International Journal of Enhanced Research in Science, Technology & Engineering
ISSN: 2319-7463, Vol. 11 Issue 8, August-2022, Impact Factor: 7.957

Create A Safe Cyberspace By Implementing A Prototype and Using A Cognitive Approach to Cyber Defense.

B Pavan Kumar[1], Dr Ashish Chandra Swami[2], Dr Sikhakolli Gopi Krishna[3]

[1]Research Scholar, Department of Computer Science & Engineering, JS University, Shikohabad, Uttar Pradesh
[2]Associate Professor, Supervisor, Department of Computer Science & Engineering, JS University, Shikohabad, Uttar Pradesh
[3]Professor, Co-Supervisor & Professor Sri Mittapalli College of Engineering, Guntur, Andhra Pradesh.

ABSTRACT

Attacks on cyber infrastructure are becoming more frequent every day. Due to the widespread nature of cyberattacks and their financial consequences, it is critical to focus research efforts on analyzing how particular factors, such as financial motivation (costs and benefits of actions from the attacker's and defender's perspective), technological limitations (network response to defender patching actions), and environmental factors (players' access to information about opponent actions and payoffs) may influence adversary and defender's attack-and-defend decisions in the cyber realm. This thesis's primary goal is to investigate how the above mentioned components affect the decisions made by players taking on the roles of attackers and defenders in cyber-security games, using both lab-based experiments and computational cognitive models. To determine the importance of monetary incentives, three separate studies were conducted. The effect of financial incentives on the decisions made by hackers and analysts was initially investigated using a security game in three different experimental scenarios. In this initial experiment, human volunteers were compelled to fight against their ideal Nash counterparts and were compensated for attacking and defending, respectively, in the role of analysts and hackers. Using these human-Nash games, the deviations of the human players from optimal proportions in comparison to their Nash counterparts were evaluated.

When human hackers and analysts got cash incentives instead of the baseline, the findings showed a drop in attack and defensive activity. Analysts also deviated greatly from optimal conduct when they accepted payment for successful but undetected attacks from human hackers. The effect of monetary rewards for human analysts and hackers was then investigated in a second trial. Players were pitted against other players rather than Nash opponents. The findings demonstrated a considerable impact of the financial motivations of analysts and hackers over the baseline. The impact of financial penalties on analysts for misses and false alarms was investigated in the third experiment on motivations. As compared to the baseline, the findings demonstrated that analyst penalties had a major impact on analysts' and hackers' decision-making. To get a deeper understanding of the cognitive mechanics behind the choices made by hackers and analysts, computational cognitive models were built using Instance-based Learning (IBL) theory, a theory of judgements based on the recency and frequency of encountered information. The outcomes of IBL models adjusted to experimental data demonstrated that frequent and up-to-date information was essential for analysts and hackers alike. Additionally, human data collected from games in which analysts were penalized financially was used to adjust IBL models. The results show that an IBL model taught under conditions where analysts faced financial penalties generalized appropriately to scenarios where hackers and analysts earned financial incentives.

An experiment examining the effects of technical constraints was conducted using Markov security games (MSGs) (i.e., how the network responds to the defender's patching efforts). Examining how patching affects hackers' and analysts' attack-and-defense decisions was the goal of this investigation. The latest action of analyst players determines the network's current condition in MSGs. Following the analyst's patching, it was discovered that 90% of the networks in an effective patching state were no longer susceptible, and 50% of the networks in a less effective patching condition were also determined to be non-vulnerable. Based on the findings, there was no discernible variation in the proportion of attack and defense actions in both effective and less successful environments.

Additionally, although the proportion of defensive activities was similar in the vulnerable and non-vulnerable phases, the non-vulnerable state had a smaller percentage of attack actions than the vulnerable condition. Both parties often deviated significantly from their Nash equilibria in a variety of scenarios. In order to understand

the cognitive processes involved in the decisions made by analysts and hackers, further study was conducted to develop a cognitive model based on IBL theory. The model demonstrated that a hacker's (analyst's) ability to patch successfully depends on low (high) levels of frequency and recency, cognitive noise, and attention to the opponent's actions. On the other hand, it showed the opposite results with less effective patching. Finally, to understand the influence of contextual circumstances (the availability or non-availability of interdependence information), an experiment was conducted in which the adversaries' behaviors and payoffs, or interdependence information, that was available to hackers and analysts, was changed. In a scenario when both players were completely aware of each other's intentions, they were blind to each other's actions and payoffs in the second condition (control). The information caused analysts and hackers to increase the proportion of attack and defense actions, respectively, based on the findings. Regarding financial incentives, technical constraints, and environmental concerns, our results have significant implications for real-world cyber decision-making.

Index Terms: Cybersecurity games, attack–defense decision making, financial incentives in cybersecurity, monetary penalties, human–Nash equilibrium comparison, Markov security games, network patching effectiveness, cognitive modeling, Instance-Based Learning (IBL) theory, human factors in cybersecurity, adversarial behavior analysis,

---

INTRODUCTION

The Cybersecurity is more crucial than ever because of a discernible rise in the number, diversity, and accuracy of attacks (Symmetry, 2019). A cyber attack is an attempt to gain unauthorized access to, or expose, change, disable, damage, or steal from a computer system, network, infrastructure, or other smart equipment (UpGuard, 2020). According to Symantec's 2019 report, data breaches alone are expected to have a global financial impact of around $5 trillion by 2020. Attackers and cybercriminals use the newest tools and technologies to search the internet for vulnerabilities. Human resources, who evaluate risks and choose how to address security issues, are equally as crucial to effective and successful cybersecurity as technology (Symmetry, 2019). A security defender assesses security levels, identifies vulnerabilities, and tries to fix them in order to protect businesses or networks (Symmetry, 2019). Although research in the subject of cybersecurity is still in its early stages, companies seldom invest in the human aspect of cybersecurity until after an assault occurs (NIST, 2017; Anwar et al., 2016; Nobles, Calvin, 2018; Vieane et al., 2016).
Cybersecurity may be analyzed as a non-cooperative game using behavioral game theory (Dutt, Ahn, & Gonzalez, 2013; Gonzalez, 2011; Do et al., 2017; Liang & Xiao, 2012). A recent analysis of game theory and cybersecurity summarized cybertools meant to increase network security (Roy, Ellis, Shiva, Dasgupta, Shandilya, & Wu, 2010). Their study's findings indicate that the current game-theoretic approaches to cybersecurity are based on either static or fully informed games, which misrepresent the current state of network security.

a fast-paced setting where defenders have to make decisions with little knowledge. Moreover, the conclusions derived from these approaches are predicated on optimum response strategies, or Nash equilibriums, which have been mathematically proven. Nevertheless, calculations of Nash equilibriums may become very complex when games are played repeatedly and with incomplete information. Consequently, current game-theoretic models ignore motivational factors and their interaction with technical constraints, which are likely to affect attacker and defender behavior.

Behavioral game theory (BGT; Camerer, 2003) is one tool used to study how incentive functions in cyber safety. In BGT, attacker-defender interaction is modeled by simple 2 x 2 (players x actions per player) games. In order to win these games, players must continually choose choices from a list of possibilities. The rewards for their efforts might vary based on what other players and opponents do. Security games, according to Lye and Wing (2005), have applications in network security since they replicate the interactions between attackers and defenders as players. Alpcan and Bapr (2011) have used security games, which provide crucial insights into the dynamics between attackers and defenders, to offer a fundamental abstraction of an attacker-defense dynamic in real-world scenarios.

Malicious attackers target a network while defenders keep an eye on it. In the simplest case, the attacker's action set is "attack" (a) and "not attack" (na).On the other hand, the defender's repertoire includes "intensified monitoring" or defensive action (d) and no-defensive action (nd). Attackers and defenders play simultaneously in an effort to maximize their gains. The following are the payoffs for the attacker: -A(a, nd) is the reward for successfully attacking the network (undetected), and A(a, d) is the penalty incurred when an attack is found. The benefitsPayoffs and actions in a security game between attackers and defenders. The payment denotes a cost and a reward for the participants. Each cell's first reward value represents the attacker, while the second value represents the defense.

This thesis uses BGT and the aforementioned games to investigate how decisions made via repeated interactions between human attackers and defenders help them refine their decision-making techniques in complex environments like cybersecurity. This thesis builds on earlier game theory research and attempts to understand how players' decisions are impacted by technological limitations (such as how the network responds to the defender's actions and how accurate the network is at reporting attacks), motivational factors (such as the costs and benefits of actions from the attacker's

and defender's perspective), and environmental factors (like player information). To understand the reasoning behind the decisions attackers make while defending, one may use the Instance-Based Learning Theory (IBLT; Dutt & Gonzalez, 2012; Gonzalez, Lerch, & Lebiere, 2003; Gonzalez & Dutt, 2011; 2012). It's been shown that IBLT effectively models human decision-making.

LITERATURE REVIEW

Research Recent advancements in cybersecurity research emphasize the integration of cognitive modeling and prototype-based systems to strengthen decision-making in adversarial environments. Studies on cognitive approaches such as Instance-Based Learning Theory (IBL) highlight the importance of human behavior, memory, recency, and frequency in shaping cyber-attack and defense strategies. These models have been applied in simulated security games to understand how hackers and analysts adjust their tactical decisions in response to incentives, penalties, uncertainty, and environmental cues. Moreover, cognitive research shows that individuals often rely on heuristic shortcuts, biased risk perception, and limited attention, which can lead to deviations from optimal defense strategies predicted by game theory. Understanding these cognitive limitations has become crucial for designing systems that support, rather than overwhelm, human decision makers.

Parallel to cognitive research, prototype-based cybersecurity frameworks have emerged to evaluate real-time interactions between users and network systems. Such prototypes, including cyber ranges, simulated networks, and Markov Security Games, enable controlled experiments to study vulnerabilities, patching mechanisms, alert handling, and adaptive responses. These platforms allow researchers to model realistic adversarial scenarios, test the timing and effectiveness of defense actions, and observe how attackers respond to system changes such as patch deployment or security upgrades. In addition, prototype systems support the integration of automated data collection, behavioral logging, and analytics that provide deeper insights into user performance and adversarial tactics.

Together, cognitive theories and prototype testbeds provide a holistic understanding of cyber decision-making and enable the development of intelligent, behavior-aware defense mechanisms essential for securing modern cyberspace. By combining human-centered cognitive insights with technically accurate prototype models, researchers can design adaptive security frameworks that anticipate attacker behavior, enhance analyst performance, reduce cognitive load, and ultimately promote more resilient and secure network environments. This integrated approach bridges the gap between human cognition and technical cybersecurity, paving the way for next-generation defense strategies that align human behavior with system-level protection goals.

METHODOLOGY

The Most cyber-security books and articles are usually quite specialized and policy-focused. Although some American strategists have concentrated on China and Russia (but primarily to consider the threat to the US), the US is the primary, and often only, venue and target of this literature. Moreover, there is a lack of coherence between this corpus of work and broader theories and research on international relations. Writing generated outside of certain US military publications and think institutes continues to be dispersed. Several academics have utilized constructivist frameworks—particularly securitization theory—to examine how security concerns in the digital age are constructed. This provides insightful information on how threats are seen and how policies respond, but further study is necessary, especially when comparing threat constructions in non-US nations. Another corpus of literature that focuses on "Postmodern War," which is seen as a discourse on technical-military interaction that also emphasizes the role of information, has been influenced by post-structuralism. This absence of theoretical scholarship in security studies is all the more perplexing as cyber-security gains prominence in the policy arena. A possible reason might be the unique characteristics of cyber-security. Many academics are inclined to exclude technological threats from security (studies) since they don't share many discursive characteristics with military or political dangers. This kind of exclusion stems from the idea that "security proper" is associated with haste and extraordinary/extreme actions. The main primary sources of information utilized in this study were the Government of India website, news announcements from the Ministry of Defense and Home Affairs, and reports from other government departments that are allies. Use has been made of newspaper articles from prestigious national and international newspapers. In addition to books, papers from prestigious academic publications on relevant subjects have been utilised as secondary sources of research. The websites of several government agencies and educational institutions have been consulted for main and secondary data.

Cyberspace security is discussed in relation to national security in the books Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World by Derek S. Reveron, Cyber power and National Security by Franklin D. Kramer, and Cyber War: The Next Threat to National Security and What to Do About It by Richard A. Clarke. They explain the ways in which the cyberspace is being used to carry out different kinds of threats against a country's security. The evaluation of these works was conducted with the intention of providing a more comprehensive knowledge of the dangers that cyberspace poses to national security. We get a general overview of the cyberspace network from the books Cyber security: The Essential Body of Knowledge by Shoemaker & Conklin and The Basics of Cyber Warfare: overview the Fundamentals of Cyber Warfare in Theory and Practice by Steve Winterfeld. Paul

Rozenweig's Cyber Warfare (The Changing Face of War) describes how cyberwar is fought online. The purpose of the book reviews was to provide us a basic understanding of the operation of the cyber world. On the subject of cyber security, Miriam Dunn Cavelty has authored many books and articles. Her conclusions have been thoroughly investigated. The papers and articles written by IDSA's cyber security specialists in India were carefully examined, and their suggestions were carefully considered. In order to have a general understanding of the cyber security debate occurring in India as well as worldwide, a number of papers written by eminent academics and activists and published in prestigious publications were examined. Government reports have been closely examined, both from India and other international peers. We've also checked the websites of every significant ministry, department, and organization for changes. We also study books on information retrieval while considering the evolving notion of security. Numerous studies were conducted for web publications in order to compile fascinating data on the dynamic nature of cyber security risks. The novels that were reviewed and referenced above are among the most recent releases. A comprehensive inventory is supplied in the references section.

There aren't many studies in the subject of cyberspace, especially when it comes to cyber security. This is due to the fact that cyber dangers are still in their infancy. Cyberspace is a dynamic environment where threats are always of a fleeting nature. Every day, non-state actors, hackers, and others come up with new ways to wreck havoc on the cyber network. Three elements have been looked at in this study: the problems, the difficulties, and the structure needed for India's cyber policy. Debate about cyber security is contentious. This is due to the fact that all users of the internet, including businesses, governments, and private citizens, are stakeholders. There are several levels of hazard to each of them, such as malware malfunction, worm assault, or virus attack. This research investigated the many procedures, frameworks, fallacies, and realities related to cyberspace and the need of its security. On both sides, there are many who argue that the Internet must be a controlled medium with governmental checks and balances in place, in addition to being a free medium of information. The purpose of this research has been to dissect the truthfulness of statements made by advocates on both sides of the dispute.

The research will only look at matters related to national security and is based on the present cyber security policy framework in India. This study has a restricted geographical and temporal scope. The research only looks at India's proposed national cyber security policy in terms of geographical scope. The Parliament has not yet ratified the measure.Since maintaining national security is a continuous endeavor, a time limit cannot be specified.

This study evaluated India's cyber security policies. Given that cyberattacks occur every minute, the discussion around cyber security is becoming more heated. The research has considered the government's opinions and concerns in addressing the threat posed by cyberwarfare. This research also made an effort to evaluate the government's readiness in the event that the country's security were threatened by an unanticipated cyberattack. Before drawing any conclusions, the dangers related to cyber security have been examined, as well as potential future threats.

The conversation around cyber security has grown in scope and importance recently, with many now seeing it as a crucial component of diplomacy and interstate relations. States must gradually turn this into an arena where they must defend their territory, use tools and strategies to maximize the benefits of the cyber world for their national interests, form alliances to further these interests, and selectively target and oppose—either individually or collectively—those actors, fields, or interests that are detrimental to or at odds with their own. varied states have varied policies when it comes to cyber security and cyberspace behavior. Several nations, including China and Russia, claim national sovereignty over the Internet. On the basis of the stability of the nation and the regimes, they support internet bans. However, the US and a number of other nations support upholding the right to free expression and human rights. The two strategies are quite different.In addition to the nations, other key stakeholders in the internet and cyberspace include economic interests, civil society organizations, and international organizations. The state's attempts to exert control over the internet have them on edge. Their preference is for the open architecture of the internet to be preserved.

THESIS ORGANISATION

The Over the course of thousands of years, humans have made enormous strides in science and technology, from "Stone Age" technology to the information and communication technologies of today. The advancement of contemporary technology has made life easier for people. When a new technology is released, people start to show interest in utilizing it. Because of their interest, some individuals hunt for ways to profit more from modern technologies, which leads to misuse and ultimately detrimental impacts. The invention of Cyber security, sometimes known as cellphones, is one of the most significant scientific and technology advances of the last few years. "Researchers have examined the impact of mobile phone use on people's lives over the past ten years, especially in light of its numerous applications and the growing number of younger generations using them. They have discovered that using Cyber security for e-mail and communication with others has decreased feelings of loneliness (Ogataet) and has also facilitated the creation of friendships" (Kamibeppu). These days, Cyber security are a necessary and fundamental component of every person's daily existence.These days, Cyber security are seen as more than just devices for receiving and making calls. Cyber security have developed into indispensable tools for organizing and managing everyday activities, interacting with others on social media, and playing newly released applications and games.

Teenagers in particular are more susceptible to the harmful effects of mobile phone use due to their high rate of penetration and excessive use of the gadget. Addiction to telephones is more common among teenagers, just as in other cases. Teenagers' inability to forge an identity and need to build close, fulfilling connections with others inside their own lives are the main causes of this reliance. It is clear that teenagers all across the world are using their phones much more often. Most of the time, using a mobile phone is never considered seriously. It is assumed that this would be accepted as a typical adolescent behavior and given little weight. However, excessive mobile phone usage is increasingly seen as a serious problem in the West since it has a severe psychological, physical, and social impact on many young people and adolescents.

Teens and young adults find it difficult to focus on their education or other creative endeavors. This is due to the fact that using a phone often results in issues including sadness, anxiety, and sleeplessness. The use of Cyber security can also have an impact on a person's overall health. The World Health Organization has defined cellphone radiation as "possibly human carcinogenic" after a group of scientists reviewed scientific studies regarding cellphone safety and declared that " Cyber security could be a health risk for the long term to health." Cyber security are classified as 2B. It is included in the same group as compounds that may cause cancer and coffee.

Teenagers are more likely to notice excessive mobile phone usage because they are determined to develop a unique identity and to be in regular contact with their friends, classmates, and other students. They want to be up to date on the most recent happenings in their friends' life as well as those around them. Teens or consumers of this kind of use are becoming less and less grounded in reality, yet they are still linked to the virtual world. Teachers and parents have often seen the harmful impact that students and their offspring have on cellphones, which have a detrimental effect on the users' personalities and behaviors. Teens play with their phones all the time, making calls and engaging in conversation.

RESULTS

According The experimental findings show that financial incentives, technical constraints, and environmental information significantly influence attacker and defender decision-making across all stages of cyber interaction. Monetary rewards consistently led to a reduction in both attack and defense actions, suggesting that incentivized players adopt more risk-averse strategies. In contrast, financial penalties increased defensive vigilance but also produced larger deviations from Nash equilibrium strategies, highlighting how stress and fear of loss distort human decision-making under uncertainty.

Prototype-based experiments demonstrated that patching effectiveness strongly shaped attacker behavior, with successful patching reducing attack attempts by more than half and altering the timing and frequency of intrusion attempts. In less effective patching scenarios, attackers maintained higher activity levels, showing that partial patching does not sufficiently discourage adversarial behavior. Analysts, however, displayed relatively stable defensive patterns across both vulnerable and patched network states, indicating a cautious “defense-first” mindset even when the system was non-vulnerable.

Cognitive models based on Instance-Based Learning Theory (IBL) accurately replicated human decisions across diverse experimental conditions, demonstrating high predictive validity and strong generalization across incentive and penalty environments. The models revealed that recency, frequency of past outcomes, cognitive noise, and attention levels were dominant contributors to both attacker and defender choices. High recency and frequency weights produced more rational, stable decisions, while increased cognitive noise resulted in greater deviations from optimal behavior.

Environmental information also played a significant role: when attackers and defenders had access to interdependence information (opponent payoffs and actions), both parties increased their activity levels. Attackers became more opportunistic, while analysts adopted more aggressive or anticipatory defense strategies.

Overall, the results indicate that combining cognitive insights with prototype-based experimentation is essential for designing adaptive, human-aware cyber defense mechanisms. This integrated approach not only improves prediction of adversarial behavior but also provides a foundation for training systems, automated decision support tools, and behavior-driven cybersecurity policies.

DISCUSSION

Moore’s law The findings of this research highlight the complex interplay between human cognition, financial motivations, technical constraints, and situational awareness in cybersecurity decision-making. Financial incentives and penalties produced notable deviations from Nash equilibrium predictions, suggesting that classical game-theoretic models are insufficient to fully capture human behavior in adversarial digital environments. The reduction in attack and defense actions under reward conditions indicates a shift toward risk-averse strategies, while penalties promoted defensive alertness but also heightened cognitive stress.

The prototype-based experiments further revealed that patching effectiveness substantially influences attacker engagement, although analysts tended to maintain stable defense patterns regardless of network vulnerability. This suggests that defenders often rely on habitual or cautious strategies rather than dynamically adjusting to system states. Cognitive models developed using IBL theory successfully replicated these behaviors, demonstrating the theory's applicability to cybersecurity decision-making and its ability to generalize across incentive and penalty conditions.

The integration of cognitive and prototype-based results confirms that cyber defense strategies must incorporate behavioral understanding rather than rely solely on technical optimization. A behavior-aware defense approach is essential for building predictive, adaptive, and resilient cybersecurity systems.

CONCLUSION

The This chapter explains why the Fogg Behaviour Model (FBM) was chosen as the theoretical foundation for the intervention's design. The FBM is explained in length in this chapter. The FBM states that when ability, cue, and motivation are present together, a behavior will occur. Additionally, the model identifies three main motivators, each of which has two aspects. The researcher supported the use of anticipation as the main motivator for developing the intervention in this chapter. The use of Cyber Suraksha, a serious game, in the intervention was also supported by the researcher. There are four main variables that drive the security awareness programs. Carpenter (2019) identifies them as information dissemination, compliance, behavior shaping, and culture molding. The author argues that knowledge is not the same as care and that if a user has no interest in cybersecurity, they are unlikely to go above and beyond to connect with it. Moreover, the author argues that if security personnel act against human nature, then efforts to raise awareness and alter behavior would fail. Because of this, it is imperative that a SETA software be developed with human nature in mind. This thesis' primary goal is to provide a framework for enhancing the cybersecurity behavior of Indian smartphone users. The FBM describes the essential prerequisites for behavior modification in a clear and concise manner. Previous research has shown the importance of optimism and fear as guiding principles.

This chapter discussed the SMITE IP traceback approach, which is particularly useful for autonomous systems that are based on SDN. The fact that SMITE is the first known combination of MPLS and SDN gives rise to the possibility that it presents a fresh approach to the process of IP address tracing. This comes with a multitude of substantial advantages, including the following: 1. Awareness of the events that took place following the passing of a person. being competent of distinguish a single packet of attack. There has been a reduction in the amount of the CAM/TCAM memory of the switches. 4. The MPLS matching process proceeds more quickly on the dataplane as a result of the use of tiny tags. 5. Even the core dataplane of the SDN network may be able to operate more quickly if that network uses matching short tags (MPLS). It is possible to lower the amount of power used by using MPLS matching for short tags. In light of the continuous efforts to enhance the performance of SDN-based networks via the integration of SDN and MPLS, it is impossible to overstate the significance of SMITE in terms of its value and prospective use. The steps involved in developing an example of an IPv4 SMITE application are described in this section.

In spite of this, it is not difficult to change a message for an IPv6 network if the source IP address is wrapped in two MPLS Labels like this. Additionally, the source codes for the OpenvSwitch and Ryu controllers have been altered in such a way that the Reserved Flag (RF) field of the IP header has been updated to keep the first bit of the source IP address. The proliferation of distributed denial of service attacks is a direct result of the rapid advancement of technology. Consequently, it is of the utmost importance that you immediately alert the authorities of any distributed denial of service attacks.

REFERENCES

[1]. N. Eddermoug, A. Mansour, M. Sadik, E. Sabir, and M. Azmi, "Klm-ppsa: Klm-based profiling and preventing security attacks for cloud environments," in 2019 International Conference on Wireless Networks and Mobile Communications (WINCOM). IEEE, 2019, pp. 1–7.
[2]. N. Eddermoug, A. Mansour, Sadik, E. Sabir, and Azmi, "Klm-based profiling and preventing security attacks for cloud computing: A comparative study," in 2021 28th International Conference on Telecommunications (ICT). IEEE, 2021, pp. 1–6.
[3]. A. Abusitta, M. Bellaiche, and M. Dagenais, "A trustbased game theoretical model for cooperative intrusion detection in multi-cloud environments," in 2018 21st Conference on Innovation in Clouds, Internet and Networks and Workshops (ICIN). IEEE, 2018, pp. 1–8.
[4]. P. A. A. Resende and A. C. Drummond, "A survey of random forest based methods for intrusion detection systems," ACM Computing Surveys (CSUR), vol. 51, no. 3, pp. 1–36, 2018.
[5]. Hasson and Timothy, "Bad bot report 2021," https://www.imperva.com/blog/ bad-bot-report-2021-the-pandemic-of-the-internet/, accessed April 13, 2021.
[6]. A. A. Aburomman and M. B. I. Reaz, "A survey of intrusion detection systems based on ensemble and hybrid classifiers," Computers & security, vol. 65, pp. 135–152, 2017.
[7]. F. Pacheco, E. Exposito, M. Gineste, C. Baudoin, and J. Aguilar, "Towards the deployment of machine learning

solutions in network traffic classification: A systematic survey," IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1988–2014, 2018.

[8]. I. A. N. Authority, "Protocol assignments," https:// www.iana.org/protocols, accessed June 24, 2020.

[9]. F. Erlacher and F. Dressler, "On high-speed flow-based intrusion detection using snort-compatible signatures," IEEE Transactions on Dependable and Secure Computing, 2020.

[10]. Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, p. e4150, 2021.

[11]. N. Krishnan and A. Salim, "Machine learning based intrusion detection for virtualized infrastructures," in 2018 International CET Conference on Control, Communication, and Computing (IC4). IEEE, 2018, pp. 366–371.

[12]. S. Sharma, P. Zavarsky, and S. Butakov, "Machine learning based intrusion detection system for webbased attacks," in 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). IEEE, 2020, pp. 227–230.

[13]. X. Dong, Z. Yu, W. Cao, Y. Shi, and Q. Ma, "A survey on ensemble learning," Frontiers of Computer Science, vol. 14, no. 2, pp. 241–258, 2020.

[14]. A. Nisioti, A. Mylonas, P. D. Yoo, and V. Katos, "From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3369–3388, 2018.

[15]. S. Ganapathy, K. Kulothungan, S. Muthurajkumar, M. Vijayalakshmi, P. Yogesh, and A. Kannan, "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey," EURASIP Journal on Wireless Communications and Networking, vol. 2013, no. 1, pp. 1–16, 2013.

[16]. S. Lee, J. Kim, S. Woo, C. Yoon, S. Scott-Hayward, V. Yegneswaran, P. Porras,and S. Shin, "A comprehensive security assessment framework for software-defined networks," Computers & Security, vol. 91, p. 101 720, 2020, issn: 0167-4048.

[17]. J. M. Vidal, A. L. S. Orozco, and L. J. G. Villalba, "Adaptive artificial immune networks for mitigating dos flooding attacks," Swarm and Evolutionary Computation, vol. 38, pp. 94–108, 2018, issn: 2210-6502

[18]. S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "SDN security: A survey," in 2013 IEEE SDN for Future Networks and Services (SDN4FNS), 2013, pp. 1–7. doi: 10.1109/SDN4FNS.2013.6702553 (page 6).

[19]. S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," IEEE Communications Surveys Tutorials, vol. 18, no. 1, pp. 623– 654, 2016. doi: 10.1109/COMST.2015.2453114 (page 6).

[20]. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," IEEE/ACM Transactions on Networking, vol. 9, no. 3, pp. 226–237, 2001. doi: 10.1109/90.929847 (pages 7, 17, 20, 21, 44, 73, 74, 79, 98).

[21]. A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E. Jones, F. Tchakountio, B. Schwartz, S. T. Kent, and W. T. Strayer, "Single-packet IP traceback," IEEE/ACM Transactions on Networking, vol. 10, no. 6, pp. 721–734, 2002. doi: 10.1109/TNET.2002.804827(pages 7, 17–19, 25, 44, 73, 78, 98).

[22]. V. A. Foroushani and A. N. Zincir-Heywood, "Deterministic and authenticated flow marking for ip traceback," in 2013 IEEE 27th International Conference on Advanced Information Networking and Applications (AINA), 2013, pp. 397–404. doi: 10.1109/AINA.2013.60 (pages 7, 17, 23, 44, 73).

[23]. V. A. Foroushani and A. N. Zincir Heywood, "IP traceback through (authenticated) deterministic flow marking: An empirical evaluation," EURASIP Journal on Information Security, vol. 2013, no. 1, 2013. doi: