Exploring Dimensions Of Defense In Cyber Space-A REVIEW

Sai Pratheek Chalamalasetty, Srinivasa Rao Giduturi

Abstract: Introduction: In this modern age, the world is advancing in terms of connectivity through new networking paradigms. There will be growth in volume, variety and veracity of the cyber data along with devices, and it is predicted that this count will reach 200 billion by 2020. Digital Criminals largely depend on deceit strategies to exploit weaknesses and masquerade their identity which in turn are pessimistic about cyber deterrence. This article presents a review of Cyber Crimes - Methods and ways to tackle them with a brief review on Cyber forensics. Methodology: Scopus Digital Library and IEEE explore were searched for relevant English papers from 2019 to reverse chronological order. Results and Conclusion: There is an alarming emergency to design new technologies that can effectively withstand any kind of cyber-attacks. The newly developed security protocols should be dynamic enough to hold their ground against the ever-changing nature of Cybercrimes.

Keywords: Cyber Security, Cyber Crimes, Cyber Forensics

1. INTRODUCTION

The networking infrastructure serves as a basic platform for information sharing among people, Corporate and defence sectors in this modern era, where the digital world is advancing rapidly [1], [2]. According to [3], there will be growth in volume, variety and veracity of the devices, and they predicted that this number will reach 200 billion by 2020 and will never stop ceasing. So, we can come to a conclusion that the cyberspace harbors huge volume of potentially useful information that is available through the networks and henceforth, that data must be protected from cybercriminals [3]. The main objectives of the Cyber Attackers can be classified as shown in Fig.1

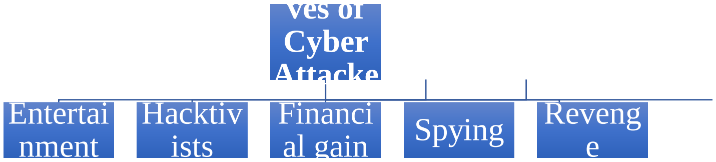

Figure 1

Areas of Cybercrime

The intensive growth of the digital economy after demonetization in India, completely changed the criminal landscape, because access to information stored in the computer's systems and mobile phones became an objective of the crime. Today, even political system is being a target to cybercrime. Previously, the crime syndicate had found safer places in countries with weaker governments and unstable rule. Now in the present days, the white-collar criminals use advantage of the country's jurisdictions and weak technical capabilities in regard to the attacks made through the process of cybercrime [4], [5]. Hence, we can say that the attribution problem appears to make counter punishment, contrasts largely with defensive denial which however is particularly ineffective. While cyberterrorism often raises concern about national security as a whole, its effects on individual psyche and cognition are overlooked which forms the majority of the issues. With the ever-changing nature of cybercrimes, the criminals have found new modus operandi and new methodologies to combat the crime and sometimes even escape it.

Cyber Deterrence

Deterrence theory differentiates between "denial leading to deterrence", the threat where effective defenses help to defeat an unplanned attack from "punishment leading to deterrence" [6]. But the costly retaliation for cybercrimes will neutralize the benefits of a successful attack [7], [8], [9]. Scholars and policy analysts are generally negative towards the concept of cyber deterrence possibly due to considerable confusion about the meaning of the concept [10], [11], [12], [13]. As cyber criminals mostly depend on security holes in the network that are likely be countered if publicly revealed, it is hardly possible to trace them for prosecution or other law procedures [14]. As the criminals had to face a choice between bad alternatives, many policy analysts argue that denial should be prioritized over other criminal procedural codes [15], [16]. Policy should thus focus on creating defensive approach in depth using detection techniques for the identification of attackers and counterintelligence [17], improving cyber etiquette [18], and building a strong infrastructure that is resilient and can tolerate the inevitable attacks [19].

Cybersecurity as a Remedy

Cybersecurity may be a source of theoretical puzzles that helps sharpen relation between many disciplines [20], [21], [22], [23]. Conventional terrorism targets in deterring its citizen's faith by sowing a seed of fear and vulnerability which results in disrupting the trust in the capability of the government and its allied agencies to protect citizens against future attacks [24]. The cybercrimes and attacks which are punishable by the judiciary grow in parallel with the rapidly advancing cyber space and the technologies involved [25]. In general, netizens leave their digital foot prints in browsing interfaces or front-end applications running on desktop that request some credentials to a server; therefore, it is of paramount importance to carefully mine forensic evidence left in a person's system by appropriate forensics toolkits [26]. With the advent of emerging technologies like cloud computing with their highly successful models-IaaS, PaaS, SaaS [27], the importance of accessing and organizing the digital evidence has increased in parallel [28]. Also, there are surveys that projects to the alarming need to consider the rapid flux in the number of products deployed on the cloud environment as client's consumables [29], [30], as forensics experts do not have access to the server in both the cases that makes cyber investigation a complex task.

2. METHODOLOGY

The review of literature is a method of identifying, evaluating, and interpreting all available and potentially viable information relevant to a particular topic domain, or suject of interest [31]. In this review study, ACM Digital Library and ieeexplore were searched for relevant English papers from 2019 to reverse chronological order. The searched key words were: “Cyber Warfare,” “Cybersecurity,” and “Cyberguerilla” in various combinations. All the relevant articles are taken for the review.

3. Review of Literature

To gain a better insight on a concept, it is highly recommended by the domain experts to study its phase shift over past and present.

Brief Review on Cyberforensics

As per the data served by the NCRB (National Crime Record Bureau), referenced by the author [32], during the past 5 years, there is a humongous difference between the enormous count of filed cases under Information Technology Act and the rate of conviction i.e. the registered cases are increasing and the conviction rate is declining by a greater margin. According to the reports of an advocate, a cyber-crime expert and senior advocate at the Honorable Supreme Court of India, Dr. Pavan Duggal, in majority of the cyber-crime cases the forensic evidence is neither acquired using the appropriate strategies nor is it stored and documented as admissible in a court of law as an evidence. The ever-expanding nature of cybercrimes is a result of the poor digital security standards followed by the cyber users [33]. However, there is no single tool or forensics mechanism that court can refer to in case of any crime [34]. There are lucrative forensic tools available in the market such as iSafe, USBDrive, Recuva, WinHex which should be used according to the need and situation [35]. Guo et al. [36] provided a decent roadmap depicting a successful forensic investigation in a broader spectrum however, it falls short of specific considerations at client’s side. Hatole Y Bawiskar [37] presented a review exclusively about email forensics, however, this study is unsuitable for other standard forensics such as network, mobile and disk. Finally, Kaur et al. [38] proposed an in-depth study on digital forensics practices and its analytical tools, however, they are from the general perspective, without taking into consideration the client approach and its perspective. According the author of [39], Cyber forensic evidences are not above the law and faces its own jurisdictional issues such as; evidence collected in one country is unfit to be submitted as an evidence in the foreign courts. The Security goals and objectives are discussed in Table 1.

Table 1: *Security goals in cyber space*

Security goals	Objective
Confidentiality	Authorized Personnel only should be given access to valuable data.
Integrity	Affirms the information accuracy
Availability	Makes sure that the authorized user always accesses the network and resource

Cyber Crimes and Cyber Security

This section of the article depicts the various studies related to cybersecurity and its relevant crimes in different platforms chronologically.

Liu et al. stressed the necessity for security while computing with the smart grid environment [40]. They also stated that by reversing the security requirements of IT networks we can obtain the same for a smart grid environment. They focused on the urgent need for new and different kinds of security protocols for smart grids. Van Niekerk and Von Soloms wrote an article where they compared and contrasted between information security and cybersecurity [41]. They concluded that the cybersecurity is a much broader aspect compared to that of data security which supplements security to information which constitutes the prima facia of cyberspace. Razzaq et al. presented a survey paper on security aspects of information and data in the cyberspace [42]. They also stated that the current cybersecurity techniques cannot hold their ground efficiently against all kinds of attacks and stresses on the ultimate need for new security approaches and practises which are not only deployed keeping in view the previous cyberattacks but also should effectively protect against future attacks. Schneider documented a report on the recommendations for efficient implementation of digital security awareness in educational institutions and universities [43]. Cyber attackers find it difficult to hack the electronic gadgets of a person that are connected to the web if he/she has basic cyber hygiene and security basics. So, it is proved that cybersecurity awareness and the number of cyberattack incidents are inversely proportional. Kaster and Sen presented their report of the study done on the world’s largest power grid [44]. They presented the necessity and prime priority of enhancing cybersecurity for power grid system by focusing that cyber threats tops the list of various threats that can bring down a power grid system to a scratch. Nepal and Jang-Jaccard presented a report on the diverse trends in attacks to social life (digital media), cloud computing, smart wearables, and various types of technical short comings in the infrastructural layout of hardware, software, and network [45]. Arlitsch and Edelman presented an analytical survey on various data breaches that happened across the globe in 2013 and 2014 [46]. They found out that one of the main targets of a cyber attacker is vulnerable data of an individual and private and public sectors like login credentials, credit card details so on. Their paper focused on the need for much more advanced and stringent network mechanisms to enhance the current standards of cybersecurity for information infrastructure on the Internet [47]. Ali et al. concluded that the most feasible solution to enhance the security standards of cyber networks is SDN (software-defined networking) [48]. They illustrated that the defence of the network system vests with the conceptual properties of SDN like dynamic and flexible policies, intrusion detection and support for remediation, along with network verification. They also demonstrated some issues, SDN is facing currently like NFV, overlay networks, and Open flow which are yet to be resolved in order to make SDN more resilient to cyber threats. Sadeghi et al. focused the dearth of privacy and security parameters in the domain of IoT (Internet of Things) [49]. They opined that, blazing growth of computing devices in the IoT environment are relatively proportional to the attacks on the devices and the newly developed security mechanisms can encompass this rapidly increased cyberspace of IoT. Singh et al. stated that, cloud computing having several feasible advantages, still lacks in adoption and vulnerability [50]. In this article, they discussed more sophisticated three-layer security architecture to sharply intensify the security of cloud computing by revisiting the existing obsolete security practises. Studer and Weber presented a document where they discussed the various parameters like the need, change, and importance of legal prospects of digital security in the paradigm of IoT [51]. Zou et al. stressed that the various strata of the OSI model which are intended for wireless systems varies greatly to that of others which is in-line with a different approach like wired systems [52].

4. TAXONOMY OF CYBER CRIME

Taxonomy of Cyber Crime	
Cyber Peddler	Doing any illegal acts that involves a cyber system and stealing valuable and confidential data for ransom.
Cyber Fraud	Accessing valuable information through social engineering and phishing and using it for their interests including personal and financial gain.
Cyber Activism	Derogating rival person (or) organization through false information and claims over social platforms such as twitter, WhatsApp, LinkedIn, Gmail, Facebook etc., [53].
Cyber Violence	The violence caused in the real world to the target party through a network connected components such as computer or mobile [54], [55].
Cyber World War	To disable or destroy the cyber infrastructure such as networks, systems of the rival country which constitutes every citizen, employees of private firms, military and even hackers.
Cyber Terrorism	This is a more classified kind of crime performed by a group who share a common interest of commanding people of other groups by destroying humanity through cyber platforms thereby proving their dominance.
Cyber Stalking	As the name, itself suggests it is stalking a target through any cyber means such as email, instant messaging etc., [56].
Cyber Revenge	It is the process of taking revenge in cyber means such as exposing confidential information, making false claims, malfunctioning computer based infrastructure.
Cyber Squatting	It is the digital crime, where a cybercriminal registers false names for trademarks so that the actual owner fails to register their name [57].
Classic Cyber Squatting	The main aim is to obtain ransom. The attacker deletes or sells the domain name only after acquiring the prescribed ransom amount from the original owner [57].
Derogatory Cyber Squatting	The attacker's main motive is to defame the victim by any means such as false propagation, content violation etc., [57].
Typographical Cyber Squatting	Impersonating the actual trademark name with an almost replica. This crime happens when the actual owner had already registered the domain name and the attacker still want to yield benefit. [57].
Cyber Trespassing	It is the crime in which an attacker crosses the boundary through unfair and unethical means violating the confidentiality and integrity [58], [59] such as analysis of SQL injection, network traffic, prying, salami attacks, tapping, guessing passwords and data swindling.
Cyber Theft	The crime in which data is stolen for financial or personal gain from a system connected through a network.
Cyber Espionage	It is also referred as cyber spying. It is the process in which sniffing is done on any individual, organization or even government to acquire potentially useful information [53].
Cyber Pornography	The attacker first obtains some private data such as nude and sexual photographs/videos through hacking the victim's system and then makes them public in the websites or social media platforms to cause shame and guilt to the victim [54], [55].

5. CLASSIFICATION OF CYBER ATTACKS

Attacks on Integrity

Salami Attack: They are sequence of unnoticeable cyber-attacks which when constituted appears as a huge cybercrime [58]. Dada diddling attack: In this attack, the data considered for financial remuneration such as salary, incentives are altered without the knowledge and authorization of actual owner [58]. Cross-site scripting: The attacker inserts infected code or script into the target website or an application which a user visit and obtains the vulnerable data through cookies and web sessions [59], [60]. SQL Injection: It is same as cross site scripting but the difference is that here data bases are affected bypassing the web applications [59], [61]. Session hijacking: This attack falls under the category of network attack in which an intruder alters the session between the authorized users to gain access to confidential and potential data [58].

6. DISCUSSION

DoS/DDoS: Service Denial/ Distributed attacks of DoS are passive network attacks. In this kind of attack the attacker creates his own network of hacked bots and sometimes a server to create a huge traffic thereby obstructing the service to the actual ones in real need [62]. TCP SYN Attack: This attack underlines the basic con of the classic three-way hand shake protocol. In this protocol, the client firstly transmits SYN(synchronization) signal to network server for connection establishment, then the server sends back ACK(acknowledgement). Now the client responds back with the same ACK to the server. The attacker sends so many SYN signals instead of ACK in order to flood the capacity of the server [63]. UDP Attack: Contrasting TCP (Transmission control protocol) UDP (user datagram protocol) is rather a connection less one. Here the attacker generates a large sum of data packets to flood the network queues thereby obstructing the intended owner to access the network service [63]. ICMP Attack: In this attack, the intruder propagates voluminous amount of ICMP (internet control message protocol) packets to the host which leads to the network crash due to the target's inability in handling the traffic [64]. This can be accomplished in two ways:

1.Ping attack: The ping command serves as a classic unix utility to check for available ip addresses in a network. In this attack, the intruder sends large size data packets than intended to the target host for which it is not configured resulting in a crash [65].

2. Smurf attack: It roots to the concept of amplification. Here, the hacker sends spoofed ICMP packets to IBA (internet based address) which acts as intermediary and can handle a maximum of 255 packets. So, the attacker sends an excess of 255 packets in a single ping [63], [66].

HTTP Attack: Unlike the attacks depicted above in this paper, HTTP (hypertext transfer protocol) packets which generally work in the application layer require much lesser bandwidth and traffic. In this attack, the hacker generates humongous count of GET or POST requests to overwhelm the target capabilities of the host. [63], [67].

Attacks on Confidentiality

Traffic Analysis: It is a kind of passive attack in which an attacker just merely analyses the network traffic between two nodes- sender and receiver without any modification of the actual data or sessions and makes some useful inferences for him/her. [68] Eavesdropping: This attack merely represents traffic analysis attack but the difference is that here, the attacker secretly sniffs and intercepts between sender and receiver and even records the data [69]. Snooping: It falls under the domain of passive attacks where an attacker tries to access confidential information such as login credentials, banking data and so on. It is even performed by Corporate and Government sector officials to keep a track on their employees [70]. It can be classified into two categories:

1. Digital Snooping: Attackers hack networking devices such as routers and even cams to capture the login credentials so that they can access their victim's organization impersonating as actual workers of the frim [70].
2. Shoulder Snooping: This is kind of physical attack in which some other outsider tries to access the information typed through unfair means which they should not have [70].

Password attacks: These attacks exclusive aim is to obtain usernames and passwords of various cyber components such as laptops, applications, interfaces. If the user has adept cyber awareness and chooses a strong password for his operations then the chances of password guessing attack diminishes accordingly. These attacks can be further narrowed down into three categories:

1. Dictionary Attacks: In this attack, the hackers try every possible combination of words that can labeled as passwords as defined in the dictionary to acquire passwords of authentic users.

2.Brute Force Attack: Here, the attacker takes the assistance of brute-force hacking utilities for his purpose. This process however has higher time complexity and relatively same amount of success rate.

3.Password guessing: This attack is also termed as web spidering. Here, the attackers visits blogs, websites, social media handles of their victims to gather useful information for guessing passwords such as employee code, designation, spouse details so on.

Keylogger: It is a malicious tool that runs secretly in the victim's system background without any icon, pop-up notification. It secretly captures all the data that is entered using key strokes and transmits the same to the hacker without the knowledge of the actual user [71], [72].

Social Engineering: It falls under the category of interactive attacks where attackers with decent amount of soft skills deceive other users to reveal potential information regarding networks and organizations [73]. It can be further classified as shown:

1.Phishing: It is obtaining the information for financial gain such as bank data, credit card details etc., by fooling the actual users with fake emails, websites that will be the exact replicas of the original ones [73]. Phishing can be further sub grouped into two categories.

1.a. DNS Phishing: This is a much-sophisticated attack in which the hacker alters host files in the victim's computer or even DNS databases, network servers so that even a genuine URL points to a fraudulent one. Unknowingly the victim enters his vulnerable data thinking that it is in fact the original one [72].

1.b. Spear Phishing: It specifies a targeted attack where the intruder first identifies a group of people, obtains their publicly visible data and send fake malicious emails with the relevant information to gain their trust. Once any target clicks on that email his/her system gets corrupted [73].

2. Dumpster Diving: It is also called as trashing. The attacker does not perform any malicious activity but gains valuable information through the recycle bin, deleted logs of system and network [73].

3. Baiting: It is same as fishing in real life. The attacker first creates a malicious device such as flash drive, CD, DVD and labels it in much more interesting fashion and keeps it near a place accessible by the victim, so that he/her would get attracted to it. When the victim uses that device, the system will get corrupted [73].

4. Waterholing: It refers to a targeted attack where, the cyber attacker infects the websites the chosen victim often visits [73].

5. Reverse Engineering: It is also a kind of interactive attack in which, the hacker introduces himself as a person who can solve the problem with his knowledge and lures the victim to share trustworthy information with the attacker [73].

TYPES OF ATTACKS

Mixed Attacks: The moment cyber researchers devise a new safety mechanism to any one of the existing crime, hackers bounce out with a much more advanced and sophisticated version of the same making the researchers' task much more daunting [52]. Cyber surface Rise: The booming technologies such as Cloud Computing and IoT paved a much easier way for the expansion of cyberspace such as devices that connects to a network such as Laptops, Mobiles, Routers, Modems, Disk Drives so on. The business vendors concentrate much on their business expansion rather than implementing stringent cyber security mechanisms resulting in the expansion of cybercrimes in a relative fashion [51]. Remote User Connectivity: With the rise in technology, VPN (Virtual Private Networks) facilitated Government and corporate sector officials to provide a free hand to their employees operating remotely. However, this paradigm shifts also enabled the hackers to operate in parallel through the same VPNs for their attack [74]. Network IP Address Infrastructure: The law of relativity does not hold good with the number of internet users and internet devices i.e., a single user can have multiple devices each with its own unique IP address, which are not feasible to configure manually. This has become an easy platform for the hackers to easily forge the IP addresses and use them for malicious activities [73]. Unified Network Control: There are various techniques to have a single, central and unified control over the network such as SDN (Software defined Networking). But, the flaw with SDN is that once the controller's security is compromised then the whole network is compromised giving the hackers access to confidential user data. This has proved as a costly challenge over time for the network security professionals [48]. Integrated Technique for all the Networking Layers: Each layer of the TCP and OSI models are equipped strongly to combat the attacks. But there is no single complex technique that can fight any attack across the layers [52].

7. CONCLUSION AND FUTURE SCOPE

Planning precedes Deployment: Before deploying a new database, precautions should be observed in identifying sensitive data, analysis and selection of data protection strategies. The company polices in parallel with the government regulations should be taken into consideration during the planning phase. Following Basic Cyber Security Practises: They include imposing strong passwords, grouping of users and assigning permissions, ensure proper authentication and authorization strategies. Right Remediation techniques: Practising techniques such as Masquerading, Encryption. Using two separate directories for encrypted and decrypted data. Encryption embedded with access control: The encryption techniques should be in line with organization's access control mechanisms. Monitoring and proper issue redressal mechanism: During the course of the time, a cyber security practise irrespective of its security strength will become obsolete one day or the other. Hence a proper monitoring and detection system should be implemented round the clock. Training and enforcement: The personnel involved in data security should be continuously trained and the security policies and framework should also be reconfigured accordingly. The Internet boom has enabled many technologies and new strategies to foray into the cyber space which also resulted in hackers making use of the same digital convenience to commit their attacks with much more precision and accuracy. Hence, there is an alarming emergency to design new technologies that can effectively withstand any kind of cyber-attacks which ought to be cross platform, low cost, and effective across inter dependent domains such as SDN, VPN, Cloud, IoT, Smart grid etc., The newly developed security protocols should be dynamic enough to hold their ground against the ever-changing nature of Cybercrimes.

REFERENCES

[1] T. Dyhouse, "A unified framework for it security - analysis - [IT security]," in Engineering & Technology, vol. 4, no.11, pp. 58-58, 20 June 2009.

[2] R. Ramirez and N. Choucri, "Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review" in IEEE Access, vol. 4, pp. 2216-2243, 2016.

[3] M. Xu, K. M. Schweitzer, R. M. Bateman and S. Xu, "Modeling and Predicting Cyber Hacking Breaches," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 11, pp. 2856-2871, Nov. 2018.

[4] Harmandeep Singh Brar, Gulshan Kumar, "Cybercrimes: A Proposed Taxonomy and Challenges," in Journal of Computer Networks and Communications, 2018.

[5] Vaclav Jirovsky, Andrej Pastorek, Max Muhlhauser and Andrea Tundis, "Cybercrime and Organized Crime", in ARES 2018, August 27–30, Hamburg, Germany, 2018.

[6] C. Fachkha and M. Debbabi, "Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization," in IEEE Communications Surveys, Tutorials, vol. 18, no. 2, pp. 1197-1227, Second quarter 2016.

[7] A. Lu and G. Yang, "Input-to-State Stabilizing Control for Cyber-Physical Systems with Multiple Transmission Channels Under Denial of Service," in IEEE Transactions on Automatic Control, vol. 63, no. 6, pp. 1813-1820, June 2018.

[8] National Research Council (ed). Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: National Academies Press, 2010.

[9] Y. Chen, K. Hwang and W. Ku, "Collaborative Detection of DDoS Attacks over Multiple Network Domains," in IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649-1662, Dec. 2007.

[10] GH. Snyder, "Deterrence and Defense: Toward a Theory of National Security", in Princeton University Press, 1961.

[11] D Peterson, "Offensive cyber weapons: construction, development, and employment", in J Strat Stud, vol.36, no.120–4, 2013.

[12] J. Solomon, "Cyberdeterrence between nation-states plausible strategy or a pipe dream?", in J Strat Stud, vol.5, no.1–25, 2011.

[13] E. Jasiello, "Is cyber deterrence an illusory course of action?", in J Strat Secure, vol. 7, pp.54–67, 2013.

[14] E. Gartzke, "The myth of cyberwar: bringing war in cyberspace back down to earth", in Internal Security, vol.38, no.41–73, 2013.

[15] D. Elliott, "Deterring strategic cyberattack", in IEEE Secure & Privacy vol. 9, pp.36–40, 2011.

[16] S. Sulaiman and B. Sreeya," Public awareness on cybercrime with special reference to Chennai", in International Journal of Innovative Technology and Exploring Engineering, vol.9 no. 1, pp. 3362-3364,2019.

[17] W. Elmasry, A. Akbulut and A.H. Zaim, "Empirical study on multiclass classification-based network intrusion detection", in Computational Intelligence, vol. 35, no.4, pp. 919-954,2019.

[18] S. Sarkar, M. Almukaynizi, J. Shakarian and P. Shakarian, "Mining user interaction patterns in the darkweb to predict enterprise cyber incidents", in Social Network Analysis and Mining, vol.9, no.1, art. no. 57, 2019.

[19] M. T. Khan, D. Serpanos and H. Shrobe, "ARMET: Behavior-Based Secure and Resilient Industrial Control Systems", in Proceedings of the IEEE, vol. 106, no. 1, pp. 129-143, Jan. 2018.

[20] A. Agrawal, M. Alenezi, R. Kumar and R.A. Khan, "A source code perspective framework to produce secure web applications", in Computer Fraud and Security, vol.10, pp. 11-18, 2019.

[21] J. Eriksson and G. Giacomello, "The Information revolution, security, and international relations: (IR) relevant theory?", in Int Polit Sci Rev Rev Int Sci Polit, vol.27, pp.221–44, 2006.

[22] Y. Harbi, Z. Aliouat, S. Harous, A. Bentaleb and A. Refoufi, "A Review of Security in Internet of Things", in Wireless Personal Communications, vol.108, no.1, pp. 325-344, 2019.

[23] L. Kello, "The meaning of the Cyber Revolution: perils to theory and statecraft", in Internal Security, vol.38, pp.7–40, 2013.

[24] SJ. Sinclair and D. Antonius, "The Political Psychology of Terrorism Fears", in Oxford University Press, 2013.

[25] S. Shringarpure and J. Dharam, "Internet trolling: Analyzing the legal myths and facts", in International Journal of Engineering and Advanced Technology, vol. 8, no.5 C, pp. 1429-1431, 2019

[26] J.D. Mireles, E. Ficke, J.H. Cho, P. Hurley and S. Xu, "Metrics towards measuring cyber agility", in IEEE Transactions on Information Forensics and Security, vol. 14, no.12, art. no. 8695107, pp. 3217-3232, 2019.

[27] S. Simou, C. Kalloniatis, S. Gritzalis and V. Katos, "A framework for designing cloud forensic enabled services

(CFeS)", in Requirements Engineering, vol.24, no.3, pp. 403-430, 2019.

[28] F. Amato, G. Cozzolino, V. Moscato and F. Moscato, "Analyse digital forensic evidences through a semantic-based methodology and NLP techniques", in Future Generation Computer Systems, vol. 98, pp. 297-307, 2019.

[29] S. Singh, M. Kubendiran and A.K. Sangaiah, "A review on intrusion detection approaches in cloud security systems", in International Journal of Grid and Utility Computing, vol.10, no.4, pp. 361-374, 2019.

[30] A. Liu, H. Fu, Y. Hong, J. Liu and Y. Li, "LiveForen: Ensuring Live Forensic Integrity in the Cloud", in IEEE Transactions on Information Forensics and Security, vol. 14, no. 10, art. no. 8638983, pp. 2749-2764, 2019.

[31] R.S. Shaji, V. Sachin Dev and T. Brindha, "A methodological review on attack and defense strategies in cyber warfare", in Wireless Networks, vol. 25, no. 6, pp. 3323-3334, 2019.

[32] Vicky Nanjappa, "Cyber Crime – 1600 arrested, only 7 convicted", in Rediff Business News, 2012.

[33] O. Burger, B. Hackel, P. Karnebogen and J. Toppel, "Estimating the impact of IT security incidents in digitized production environments", in Decision Support Systems, vol. 127, art. no. 113144, 2019.

[34] N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis and G.J. Pangalos, "Actionable threat intelligence for digital forensics readiness", in Information and Computer Security, vol. 27 no. 2, pp. 273-291, 2019.

[35] G.M. Jagadeesha, K. Sirbi and T.M. Veeragangadhara Swamy, "Digital forensic process in cybercrime data mining", in International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 6, pp. 365-369, 2019.

[36] H. Guo, B. Jin, and D. Huang, "Research and Review on Computer Forensics," Forensics in Telecom., Inf., and Multimedia, 2010.

[37] P. P. Hatole and D. S. K. Bawiskar, "Literature Review of Email Forensics," Imp. J. Interdiscip. Res., vol. 3, no. 4, Apr. 2017.

[38] M. Kaur, N. Kaur, and S. Khurana, "A literature review on cyber forensic and its analysis tools," Int. J. Adv. Res. Comput. Commun. Eng., vol. 5, no. 1, pp. 23–28, 2016.

[39] S.Al-Haj Baddar, A. Merlo and M. Migliardi, "Behavioral Anomaly Detection in Forensics Analysis", in IEEE Security and Privacy, vol. 17, no. 1, art. no. 8674039, pp. 55-62, 2019.

[40] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. Philip Chen, "Cyber security and privacy issues in smart grids," IEEE Commu- nications Surveys & Tutorials, vol. 14, no. 4, pp. 981–997, 2012.

[41] F. Iqbal, B. C. M. Fung, M. Debbabi, R. Batool and A. Marrington, "Wordnet-Based Criminal Networks Mining for Cybercrime Investigation", in IEEE Access, vol. 7, pp. 22740-22755, 2019.

[42] A. Razzaq, A. Hur, H. Farooq Ahmad, and M. Masood, "Cyber security: threats, reasons, challenges, methodologies and state of the art solutions for industrial applications," in Proceedings of the 2013 IEEE Eleventh International Symposium on Autonomous Decentralized Systems (ISADS), pp. 1–6, Mexico City, Mexico, March 2013.

[43] F. B. Schneider, "Cybersecurity education in universities," IEEE Security & Privacy, vol. 11, no. 4, pp. 3-4, 2013.

[44] S. Soltan, M. Yannakakis and G. Zussman, "REACT to Cyber Attacks on Power Grids", in IEEE Transactions on Network Science and Engineering, vol. 6, no. 3, art. no. 8360557, pp. 459-473, 2019.

[45] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," in Journal of Computer and System Sciences, vol. 80, no. 5, pp. 973–993, 2014.

[46] A. Al-Dhaqm et al., "CDBFIP: Common Database Forensic Investigation Processes for Internet of Things" in IEEE Access, vol. 5, pp. 24401-24416, 2017.

[47] T. Kurpjuhn, "The guide to ransomware: how businesses can manage the evolving threat", in Computer Fraud and Security, vol. 11, pp. 14-16, 2019.

[48] S. T. Ali, V. Sivaraman, A. Radford, and S. Jha, "A survey of securing networks using software defined networking," IEEE Transactions on Reliability, vol. 64, no. 3, pp. 1086–1097, 2015.

[49] A. R. Sadeghi, C. Wachsmann, and M. Waidner, "Security and privacy challenges in industrial internet of things," in Proceedings of the 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), pp. 1–6, San Francisco, CA, USA, June 2015.

[50] S. Singh, Y.S. Jeong, and J. H. Park, "A survey on cloud computing security: issues, threats, and solutions," Journal of Network and Computer Applications, vol. 75, pp. 200–222, 2016.

[51] H. Naeem, "Detection of Malicious Activities in Internet of Things Environment Based on Binary Visualization and Machine Intelligence" in Wireless Personal Communications, vol. 108, no. 4, pp. 2609-2629, 2019.

[52] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," Proceedings of the IEEE, vol. 104, no. 9, pp. 1727–1765, 2016.

[53] G. Kumar, A. Kaur, and S. Sethi, "Computer network attacks- a study," International Journal of Computer Science and Mobile Applications, vol. 2, no. 11, pp. 24–32, 2014.

[54] R. Ismailova, G. Muhametjanova, T.D. Medeni, I.T. Medeni, D. Soylu and O.A. Dossymbekuly, "Cybercrime risk awareness rate among students in Central Asia: A comparative study in Kyrgyzstan and Kazakhstan" in Information Security Journal, vol. 28, no. 4-5, pp. 127-135, 2019.

[55] P. Mihci Turker and E. Kilic Cakmak, "An Investigation of Cyber Wellness Awareness: Turkey Secondary School Students, Teachers, and Parents", in Computers in the Schools, vol. 36, no. 4, pp. 293-318, 2019.

[56] W. M. Al-Rahmi, N. Yahaya, M. M. Alamri, N. A. Aljarboa, Y. B. Kamin and M. S. B. Saud, "How Cyber Stalking and Cyber Bullying Affect Students' Open Learning", in IEEE Access, vol. 7, pp. 20199-20210, 2019.

[57] S. L. Pfleeger, J. B. Predd, J. Hunker and C. Bulford, "Insiders Behaving Badly: Addressing Bad Actors and Their Actions", in IEEE Transactions on Information Forensics and Security, vol. 5, no. 1, pp. 169-179, March 2010.

[58] J. Shin, S.H. Choi, P. Liu and Y.H. Choi, "Unsupervised multi-stage attack detection framework without details on single-stage attacks", in Future Generation Computer Systems, vol. 100, pp. 811-825, 2019.

[59] H. Jeon and Y. Eun, “A Stealthy Sensor Attack for Uncertain Cyber-Physical Systems”, in IEEE Internet of Things Journal, vol. 6, no. 4, art. no. 8669856, pp. 6345-6352, 2019.

[60] S. Ndichu, S. Kim, S. Ozawa, T. Misu and K. Makishima, “A machine learning approach to detection of JavaScript-based attacks using AST features and paragraph vectors”, in Applied Soft Computing Journal, vol. 84, art. no. 105721, 2019.

[61] Ed Pearson and C.L. Bethel, “A design review: Concepts for mitigating SQL injection attacks”, in IEEE: ISDFS”, 2016.

[62] B. Chen, D. W. C. Ho, W. Zhang and L. Yu, “Distributed Dimensionality Reduction Fusion Estimation for Cyber-Physical Systems Under DoS Attacks”, in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 2, pp. 455-468, Feb. 2019.

[63] O. Osanaiye, K.-K. Raymond Choo, and M. Dlodlo, “Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework,” Journal of Network and Computer Applications, vol. 67, pp. 147–165, 2016.

[64] D. Arivudainambi, K.A., V.K., S., S.C., and P. Visu, “Malware traffic classification using principal component analysis and artificial neural network for extreme surveillance” in Computer Communications, vol. 147, pp. 50-57, 2019.

[65] A. Bodhani, “Feeling lucky? [Special Report Cyber Security]”, in Engineering & Technology, vol. 10, no. 1, pp. 44-47, Feb. 2015.

[66] R. Heartfield, G. Loukas and D. Gan, “You Are Probably Not the Weakest Link: Towards Practical Prediction of Susceptibility to Semantic Social Engineering Attacks”, in IEEE Access, vol. 4, pp. 6910-6928, 2016.

[67] W. Fan, Z. Du, M. Smith-Creasey and D. Fernandez, “HoneyDOC: An Efficient Honeypot Architecture Enabling All Round Design”, in IEEE Journal on Selected Areas in Communications, vol. 37, no. 3, pp. 683-697, March 2019.

[68] A. Binbusayyis and T. Vaiyapuri, “Identifying and Benchmarking Key Features for Cyber Intrusion Detection: An Ensemble Approach”, in IEEE Access, vol. 7, pp. 106495-106513, 2019.

[69] Z. Tan, A. Jamdagni, X. He, P. Nanda, R. P. Liu and J. Hu, “Detection of Denial-of-Service Attacks Based on Computer Vision Techniques”, in IEEE Transactions on Computers, vol. 64, no. 9, pp. 2519-2533, 1 Sept. 2015.

[70] F. Ullah et al., “Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach”, in IEEE Access, vol. 7, pp. 124379-124389, 2019.

[71] M. Khonji, Y. Iraqi and A. Jones, “Phishing Detection: A Literature Survey”, in IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2091-2121, Fourth Quarter 2013.

[72] Z. Dou, I. Khalil, A. Khreishah, A. Al-Fuqaha and M. Guizani, “Systematization of Knowledge (SoK): A Systematic Review of Software-Based Web Phishing Detection”, in IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2797-2819, Fourth quarter 2017.

[73] R.S. Rao and A.R. Pais, “Detection of phishing websites using an efficient feature-based machine learning framework”, in Neural Computing and Applications, vol. 31, no. 8, pp. 3851-3873, 2019.