Crime Risk Forecasting using Cyber Security and Artificial Intelligent

Mr. Umakant Dinkar Butkar, Manisha J Waghmare
Sir Visvesvaraya Institute of Technology, Nashik, India.
Matoshri College of Engineering & Research Centre

Abstract:
The topic of cybersecurity has rapidly advanced over the past ten years, making headlines frequently as threats increase and hackers try to elude law authorities. The techniques used by cybercriminals have improved over time, despite the fact that their fundamental motives for launching assaults have largely remained the same. Using conventional cybersecurity tools, it is getting harder to identify and stop evolving threats. Because of improvements in cryptographic and Artificial Intelligence (AI) techniques, particularly machine learning and deep learning, cybersecurity experts may soon be able to defeat the attackers' continually evolving threat. Here, we emphasize both the benefits and drawbacks of AI in order to analyze how it might improve cybersecurity solutions. Additionally, we discuss the possibilities for further study in the field of cybersecurity related to the advancement of AI methodologies across numerous application areas. One of our society's most significant and pervasive issues is crime. Numerous crimes are perpetrated often each day. The dataset in this instance consists of the date and the annual crime rate for the corresponding years. The crime rate used in this project is only based on robberies. Utilizing historical data, we employ the linear regression algorithm to forecast the percentage of crime rate in the coming years. The algorithm receives a date as input, and the result is the proportion of crime for that particular year.

Keywords: Artificial intelligence, Cyber security, Cyberattack, Machine learning, Crime rate, number of crimes, regression algorithm.
DOI: 10.24297/j.cims.2023.2.4

1. Introduction

Humanity is seriously threatened by crime. Numerous crimes happen frequently and at predictable times. Perhaps it is spreading swiftly and broadly. Crime happens everywhere, from little towns and villages to big cities [1,2,3]. In addition to robbery, manslaughter, rape, assault, battery, and false imprisonment, there are numerous other unique categories of crime. Due to the increase in crime, cases must be resolved considerably more rapidly [4,5]. The police department is in charge of controlling and reducing the criminal activity, which has accelerated in recent years. For case solving to be performed more rapidly, technology is needed. It was found through thorough documentation and instances that data science and machine learning may speed up and simplify the process. Using the properties in the dataset, this research aims to forecast crime [6-9]. The dataset was gathered from the official websites. Using the use of a machine learning system with Python at its core, we can predict the sort of crime that will occur in a particular region. To train a model for prediction would be the goal. The training on the training data set will be validated using the test dataset [10-13]. The Multi Linear Regression (MLR) will be used in order to forecast crime. To examine potential crimes that may have happened in a specific year based on population and number of crimes, a dataset is visualized [14-16]. This work aids law enforcement organizations in forecasting and identifying the crime percapita in a region, which lowers the crime rate. Recently, experts in cybersecurity have been examining Artificial Intelligence (AI) methods to enhance cybersecurity. Comparable to how hackers use ever-more-advanced techniques to avoid being caught[17-22]. The potential for AI-based cybersecurity solutions to decrease or fully avoid data breaches and better combat attackers is the main focus of this work [23-32]. Since artificial intelligence (AI) was first developed in the 1950s, a wide range of fascinating systems and research findings have been produced. Deep learning and machine learning emerged as a result of additional developments. A few of the sectors using AI nowadays are manufacturing, law, healthcare, agriculture, and space exploration [33-36].

2. Threats To Cybersecurity And Legacy Solutions For Cybersecurity

Over the past ten years, there have been numerous varieties of cyberthreats. Then, we briefly discuss those risks. The top 10 cyberthreats that we currently face are as follows:

1) Denial of Service (DoS) attacks: These try to overwhelm a victim system's processing power by flooding it with numerous urgent requests. One attacker system can perform a distributed denial of service (DDoS) assault against a victim machine while evading security measures by sending numerous network traffic packets that seem to be normal.

2) Attacks by a man in the middle (MiTM): These traditional assaults involve intercepting data being transmitted on a channel between two legitimate parties that are conversing. The attacker steps in between A and B, either physically or virtually, posing as A to communicate with B by intercepting A B messages and substituting malicious or changed messages for A B messages. The attacker then repeats the operation, posing as B and speaks to A, on the B communication

channel. One of the attack's alternative implementations is IP address spoofing, in which a hostile actor tricks legitimate systems into thinking it is a reliable entity in order to get access to the system. When an adversarial actor utilizes the communication channel to repeatedly send an old, previously stored message, this is known as a message replay attack.

3) Phishing and spear-phishing attacks: These involve creating emails that seem real and sending them to reliable systems in an effort to trick trusted end users into clicking a link and providing personal information. These attacks involve social engineering methods, in which emails are made to appear trustworthy to recipients in an effort to win their trust.In order to craft emails that seem extremely legitimate and frequently contain trusted email addresses in the "from" field, bad actors must first conduct a thorough background check on potential victims. This technique is known as spear phishing.

4)Drive-by attacks: These are committed by hostile actors that browse the web looking for vulnerable websites in order to infect the web servers with harmful scripts.Visitors to the website eventually get the malware, which compromises systems, exposes confidential information, and does other harm.

5) Password attacks: These include utilizing common passwords to brute force their way into a system, spying on user keyboard activity, and creating complex passwords using artificial intelligence (AI) techniques.

6)Attacks involving Structured Query Language (SQL) Injection: are a common type of cyberattack that work by injecting SQL query code into a webpage's input fields in order to exploit SQL language bugs.The data held on a backend database server, maybe including usernames and passwords, may be partially or completely revealed when the webserver executes the SQL code.

7) Cross-site scripting assaults: These entail injecting malicious code into a flimsy web server. When uninformed end users later access the hosted webpages, malware would be downloaded into the victim's PC. Such malware may transmit user information from the victim's computer to the malicious actor's servers, which may then make it possible to hijack web sessions, steal login information, install keyboard loggers, take screenshots, and even remotely control the victim's machine.

8) Attempts at eavesdropping can be undertaken by sniffing out the network connection channel and then utilizing the information obtained. Malicious individuals could attack the line violently, substituting messages with bogus ones, and pose as normal users, or they may passively sniff the connection and collect user data.

9) Birthday attacks: This message digest, also known as a hash, can be created by applying a well-known method like the Secure Hash Algorithm 1. (SHA-1). When this method is used to a message of any length, a hash value with a predetermined length is generated. The birthday attack outlines an attempt by a hostile actor to determine which two different messages produce the same hash value. These attacks look for random messages with the same hash value as real communications using artificial intelligence.

10) Malware attacks: The potential for malware to spread through hosting firms' websites is one of the major problems they face. A website's defenses can be strengthened by implementing the appropriate security controls, such as web proxies, firewalls, and intrusion detection systems.The trade-off between the appropriate amount of security controls and the usability of the hosted websites is a significant problem in this situation. The region of vulnerability for a website increases with its level of usability.

Attempts are made to initiate network assaults against the environment in order to obstruct services, steal personal or business data, and gather network intelligence. Malicious people acquire access and manipulate the operating system (OS) by taking advantage of a flaw in the OS that allows them to do so. Some of these assaults involve the theft of personal data, which can be exploited to access private or business information. According to the attack objectives, anticipated targeted device or application, data/information revealed while a certain assault is in progress, kind of environment impacted when a certain attack occurs, and how these attacks are discovered, we classified numerous network attacks in Table 1.

We then quickly go over conventional (non-AI) cybersecurity methods for spotting cyberattacks:
1) Game theory has previously been used to cybersecurity.The victim's computer is the other participant in the game, with the malicious actor acting as the first player. Each person makes an effort to maximize their incentive by strategic movement, arguing logically that the move will achieve the desired result. The actions of each participant can either be predicted in advance or remain a secret.

2) Rate control: DoS and DDoS assaults aim to reduce system availability. Rate-control strategies can reduce the impact on such systems' functionality when they are attacked by limiting incoming network traffic, changing permission lists, and basic traffic throttling .

3) Heuristics: Firewalls and intrusion detection systems commonly employ heuristics to choose the appropriate rule for classifying network input as legitimate or anomalous. One such technique searches for suspicious URL addresses using a variety of procedures that include substring matching.

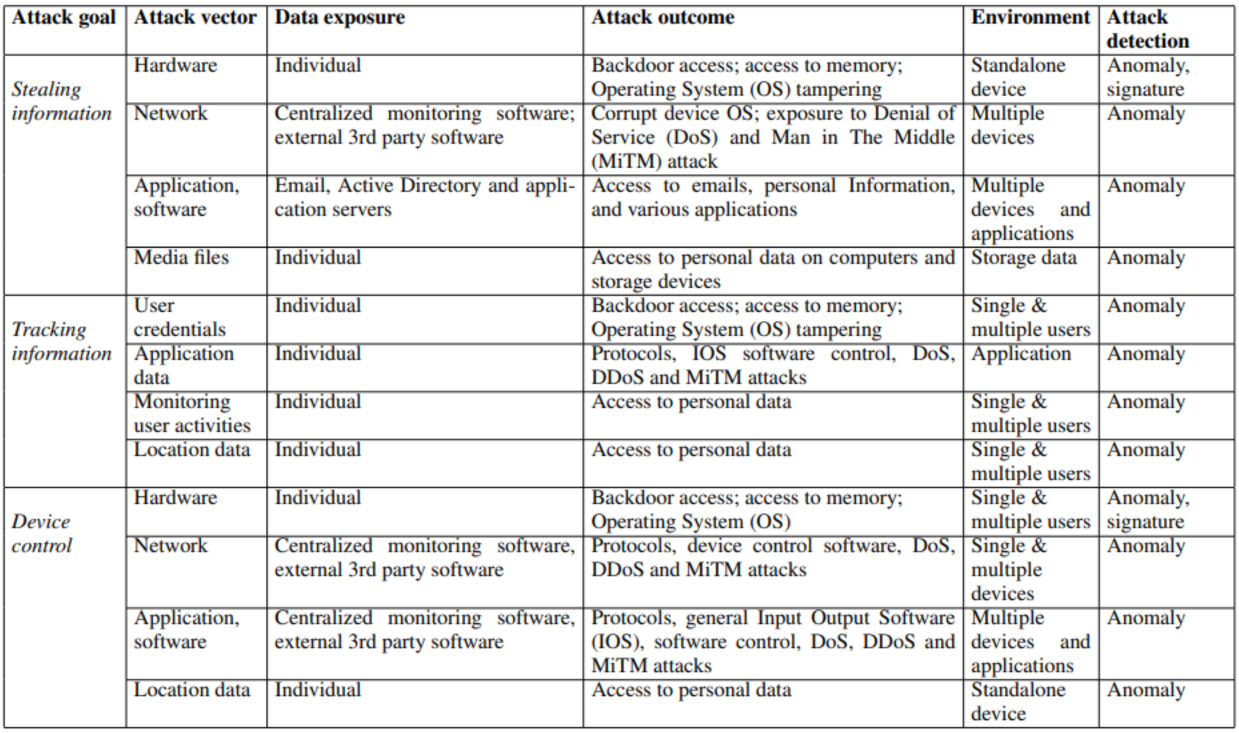
4) Signature-based intrusion detection: This type of intrusion detection system uses a database to hold either attack signatures that are in response to malicious behavior or valid signatures that are in response to normal traffic.

5) Anomaly-based intrusion detection: This technique creates an internal representation of the typical observed phenomena. The models could be rule-based systems, mathematical models, or statistical techniques. Agressions are considered to be deviations from the norm.

6) Autonomous systems: These can offer dependability and availability, as well as the ability to defend against harm and heal themselves, as seen with the Bionic Autonomic Nervous System (BANS). Malware and spy ware are protected from by Cyber Neuron. An sophisticated tool to repair spyware and malware damage is called Cyber Axon. Similarly, Peripheral Nerve establishes a communication link between numerous cyberneurons placed on various devices to provide a strong protection against DoS/DDoS attacks. The last function of Central Nerve is to provide information to other security devices and act as a knowledge base for potential attacks. The idea of collaborative defense by peripheral nerves is to have network devices work together to thwart DoS and DDoS attacks.

7) Security controls for end users: Mobile phones, iPads, and other modern end-user gadgets like smart portable devices (PCs) require built-in security rather than add-ons. Despite the fact that some vendors advocate automated updates, end users may fail to update their devices with the most recent security patches, which prevents security fixes from being implemented. The Wannacry ransomware attack is an illustration of an attack where the most recent vendor-provided security fixes were not installed on all end-user devices. Users frequently aren't aware of the consequences of not installing patches. Even though some users may be aware of this

reality, there are times when they either fail to take the necessary steps to secure their devices or carry out the wrong processes, leaving the devices vulnerable to other attacks.



Attack goal	Attack vector	Data exposure	Attack outcome	Environment	Attack detection
Stealing information	Hardware	Individual	Backdoor access; access to memory; Operating System (OS) tampering	Standalone device	Anomaly, signature
	Network	Centralized monitoring software; external 3rd party software	Corrupt device OS; exposure to Denial of Service (DoS) and Man in The Middle (MiTM) attack	Multiple devices	Anomaly
	Application, software	Email, Active Directory and application servers	Access to emails, personal Information, and various applications	Multiple devices and applications	Anomaly
	Media files	Individual	Access to personal data on computers and storage devices	Storage data	Anomaly
Tracking information	User credentials	Individual	Backdoor access; access to memory; Operating System (OS) tampering	Single & multiple users	Anomaly
	Application data	Individual	Protocols, IOS software control, DoS, DDoS and MiTM attacks	Application	Anomaly
	Monitoring user activities	Individual	Access to personal data	Single & multiple users	Anomaly
	Location data	Individual	Access to personal data	Single & multiple users	Anomaly
Device control	Hardware	Individual	Backdoor access; access to memory; Operating System (OS)	Single & multiple users	Anomaly, signature
	Network	Centralized monitoring software, external 3rd party software	Protocols, device control software, DoS, DDoS and MiTM attacks	Single & multiple devices	Anomaly
	Application, software	Centralized monitoring software, external 3rd party software	Protocols, general Input Output Software (IOS), software control, DoS, DDoS and MiTM attacks	Multiple devices and applications	Anomaly
	Location data	Individual	Access to personal data	Standalone device	Anomaly

TABLE 1: many assault types, their results, and techniques for identifying them

3. Artificial Intelligence

AI is interested in how computers can comprehend or behave appropriately given their knowledge. This broad concept includes the extent to which machines can imitate human thought or behavior (Figure 1).

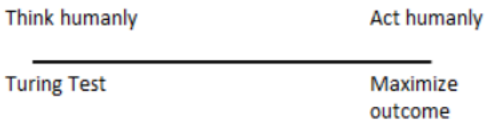


FIGURE 1: The breadth of intelligent measures includes everything from acting to maximize the outcome to thinking like a human utilizing the Turing Test.

The first applications of AI led to thinking machines that figured out complex problems like geometry checkers, and a group of block-world issues. Agent-based artificial intelligence (AI) or "bots"—software that acts like humans—became increasingly popular after the rise of the

Internet in the late 1990s. Search engines, online directories, and recommendation services have all benefited from the creation of ethical bots that crawl the Internet. They offer vandalism defense in Wikipedia pages where anyone can participate as an author. On the other hand, malevolent bots have also been developed to transmit malware, publish spam, and cheat at online games. Malicious bots hinder the correct operation of cyber services, harming the service providers by discouraging online users. As a result, several cybersecurity research looked into ways to identify and defend against rogue bots. When compared to humans, studies have shown that game bots are more persistent, less sociable (exchanging goods or bidding on products), and exhibit fewer variability in their activity sequences. Additionally, while human players like to work together with other players to fulfill tasks and missions, gaming bots are more motivated to collect things. Similar to spambots, malware bots can be identified by their behavior, which can be seen in various distinguishing communication patterns. Intrusion detection systems are where artificial intelligence is most applicable in the field of cyber security. Internet traffic is regularly analyzed by cyber security solutions to determine if it is benign or dangerous. Rule-based systems, which could locate assaults based on their signatures, were used in the early days of the Internet to detect cyberattacks. As the landscape of cyberthreats keeps growing, we need cutting-edge tools and technologies that can help in quicker identification, investigation, and decision-making for new risks .Since machine learning is applied so frequently to tackle cybersecurity difficulties, it is significant to note that the terms "machine learning" and "artificial intelligence" have come to be used interchangeably in the cybersecurity business.

MACHINE LEARNING

Machine learning approaches are often classified into two categories: supervised learning and unsupervised learning. In supervised learning, data samples are classified according to their class (e.g., malicious or legitimate). Unsupervised algorithms can label the data required for supervised algorithms using machine learning techniques, which employ mathematical, statistical, and probabilistic methodology. With rows representing samples of the data and columns representing their qualities, the processed data is arranged in a table with rows and columns. Assuming that each characteristic is the outcome of a distinct event, Naive Bayes is a machine learning technique that applies the Bayesian theorem to categorize data. The technique starts with the calculated probabilities of each class across all instances and calculates the likelihood that additional data samples will belong to each class.

B.DECISION TREES

A method for developing a collection of rules using training data samples is to utilize a decision tree. The algorithm repeatedly selects a feature to classify data samples. Since the approach classifies observed cybersecurity events as either genuine events or attacks, depending on feature values, and shows the decision's result as necessary, it provides an intuitive manner to discover cybersecurity concerns. For instance, decision trees evaluated size, duration, flow rate, and source/destination error rates to identify DoS assaults. Decision trees were also used to classify data from CPU utilization, network flow, and the amount of data presented in order to detect command injection attacks against robotic vehicles. The advantage of this strategy is that intrusion detection systems can categorize Internet traffic in real time once the best set of criteria has been identified. One of the most crucial factors in determining whether a cyberattack has occurred is the quality of generated real-time notifications. A rule-learning technique has the advantage of adding expert human input when developing rules. Consider a study that discovered DoS attacks in cloud networks using 28 features.

C. K-NEAREST NEIGHBORS

The k-Nearest Neighbor (k-NN) method classifies or clusters data based on data samples. In order to form clusters, the neighborhood was specified as k number of data samples based on a distance measure, typically the Euclidian distance. The distribution of additional data samples among the clusters is determined by the votes of all k neighbors. The approach described above is shown in Figure 3. The data now includes an additional sample (the red dot). In this case, the majority of data samples from one nearby cluster were the deciding factor. Consequently, the sample was classified as Class 2 when k=3. The sample was classified as Class 1 when k=9. Even for tiny values of k, the computational complexity of this method is high. However, because it can learn from fresh traffic patterns to identify zero-day attacks as one of its unknown classes, it appeals to intrusion-detection systems. Thus, there is now active study in this field to determine how k-NN might be employed for real-time cyberattack detection.

D.SUPPORT VECTOR MACHINES

The linear regression model is expanded upon by the Support Vector Machines (SVMs) method. SVMs classify data samples by locating a plane that divides them into two classes (as shown in Figure 4). Depending on the function used (referred to as a kernel), the separation plane can take the form of a linear, nonlinear, polynomial, Gaussian, Radial, sigmoid, and so forth. As a result, it is utilized in applications that allow for the simulation of attacks. As an illustration, network traffic from penetration tests on network systems was utilized as the training data Figure 2.

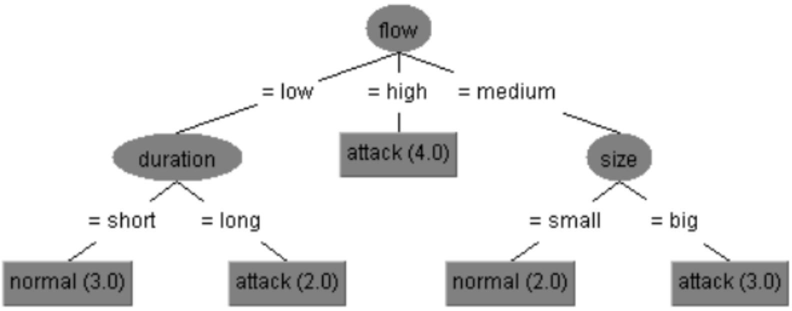


FIGURE 2: a decision tree example that distinguishes between attack and non-attack forms of network traffic

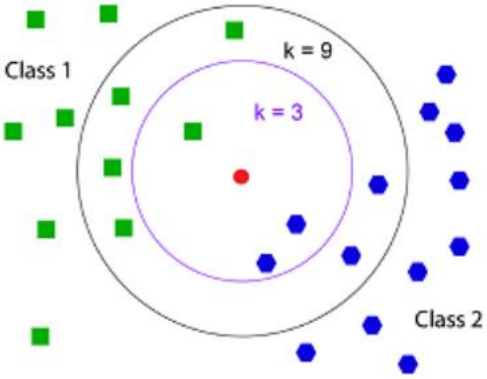


FIGURE 3. The k-Nearest Neighbor (k-NN) approach is used to divide data into classes 1 and 2 based on the k nearest data samples from the new data sample.

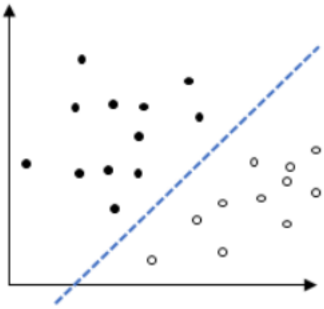


FIGURE 4. Support vector machines, or SVMs, find the plane splitting data samples.

E. ARTIFICIAL NEURAL NETWORKS

The functioning of neurons in the brain serves as inspiration for the Artificial Neural Networks (ANNs) learning technique. A target value is output using a series of data samples, and ANN approaches model neurons as a mathematical equation. The formula closely matches the equation for linear regression, in which a sample's data properties are weighted to produce an output value. The ANN algorithm cycles through its iterations until the output value is within the allowable error bounds of the target value. When given specific patterns seen in the data samples, the neurons learn by adjusting their weights in each iteration by calculating the deviation from the target value. When the mistake is small enough, the process produces a mathematical equation that, when given unknown data samples, gives an instructive result like the class. ANN approaches are capable of identifying patterns in noisy to incomplete data samples. They can adapt to new types of communication, making them appropriate for intrusion-detection systems. The Cascade Correlation Neural Network (CCNN), an ANN application that gradually adds additional hidden units to the hidden layer, was employed in a cybersecurity investigation.The proliferation of mobile devices over the past ten years has given rise to new traffic patterns, rendering outdated earlier detection algorithms derived from desktop traffic. The number of ports searched per second and the frequency of received packets varied between port-scanning operations against mobile devices.

F. SELF-ORGANIZING MAPS

A step up from ANNs, self-organizing maps (SOMs) construct two- or three-dimensional (2D or 3D) maps that show potential data organization by self-adjusting the weight of the neurons. The technique finds new data by spotting correlations in data sets.Their primary benefit is the ability to view the data, which enables the identification of network anomalies. Without visualization, it is difficult to understand the findings from intrusion-detection systems. With the aid of visualization tools that enable them to observe the regular pattern of traffic data, network managers can more easily discover anomalies in network traffic, such as zero-day assaults. Although anomalous occurrences can be efficiently highlighted by visualization approaches, professional eyes are still required to identify anomalies in the data.

G. BIOLOGICALLY INSPIRED TECHNIQUES

In addition to network traffic, offensive human language such as profanity, insults, hate speech, and racist/sexist statements can also cause cyberintrusions. Applications for Natural Words Processing (NLP) have evolved to separate offensive discourse from typical language. Language patterns like the usage of punctuation, sentence length, or a collection of words that are frequently used together in a sentence are examples of how NLP generates semantics. By recognizing word groupings that are different from those classified as normal, NLP is able to detect sentiments . Numerous evolutionary and biologically inspired algorithms can be used to identify offensive human languages. A variant of ANNs called Deep Neural Networks (DNNs) is the most often used algorithm.A variant of ANNs are Generative Adversarial Networks (GANs). The methods look for features in data samples based on their classes.The two groups of neurons fight against one another while changing their weights in each iteration to either produce undetected fake images or correctly identify fake from real ones.

4. Conclusion

As the frequency and level of sophistication of attacks increase, AI has become an essential tool in the field of cybersecurity. This article showed how cyberthreats have increased in size, complexity, and range. We emphasize how historical cyberthreats continue to have an impact on contemporary risks. We gave a comprehensive study of cyberthreats and possible defenses. We specifically covered how cyberattacks affect various network topologies and applications.As a result of these advancements, AI will continuously contribute more to cybersecurity. Innovative AI solutions must be developed in order to quickly identify and eliminate threats that endanger social stability and human welfare. Cybersecurity solutions are probably going to develop intelligent agents that think like people as opposed to just acting like humans. There are several fundamental problems regarding how and where AI deployment can be managed, despite the fact that the role of AI in tackling cybersecurity challenges is still being investigated. Intelligent machines, for instance, would eventually exhaust life's vital resources as they become increasingly important solutions for humanity. A new kind of governance will develop as technology and people compete for scarce resources. This will then lead to a new area of research.

Conflict of interest:

There is no conflict of interest.

Data availability statement:

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Funding Statement:

This study did not receive any funding in any form.

References

1. D. Venable, “Cybersecurity in 2017: when Moore’ s law attacks,” 2017. [Online]. Available: https://www.channelpartnersonline.com/blog/ cybersecurity-in-2017-when-moore-s-law-attacks/ [Accessed: 5-Jun2019].
2. S. Morgan, “Global cybersecurity spending predicted to exceed $1 trillion from 2017-2021,” Cybercrime Magazine, Jun. 2019. [Online]. Available: https://cybersecurityventures.com/cybersecuritymarket-report/ [Accessed: 22-Dec-2019].
3. Spending on cybersecurity in the united states from 2010 to 2018,” Statista Research Department, Aug. 2019. [Online]. Available: https://www.statista.com/statistics/615450/ cybersecurity-spending-in-the-us/ [Accessed: 22-Dec-2019].
4. How artificial intelligence and machine learning will impact cyber security,” Wall Street, Aug. 2018. [Online]. Available: https://wall-street.com/how-artificial-intelligence-and-machinelearning-will-impact-cyber-security/ [Accessed: 5-Jan-2020].
5. D. Yuhas, “Doctors have trouble diagnosing alzheimer’ s. AI doesn’ t,” NBC News, Oct. 2017. [Online]. Available: https://www.nbcnews.com/mach/science/doctors-have-troublediagnosing-alzheimer-s-ai-doesn-t-ncna815561 [Accessed: 25-Dec2019].
6. M. McFarland, “Farmers spot diseased crops faster with artificial intelligence,” CNN Business, Dec. 2017. [Online]. Available: https://money.cnn.com/2017/12/14/technology/corn-soybeanai-farming/index.html [Accessed: 25-Dec-2019].
7. C. Geib, “Nasa-funded research will let unmanned spacecraft "think" using AI and blockchain,” Futurism, Jan. 2018. [Online]. Available: https://futurism.com/nasa-funds-autonomousunmanned-spacecraft [Accessed: 20-Dec-2019].
8. E. Winick, “Lawyer-bots are shaking up jobs,” MIT Technology Review, Dec. 2017. [Online]. Available: https://www.technologyreview.com/s/ 609556/lawyer-bots-are-shaking-up-jobs/ [Accessed: 25-Dec-2019].
9. B. Morey, “Manufacturing and AI: Promises and pitfalls,” SME, Jun. 2019. [Online]. Available: https://www.sme.org/technologies/articles/ 2019/june/manufacturing-and-ai-promises-and-pitfalls/ [Accessed: 25- Dec-2019].
10. S. Morrow and T. Crabtree, “The future of cybercrime & security,” Juniper Research, Aug. 2019. [Online]. Available:

https://www.juniperresearch.com/researchstore/innovationdisruption/cybercrime-security?utm_source=juniperpr&utm_campaign= pr1_thefutureofcybercrime_technology_aug19 [Accessed: 25-Dec 2019].

11. H. Taylor, "What are cyber threats: How they affect you and what to do about them," Sep. 2018. [Online]. Available: https://preyproject.com/blog/en/what-are-cyber-threats-howthey-affect-you-what-to-do-about-them/ [Accessed: 5-Jun-2019].
12. M. Cohen, "Zero-day attacks are difficult but not impossible to defend against." [Online]. Available: https://eccitsolutions.com/zeroday-attacks-difficult-not-impossible-defend/ [Accessed: 5-Jun-2019].
13. Malware," German AV-TEST GmbH research institute. [Online]. Available: https://www.av-test.org/en/statistics/malware/ [Accessed: 22- Dec-2019].
14. W. Hall and J. Pesenti, "Growing the artificial intelligence industry in the uk," Department for Digital, Culture, Media & Sport and Department for Business, Energy & Industrial Strategy. Part of the Industrial Strategy UK and the Commonwealth, 2017.
15. C. Cath, S. Wachter, B. Mittelstadt, M. Taddeo, and L. Floridi, "Artificial intelligence and the 'good society': the us, eu, and uk approach," Science and engineering ethics, vol. 24, no. 2, pp. 505–528, 2018.
16. E. Brynjolfsson, D. Rock, and C. Syverson, "Artificial intelligence and the modern productivity paradox: A clash of expectations and statistics," National Bureau of Economic Research, Tech. Rep., 2017.
17. E. W. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," Decision support systems, vol. 50, no. 3, pp. 559–569, 2011.
18. J. Borenstein, "The challenges of adopting a consistent cybersecurity framework in the insurance industry," Dec. 2018. [Online]. Available: https://www.microsoft.com/security/blog/2018/12/20/the-challengesof-adopting-a-consistent-cybersecurity-framework-in-the-insuranceindustry/ [Accessed: 5-Jun-2019].
19. C. Alcaraz and S. Zeadally, "Critical infrastructure protection: Requirements and challenges for the 21st century," International journal of critical infrastructure protection, vol. 8, pp. 53–66, 2015.
20. Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," Computers & security, vol. 56, pp. 1–27, 2016.

21. J. Melnick, "Top 10 most common types of cyber attacks," May 2018. [Online]. Available: https://blog.netwrix.com/2018/05/15/top-10-mostcommon-types-of-cyber-attacks/ [Accessed: 5-Jun-2019].
22. T. S. Hyslip and T. J. Holt, "Assessing the capacity of drdos-for-hire services in cybercrime markets," Deviant Behavior, pp. 1–17, 2019. [23] K. Trieu and Y. Yang, "Artificial intelligence-based password brute force attacks," MWAIS 2018 Proceedings, vol. 39, 2018. [Online]. Available: http://aisel.aisnet.org/mwais2018/39
23. E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang, "Accessory: password inference using accelerometers on smartphones," in Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications. ACM, 2012, p. 9.
24. S. Prakashkumar, E. Murugan, R. Thiagarajan, N. Krishnaveni, and E. Babby, "Analysis of cryptography performance measures using artificial neural networking," in International Conference on Emerging Current Trends in Computing and Expert Technology. Springer, 2019, pp. 313–324.
25. P. Brucciani, "Why cyber security is so hard," Sep. 2018. [Online]. Available: https://medium.com/datadriveninvestor/why-cyber-securityis-so-hard-fe05921a72a0 [Accessed: 5-Jun-2019]. [27] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in 2010 43rd Hawaii International Conference on System Sciences. IEEE, 2010, pp. 1–10.
26. A. Zarreh, C. Saygin, H. Wan, Y. Lee, and A. Bracho, "A game theory based cybersecurity assessment model for advanced manufacturing systems," Procedia Manufacturing, vol. 26, pp. 1255–1264, 2018.
27. J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy," ACM Computing Surveys (CSUR), vol. 52, no. 4, p. 82, 2019.
28. W. Tushar, T. K. Saha, C. Yuen, T. Morstyn, M. D. McCulloch, H. V. Poor, and K. L. Wood, "A motivational game-theoretic approach for peerto-peer energy trading in the smart grid," Applied energy, vol. 243, pp. 10–20, 2019.
29. P. Chakraborty, E. Baeyens, K. Poolla, P. P. Khargonekar, and P. Varaiya, "Sharing storage in a smart grid: A coalitional game approach," IEEE Transactions on Smart Grid, 2018.
30. R. Tang, S. Wang, and H. Li, "Game theory based interactive demand side management responding to dynamic pricing in price-based demand response of smart grids," Applied Energy, vol. 250, pp. 118–130, 2019. [33] C. T. Do, N. H. Tran, C. Hong, C. A.

Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, and S. S. Iyengar, "Game theory for cyber security and privacy," ACM Computing Surveys (CSUR), vol. 50, no. 2, p. 30, 2017.

31. "Configuring denial of service protection." [Online]. Available: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ ios/12-2SX/configuration/guide/book/dos.pdf [Accessed: 22-Dec-2019].

32. I. Mukhopadhyay, K. S. Gupta, D. Sen, and P. Gupta, "Heuristic intrusion detection and prevention system," in 2015 International Conference and Workshop on Computing and Communication (IEMCON). IEEE, 2015, pp. 1–7.

33. O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, "An intelligent intrusion detection system (ids) for anomaly and misuse detection in computer networks," Expert systems with Applications, vol. 29, no. 4, pp. 713–722, 2005.