Journal of Cyber Security
DOI:10.32604/jcs.2021.019158
Article

Enterprise Cyberspace Threat Landscape: An Analysis

Emmanuel U. Opara[1,*] and Oredola A. Soluade[2]

[1]College of Business, Prairie View A&M University, Prairie View, 77446, USA
[2]Iona College, LaPenta School of Business, New Rochelle, 10801, USA
[*]Corresponding Author: Emmanuel U. Opara. Email: euopara@pvamu.edu
Received: 08 July 2021; Accepted: 22 September 2021

Abstract: The ecosystem security platform described in this research is already impacting the threat spectrum in quantifiable ways. The global network has undergone a dramatic transformation over the course of 2020, with an unprecedented destabilization of events. Security breaches of all kinds are growing in complexity, sophistication, and impact. The bad actors are bypassing predictable security devices at will by breaching network systems at an escalating rate. This study will analyze these developments by creating awareness among security practitioners so they can be prepared to defend their enterprise systems.

Keywords: Breaches; exploits; network security; threats; vulnerabilities

1 Introduction

Cyber Security attacks are on the rise as advisories are attacking numerous governmental agencies, enterprise systems, hospitals, financial institutions, education, including the United States departments of Energy, Defense, and Treasury [1–3]. The 2019 Coronavirus pandemic transformed the cyber security ecosystem by creating a "New Normal" in the cyberwar [4]. Enterprise systems, educational institutions, and organizations of all sizes moved their workforce to work from home without the adequate security apparatus in place [5–8]. This enterprise cyber-threat landscape is a collection of threats within the ecosystem, with information on identified vulnerability assets, risks, adversaries, and observed trends [9–11]. This study aims to analyze the enterprise cyberspace threat landscape and recommend solutions to remedy the threats.

Cyberspace has witnessed attacks and how breaches to critical infrastructure affected the ecosystem [12–15]. One such instance is the Russian advisories that infiltrated computer networks through a popular software product from Solar Winds that serviced several American corporations [16]. The attack compromised several governmental agencies and critical infrastructure with sophisticated attack tools that made detection challenging. Therefore, sustaining security is vital to prevent surging effects on other sectors and societies in general in successful cyberattacks.

The pandemic of the 2019 crisis reshaped the cyber-threat landscape around the ecosystem [17]. The enterprise network is much interconnected that trying to understand an anomaly is almost impossible. The fact remains that, in an intrusion incident, identifying the difference between abnormal and normal is often the difference between success and failure.

Employees' "new normal" of working from home created a nightmare of complexities for enterprise systems wanting to protect themselves against cyberattack [18]. As attacks continue to increase, nation-states continue to pursue new targets, push boundaries, and breach the weak links of their adversaries working from home. In addition, the pandemic shifted the working culture toward a remote work environment, thereby creating a challenge on how to protect the ecosystem. Resolving this problem will not be easy, but enforcing threat prevention at all network points is essential. The reason is that prevention, compared to detection, is a cybersecurity tactic of blocking anything abnormal and evil. Enterprise

ecosystems need solutions that will detect signature and signature-less oriented attacks in real-time to remediate actions automatically. There are algorithms built into defensive security tools that scan objects in real-time to ascertain the type of digital signatures that is at play.

Malware families come in various forms. They include: shellshock, XMRig, zero-day, advance persistent threats [APTs] Zeus, Trojan [Zbot], Stuxnet, duqu, flame, RATs, emotet, dridex, trickbot, ramnit, GhOst Rat, ransomware, phishing, rombertik, cryptonwall, armored, sparse-infector, multi-partite, polymorphic, fakeav, macdefender, the Sobig, mimail, bagle, regin, bots and botnets, etc. In 2020, Emotet and XMRig were the prominent malware families affecting twelve percent of cyberspace networks globally [19–21]. This study will analyze activities across cyberspace and identify actionable solutions to remedy the threats while leveraging security as a business enabler.

2 Literature Review

References [22–25], among others, in their report, noted that adversaries focused their tradecraft and custom malware on managed service providers. However, they concluded that the average ransomware financial request during 2020 was significant. Our study created awareness of ransomware threats to the ecosystem.

References [26–29], among others, cited that the new normal of working from home is adding to the problem for cyber-spies. Our study narrated the malware families that could pose as potential actors in the cyber war.

References [30,31], in their report, noted that several of the enterprise systems were unprepared as they face situations in which they must migrate their entire workforce to a work-from-home environment. The study concluded that the deficiency for contingency planning exposed many organizations to potential vulnerabilities and misconfigurations that threat actors could have easily leveraged to score breaches, exfiltrate data, or even generate additional profit by extorting vulnerable companies.

References [32,33], in their study, stated that chaos rampaged the security landscape as COVID-19 pandemic exploded in 2020. These put tremendous pressure on cybersecurity platforms. The study concluded that the pandemic exposed challenges in organizations' preparedness for remote work. Our study narrated why cyber professionals should be concerned.

References [34,35], among others, noted that the legacy approach of protection against adversaries is simply not up to the task any longer. This is because enterprise systems need breakthrough solutions to defend their networks. Their study concluded that a unified endpoint security solution is an approach to alleviate today's ever-increasing cybersecurity requirements.

Recent studies by [36,37], noted that Cybercrime damages will cost the world approximately $6 trillion annually by the end of 2021, and that this number was up from $3 trillion projected in 2015. The studies conclude that companies can no longer afford to wait before addressing essential securities remedies.

In other studies [38], they narrated that ninety-seven percent of organizations have experienced a breach, but only a small segment believe they can effectively deal with these intrusions. The studies summarized that enterprise systems need to know what to protect and where to bolster their platforms.

Reports from [39] revealed in 2016 that cyberattacks increased by 48 to 54 percent globally during 2017, and that the speed of attacks since then have continued to increase exponentially.

Other studies reported by [40], among others, found evidence that malware infections have plagued organizations and users for years and are growing stealthier and increasing in number by the day. They summarized that security experts have created commercial antivirus (AV) protection and have actively researched better ways to detect malware.

3 Methodology

To pilot-test the network-security concerns, the authors developed, distributed, and collected responses from survey questionnaires at a network-security business professional conference in Washington in 2019.

The survey population comprises professionals who publish research findings and work in their respective fields. These are experts with an extensive history in teaching and the business world. We distributed survey data to senior IT professionals from midmarket (100 to 999 employees) and enterprise-class (1,000 employees or more] organizations. The survey questionnaires were distributed to 366 attendees. The number completed and returned was 250. Overall, we consider these as an equitable representative random population. Most of the survey items were Likert scale types, yes/no responses or categorical, ordinal items, gender, ranks of personnel, etc.

The study conducted a survey of 23 questions covering a range of security issues that are of importance and of concern to IT and security administrators in small and medium-sized businesses [SMBs]. The questions were designed and conducted to obtain a snapshot of the state of security issues in SMBs and to confirm issues that have been raised in other security studies.

4 Data Analysis/Results

In order to establish the relationship between respondents' attitude and their role in industry, it was necessary to break down the research into a series of Hypotheses as listed below:

1. Is there a relationship between the perceptions of threat to endpoint security when compared to the use of transform software to search the network for malware?

2. Do network scanning tools have an impact on the global threat to cybersecurity?

3. How much confidence do the respondents have when there is a threat of an imminent cyber-attack on the organization?

4. How strongly does the threat of an imminent cyber-attack influence the confidence that male respondents have in their organization's endpoint security posture?

5. How strongly does the threat of an imminent cyber-attack influence the confidence that female respondents have in their organization's endpoint security posture?

6. How strongly does the threat of an imminent cyber-attack influence the confidence that Executives have in their organization's endpoint security posture?

Tests were also performed to determine if there was any difference based on the gender of the respondents.

Hypothesis I:

H_0: There is no correlation between how endpoint security has changed in the past 12 months when contrasted with the use of threat transform software to search the network for malware.

H_1: There is correlation between how endpoint security has changed in the past 12 months when contrasted with the use of threat transform software to search the network for malware.

H_0: $= 0$

H_1: $\neq 0$

Table 1: Correlations

		V003	V006	V007	V008	V009	V010	V011
V004	Pearson Correlation	–0.121	–0.108	–0.056	–0.035	–0.003	–0.075	0.061
	Sig. (2-tailed)	0.104	0.147	0.451	0.642	0.970	0.313	0.415
	N	182	182	182	182	182	182	182

Conclusion:

In general, there does not appear to be any correlation between how endpoint security has changed in the past 12 months when contrasted with the frequency of the use of threat transform software to search the network for malware. However, the correlation between the frequency of use of threat transform software

and recent changes in endpoint security (0.104) can be said to be somewhat more substantial than the rest of the variables.

Hypothesis II:

H_0: There is no correlation between how respondents perceive groups that pose the greatest cybersecurity threat to global business and the utility of network scanning tools in mitigating threats to their organization.

H_1: There is a strong positive correlation between how respondents perceive groups that pose the greatest cybersecurity threat to global business and the utility of network scanning tools in mitigating threats to their organization.

H_0: $r = 0$

H_1: $r \neq 0$

Table 2: Correlations

		V013	V015	V016	V022
V013	Pearson Correlation	1	0.051	–0.087	–0.172*
	Sig. (2-tailed)		0.494	0.245	**0.021**
	N	182	182	182	182
V015	Pearson Correlation	0.051	1	–0.190*	–0.077
	Sig. (2-tailed)	0.494		**0.010**	0.300
	N	182	182	182	182
V016	Pearson Correlation	0.087	0.190*	1	–0.061
	Sig. (2-tailed)	0.245	**0.010**		**0.413**
	N	182	182	182	182
V022	Pearson Correlation	0.172*	0.077	–0.061	1
	Sig. (2-tailed)	**0.021**	0.300	0.413	
	N	182	182	182	182

Note: *Correlation is significant at 0.05 level (2-tailed).

Conclusion:

Respondents who find *Hijackthis* especially useful in mitigating threats to the organization are more likely to regard contractors as the ones that pose the greatest threat to their organization. This is true, regardless of the gender or status of the respondent.

Hypothesis III:

H_0: The confidence that respondents have in their organization's endpoint security posture does not depend on the likelihood that their organization will be compromised by a successful cyberattack within one year.

H_0: The confidence that respondents have in their organization's endpoint security posture is a function of the likelihood that their organization will be compromised by a successful cyberattack within one year.

H_0: $b_i = 0$

H_1: $b_i \neq 0$

where i = Maltego, Autopsy, Virus Total Public, FireEye Sight Intelligence, Shoden, and Zero Fox Transform.

Table 3: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig
1	(Constant)	6.194	1.229		5.039	0
	Imminent Cyberattack	–0.026	0.078	–0.026	–0.337	0.737
	Maltego	–0.223	0.131	–0.13	–1.697	0.091
	Autopsy	–0.164	0.171	–0.072	–0.958	0.339
	Virus Total Public	–0.032	0.073	–0.033	–0.439	0.661
	FireEye Sight Intelligence	0.004	0.069	0.005	0.064	0.949
	Shoden	–0.091	0.072	–0.096	–1.261	0.209
	Zero Fox Transform	0.053	0.062	0.065	0.859	0.392

Note: a. Dependent Variable: V004–Measure of Confidence.

Respondents whose organization use Maltego as their threat hunting transform software seem to have more confidence in the organization's endpoint security posture.

Hypothesis IV:

H_0: Male respondents have little confidence that their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

H_1: The confidence that male respondents have in their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

Table 4: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig
1	(Constant)	5.863	1.618		3.623	0
	Imminent Cyberattack	–0.223	0.097	–0.233	–2.296	**0.024**
	Maltego	0.003	0.173	0.002	0.018	0.986
	Autopsy	–0.158	0.222	–0.072	–0.714	0.477
	Virus Total Public	–0.096	0.09	-0.107	–1.062	0.291
	FireEye Sight Intelligence	–0.071	0.091	–0.08	–0.784	0.435
	Shoden	0.012	0.096	0.013	0.121	0.904
	Zero Fox Transform	0.097	0.084	0.118	1.159	0.249

Note: a. Dependent Variable: V004–Measure of Confidence.

Conclusion:

The confidence that male respondents have in their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

Hypothesis V:

H_0: Female respondents have little confidence that their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

H_1: The confidence that female respondents have in their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

Table 5: Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig
1	(Constant)	4.696	1.999		2.349	0.021
	Imminent Cyberattack	0.239	0.133	0.213	1.795	0.077
	Maltego	–0.353	0.214	–0.195	–1.648	0.104
	Autopsy	–0.049	0.266	–0.02	–0.183	0.855
	Virus Total Public	0.103	0.12	0.098	0.862	0.391
	FireEye Sight Intelligence	0.03	0.107	0.031	0.278	0.782
	Shoden	–0.09	0.113	–0.093	–0.798	0.427
	Zero Fox Transform	0.045	0.098	0.053	0.456	0.65

Note: a. Dependent Variable: V004–Measure of Confidence.

In addition to the confidence female respondents have that their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised, they also believe that it is strongly influenced by the frequency of the use of Maltego as a threat hunting transform software.

Hypothesis VI:

H_0: IT Executive respondents have little confidence that their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

H_1: The confidence that IT Executive respondents have in their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

Table 6: Coefficients[a]

		Unstandardized Coefficients		Standardized Coefficients		
Model		B	Std. Error	Beta	t	Sig
1	(Constant)	5.877	1.328		4.426	0
	Imminent Cyberattack	–0.005	0.086	–0.005	–0.056	0.955
	Maltego	–0.223	0.144	–0.13	–1.546	0.124
	Autopsy	–0.115	0.186	–0.051	–0.618	0.538
	Virus Total Public	–0.02	0.08	–0.021	–0.25	0.803
	FireEye Sight Intelligence	–0.019	0.077	-0.02	–0.245	0.807
	Shoden	–0.077	0.076	–0.085	–1.013	0.313
	Zero Fox Transform	0.05	0.068	0.06	0.728	0.468

Note: a. Dependent Variable: V004–Measure of Confidence.

Conclusion:

IT Executives do not believe that their confidence in their organization's endpoint security posture is contingent upon the likelihood of an imminent threat on their organization.

Hypothesis VII:

H_0: Male Executive respondents have little confidence that their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

H_1: The confidence that Male Executive respondents have in their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

Table 7: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig
1	(Constant)	4.942	1.755		2.816	0.006
	Imminent Cyberattack	–0.181	0.104	–0.191	–1.73	0.088
	Maltego	0.099	0.195	0.06	0.506	0.614
	Autopsy	–0.13	0.246	–0.059	–0.53	0.598
	Virus Total Public	–0.06	0.097	–0.069	–0.625	0.534
	FireEye Sight Intelligence	–0.121	0.106	–0.129	–1.142	0.257
	Shoden	0.047	0.102	0.053	0.456	0.65
	Zero Fox Transform	0.133	0.092	0.163	1.439	0.154

Note: a. Dependent Variable: V004–Measure of Confidence.

Conclusion:

The confidence that male executive respondents have in their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

Scenario 2G: What impact do v005-011 have on v004 For FEMALE EXECUTIVE respondents?

Hypothesis VIII:

H_0: Female Executive respondents have little confidence that their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

H_1: The confidence that Female Executive respondents have in their organization's endpoint security posture is strongly influenced by the belief that their organization will soon be compromised.

Table 8: Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients		
		B	Std. Error	Beta	t	Sig
1	(Constant)	4.857	2.176		2.233	**0.029**
	Imminent Cyberattack	0.257	0.156	0.219	1.649	**0.104**
	Maltego	–0.395	0.230	–0.218	–1.721	**0.090**
	Autopsy	–0.024	0.283	–0.010	-0.084	0.933
	Virus Total Public	0.095	0.139	0.086	0.682	0.498
	FireEye Sight Intelligence	0.018	0.116	0.019	0.156	0.877
	Shoden	–0.084	0.118	–0.090	–0.717	0.476
	Zero Fox Transform	0.012	0.105	0.014	0.115	0.909

Note: a. Dependent Variable: V004–Measure of Confidence.

Conclusion:

The confidence that female executive respondents have in their organization's endpoint security posture is contingent on both their rating of the Maltego threat hunting transform software, and their belief in the likelihood of an imminent cyberattack.

5 Overall Conclusion

This work introduces the ecosystem threat landscape that has evolved to the scope where enterprise systems are on constant cyberattacks from adversaries. The "new normal" effects of the 2019 pandemic exacerbated attacks forcing enterprise systems to update their training and awareness security programs. Employees now work remotely from home, thereby enabling adversaries to expand their attack vectors to include online infrastructures and services that were previously shielded, as well as company endpoints that are situated away from the corporate network. In this study, we explored breaches occurring in the cyberspace landscape and the attack strategies used by various adversaries. The study also highlighted different types of architecture and detection schema.

This study recommends organizations implore the Blue Team and Red Team philosophies as mitigation strategies. Instituting the Blue Team philosophy involves enterprise systems setting a platform of detecting adversaries and preventing them from breaking into the organization's infrastructure. This strategy includes identifying breaches swiftly, limiting the spread of infection by confining it to the system it entered through, and successfully stopping the attacks in their tracks. Security Onion is the tool recommended to use. This tool offers full packet capture both for network-based and host-based intrusion detection schema. Instituting the Red Team philosophy involves setting up an enterprise systems platform of protecting sensitive data by ensuring the enterprise systems are operating out of a healthy security posture. Enterprise systems will be able to identify and assess vulnerabilities, test assumptions, view alternate options for attack, and reveal the limitations and security risks for the organization. This tool will enable security teams to conduct advanced penetration tests with ease.

The study recommends using deep learning, artificial intelligence, and machine learning technologies to detect anomalies. Because massive amounts of data are generated on a regular basis, businesses will be able to analyze and identify new insights faster than the competition.

6 Implication for Practitioners and Researchers

In the future, when anomalies malicious code malware is identified and analyzed, the output from a PCAP, Wire-shack or a Virus Total engine should be fully leveraged. The goal is to spot the difference between abnormal and normal in an intrusion schema and prevent any infection from spreading to other parts of the network.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Jeong, S. Naqvi and M. Yoon, "Accurate and communication-efficient detection of widespread events," *IEEE Access*, vol. 6, pp. 61728–61734, 2018.

[2] J. Cheng, C. Cai, X. Tang, V. Sheng, W. Guo *et al.,* "A DDoS attack information fusion method based on CNN for multi-element data," *Computers, Materials & Continua*, vol. 62, no. 3, pp. 131–150, 2020.

[3] S. F. Li, Y. H. Cui, Y. F. Ni and L. S. Yan, "An effective SDN controller scheduling method to defence DDoS attacks," *Chinese Journal of Electronics*, vol. 28, no. 2, pp. 404–407, 2019.

[4] B. Dumitru, "The 'New Normal' State of Cybersecurity, 2020-BUSINESS THREAT LANDSCAPE REPORT," 2020. [Online]. Available: https://www.bitdefender.com/files/News/CaseStudies/study/378/Bitdefender-Whitepaper-2020-Business-Threat-Landscape-Report.pdf.

[5] Z. Whittaker, "DoorDash confirms data breach affected 4.9 million customers, workers and merchants," *Techcrunch*, 2019.

[6] T. Subbulakshmi, P. Parameswaran, C. Parthiban, M. Mariselvi, J. A. Anusha *et al.,* "A unified approach for detection of DDoS attacks using enhanced support vector machines and filtering mechanisms," *ICTACT Journal on Communication Technology*, vol. 4, no. 2, pp. 737, 2014.

[7] M. Alkasassbeh, G. Al-Naymat, A. Hassanat and M. Almseidin, "Detecting distributed denial of service attacks using data mining techniques," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 1, pp. 436–445, 2016.

[8] S. Bravo and D. Mauricio, "New features of user's behavior to distributed denial of service attacks detection in application layer," *International Journal of Online Engineering*, vol. 14, no. 12, pp. 164–178, 2018.

[9] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, "The effect of IoT new features on security and privacy: New threats existing solutions and challenges yet to be solved," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1606–1616, 2019.

[10] J. Zhang, Q. Liang, R. Jiang and X. Li, "A feature analysis based identifying scheme using GBDT for DDoS with multiple attack vectors," *Applied Sciences*, vol. 9, no. 21, 2019.

[11] B. Jia, X. Huang, R. Liu and Y. Ma, "A DDoS attack detection method based on hybrid heterogeneous multiclassifier ensemble learning," *Journal of Electrical and Computer Engineering*, vol. 2017, 2017.

[12] L. Arsene, "Half of security professionals had no contingency plan in place for COVID-19," 2020. [Online]. Available:https://businessinsights.bitdefender.com/half-of-security-professionals-had-no-contingency-plan-inplace-for-covid-19.

[13] D. Peraković, M. Periša, I. Cvitić and S. Husnjak, "Model for detection and classification of DDoS traffic based on artificial neural network," *Telfor Journal*, vol. 9, no. 1, pp. 26–31, 2017.

[14] K. Singh, S. Paramvir and K. Krishan, "User behavior analytics-based classification of application layer HTTPGET flood attacks," *Journal of Network and Computer Applications*, pp. 97–114, 2018.

[15] F. S. de Lima Filho, F. A. F. Silveira, A. de Medeiros Brito Junior, G. Vargas-Solar and L. F. Silveira, "Smart detection: An online approach for DoS/DDoS attack detection using machine learning," *Security and Communication Networks*, vol. 2019, 2019.

[16] I. Boniface, "Microsoft accidently exposed 250 million customer service records," *Engadget*, 2020.

[17] BitDefender, "Bitdefender 10 IN 10 Study: The indelible impact of COVID-19 on cybersecurity," 2020. [Online]. Available:
https://download.bitdefender.com/resources/files/News/CaseStudies/study/348/Bitdefender-10-IN-10-The-Indelible-Impact-of-COVID-19-on-Cybersecurity.pdf.

[18] A. Spadafora, "Major data breach exposes database of 200 million users," *TechRadar*, 2020.

[19] H. C. Chen and S. S. Kuo, "Active detecting DDoS attack approach based on entropy measurement for the next generation instant messaging App on smartphones", *Intelligent Automation & Soft Computing*, 2019.

[20] J. Valinsky, "Clearview AI has billions of our photos. Its entire client list was just stolen," *CNN*, 2020.

[21] A. W. Al-Dabbagh, Y. Li and T. Chen, "An intrusion detection system for cyber attacks in wireless networked control systems," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, pp. 1049–1053, 2018.

[22] D. Douglas, J. Santanna, R. Schmidt, L. Granville and A. Pras, "Booters: can anything justify distributed denial-of-service (DDoS) attacks for hire?" *Journal of Information, Communication and Ethics in Society*, 2017.

[23] X. Y. Tang, Q. D. Zheng, J. R. Cheng and V. S. Sheng, "A ddos attack situation assessment method via optimized cloud model based on influence function", *Computers, Materials & Continual*, vol. 58, no. 2, pp. 1263–1281, 2019.

[24] J. Cheng, R. M. Xu, X. Y. Tang and V. S. Sheng, "An abnormal network flow feature sequence prediction approach for DDoS attacks detection in big data environment," *Computers, Materials & Continua*, vol. 55, no. 1, pp. 95–119, 2018.

[25] M. Gamal, H. M. Abbas, N. Moustafa, E. Sitnikova and R. A. Sadek, "Few-shot learning for discovering anomalous behaviors in edge networks," *Computers, Materials & Continua*, vol. 69, no. 2, pp. 1823–1837, 2021.

[26] N. V. Abhishek, T. J. Lim, B. Sikdar and A. Tandon, "An intrusion detection system for detecting compromised gateways in clustered IoT networks," in *Proc. IEEE Int. Workshop Technical Committee on Communications Quality and Reliability*, pp. 1–6, 2018.

[27] N. Almolhis and M. Haney, "IoT forensics pitfalls for privacy and a model for providing safeguards," *Computational Science and Computational Intelligence*, 172–178, 2019.

[28] T. Aldwairi, D. Perera and M. A. Novotny, "An evaluation of the performance of restricted Boltzmann machines as a model for anomaly network intrusion detection," *Computer Networks*, vol. 144, pp. 111–119, 2018.

[29] Y. Xiang and W. L. Zhou, "Protecting web applications from DDoS attacks by an active distributed defense systems," *International Journal of Web Information Systems*, vol. 2, no. 1, pp. 37–44, 2006.

[30] M. Conti, A. Dehghantanha, K. Franke and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generations Computer Systems*, vol. 78, pp. 544–546, 2018

[31] R. Doshi, N. Apthorpe and N. Feamster, *Machine Learning DDoS Detection for Consumer Internet of Things Devices*. IEEE Security and Privacy Workshops, San Francisco, pp. 29–35, 2018.

[32] Y. Zhu, M. Mattina, P. Whatmough, "Moble machine learning hardware at ARM: A Systems-on-Chip (SoC) perspective," arXiv:1801.06274. 2018.

[33] N. Shone, T. T. Ngoc, V. D. Phai, Q. Shi, "A deep leeraning approach to network intrusion detection," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 2, no. 1, pp. 41–50, 2017.

[34] E. U. Opara and A. Y. Mahfouz, "The unwitting danger within-Detection, investigation and mitigation of a compromised network," *International Journal of Cyber-Security and Digital Forensic*, vol. 5, no. 4, pp. 208–222, 2017.

[35] E. U. Opara, A. Y. Mahfouz and R. Holloway, "Network platforms, advanced persistence threat–The changing patterns of cyber-attacks," *Journal of Forensic Sciences & Criminal Investigation*, vol. 1, no. 1, pp. 104, 2017.

[36] E. U. Opara and A. Y. Mahfouz, "Conquering the cyberattacks: Analysis and protecting the enterprise resources," *International Journal of Business Continuity and Risk Management,* vol. 6, no. 4, pp. 314–329, 2016.

[37] E. U. Opara and O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities solutions," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.

[38] M. Kang and J. W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS One*, vol. 11, no. 6, 2016.

[39] C. Yin, H. Wang, X. Yin, R. Sun and J. Wang, "Improved deep packet inspection in data stream detection," *The Journal of Supercomputing*, vol. 75, pp. 4295–4308, 2019.

[40] K. M. Prasad, A. R. M. Reddy and K. V. Rao, "BARTD: Bio-inspired anomaly based real time detection of under rated App-DDoS attack on web," *Journal of King Saud University–Computer and Information Sciences*, vol. 32, no. 1, pp. 73–87, 2020.