DSIM

Performance Analysis of Big data and Blockchain based IoT Security Techniques

AVADHESH KUMAR GUPTA [1], DOMENICO SANTANIELLO[2]
[1]Unitedworld School of Computational Intelligence , Karnavati University (Gujarat)- INDIA (e-mail: dr.avadheshgupta@gmail.com)
[2]University of Salerno, Italy (e-mail: dsantaniello@unisa.it)

ABSTRACT The applications of the Internet of Things (IoT), big data, and blockchain are growing rapidly. Also, during the COVID-19 period, the use of smart devices increased. However, the security of protocols of IoT data handling is still vulnerable to advanced cyberattacks. In addition to that, with the introduction of cloud computing, IoT devices become more vulnerable. In this context, in this article, we analyze the performance of IoT in light of big data analytics and blockchain techniques. We search the Scopus database and selected relevant literature and built our analysis results.

KEYWORDS Big Data, Blockchain, IoT, Security

I. INTRODUCTION

The Internet of Things (IoT) is a network of interconnected smart devices that exchanges data in real time to improve efficiency and effectiveness in areas as diverse as energy management, smart transportation, smart grid, supply chain management, healthcare, and environmental assistance. Given the breadth of these use cases, it's not surprising that projections put the total sales income of IoT devices at more than $14.4 trillion by 2022 and the total number of IoT devices in use at over 22 billion by 2025. IoT devices are susceptible to various cyber assaults because of their low power and limited processing capability. Malicious software is installed on IoT devices and subsequently sensitive data is retrieved through application programming interfaces (APIs) once the attackers have gained control of the device. Recent examples of malware assaults on the IoT include the Maria virus in 2017, which generated around $427.03 in damage per hour. Malware on the edge device might cause it to send skewed or fabricated data to the cloud storage system. Malware attacks like this often target IIoT networks and may result in significant financial and reputational damage. As reported by Panda Security, over 230,000 new malware assaults are created daily. So, researchers have a constant emphasis on the creation of security architecture for IoT devices. The basic architecture for IoT environment is presented in Figure 1. As represented in Figure 1, IoT architecture consists of three layers.

- **Perceptron Layer**: It is the lowest layer and consists of smart devices.
- **Network Layer**: It includes all the networking devices such as routers.
- **Application Layer**: It is the highest layer, which includes web applications used by the users.

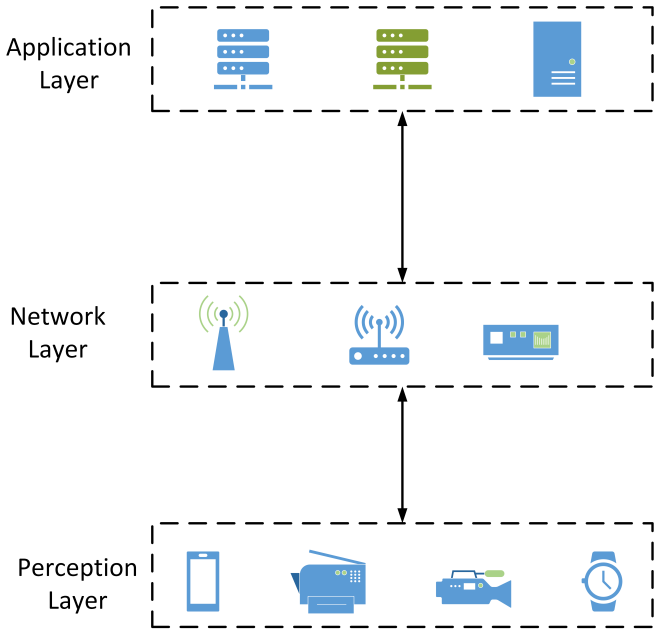
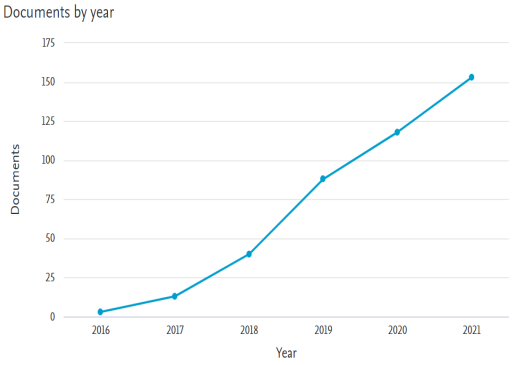


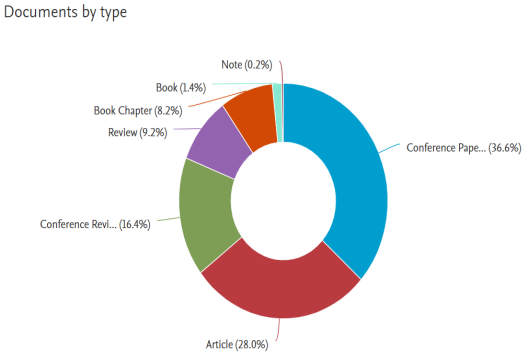
FIGURE 1: IoT Architecture

II. LITERATURE SURVEY

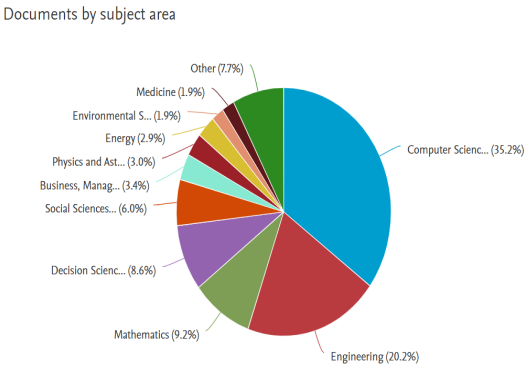
Authors in [21] proposed joint computation offloading and task caching for multi-user and multi-task MEC systems. Authors in [22] proposed accelerating 3D medical volume segmentation using GPUs. In another work, authors [23] proposed accelerating compute-intensive medical imaging segmentation algorithms using hybrid CPU-GPU implementations. Authors in [24] proposed a prototype method to discover workflow violations and XSS vulnerabilities in PHP web applications. Author in [25] review XSS abuse and



(a) Production of Publication

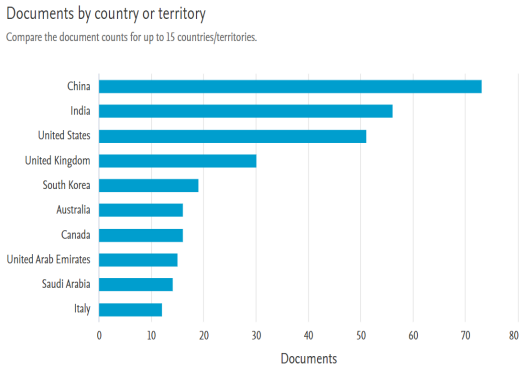


(b) Distribution of Type

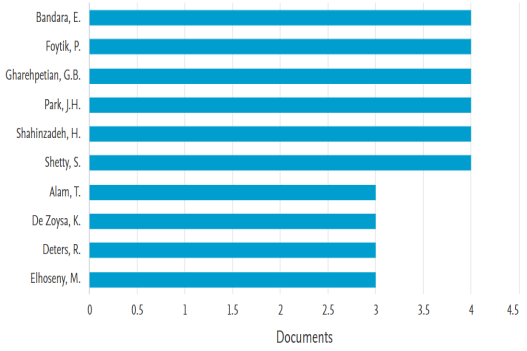


(c) Distribution of Subject

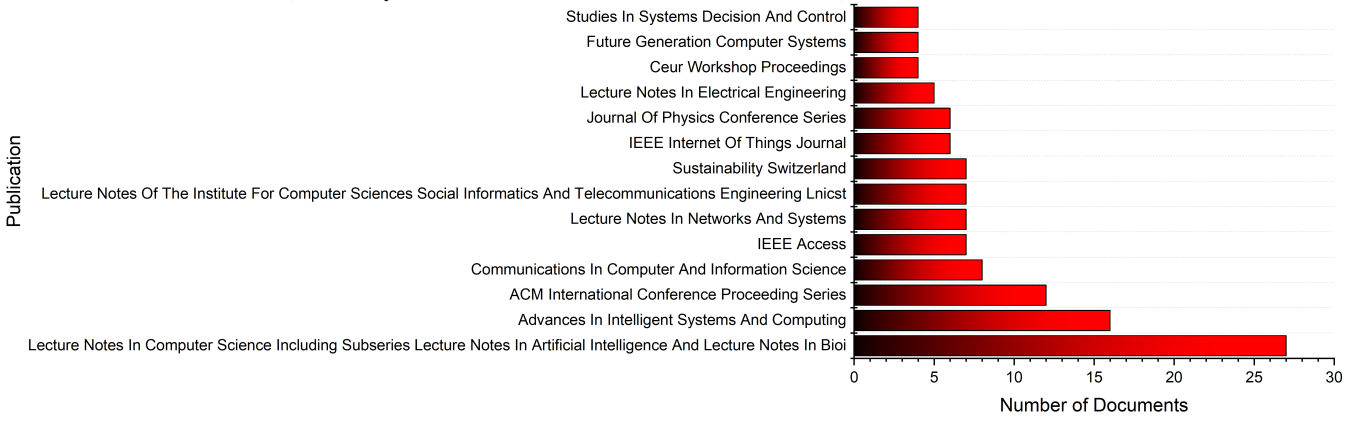
(d) Important Keywords



(e) Country Distribution



(f) Author Distribution



(g) Publication Distribution

FIGURE 2: Stastical Analysis

TABLE 1: Highly Cited Papers

Paper	DOI	Total Citations	TC per Year	Normalized TC
ZHENG Z, 2017, PROC - IEEE INT CONGR BIG DATA, BIGDATA CONGRESS [1]	10.1109/BigDataCongress.2017.85	1869	311.500	10.1449
REYNA A, 2018, FUTURE GENER COMPUT SYST [2]	10.1016/j.future.2018.05.046	859	171.800	23.5827
DWIVEDI AD, 2019, SENSORS [3]	10.3390/s19020326	394	98.500	13.9469
QADRI YA, 2020, IEEE COMMUN SURV TUTOR [4]	10.1109/COMST.2020.2973314	278	92.667	20.7358
LU Y, 2019, J IND INFOR INTEGR [5]	10.1016/j.jii.2019.04.002	224	56.000	7.9292
KARAFILOSKI E, 2017, IEEE INT CONF SMART TECHNOL, EUROCON - CONF PROC [6]	10.1109/EUROCON.2017.8011213	199	33.167	1.0802
MOSAVI A, 2019, ENERGIES [7]	10.3390/en12071301	195	48.750	6.9027
JIANG T, 2019, IEEE INTERNET THINGS J [8]	10.1109/JIOT.2018.2874398	189	47.250	6.6903
SINGH SK, 2020, FUTURE GENER COMPUT SYST [9]	10.1016/j.future.2019.09.002	175	58.333	13.0531
VENKATESH VG, 2020, ROB COMPUT INTEGR MANUF [10]	10.1016/j.rcim.2019.101896	140	46.667	10.4425
SHAE Z, 2017, PROC INT CONF DISTRIB COMPUT SYST [11]	10.1109/ICDCS.2017.61	132	22.000	0.7165
ACETO G, 2019, IEEE COMMUN SURV TUTOR [12]	10.1109/COMST.2019.2938259	129	32.250	4.5664
ASTILL J, 2019, TRENDS FOOD SCI TECHNOL [13]	10.1016/j.tifs.2019.07.024	125	31.250	4.4248
ZHENG T, 2021, INT J PROD RES [14]	10.1080/00207543.2020.1824085	124	62.000	16.3552
TARIQ N, 2019, SENSORS [15]	10.3390/s19081788	122	30.500	4.3186
ALONSO RS, 2020, AD HOC NETW [16]	10.1016/j.adhoc.2019.102047	113	37.667	8.4286
ABDEL-BASSET M, 2021, TECHNOL FORECAST SOC CHANGE [17]	10.1016/j.techfore.2020.120431	107	53.500	14.1129
ZHANG A, 2020, RESOUR CONSERV RECYCL [18]	10.1016/j.resconrec.2019.104512	104	34.667	7.7573
GAO W, 2018, PROC INT CONF COMPUT COMMUN NETWORKS ICCCN [19]	10.1109/ICCCN.2018.8487348	87	17.400	2.3885
KOCHOVSKI P, 2019, FUTURE GENER COMPUT SYST [20]	10.1016/j.future.2019.07.030	86	21.500	3.0442

defense techniques. Author in [26] proposed an ISP level solution to combat DDoS attacks. Authors in [27] proposed a neural fuzzy framework for phishing detection. Author in [28] review DDoS attack detection techniques. Author in [29] proposed URL features-based phishing detection system using machine learning. Author in [30] proposed an identity-based authentication mechanism for the maritime transport system. Authors in [31] review recent advances in fog and mobile edge computing.

III. IMPLICATIONS

In this research paper, we analyze the development and security implications of IoT devices. We use the Scopus database for this analysis. As there is a large number of available articles, we limit our analysis to the Scopus database. The combined analysis of the literature is presented in Figure 2. The annual production of articles is presented in Figure 2a and in Figure 2a it is clear that the number of articles published in the field of IoT, big data analytics and blockchain is increasing exponentially. This is proof that researchers are constantly working to find new protocols and theories for the IoT environment. From Figure 2b, it is clear that the majority of work in the field of IoT devices is published in international conferences. In addition to the type of publication, the subject area is also a good factor to analyzing the research field. The topic distribution is presented in Figure 2c. From Figure 2c it is clear that the majority of researchers in the computer science domain are working in the field of IoT devices.

Figure 2d presents the distribution of keywords according to the frequency of occurrence. As the frequency of occurrence increases, the size of the keyword increases in Figure 2d. The distribution of countries is also a good factor for analyzing the distribution of researchers. The distribution of researchers is presented in Figure 2e and from the figure it is clear that researchers from *China* and *India* are working in the field of IoT, big data analytics, and blockchain. Figure 2f presents the distribution of most cited authors. Figure 2g represent the distribution of sources. All the statistical distribution presented in Figure 2 helps us to understand the topic in more depth. Finally, higely cited papers are presented in .

IV. CONCLUSION

The Internet of Things has become pervasive for every individual. In fact, the IoT affects every aspect of human life. Due to the limited power supply and memory capacity, It is easy for a large number of simple IoT devices to be invaded by cyber attacks. Therefore, researchers are actively working on the development of optimal attack detection models for IoT devices. In this context, we analysis the performance of IoT security techniques that are based on big data and blockchain.

REFERENCES

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," 2017, pp. 557–564.

[2] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," Future Generation Computer Systems, vol. 88, pp. 173–190, 2018.

[3] A. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," Sensors (Switzerland), vol. 19, no. 2, 2019.

[4] Y. Qadri, A. Nauman, Y. Zikria, A. Vasilakos, and S. Kim, "The future of healthcare internet of things: A survey of emerging technologies," IEEE Communications Surveys and Tutorials, vol. 22, no. 2, pp. 1121–1167, 2020.

[5] Y. Lu, "The blockchain: State-of-the-art and research challenges," Journal of Industrial Information Integration, vol. 15, pp. 80–90, 2019.

[6] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," 2017, pp. 763–768.

[7] A. Mosavi, M. Salimi, S. Ardabili, T. Rabczuk, S. Shamshirband, and A. Varkonyi-Koczy, "State of the art of machine learning models in energy systems, a systematic review," Energies, vol. 12, no. 7, 2019.

[8] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4640–4649, 2019.

[9] S. Singh, S. Rathore, and J. Park, "Blockiotintelligence: A blockchain-enabled intelligent iot architecture with artificial intelligence," Future Generation Computer Systems, vol. 110, pp. 721–743, 2020.

[10] V. Venkatesh, K. Kang, B. Wang, R. Zhong, and A. Zhang, "System architecture for blockchain based transparency of supply chain social sustainability," Robotics and Computer-Integrated Manufacturing, vol. 63, 2020.

[11] Z. Shae and J. Tsai, "On the design of a blockchain platform for clinical trial and precision medicine," 2017, pp. 1972–1980.

[12] G. Aceto, V. Persico, and A. Pescapé, "A survey on information and communication technologies for industry 4.0: State-of-the-art, taxonomies, perspectives, and challenges," IEEE Communications Surveys and Tutorials, vol. 21, no. 4, pp. 3467–3501, 2019.

[13] J. Astill, R. Dara, M. Campbell, J. Farber, E. Fraser, S. Sharif, and R. Yada, "Transparency in food supply chains: A review of enabling technology solutions," Trends in Food Science and Technology, vol. 91, pp. 240–247, 2019.

[14] T. Zheng, M. Ardolino, A. Bacchetti, and M. Perona, "The applications of industry 4.0 technologies in manufacturing context: a systematic literature review," International Journal of Production Research, vol. 59, no. 6, pp. 1922–1954, 2021.

[15] N. Tariq, M. Asim, F. Al-Obeidat, M. Farooqi, T. Baker, M. Hammoudeh, and I. Ghafir, "The security of big data in fog-enabled iot applications including blockchain: A survey," Sensors (Switzerland), vol. 19, no. 8, 2019.

[16] R. Alonso, I. Sittón-Candanedo, García, J. Prieto, and S. Rodríguez-González, "An intelligent edge-iot platform for monitoring livestock and crops in a dairy farming scenario," Ad Hoc Networks, vol. 98, 2020.

[17] M. Abdel-Basset, V. Chang, and N. Nabeeh, "An intelligent framework using disruptive technologies for covid-19 analysis," Technological Forecasting and Social Change, vol. 163, 2021.

[18] A. Zhang, R. Zhong, M. Farooque, K. Kang, and V. Venkatesh, "Blockchain-based life cycle assessment: An implementation framework and system architecture," Resources, Conservation and Recycling, vol. 152, 2020.

[19] W. Gao, W. Hatcher, and W. Yu, "A survey of blockchain: Techniques, applications, and challenges," vol. 2018-July, 2018.

[20] P. Kochovski, S. Gec, V. Stankovski, M. Bajec, and P. Drobintsev, "Trust management in a blockchain based fog computing platform with trustless smart oracles," Future Generation Computer Systems, vol. 101, pp. 747–759, 2019.

[21] I. A. Elgendy and et al., "Joint computation offloading and task caching for multi-user and multi-task mec systems: reinforcement learning-based algorithms," Wireless Networks, vol. 27, no. 3, pp. 2023–2038, 2021.

[22] M. Al-Ayyoub and et al., "Accelerating 3d medical volume segmentation using gpus," Multimedia Tools and Applications, vol. 77, no. 4, pp. 4939–4958, 2018.

[23] M. A. Alsmirat and et al., "Accelerating compute intensive medical imaging segmentation algorithms using hybrid cpu-gpu implementations," Multimedia Tools and Applications, vol. 76, no. 3, pp. 3537–3555, 2017.

[24] S. Gupta and et al., "Php-sensor: a prototype method to discover workflow violation and xss vulnerabilities in php web applications," in Proceedings of the 12th ACM international conference on computing frontiers, 2015, pp. 1–8.

[25] B. Gupta, S. Gupta, S. Gangwar, M. Kumar, and P. Meena, "Cross-site scripting (xss) abuse and defense: exploitation on several testing bed environments and its defense," Journal of Information Privacy and Security, vol. 11, no. 2, pp. 118–136, 2015.
[26] B. B. Gupta, M. Misra, and R. C. Joshi, "An isp level solution to combat ddos attacks using combined statistical based approach," arXiv preprint arXiv:1203.2400, 2012.
[27] A. Almomani and et al., "Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email," arXiv preprint arXiv:1302.0629, 2013.
[28] A. Mishra and et al., "A comparative study of distributed denial of service attacks, intrusion tolerance and mitigation techniques," in 2011 European Intelligence and Security Informatics Conference. IEEE, 2011, pp. 286–289.
[29] A. K. Jain and et al., "Phish-safe: Url features-based phishing detection system using machine learning," in Cyber Security. Springer, 2018, pp. 467–474.
[30] B. B. Gupta, A. Gaurav, C.-H. Hsu, and B. Jiao, "Identity-based authentication mechanism for secure information sharing in the maritime transport system," IEEE Transactions on Intelligent Transportation Systems, 2021.
[31] E. Ahmed and et al., "Recent advances in fog and mobile edge computing," p. e3307, 2018.