Volume: 14 Issue: 02 Pages: 5334-5341(2022) ISSN: 0975-0290

Cyber Awareness Learning Imitation Environment (CALIE): A Card Game to provide Cyber Security Awareness for Various Group of Practitioners

P.Mohana Priya
Department of Information Technology, SASTRA Deemed University, Thanjavur – 613 401
Email: mohanapriyatce@gmail.com
Abhijit Ranganathan
Department of Computer Science, SASTRA Deemed University, Thanjavur – 613 401
Email: abhijitranganathan3108@gmail.com

ABSTRACT

Cyber attacks produced a massive impact for all online users, interrupted intended user's internet services, financial losses, business interruptions for a large-scale industry. A proper cyber security education is must for the employees of an organization. The management prefers active based learning environment to train all non-IT and non-professionals working in an organization. This research work concentrates on development of gaming platform in both local host and in an online mode as a videogame for cyber security education. With this regard, Cyber Awareness Learning Imitation Environment – a card deck gaming environment is proposed where attackers can choose the attack cards to learn various cyber-attacks, defense cards are used for providing the suitable defense mechanism, Instruction card- to be used for learning about how to generate cyber-attacks and recent incident card used to train the players with recent incidents of various cyber-attacks discussed such as malware attack, phishing attack, password attack, Man-in-the-Middle attack, Structured Query Language injection attack, denial of service attack, insider threats, crypto jacking, zero-day exploit and watering hole attack. Questionnaire based feedback report is collected from the players to analyze their understanding about various cyber-attacks.

Keywords – **Active Learning, Card-Deck Game, Cyber Attacks, Cyber Education, Cyber Education Training Methods, Gaming Environment**

Date of Submission: Jul 23, 2022 Date of Acceptance: Aug 11, 2022

I. INTRODUCTION

Most of the critical infrastructures are deployed with an internet service to maintain and regulate various services offered. Various vectors of cyber security attacks that harms the critical infrastructure includes malware attacks [1], phishing attacks [2], password attacks[3], Man-In-The-Middle (MITM) attack[4], SQL injection attacks[5], Denial of Service (DoS) attacks[6], Insider threat[7], crypto jacking[8], zero-day exploit[9], watering hole attack[10].

Organizations, corporations, and sectors are broadening their range of capabilities in the area of cyber security[11][12][13]by strengthening their security procedures and recruiting top executives to guarantee the protection of their respective data. However, merely employing officials will only partially resolve the issue. The mentioned issue can be resolved by training a company's management to help officials with no background in computer science or cybersecurity comprehend the significance of techniques used by highly skilled officials in the field and to keep them informed about potential security threats.

A tabletop game[14]named CALIE is designed to raise cyber security awareness among employees with non-technical backgrounds, can be used to complete this objective quite effectively. By taking on the roles of both the attacker and the defender of vital assets in a hypothetical firm, board game offers a hands-on learning environment where users may gain understanding of cyber security attacks and defenses.

In the board game, players can learn about different attacks and defenses in an active learning environment.

By employing cards for assaults and defense against other playersin this active learning environment. The player can learn cybersecurity attacks[15]and defensetechniques by selecting several defense methods, each player can be inventive with theirdefensive plan. Each player has the opportunity to assault another player in an effort toundermine the defense mechanism or take advantage of any weaknesses in the defensive plan ofthat player. Every time a player makes a move, the "game master" gives them feedback.

The Game is designed to highlight cybersecurity awareness and educate beginners andenthusiasts about cybersecurity mechanisms. The game represents realistic scenarios and catersto the needs of the audience playing it.

Volume: 14 Issue: 02 Pages: 5334-5341(2022) ISSN: 0975-0290

This game was created in an effort to eliminate a lectureon cybersecurity and introduce a friendly environment for enthusiastic learners to learn as well asparticipators.

The objective of this research work is to propose the game based active learning environment to train the non-IT employees and non-professionals of an institution about various cyber security attacks with its associated risk factors. The game based active learning environment trains the player about how to generate attacks, choosing suitable defense method, understand the severity of risk factors and scores associated with it. The contribution of this research work includes cyber security education, design of game done for both local host, video game environment for public and cryptographic methods used to transform the card number as a nonce when the game play done in online mode. The idea of enhancing active learning capabilities through an engaging and tutored environment is a key motivation for producing this article.

The article is organized in such a way that chapter 2 discusses about related state of the art cyber security attacks, chapter 3 discusses about various mode of cyber security education training methods, chapter 4 discusses the proposed CALIE gaming environment, chapter 5 discusses about environment setup, chapter 6 discusses about results and discussion and chapter 7 concludes with future research directions.

II. STATE OF THE ART CYBER SECURITY ATTACKS

This section discusses about various state of the art cyber security attacks and its impact on the deployed critical infrastructure. Hackers makes use of cyber-attacks to target banking sectors in order to steal customer account details. The other form of Phishing attacks is generated through sending fake emails[16]and make the clients to feel look a like legitimate emails originated from banks with relevant information like sbi.in, icici.com, yes bank etc. This kind of phishing attacking sites grow more than 100% over 2018[17]. The most reputed is gmail phishing attack scam occurred worldwide which leads to service interruptions for all google servers in the year 2017[18]. Denial of Service attacks[19] leads to service interruption of its intended clients, when an attack originates from a single point of contact and also as a variant from distributed multiple sources namely Distributed Denial of Service attacks[20]. These attacks are multiplied in quantum of double the rate of malicious traffic flows when a reflector component is used by the attacker [21]. Hence the various of DoS attacks are represented as DDoS and DRDoS attacks. DoS attack creates a big impact on various networking architectures such as obsolete network, software defined network and Internet of Things[22]. Representation of DDoS attacks will vary based on the network architecture, in SDN these attacks are represented as data plane [23]DDoS attacks, control plane[24] DDoS attacks and application plane[25] DDoS attacks. In IoT, these attacks are represented as IoDDoS attacks. Password attacks[26] are most common in cyber space in which dictionary attack[27]and bruteforcing attack[28] with a nature of trial-and-error methods which is chosen by the attacker to obtain the password of the user. In MITM attack[29][30][31][32], the attacker intercepts the communication channel and conceives user's data without their awareness. MITM attacks bypass both the channels and system to intercept the data being transmitted and stored in the system. The next category of cyber threat is SQL injection attack, in which the attack is generated by attackers by triggering a poisoned SQL query[33]by using clauses such as SELECT, WHERE, INSERT, DELETE, UPDATE etc. The malicious (or) an incorrect query is triggered which ends with value = = 1, so that the web application retrieves the actual data to the attackers. This attack is also represented as SQL poisoning attacks[34] where the fake query is triggered which seems to be like an actual query.

III. STATE OF THE ART CYBER SECURITY EDUCATION TRAINING METHODS

This section discusses about existing game scenarios used for cyber security education and awareness. Conceptual Framework for eLearning and Training (COFELET)[35] consist of goals, tasks, Scenario Execution Flows (SEF), conditions to be followed for the game. COFELET simulates cyber-attacks and derives the properties of Capture the Flag (CTF) events and Hack Learn events. Digital power twin[36] is deployed in the Smart Grid (SG) to integrate with the physical test bed to learn about cyber security attacks. The architecture is designed in such a way that separates the physical system and control network simulation which thereby provides game testing, game learning in distinct phases. Simulated Critical Infrastructure Protection Scenarios (SCIPS)[37] is designed from the base of COFELET with additional features for cyber security education gaming such as event, discussion, decision and performance. SCIPS can remodel for a variety of cyber security training methods and it can be planned for cyber awareness, strategic banking, emergency planning and telecommunications. Serious game[37] acts as a tool which is designed in a form of Graphical User Interface (GUI) where the user can drag and drop the necessary features available to train the cyber security attacks. The game also provides a layer of abstraction to test both attack and defense scenarios. Serious game tool set also provides a cyber mission platform to generate cyber security attacks, Ethical Hacking (EH) is the most targeted cyber security attack discussed in this research work. Bayesian Stackelberg[38] model – a multi-stage cyber-attack defending mechanism used to prevent cyber issues by invoking various phases to understand the state of the cyber security attack. Learning phase finds the present state of the cyber security attack with node information. Bayesian Stackelberg model relies on mathematical foundation such as Mixed Integer Conic Programming (MICP), strong duality and unimodular matrices. Gamification[39] based cyber security attacks defense mechanism is created in such a way to build interest for the learners to feel a kind of playing game. It is incorporated with chat boxes, leader boards, level up feature, unlocking badges for the next levels, virtual environments. CyberCIEGE[40], a security awareness tool provides organizational cyber security training objectives.

Volume: 14 Issue: 02 Pages: 5334-5341(2022) ISSN: 0975-0290

CyberCIEGE mainly focuses on an information assurance education and also acts as a basic information security awareness for the computer users but the game is designed only for wired networks.

IV. CALIE GAMING ENVIRONMENT

The proposed CALIE gaming environment comprises of two phases namely training phase and questionnaire phase. Training phase is composed of attack card decks in the first module, defense card decks in the second module along with instruction card decks. All components of CALIE is shown in fig 4.1. Attack card decks are created for ten different cyber security attacks namely Malware attacks, Phishing attack, Password attacks, MITM attacks, SQL injection attack, DoS attack, Insider attack, Crypto jacking, Zero-day exploits and watering hole attacks. Each attack card comprises details of all attacks, tools, methods used to generate attacks and recent incidents about the attack. The unique feature of this game is about displaying the recent incidents of an attack occurred all around the world. For each attack card, there exists corresponding defense card which suggest suitable defense procedures and methods to prevent those attack vectors. Instruction card decks will guide the players about how to play the game. Once training gets completed, players will move on to game trigger mode, for each click of the user, random attack cards will be displayed. For the chosen attack card, player have to choose the suitable defense card, thereby score points will be added to the user account.

Game trigger module will be repeated 9 times in order to cover rest of the attack cards. For each player, 3 turns will be allowed to play Finally, the player who scores maximum points can be considered as winner of the game. CALIE Dashboard is displayed with top 3 players of the game on a monthly basis and rewards will be provided in three categories such as digital gold medal for winner, digital silver medal for first runner up and digital bronze medal for second runner up. Feedbacks about the game played will be collected in the form of questionaries in order to analyze the understanding of players about various attacks. Questionnaire forms will be collected from the same set of players at a periodical attempt interval in order to analyze their acquired knowledge about the game. Fig. 4.1(a)shows attack cards, in which each card consists of a unique number that begins from 1 and ends with number 10. Table 4.1shows the details of card name with corresponding attack information. The card number is printed at the front deck for the beginners to understand the gaming environment but when the game begins in online mode, the card numbers will be transformed using cryptographic methods.

Table 4.1 : Card Details

Card Number	Name of the Cyber Attack
1	Malware Attack
2	Phishing Attack
3	Password Attack
4	MITM Attack
5	SQL Injection
6	Denial of Service
7	Insider
8	Cryptojacking
9	Zero-day exploit
10	Watering Hole

When card number 1 is chosen by the player, details of malware attack will be displayed. Malware attacks execute unauthorized access on the target computer. It incorporates various types with it for launching such attacks. When card number 2 is chosen by the player, details of phishing attack will be provided. In this attack, malicious attackers will send messages that is pretending as legitimate user and this type of attack is mostly found in vulnerable web pages, in which the malicious attacker will create scam messages, bogus pages where sensitive information like user credentials and banking transaction account details will be displayed. When card number 3 is selected, details of password attack will be displayed, in which password attack will be generated based on two methods either by dictionary attack, password guessing attack (or) brute force attack. If dictionary attack is generated, list of words will be referred (or) taken from dictionary and if brute force attack is chosen, trial and error method is used in which relevant information of the user is randomly selected by the attacker.

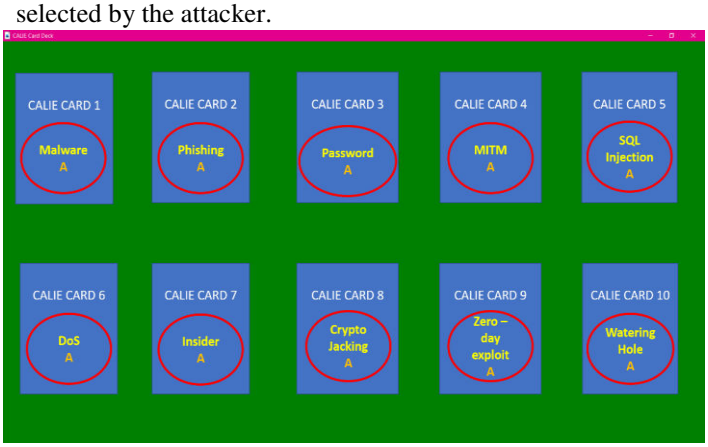

Fig 4.1 (a) : CALIE Attack Card

Volume: 14 Issue: 02 Pages: 5334-5341(2022) ISSN: 0975-0290

If card number 4 is selected, details of Man-In-The-Middle (MITM) attack will be displayed with how the malicious attacker intercepts the communication channel between the user end points. This can also be eaves dropping the communication channel (or) shoulder surfing the attacks. If card number 5 is selected, details of SQL injection attack will be displayed. SQL injection attack is generated by attackers through execution of incorrect query, SQL table poisoning attack. If card number 6 is selected, details of DoS attack about service interruption will be shown along with its impact on the affected resources. If card number 7 is selected, it shows the possible insider attacks occurring within an organization (or) critical IT infrastructure. If card number 8 is selected, details about how user's information are mined to steal their cryptocurrency will be displayed. If card number 9 is selected, details about zero-day exploits, newly emerging attacks has been displayed and if card number 10 is selected, details of watering hole attack will be displayed in which victim most frequently used websites have been listed. The followingfig 4.1 (b) shows the list of defense cards on all above stated attacks from existing related works and trained dataset for each defense card. If the player can't understand attack logic, then instruction card as shown in fig 4.1 (c)will be helpful to execute the attack traffic flows. In case, if the player wants to know recent incidents about various attacks, fig 4.1 (d)as shown in recent incident cards will be helpful to learn those.

The following table 4.2 is tabulated with set of questionnaires about the proposed gaming platform and to make a decision making whether the game is preferrable for cyber security education.

Table 4.2 :Questionnaires Feedback of CALIE Game

Q1	Is CALIE provides ease of game play?
Q2	Is CALIE game provides cyber security awareness?
Q3	Is CALIE game details about cyber security attacks ?
Q4	Is CALIE game provide players to pick suitable defense solution?
Q5	I feel playing a card game is the best practice for teaching cyber security attacks?
Q6	Is CALIE game recommended for industry?
Q7	Is CALIE game consumes more time for learning about cyber security attacks?

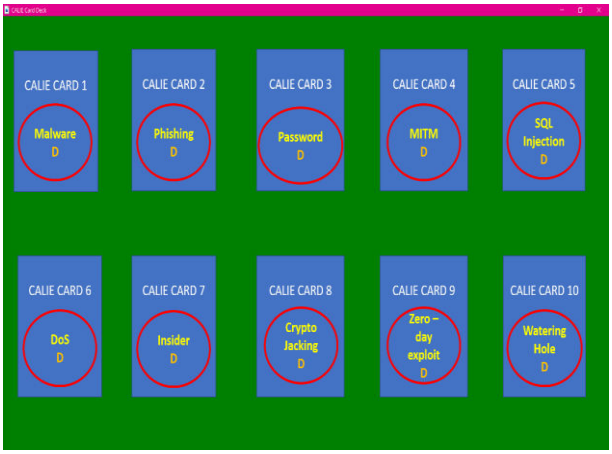

Fig 4.1 (b) : CALIE Defense Card

Fig 4.1 (c) : CALIE Instruction Card

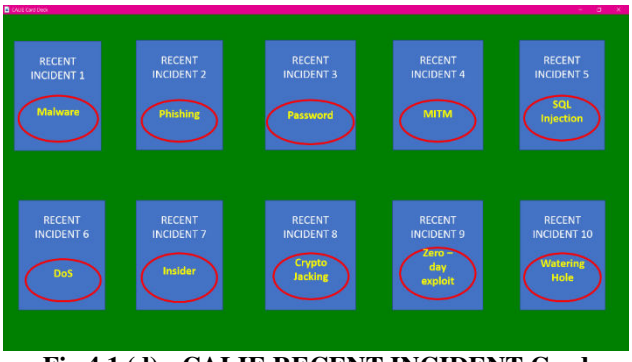

Fig 4.1 (d) : CALIE RECENT INCIDENT Card

The above-mentioned questionnaire will be circulated as a survey google form to the players for interpreting results of imitation learning platform. Analysis of google form survey responses is tabulated in the following table 4.2.

V. CALIE GAME DESIGN FOR MULTIPLAYER MODE

In this gaming platform, the players can use their interested avatar characters as a play role as shown in fig 5.1 followed by location of the competent fellow players. Design of cards and its appropriate location placement can be done in this phase as shown in fig 5.2. Once the players

Volume: 14 Issue: 02 Pages: 5334-5341(2022) ISSN: 0975-0290

clicks start new game, card decks will be displayed in which the player have to choose any one attack card, if the opponent chose the suitable solution for the attack card, then the opponent scores 1000 gold coins.

Fig 4.1: Components of proposed CALIE GAME

Fig 5.1: Selection of Avatars

For each and every suitable selection of defense cards, 1000 gold coins will be added to the present scores. If the opponent chooses the incorrect defense card, 1000 gold coins will be deducted from his account. If the player wants to make use of instruction card during the game play, the player supposed to pay 2 gold coins earned. The game allows a maximum of 10 players at a time. The video game is in development stage for multiplayer mode option. Fig 5.3 shows the home page of CALIE game designed in dulst in which rest of the modules have to be linked further to be considered as future research directions.

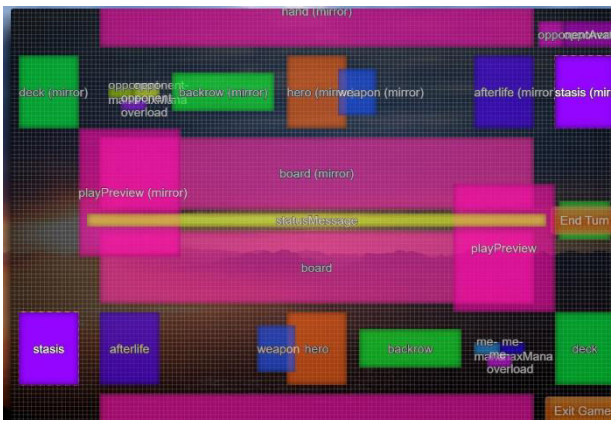

Fig 5.2: Design of Cards in Panel

Fig 5.3: Home Page of CALIE in Video Game

VI. ENVIRONMENTAL SETUP

The proposed modules of CALIE game is implemented using fourth generation high level language named python 3.9 in windows operating system 10. Various python modules used in this game includes PYINPUT.KEYBOARD, TIME, SYS, KEY, LISTENER and OS. PYINPUT.KEYBOARD module is used to control and monitor input devices. TIME module is used to obtain the current time stamp. OS module consists of functions for adding and deleting folders, retrieving the game contents, changing and locating the directories. OS module communicates with the underlying real time operating system incorporated. SYS module allows system specific parameter and functions. CALIE game environment is designed with python Tkinter package for attack and defense cards. CALIE game is also implemented using Dulst, to create a own card game.

VII. RESULTS AND DISCUSSIONS

The above sections named 5 and 6 shows the attack and its defense logic in gaming console. This section discusses how the same attack and its defense logic is practiced as a hands-on in a local host with an appropriate screenshot. Fig 7.1 shows the details of level one, where hint about how the game needs to be played is listed, followed by the next feature prompting the user to enter their credentials. For a successful login attempt, players will move on to level 2 in which the attack program will be executed by opening a terminal shell. Fig 7.2 list the details of attack codes like logger.py, keylogger.py at an early stage of this research work.

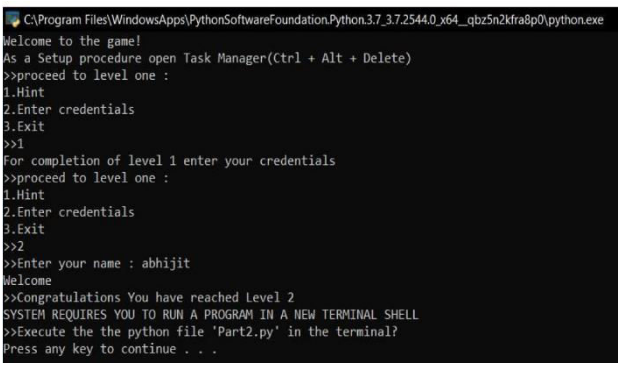

Fig 7.1: Login and Hint of the Game

Volume: 14 Issue: 02 Pages: 5334-5341(2022) ISSN: 0975-0290

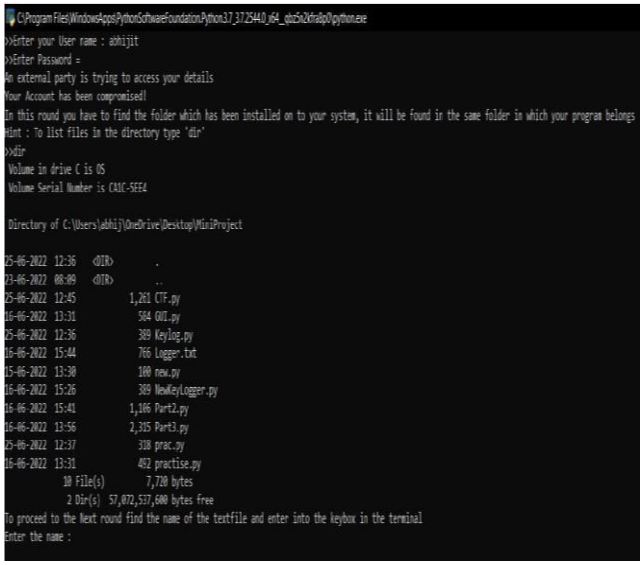

Fig 7.2: Details of attack files

Fig 7.3 list out the details of user keystrokes when a keylogger attack is generated through keylog.py. Key strokes such as back space, enter, “a”, “b”, “h”, “i”, “j”, “i”, “t”, \xl3, alt, tab details are traced in the terminal command prompt. Fig 7.4 shows the successful execution of logging attack done by the attacker.

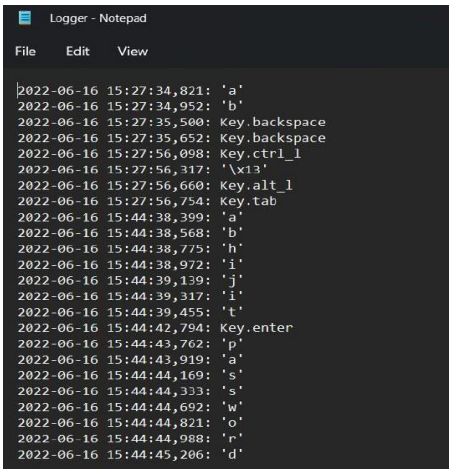

Fig 7.3: Trace of Keylog attack

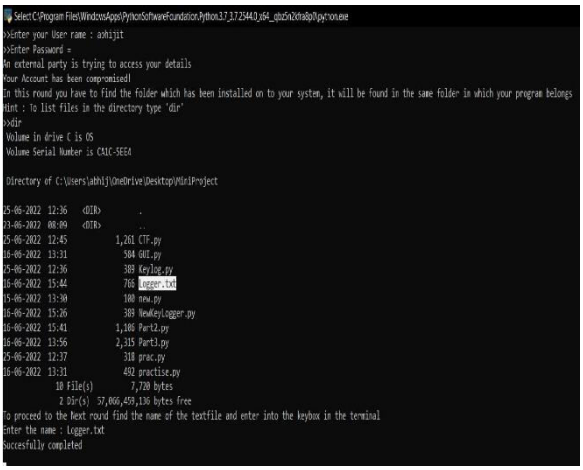

Fig 7.4: Trace of Logging Attack

Fig 7.5: Defense Solution for Login Attack

Once the logging attack is generated, the user has been denied with the execution permission which will be defense solution for this attack category as shown in fig 7.5.

VIII. CONCLUSION AND FUTURE WORK

Cyber security education is important for various practitioners who incorporates the logic in their area of domains. Rather than preferring educating non-professionals through webinars, workshops, faculty development programs and through MOOC courses, active based learning via gaming scenarios will be the better choice so that the learners can gain knowledge through experience. In this research work, card deck game is proposed for educating cyber security awareness for non-IT and non-professionals where the questionaries survey report collected from the players seems to be positive in many aspects like ease of game play, knowledge acquiree of various cyber-attacks. In this phase, CALIE is developed as card deck game in the local host, further it will also to be published as a video game in an online platform.

REFERENCES

[1] Rathore, H., Samavedhi, A., Sahay, S.K. and Sewak,M.,2021. Robust malware detection models: learning from adversarial attacks and defenses. *Forensic Science International: Digital Investigation*, 37, p.301183.

[2] Bhardwaj, A., Al-Turjman, F., Sapra, V., Kumar, M.and Stephan, T., 2021. Privacy-aware detection framework to mitigate new-age phishing attacks. *Computers & Electrical Engineering*, 96, pp.107546.

[3] Kwon, T. and Song, J., 1998. Efficient and secure password-based authentication protocols against guessing attacks. *Computer communications*, 21(9), pp.853-861.

[4] Lu, J.Z. and Zhou, J., 2012. Preventing delegation-based mobile authentications from man-in-the-middle attacks. *Computer Standards & Interfaces*, 34(3), pp.314-326.

[5] Natarajan, K. and Subramani, S., 2012. Generation of SQL-injection free secure algorithm to detect and prevent SQL-injection attacks. *Procedia Technology*, 4, pp.790-796.

Volume: 14 Issue: 02 Pages: 5334-5341(2022) ISSN: 0975-0290

[6] Ramasubramanian, B., Rajan, M.A., Chandra, M.G., Cleaveland, R. and Marcus, S.I., 2022. Resilience to denial-of-service and integrity attacks: A structured systems approach. *European Journal of Control*, 63, pp.61-69.

[7] Wei, Y., Chow, K.P. and Yiu, S.M., 2021. Insider threat prediction based on unsupervised anomaly detection scheme for proactive forensic investigation. *Forensic Science International: Digital Investigation*, 38, pp.301126.

[8] Xu, G., Dong, W., Xing, J., Lei, W., Liu, J., Gong, L., Feng, M., Zheng, X. and Liu, S., 2022. Delay-CJ: A novel cryptojacking covert attack method based on delayed strategy and its detection. *Digital Communications and Networks.*

[9] Singh, U.K., Joshi, C. and Kanellopoulos, D., 2019. A framework for zero-day vulnerabilities detection and prioritization. *Journal of Information Security and Applications*, 46, pp.164-172.

[10] Ismail, K.A., Singh, M.M., Mustaffa, N., Keikhosrokiani, P. and Zulkefli, Z., 2017. Security strategies for hindering watering hole cyber crime attack. *Procedia Computer Science*, 124, pp.656-663.

[11] Li Y, Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 2021 Nov 1;7: pp. 8176-86.

[12] Alghamdie, M.I., 2021. A novel study of preventing the cyber security threats. *Materials Today: Proceedings.*

[13] Bhol, S.G., Mohanty, J.R. and Pattnaik, P.K., 2021. Taxonomy of cyber security metrics to measure strength of cyber security. *Materials Today: Proceedings.*

[14] Hart, S., Margheri, A., Paci, F. and Sassone, V., 2020. Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95, p.101827.

[15] Zha, L., Liao, R., Liu, J., Cao, J. and Xie, X., 2022. Dynamic event-triggered security control of cyber-physical systems against missing measurements and cyber-attacks. *Neurocomputing*.

[16] https://www.statista.com/statistics/266161/websites-most-affected-by-phishing/

[17] Ali, W., 2017. Phishing website detection based on supervised machine learning with wrapper features selection. *International Journal of Advanced Computer Science and Applications*, 8(9).

[18] A. Mishra, B.B. Gupta Intelligent phishing detection system using similarity matching algorithms *Int. J. Inf. Commun. Technol.,* 12 (2018), pp. 51-73

[19] Gupta, B.B., Chaudhary, P., Chang, X. and Nedjah, N., 2022. Smart defense against distributed Denial of service attack in IoT networks using supervised learning classifiers. *Computers & Electrical Engineering*, 98, p.107726.

[20] Rao, Y.S., Keshri, A.K., Mishra, B.K. and Panda, T.C., 2020. Distributed denial of service attack on targeted resources in a computer network for critical infrastructure: A differential e-epidemic model. Physica A: *Statistical Mechanics and Its Applications*, 540, p.123240.

[21] Ismail, S., Hassen, H.R., Just, M. and Zantout, H., 2021. A review of amplification-based distributed denial of service attacks and their mitigation. *Computers & Security*, 109, p.102380.

[22] Ahmad, S., Umirzakova, S., Jamil, F. and Whangbo, T.K., 2022. Internet-of-things-enabled serious games: A comprehensive survey. *Future Generation Computer Systems.*

[23] Sviridov, G., Bonola, M., Tulumello, A., Giaccone, P., Bianco, A. and Bianchi, G., 2021. LOcAl DEcisions on Replicated States (LOADER) in programmable dataplanes: Programming abstraction and experimental evaluation. *Computer Networks*, 184, p.107637.

[24] Kaur, S., Kumar, K., Aggarwal, N. and Singh, G., 2021. A comprehensive survey of DDoS defense solutions in SDN: Taxonomy, research challenges, and future directions. *Computers & Security*, 110, p.102423.

[25] Myneni, S., Chowdhary, A., Huang, D. and Alshamrani, A., 2022. SmartDefense: A distributed deep defense against DDoS attacks with edge computing. *Computer Networks*, 209, p.108874.

[26] Chen, H.B., Chen, T.H., Lee, W.B. and Chang, C.C., 2008. Security enhancement for a three-party encrypted key exchange protocol against undetectable on-line password guessing attacks. *Computer Standards & Interfaces*, 30(1-2), pp.95-99.

[27] Satoh, A., Nakamura, Y. and Ikenaga, T., 2015. A flow-based detection method for stealthy dictionary attacks against Secure Shell. *Journal of Information Security and Applications*, 21, pp.31-41.

[28] Joshi, A., Wazid, M. and Goudar, R.H., 2015. An efficient cryptographic scheme for text message protection against brute force and cryptanalytic attacks. *Procedia Computer Science*, 48, pp.360-366.

[29] Boyle, R.J. and Panko, R., 2012. Corporate computer security. *Prentice Hall Press.*

[30] Pang, Z.H., Fan, L.Z., Sun, J., Liu, K. and Liu, G.P., 2021. Detection of stealthy false data injection attacks against networked control systems via active data modification. *Information Sciences*, 546, pp.192-205.

[31] Ren, X.X. and Yang, G.H., 2020. Adaptive control for nonlinear cyber-physical systems under false data injection attacks through sensor networks. *International Journal of Robust and Nonlinear Control*, 30(1), pp.65-79.

Volume: 14 Issue: 02 Pages: 5334-5341(2022) ISSN: 0975-0290

[32] Wang, J.S. and Yang, G.H., 2018. Data-driven methods for stealthy attacks on TCP/IP-based networked control systems equipped with attack detectors. *IEEE transactions on cybernetics*, 49(8), pp.3020-3031.
[33] Natarajan, K. and Subramani, S., 2012. Generation of SQL-injection free secure algorithm to detect and prevent SQL-injection attacks. *Procedia Technology*, 4, pp.790-796.
[34] Zhang, Z., Zhang, Y., Guo, D., Yao, L. and Li, Z., 2022. SecFedNIDS: Robust defense for poisoning attack against federated learning-based network intrusion detection system. *Future Generation Computer Systems*, 134, pp.154-169.
[35] Katsantonis, M.N., Mavridis, I. and Gritzalis, D., 2021. Design and evaluation of cofelet-based approaches for cyber security learning and training. *Computers & Security*, 105, p.102263.
[36] Kandasamy, N.K., Venugopalan, S., Wong, T.K. and Leu, N.J., 2022. An electric power digital twin for cyber security testing, research and education. *Computers and Electrical Engineering*, 101, p.108061.
[37] O'Connor, S., Hasshu, S., Bielby, J., Colreavy-Donnelly, S., Kuhn, S., Caraffini, F. and Smith, R., 2021. SCIPS: A serious game using a guidance mechanic to scaffold effective training for cyber security. *Information Sciences*, 580, pp.524-540.
[38] Zhang, Y. and Malacaria, P., 2021. Bayesian Stackelberg games for cyber-security decision support. *Decision Support Systems*, 148, p.113599.
[39] Wolfenden, B., 2019. Gamification as a winning cyber security strategy. *Computer Fraud & Security*, 2019(5), pp.9-12.
[40] Cone, B.D., Irvine, C.E., Thompson, M.F. and Nguyen, T.D., 2007. A video game for cyber security training and awareness. *computers & security*, 26(1), pp.63-72.

AUTHOR'S PROFILE

Dr.P. Mohana Priya, currently working as an Assistant Professor in SASTRA Deemed University. Pursued PhD and M.E CSE from Thiagarajar College of Engineering, Madurai. Done B.E CSE from Raja College of Engineering and Technology. My area of research includes Network Security and Software Defined Networks. She has decent publications in Internal conferences/Journals. Her areas of interest include Network Security, Software Defined Networks, Cyber Security, Cryptography, Machine Learning.

Mr.Abhijit Ranganathan, currently a student at SASTRA Deemed University. Pursuing my Final Year B.Tech Computer Systems and Business Systems degree. I am NSE level 1 certified and NSE level 2 certified. My area of interest includes Cyber Security, Computer Networks and Ethical Hacking.