# Cyber Security and People: Human Nature, Psychology, and Training Affect User Awareness, Social Engineering, and Security Professional Education and Preparedness

Mohammad Naveed Hossain
*Computer Science and Engineering*
*BRAC University*
Dhaka, Bangladesh
naveedhossain99@gmail.com

Tazria Zerin Khan
*Computer Science and Engineering*
*BRAC University*
Dhaka, Bangladesh
1611khan.tazria@gmail.com

Sheikh Fahim Uz Zaman
*Computer Science and Engineering*
*BRAC University*
Dhaka, Bangladesh
sheikh.fahim.zaman@gmail.com

Mohammad Shaba Sayeed
*Computer Science and Engineering*
*BRAC University*
Dhaka, Bangladesh
shaba.sayeed@gmail.com

S. M. Wazid Ullah
*Information and Communication Technology*
*MBSTU*
Dhaka, Bangladesh
wazidullahmurad@gmail.com

Md Jahid Raihan
*Computer Science and Engineering*
*University of Dhaka*
Dhaka, Bangladesh
jahid.raihan10@gmail.com

***Abstract*—This work focuses on how machine learning methods may be used to identify threats and provide countermeasures. Security threats and vulnerabilities pose significant difficulties in today's digital world. Algorithms trained with machine learning can sift through massive volumes of data, look for trends, and spot possible security breaches as they happen. These algorithms can offer preventative security measures and actions because they use sophisticated analytics and predictive models. This abstract delves into the use of machine learning to bolster security, focusing on its potential to improve threat detection and provide implementable suggestions for shoring up overall security.**

***Index Terms*—Predictive Models, Security Detection, Machine Learning, Predictive Models, Threat Detection, Risk Mitigation**

## I. Introduction

As the number of digital systems and networks that connect keeps growing, it becomes increasingly important to understand how people affect cyber security. This study examines how human behaviour, psychological factors, and educational methods affect cybersecurity, focusing on user knowledge, social engineering, and security education. By considering all these factors, companies can develop better security measures, make users more resistant to online dangers, and create a culture that values security awareness.

This study aims to discover how human behaviour affects privacy, focusing on how important it is to be aware of common behavioural trends and biases. Using this information, security experts can make strategies and technologies that work with how users act. This makes the system less vulnerable to risks and improves its security.

This study looks at psychology and how it affects how people think and make decisions about safety. Academics can learn much about how vulnerable people are to social engineering plans by looking at psychological factors like inquisitiveness, sensitivity to time, and fear. The information above can help make remedies, such as programs to teach and update people, that make these methods less successful. [19]

This paper also stresses the importance of user knowledge. It is emphasized how important it is to teach people about privacy dangers, best practices, and the possible outcomes of their actions. By raising user knowledge and supporting responsible behaviour, entities can give users the tools to implement security measures and protect themselves from common dangers like scams, malware, and identity theft.

This study looks at social engineering, a way for hackers to get private information or do things that pose a security risk by taking advantage of how people think. By looking at different types of social engineering, like fake emails, phone scams, and impersonation schemes, experts can develop successful training programs that teach people how to spot these attacks and what to do about them.

The paper's conclusion emphasizes the importance of security education as an essential part of defence. Organizations can give their users the power to make good choices and protect themselves from new online threats by giving them thorough training programs. These classes might talk about things like how to use email safely, how to browse the web safely, how to report an incident, and how to keep your passwords safe.

### A. Human Behavior

Human behaviour can have a significant influence on cybersecurity. Understanding prevalent behavioural patterns and prejudices can facilitate the creation of security measures that



align with users' innate tendencies. In addition, assessing user behaviour enables cybersecurity specialists to identify vulnerabilities and develop educational programs to minimize potential threats.

### *B. Psychology*

Psychological variables impact people's propensity for risky behaviour online and their ability to make sound decisions under pressure. For instance, individuals may fall prey to phishing assaults owing to emotions like curiosity, haste, or fear. With a deeper understanding of human nature, cybersecurity experts can create robust remedies to fortify defences against engineering. [12]

### *C. User Awareness*

What we mean by "user awareness" is the degree to which a person is informed about and comprehends cybersecurity threats, best practices, and the consequences of their activities. Users must be made aware of cyber risks like phishing, malware, and identity theft if we ever hope to stop them from happening. Strong passwords, multi-factor authentication, and frequent software upgrades are some security measures that may be bolstered via an effective awareness campaign that educates users and encourages responsible conduct. [13]

### *D. Social Engineering*

In information security, "social engineering" refers to persuading individuals to provide sensitive data or do other actions that leave a network vulnerable to attack. Cybercriminals prey on victims' emotions and instincts to deceive and manipulate them. Deception, in the form of phishing emails, phone calls, or impersonation, is a critical component of most social engineering techniques. By teaching people how to recognize and appropriately respond to social engineering attacks, we can significantly lessen their associated risks.

### *E. Security Education*

In order to equip people to make educated choices and defend themselves against cyber risks, it is crucial to provide extensive security education. Password hygiene, safe web practices, proper email protocol, and incident reporting are some issues that should be included in training programs. Employees should be aware of new security risks, and organizations should update training materials often to keep up with the latest attack methods.

Organizations may strengthen their cybersecurity posture by considering employees' habits, psychology, and education. For effective risk management, combining technological controls with deploying user awareness campaigns, continuing education, and simulated exercises is necessary.

It is important to remember that even if technology may improve security, people are still a crucial part of the puzzle. Human-centred cybersecurity requires an organization to promote a security-aware culture, instil a feeling of collective responsibility, and provide ongoing training and assistance to its employees.

## II. Related Works

Closed-loop automation of network and service management operations is becoming more popular due to the expected difficulty of operating and sustaining 5G and beyond networks. For this reason, AI is expected to play a crucial role in enabling self-managing capabilities, which will result in reduced operational costs, accelerated time to value, and mitigated risk of human error. [1]

The advent of implantable medical devices (IMDs) is an exciting development in medical technology that can improve patient care quality. Implantable medical devices (IMDs) are used in modern medicine to monitor and treat various diseases and conditions affecting different organs and to increase the impaired functioning of various biological structures. This article presents a high-level overview, from a cybersecurity point of view, of the difficulties involved in the design of implantable medical devices (IMDs). In the past, the design goals of IMDs have sometimes placed a premium on the implementation of strong security mechanisms. There are flaws in the currently accessible IMDs that, if exploited, might have far-reaching consequences. This article examines a variety of threats that potentially undermine the security of implanted medical devices (IMDs), highlighting the need to do so. Methods for improving IMD security and possible directions for further work in this area are presented. Wirelessly recharging batteries and lightweight cryptography are two examples that make it possible for devices to communicate across limited distances. [2]

The Internet of Things (IoT) results from the collaborative efforts of many fields of expertise. With the development of sensing, actuation, communication, and control technologies, there is a notable convergence amongst these domains, but with different perspectives. It is suggested that communities work together more closely. One way to get the conversation going on open research questions in the Internet of Things (IoT) is to describe a made-up scenario in which IoT may one day drastically alter human society. A list of eight foundational study fields is then offered, and the research difficulties related to each area are discussed in length. [3]

This paper argues for a human-in-the-loop approach to studying situational awareness related to computer defence analysis (CDA). Cybersecurity and cyber defence analysis (CDA) researchers have paid much attention to the cognitive phenomena known as situation awareness (SA). However, the cognitive aspects of situation awareness in the context of Cognitive Decision Support (CDS) have yet to receive much research. Instead, the human operator has been seen as a mere abstraction within the larger context of the interaction between humans and machines. Creating CDA tools and interfaces may benefit from a more in-depth knowledge of the human operators' socio-cognitive work if we adopt a human-centric approach. To support this assertion, we provide original research conducted within a "Living Lab," which enables us to place our empirical findings into the larger framework of their actual, worldly application. [4]

Improvements in effectiveness, dependability, and manageability are the goals of modernizing ICS. Several advantages have resulted from the connectivity of Industrial Control System (ICS) components made possible by the widespread use of information technology. However, because of this progress, new security concerns and vulnerabilities in industrial processes have emerged that were not apparent before because of the systems' bespoke architecture. Securing the foundation of critical infrastructure via cyber-security assessments relies heavily on selecting a suitable assessment environment. The current research provides a hierarchical analysis of vulnerabilities and risks in ICS components, demonstrating the need to use physical hardware in the evaluation setting. Hardware-In-The-Loop testbeds are a useful tool for gauging the cyber security of ICS and detailing how they stack up against other types of evaluation settings. [5]

The smart grid cyber-physical system architecture now includes automated detection, prevention, and mitigation techniques to lessen the mental burden on human security operators. Information gleaned via C2 tools is often shown in command and control centres using visualization frameworks that could be more user-friendly and relevant to the situation. Because of this shortcoming, the decision-making process is slowed, and situational awareness is reduced. Before visualization, it is crucial to use frameworks that put data into context so humans can understand it. A thorough literature review is conducted in this study, and a theoretical framework called the "human-on-the-loop" framework is proposed. [6]

## III. Proposed Model

Data cleansing, regression analysis, user education, behavioural science, social engineering, and precautionary measures are all part of the Workflow we recommend. Collect the data set that includes occurrences and actions involving users, social engineering, user behaviour, and security. Remove any outliers, missing numbers, or discrepancies from the data by doing data cleaning. Explore and visualize the data to discover hidden patterns and trends. Do a regression analysis to investigate the interplay between user education, psychology, and social engineering. Find out what factors have the most bearing on security incidents and how. Create a regression model using statistical approaches to predict security events based on the chosen criteria. To fairly assess the effectiveness of the regression model, separate the data into training and testing sets. Common percentage splits between training and testing are 70-30 and 80-20, respectively. Human behaviour, psychology, user awareness, and social engineering elements may all be trained using the training data set. Maximize efficiency by fine-tuning the model's settings. Evaluate the model's efficacy by analyzing the projected outcomes and using suitable measures (such as accuracy, precision, and recall). Examine human behaviour, psychology, user awareness, social engineering, and security events to find trends and connections. Give consumers specific advice on better protecting themselves in light of your findings and projections. [11] Training initiatives to raise user awareness, enhanced authentication systems, safe web surfing practices, and vigilance against social engineering assaults are all possible recommendations.

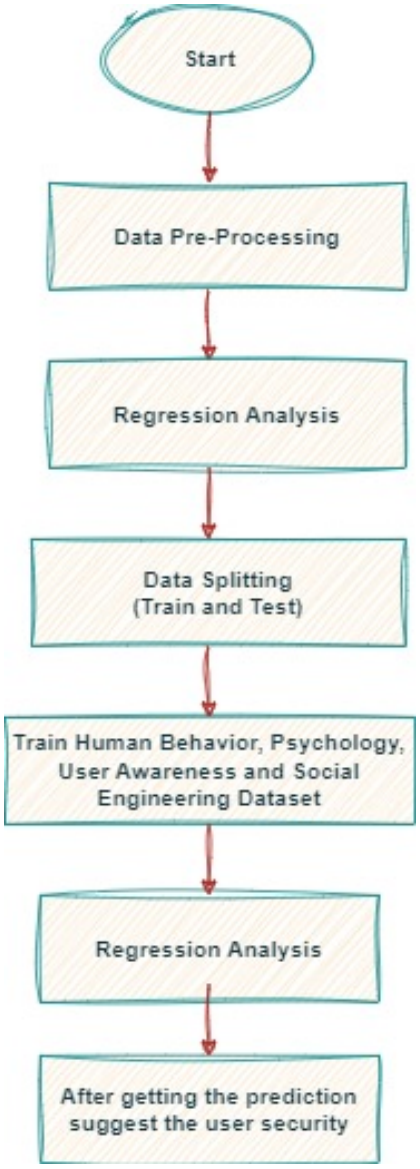


Fig. 1. Work flow

## IV. Result Analysis

The respondent's overall accuracy, precision, and memory scores are averaged before determining the respondent's final grade by comparing the respondent's overall accuracy, precision, and memory scores to the question's F1 score. Additionally, the respondent's F1 result is taken into consideration. This step must be completed before moving on to the next phase, which entails calculating the respondent's aggregate grade. Regardless of the size of an individual's contribution, the entire process of generating the data used for training and testing benefited from each of these techniques.

| Method name | Accuracy |
|---|---|
| Naive Baised | 85% |
| Random Forest | 86% |
| Bagges Tree | 89% |
| SVM | 92% |
| XGBoost | 91% |
| KNN | 98% |

TABLE I
PREDICTION TABLE

This was the case regardless of how many of these strategies were implemented. With the assistance of the produced data, training and examination were conducted. This was the case even though the contribution could have been made through the abovementioned methods. By iteratively modifying each of the model's parameters, we significantly increased our classification model's accuracy. As a direct result of this, we were able to improve the accuracy of our model significantly. The fact that we attempted to do so was the impetus that propelled us in the right direction toward making this a reality. The fact that we attempted to do so was the impetus for our success. The impetus was supplied by the fact that we made an effort to do so. We were motivated by the fact that we forced ourselves to go through the inconvenience of doing so. The results of comparing the six various categorization models used during this investigation are presented in Table 1, which can be found at the end of this paragraph. The models are depicted similarly to a side-by-side comparison in the table beneath this paragraph. If you search around this area, you should find Table 1 in this exact location. Of all the phrases analyzed, "counterfeiting and skimming" had the highest f1-score. In addition to having the highest Random Forest recall score, it also had the highest recall score. This was the case with every single one of the analyzed sentences. In total, 0.85 points were awarded for completing this exercise. To achieve an accuracy of 0.86, only "counterfeiting" and "skimming" may be employed as strategies, and these are the only two strategies that may be employed at all. The use of alternative methods is rigorously prohibited under all circumstances. The "Card-not-present" option received the highest attainable grade due to its superior f1-score (0.84), as well as its SVM recall (0.83). This was because the sum of both of these metrics was 0.83. This event occurred as a direct result of the fact that all of these indicators were significantly above average. Together, these two factors played a significant role in achieving this objective, ultimately accomplished to the satisfaction of all parties involved. This holds for both proposed solutions to the identified issue. Due to its accuracy rating of 0.89, the subcategory "False application" was chosen as the category with the maximum degree of dependability. This was because it was the subcategory for which the most applications were received. This was because the subcategory received the highest aggregate grade out of the entire category. This decision was made because this particular subcategory received the highest cumulative grade of all the others. This decision was made because the specific subcategory in the issue had the fewest options for which no definitive answer could be given. The "Lost and Stolen Card" function, added to XGBoost in version 0.93, provides the maximum possible degree of accuracy in terms of the degree of precision a user can achieve. This function provides the utmost level of precision that a user can achieve. This functionality, now included in the app, was developed in response to a user's request. This capability was made accessible for the first time in XGBoost version 0.93, the released version. This function produces this result because it provides the highest achievable level of precision that a single individual can achieve because it produces the most accurate results imaginable and the highest achievable level of precision. The phrase combination "counterfeiting and skimming" obtained the highest percentage of recall and the highest f1-score of all the keywords used. This was a direct result of the scheme involving both the fabrication and cloning of credit card numbers. In every occurrence, this was the situation that occurred. In the game known as Bagged Tree, the "Last and Stolen Card" category has been assigned an accuracy score of 0.92, while the "False Application" category has been assigned an accuracy score of 0.89 and an f1-score of 0.85. The numerals represent these scores. These figures accurately depict both of these scores in their entirety. While "card-never-received" has the highest recall and f1-score (0.98), "counterfeiting and skimming" has the highest KNN accuracy (0.92). The Naive Biased model achieved the highest possible F1 score (0.85 out of 1.00) and the highest possible recall for "counterfeiting and skimming" (0.91 out of 1.00). These accomplishments were accomplished simultaneously. Due to the model's inherent biases and naivety, both of these accomplishments were attainable. The LSTM algorithm is both practical and efficient, which is one of the contributing factors to the algorithm's high level of efficiency. The most effective algorithm is one that is accessible to everyone. This is one of several algorithms. According to all classifiers, including accuracy, recall, and F1, forgery and skimming are both offences committed more than one hundred ninety-nine per cent of the time. KNN 98%, SVM 92%. 91% RF/XGBoost.A latent semantic topology model (LSTM), which is not currently being utilized, has a greater chance of revealing patterns not previously observed. This is because no one is presently utilizing it. LSTMs are vastly preferable to other classification techniques due to how they are implemented. This indicates that they are substantially more effective in the categorization process.

## V. CONCLUSION AND FUTURE WORK

The sector may be expanded to include Emotional and Cognitive Factors, Behavioral Analytics, Biometric Authentication, User-Centric Design, Gamification, Privacy Consider-

ations, Continuous Education and Training, and other similar features. In conclusion, this study emphasizes the significant importance that human behaviour, psychological research, and training have in cybersecurity. Organizations can build effective security plans, foster a culture of security awareness, and reduce human-related risks if they understand and address the abovementioned elements. The results of this research contribute to a deeper understanding of the human-centric elements of cybersecurity and offer significant insights for building effective security measures and educational programs to defend digital systems and networks. These findings were published in a paper titled "Cybersecurity: Human-Centric Aspects."Human behaviour, psychology, and training greatly influence how successful security measures are, which is why human factors play an essential part in cybersecurity. It is necessary to have a thorough understanding of these aspects to create robust security systems and educate users on how to protect themselves from potential cyber dangers. Let us investigate the impact that user awareness, social engineering, and security education have on human behaviour and the role that psychology and training play in cybersecurity.

## REFERENCES

[1] Lee, Sang-Woong, et al. "Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review." Journal of Network and Computer Applications 187 (2021): 103111.

[2] Bhardwaj, Akashdeep, and Keshav Kaushik. "Predictive analytics-based cybersecurity framework for cloud infrastructure." International Journal of Cloud Applications and Computing (IJCAC) 12.1 (2022): 1-20.

[3] Garcia, Anna Baron, Radu F. Babiceanu, and Remzi Seker. "Artificial Intelligence and Machine Learning Approaches For Aviation Cybersecurity: An Overview." 2021 Integrated Communications Navigation and Surveillance Conference (ICNS). IEEE, 2021.

[4] Dumbere, Dhananjay M., and Asha Ambhaikar. "An ML Bio-inspired Model for improving Security and Speed of FHE for Cybersecurity." 2021 IEEE International Conference on Technology, Research, and Innovation for Betterment of Society (TRIBES). IEEE, 2021.

[5] Nikoloudakis, Yannis, et al. "Towards a machine learning based situational awareness framework for cybersecurity: an SDN implementation." Sensors 21.14 (2021): 4939.

[6] Miao, Yuantian, et al. "Machine learning–based cyber attacks targeting on controlled information: A survey." ACM Computing Surveys (CSUR) 54.7 (2021): 1-36.

[7] Gumusbas, Dilara, and Tulay Yildirim. "AI for Cybersecurity: ML-Based Techniques for Intrusion Detection Systems." Advances in Machine Learning/Deep Learning-based Technologies: Selected Papers in Honour of Professor Nikolaos G. Bourbakis–Vol. 2 (2022): 117-140.

[8] Hossain, Mohammad Naveed, Nafim Ahmed, and SM Wazid Ullah. "Traffic Flow Forecasting in Intelligent Transportation Systems Prediction Using Machine Learning." 2022 International Conference on Futuristic Technologies (INCOFT). IEEE, 2022.

[9] Singh, Sujay, et al. "AI and ML in Vehicular Communication: A Cybersecurity Perspective." 2022 7th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2022.

[10] Watney, M. M. "Artificial intelligence and its' legal risk to cybersecurity." European conference on cyber warfare and security. Academic Conferences International Limited, 2020.

[11] Franco, Muriel F., et al. "SecRiskAI: a Machine Learning-Based Approach for Cybersecurity Risk Prediction in Businesses." 2022 IEEE 24th Conference on Business Informatics (CBI). Vol. 1. IEEE, 2022.

[12] Tsukerman, Emmanuel. Machine Learning for Cybersecurity Cookbook: Over 80 recipes on implementing machine learning algorithms for building security systems using Python. Packt Publishing Ltd, 2019.

[13] Abdullahi, Mujaheed, et al. "Detecting cybersecurity attacks in internet of things using artificial intelligence methods: A systematic literature review." Electronics 11.2 (2022): 198.

[14] Hossain, Mohammad Naveed, Sheikh Fahim Uz Zaman, and Md Shaba Sayeed. "Adding Knock Code Technology as a Third Authentication Element to a Global Two-factor Authentication System." 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT). IEEE, 2023.

[15] Gupta, Maanak, Sudip Mittal, and Mahmoud Abdelsalam. "AI assisted malware analysis: a course for next generation cybersecurity workforce." arXiv preprint arXiv:2009.11101 (2020).

[16] Kuppa, Aditya, and Nhien-An Le-Khac. "Black box attacks on explainable artificial intelligence (XAI) methods in cyber security." 2020 International Joint Conference on Neural Networks (IJCNN). IEEE, 2020.

[17] Dash, Bibhu, and Meraj F. Ansari. "An Effective Cybersecurity Awareness Training Model: First Defense of an Organizational Security Strategy." Int. Res. J. Eng. Technol.(IRJET) 9 (2022).

[18] Shahriar, Hossain, et al. "Case Study-based Portable Hands-on Labware for Machine Learning in Cybersecurity." Proceedings of the 51st ACM Technical Symposium on Computer Science Education. 2020.

[19] Omar, Marwan. "Application of Machine Learning (ML) to Address Cybersecurity Threats." Machine Learning for Cybersecurity: Innovative Deep Learning Solutions. Cham: Springer International Publishing, 2022. 1-11.

[20] Azmim, T., Alam, M., Mishu, S. A., Chowdhury, N. A. (2021). Brain tumour detection through image processing.

[21] Löffler, Emanuel, et al. "Cysecescape 2.0—a virtual escape room to raise cybersecurity awareness." International Journal of Serious Games 8.1 (2021): 59-70.