable in a variety of organizational contexts. The process from the input data—behavioral scores and centrality metrics—to the outputs—ranked high-risk individuals and intervention plans—is shown in detail in Figure 2.

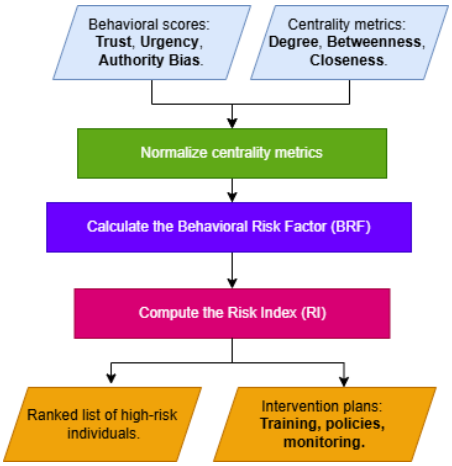

Fig 2. Flowchart of the BRP algorithm

The proposed approach also incorporates sector-specific modifications, like training with simulated healthcare scenarios and incorporating adherence to medical data protection laws (like HIPAA). The framework is intended to successfully improve the security posture of medical and rehabilitation facilities by including these sector-specific factors.

4. Results and Discussion

5.1 Data Collection

The suggested implementation entails gathering information from organizational-level surveys and simulated phishing campaigns to assess how successfully this framework detects and mitigates social engineering threats. By simulating phishing attacks in controlled settings, it will assess each person's vulnerability to manipulation techniques and offer insights into behavioral characteristics including trust, urgency, and authority bias. Organizational surveys that gather qualitative information on staff awareness, prior social engineering experiences, and compliance with current security protocols will be used to augment this. Social network graphs with nodes representing people and edges denoting interactions or communication patterns will be used to illustrate organizational ties. These graphs will be created using tools such as NetworkX. To determine who is influential in the network, centrality metrics including degree, betweenness, and closeness will be calculated for every node. Responses to customized questions will be used to quantify behavioral patterns, which will subsequently be combined with network indicators to produce thorough risk profiles.

5.2 Simulation Results

By combining behavioral risk indicators and centrality metrics, this suggested methodology shall uncover high-risk nodes, highlighting the people who are most vulnerable to social engineering attempts.

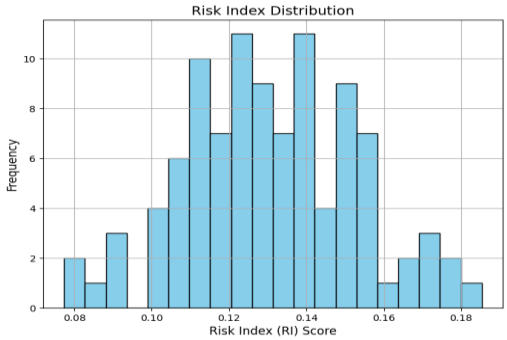

Fig 3. Risk Index Distribution

The risk index scores for each network member are plotted in Figure 3. The RI ratings in figure 3 are the result of combining structural network measures like degree, betweenness, and closeness centrality with behavioric characteristics like urgency, authority bias, and trust. The histogram shows how people are distributed across various risk levels and suggests the frequency of RI values. This will make it possible to target interventions and assist in identifying groups of people who are more likely to be the target of social engineering attacks.

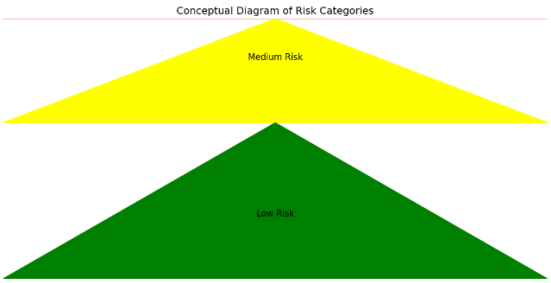

Figure 4: Conceptual Diagram of Risk Categories

Tiered Pyramid in Figure 4 classifies the people into high-, medium-, and low-risk groups based on their calculated RI scores. In addition to having more power inside the network, those at the top of the pyramid are more susceptible. The susceptibility of those in the middle tier is moderate. Low-risk people, on the other hand, are created at the wide base of the pyramid and have little exposure or vulnerability. The network's risk stratification is depicted in this figure, and each group needs a different approach to mitigation.

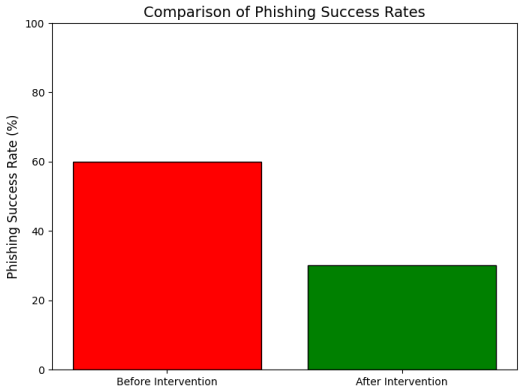

Figure 5: Comparison of Phishing Success Rates

Phishing success rates before and after the suggested framework was put into practice are contrasted in Figure 5. Following the implementation of focused training, revised policies, and sophisticated detection systems, the bar graph clearly shows a significant drop in phishing success rates, from 60% to 30%. This comparison demonstrates how well the suggested architecture mitigates social engineering risks and strengthens an organization's defenses against phishing attempts.

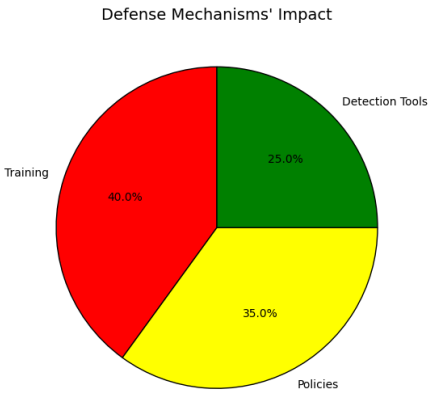

Figure 5: Pie Chart of Defense Mechanisms' Impact

Figure 5 shows how several defense mechanisms, including policies, detection tools, and training, are helping to lower the overall risk of social engineering attacks. According to a pie chart analysis, training has lowered risk levels the greatest at 40%, followed by policy updates at 35% and detection tools at 25%. This would imply that any multifaceted strategy must consider each of these elements since technical interventions and appropriate organizational policies must be employed in conjunction with user awareness and behavioral change.

Figure 6: Improvement in Security Metrics

Figure 6 shows a line graph can be used to illustrate the intervention based on the enhanced critical security KPIs, which include successful phishing rates, training completion rates, and real-time threat detection. As can be seen, there was a noticeable improvement in all areas: threat detection increased from 40% to 65%, training improved from 70% to 90%, and phishing success increased from 60% to 30%. These three metrics can demonstrate how the suggested framework affects the organization's overall cybersecurity posture.

5. Defense Mechanism Integration

Several defense mechanisms are integrated into the suggested structure. The framework suggests technological solutions, regulatory changes, and training initiatives to assist reduce the risk of social engineering. Training programs are created for high-risk individuals identified by the BRP algorithm. Programs will try to raise targeted individuals' understanding of manipulation techniques like phishing and pretexting as well as ways to fend them off. By addressing the human element directly, these approaches eventually lessen vulnerability to assaults by producing a knowledgeable and extremely vigilant staff (Heartfield & Loukas, 2015).

By implementing new regulations that limit the sharing of private information and enforce stricter access controls, policy enhancements support these training initiatives. These regulations lessen the likelihood that an attacker may exploit organizational flaws. Lastly, advanced detection tools offer a technological layer of protection by keeping an eye on network activity for unusual activity and sending out real-time notifications to stop possible attacks. Together, these processes create a cohesive and flexible approach that combines organizational policies, behavioral insights, and state-of-the-art technology to create a strong defense against social engineering (Burda et al., 2024).

6. Conclusion and Future Work

By combining the perceptive elements of behavior with SNA in detecting and fixing vulnerabilities, this study presents the Behavioral-Driven Framework, which reduces the impact of social engineering attacks. In order to prioritize those at the highest risk for focused interventions like training, policy updates, and real-time monitoring, the framework uses the BRP algorithm to calculate a detailed RI for each individual. In addition to addressing human variables that are overlooked in conventional security measures, this strategy combines behavioral and technical protections to increase organizational resilience. By encouraging a knowledgeable and security-conscious staff, the suggested framework can significantly increase the effectiveness of social engineering attacks. Future research will focus on advancing the framework through the use of dynamic adaptive machine learning algorithms that react to new forms of social engineering threats and assault patterns. Additionally, the framework's applicability will be expanded to include a wider range of organizational situations, including government agencies, large corporations, and small businesses. Adjusting the Risk Index thresholds and improving intervention tactics will be made easier with additional validation using simulations and real-world case studies. In an effort to establish a new standard for proactive cybersecurity tactics and provide enterprises with the tools they need to remain ahead of increasingly complex social engineering attacks, this framework keeps incorporating behavioral insights and advanced analytics.

Acknowledgement

Authors are thankful to Impetus Educational and Welfare Society, Bhopal, MP for their support in carrying out this work.

References

Ahmed, Y. A., Koçer, B., Huda, S., Al-rimy, B. A. S., & Hassan, M. M. (2020). A system call refinement-based enhanced Minimum Redundancy Maximum Relevance method for ransomware early detection. Journal of Network and Computer Applications, 167, 102753.

Ahmed, Y. A. (2020). Automated analysis approach for the detection of high survivable ransomwares. acikerisim.selcuk.edu.tr

Baliyan, H., & Prasath, A. R. (2024, June). Enhancing Phishing Website Detection Using Ensemble Machine Learning Models. In 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0 (pp. 1-8). IEEE.

Bello, A., & Maurushat, A. (2020). Technical and behavioural training and awareness solutions for mitigating ransomware attacks. In Applied Informatics and Cybernetics in Intelligent Systems: Proceedings of the 9th Computer Science On-line Conference 2020, Volume 3 9 (pp. 164-176). Springer International Publishing.

Burda, P., Allodi, L., & Zannone, N. (2024). Cognition in social engineering empirical research: a systematic literature review. ACM Transactions on Computer-Human Interaction, 31(2), 1-55.

Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. ACM Computing Surveys (CSUR), 48(3), 1-39.

Montañez, R., Golob, E., & Xu, S. (2020). Human cognition through the lens of social engineering cyberattacks. Frontiers in psychology, 11, 1755.

Ofoegbu, K. D. O., Osundare, O. S., Ike, C. S., Fakeyede, O. G., & Ige, A. B. (2024). Proactive cyber threat mitigation: Integrating data-driven insights with user-centric security protocols. Computer Science & IT Research Journal, 5(8).

Paul, S., Mukherjee, D., Mitra, A., Mitra, A., & Dutta, P. K. (2024). Unravelling the Complex Networks of Social Physics: Exploring Human Behavior, Big Data, and Distributed Systems. Journal of Social Computing, 5(2), 165-179.

Ribera Martínez, A. (2023). An inverse analysis of the digital markets act: applying the Ne bis in idem principle to enforcement. European Competition Journal, 19(1), 86-115.
Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future internet, 11(4), 89.
Satpute, S., Cooper, R., Dicianno, B. E., Joseph, J., Chi, Y., & Cooper, R. A. (2021). Mini-review: Rehabilitation engineering: Research priorities and trends. Neuroscience Letters, 764, 136207.
Syafitri, W., Shukur, Z., Asma'Mokhtar, U., Sulaiman, R., & Ibrahim, M. A. (2022). Social engineering attacks prevention: A systematic literature review. IEEE access, 10, 39325-39343.
Udofia, E. (2024). A human-centric approach to cyber risk mitigation. In The Art of Cyber Defense (pp. 241-259). CRC Press.