Analysis of Machine learning based XSS attack Detection Techniques

Kwok Tai Chui[1] and Avadhesh Kumar Gupta[2]
[1]Hong Kong Metropolitan University (HKMU) , Hong Kong, (e-mail: jktchui@hkmu.edu.hk)
[2]Karnavati University, Gujrat, India. (email: dr.avadheshgupta@gmail.com)

ABSTRACT

After the COVID-19 epidemic, most businesses move to online mode. Hence, the online activity of users increases, and the dependence on the Internet increases. There are many benefits of providing services on the internet; however, there are some vulnerability's of online transactions. Cross-Site Scripting (XSS) is one of the cyber attacks that is used by the attackers to steal the conditionals of the Vitim. In this context, we analyze the present machine learning-based XSS attack detection technique proposed by different researchers. The purpose of this study is to analyze machine learning-based XSS attack detection techniques that affect the web pages. Our research helps young researchers to understand the topic in more detail.

KEYWORDS XSS, Cloud computing, fog computing

I. INTRODUCTION

These days, the World Broad Web is more like a complex network that makes use of a wide range of components and technologies, such as client-side and server-side technologies, the HTTPs Protocol, and many more [1]. Web apps built on these frameworks are flexible enough to serve a large audience, and they make it easier for people to utilize the Internet by providing them with the many benefits of cutting-edge technology. However, supplying the necessary security measures for the secure creation of web applications is made more difficult by the differences between these technologies. Since so many online apps run on the open Internet, many of them are susceptible to critical flaws. White-hat security researchers and the Open Web Application Security Project (OWASP) have recently shown that XSS attacks are one of the most common types of vulnerability in web applications [2]–[4]. different XSS attacks are presented in Figure 1.

Cross-site scripting (XSS) [5], [6] is an example of a flaw in the application layer. Eighty percent or more of all online apps are vulnerable to XSS [7]–[9]. An attacker employs this technique by planting malicious JavaScript code in a web application's weak spots, where it will be executed by the browser when a user accesses the page in good faith. In order to mitigate the effects of the XSS attack, academic scientists and researchers have offered several cutting-edge methods [10]. However, there are still certain open research questions that prevent existing frameworks from adequately protecting web applications against XSS attacks. As a result, in this article, we highlight the most important aspects of current defensive solutions for XSS attacks for online applications and the performance concerns they cause [11]–[14].

II. LITERATURE REVIEW

There are wide verity of cyber-attacks present in today's world. Many researches are working in the field for detection of DDoS attacks [15]–[20], phishing attacks [21], [22], smart card attack [23] in fog/cloud computing [24]–[28]. Author in [29] proposed handoop based attacks detection technique. Also in [30] author proposed a game theory based attack detection techniques. Author in [31] proposed deep neural learning based technique for attack detection. Authors in [32]–[34] proposed soft-computing based attack detection method. Also, in [35] proposed attack detection technique in cloud computing. Author in [36] proposed DNS based attack detection technique. Authors in [37]–[41] proposed cryptography based attack detection techniques. Attack detection technique in smart vehicles is proposed in [42], [43]. For RFID tages author proposed a attack detection technique in [44]. Author in [45] proposed neural network based techniques. Author present a review for attack detection. Author in [46] proposed attack detection techniques for MANET. Author in [47] proposed attack detection method in virtual environment. Author in [48] proposed new rooting protocol. Author in [49] proposed machine learning technique for attack detection in IoT. Author in [6] proposed different XSS attack detection technique. Author in [50] review many attack detection technique. A URL based attack detection technique is proposed by author in [51]. Author in [19] proposed an ISP based attack detection technique. Author in [12] proposed machine learning based attack detection

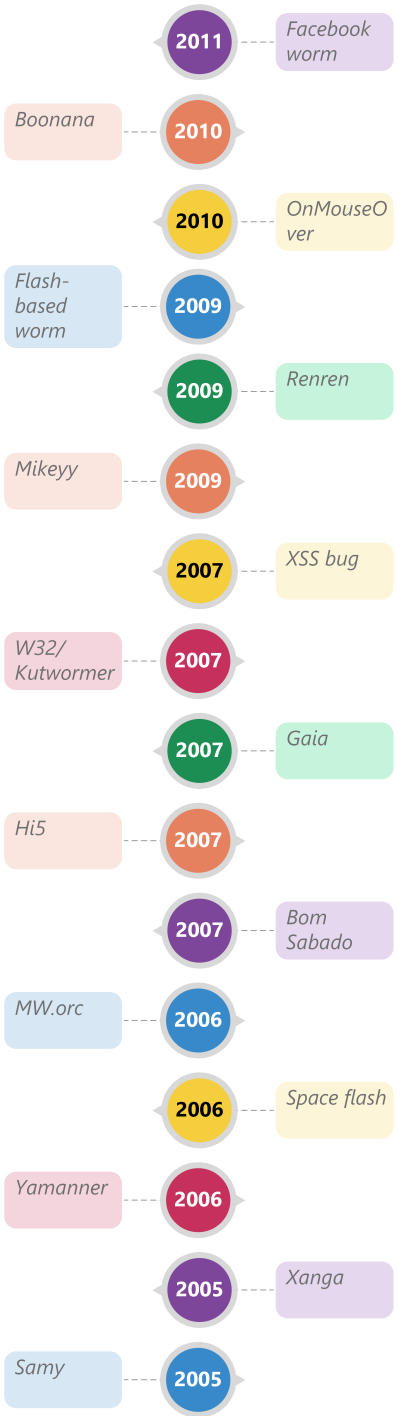


FIGURE 1: XSS Attack Timeline

technique. Author in [52] proposed blockchain based attack detection technique. Author in [53] proposed graph learning based attack detection technique. Author in [54] proposed deep learning approach for attack detection.

III. RESULTS AND DISCUSSION

In this research paper, we try to understand the types of XSS attack and different machine learning techniques available for its detection. As there is a large amount 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 XSS attack detection increases. This is a proof that researchers are constantly working to find an optimal XSS attack detection technique. Hence, if a new researcher wants to work in this field, he or she can start his work. The type of publication is also a good criteria that may help young researchers find relevant papers. From Figure 2b, it is clear that the majority of work in the field of XSS detection is published in international conferences. In addition to the type of publication, the subject area is also a good factor to analysis 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 XSS attack detection.

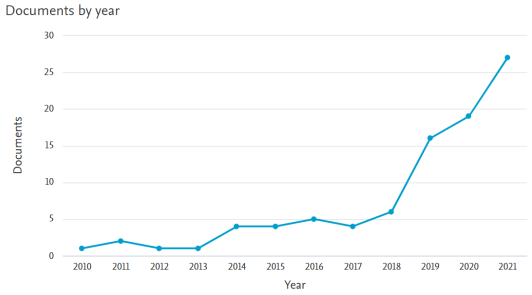
Figure 2d represent the distribution of sources. From Figure 2d it is clear that *ACM* is the most popular source and the majority of researchers are willing to publish their research in *ACM*. The distribution of countries is also a good factor for analyzing the distribution of researchers. The distribution of researchers is presented in Figure 2e and from the figure it is clear that researchers from *India* and *China* are working in the field of XSS attack detection. Finally, the distribution of keywords helps to find the current research trend and helps to find potential future research areas. Figure 2e represent the keyword distribution.

IV. CONCLUSION

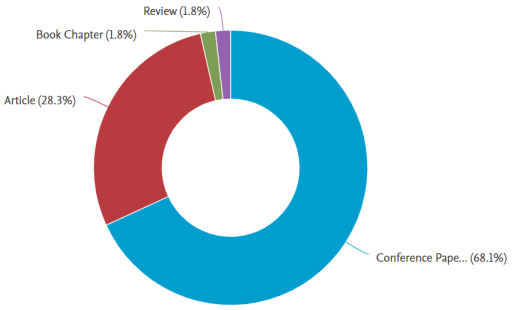
As the internet evolves, developers may take use of tools like browsers to send more complex web apps to users. Online online applications are put at risk, especially from XSS attacks, because of this. As a result, this article provides a thorough overview of the state of XSS defenses so that its readers may better understand their contributions and the limitations they now face in terms of performance.

REFERENCES

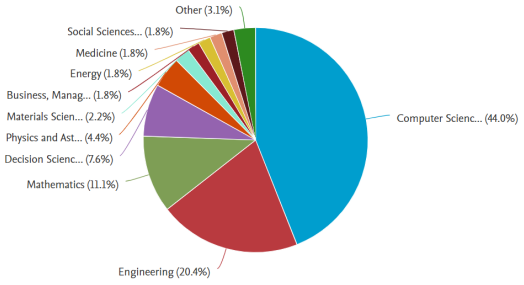
[1] S. R. Sahoo and et al., "Security issues and challenges in online social networks (osns) based on user perspective," Computer and cyber security, pp. 591–606, 2018.
[2] S. Gupta and et al., "Xss-safe: a server-side approach to detect and mitigate cross-site scripting (xss) attacks in javascript code," Arabian Journal for Science and Engineering, vol. 41, no. 3, pp. 897–920, 2016.
[3] S. Gupta and et al, "Hunting for dom-based xss vulnerabilities in mobile cloud-based online social network," Future Generation Computer Systems, vol. 79, pp. 319–336, 2018.



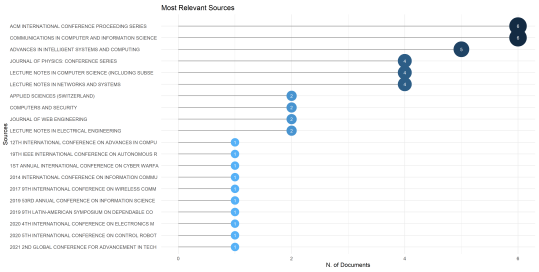
(a) Scientific Production



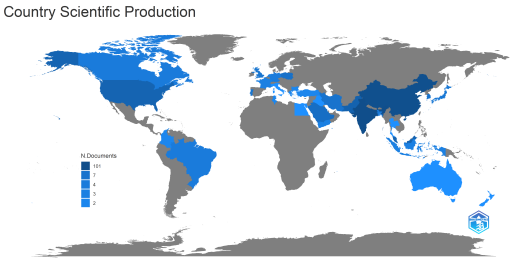
(b) Type of Articles



(c) Important Topics



(d) Popular Sources



(e) Country Scientific Production

(f) Important Keywords

FIGURE 2: Analysis of Available Literature

[4] H. Yang and et al, "A location-based privacy-preserving oblivious sharing scheme for indoor navigation," Future Generation Computer Systems, vol. 137, pp. 42–52, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85134230622&doi=10.1016%2fj.future.2022.06.016&partnerID=40&md5=7b58d43e597269721a612653304d9501

[5] 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.

[6] 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.

[7] K. Bhushan and et al., "Security challenges in cloud computing: state-of-art," International Journal of Big Data Intelligence, vol. 4, no. 2, pp. 81–107, 2017.

[8] B. B. Gupta and A. Gupta, "Assessment of honeypots: Issues, challenges and future directions," International Journal of Cloud Applications and Computing (IJCAC), vol. 8, no. 1, pp. 21–54, 2018.

[9] A. P. Pljonkin and et al., "Features of detection of a single-photon pulse at synchronisation in quantum key distribution systems," in 2017 6th International Conference on Informatics, Electronics and Vision & 2017 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT). IEEE, 2017, pp. 1–5.

[10] A. Gaurav and et al., "Ddos attack detection in vehicular ad-hoc network (vanet) for 5g networks," in Security and Privacy Preserving for IoT and 5G Networks. Springer, 2022, pp. 263–278.

[11] E. Ahmed and et al., "Recent advances in fog and mobile edge computing," Transactions on Emerging Telecommunications Technologies, vol. 29, no. 4, p. e3307, 2018.

[12] 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.

[13] N. Kumar and et al., "A novel framework for risk assessment and resilience of critical infrastructure towards climate change," Technological Forecasting and Social Change, vol. 165, p. 120532, 2021.

[14] B. B. Gupta and A. Tewari, A Beginner's Guide to Internet of Things Security: Attacks, Applications, Authentication, and Fundamentals. CRC Press, 2020.

[15] B. B. Gupta, R. C. Joshi, and M. Misra, "Defending against distributed denial of service attacks: issues and challenges," Information Security Journal: A Global Perspective, vol. 18, no. 5, pp. 224–247, 2009.

[16] L. Wang and et al., "Compressive sensing of medical images with confidentially homomorphic aggregations," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1402–1409, 2018.

[17] A. Gaurav and et al., "A novel approach for ddos attacks detection in covid-19 scenario for small entrepreneurs," Technological Forecasting and Social

Change, vol. 177, p. 121554, 2022.
[18] P. Negi and et al., "Enhanced cbf packet filtering method to detect ddos attack in cloud computing environment," arXiv preprint arXiv:1304.7073, 2013.
[19] 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.
[20] P. Gulihar and et al, "Cooperative mechanisms for defending distributed denial of service (ddos) attacks," in Handbook of Computer Networks and Cyber Security. Springer, 2020, pp. 421–443.
[21] A. K. Jain and et al., "Comparative analysis of features based machine learning approaches for phishing detection," in 2016 3rd international conference on computing for sustainable global development (INDIACom). IEEE, 2016, pp. 2125–2130.
[22] A. Almomani and et al., "Phishing dynamic evolving neural fuzzy framework for online detection zero-day phishing email," arXiv preprint arXiv:1302.0629, 2013.
[23] B. B. Gupta and M. Quamara, Smart Card Security: Applications, Attacks, and Countermeasures. CRC Press, 2019.
[24] S. Rathi, R. Nagpal, D. Mehrotra, and G. Srivastava, "A metric focused performance assessment of fog computing environments: A critical review," Computers and Electrical Engineering, vol. 103, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138091451&doi=10.1016%2fj.compeleceng.2022.108350&partnerID=40&md5=44ded871498eda5e431e256949a74975
[25] I. Kouatli, "The use of fuzzy logic as augmentation to quantitative analysis to unleash knowledge of participants' uncertainty when filling a survey: Case of cloud computing," IEEE Transactions on Knowledge and Data Engineering, vol. 34, no. 3, pp. 1489–1500, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85124668060&doi=10.1109%2fTKDE.2020.2993326&partnerID=40&md5=ede018668d19d7c77df8745f58f84ed4
[26] F. Ahmad, M. Shahid, M. Alam, Z. Ashraf, M. Sajid, K. Kotecha, and G. Dhiman, "Levelized multiple workflow allocation strategy under precedence constraints with task merging in iaas cloud environment," IEEE Access, vol. 10, pp. 92 809–92 827, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137568896&doi=10.1109%2fACCESS.2022.3202651&partnerID=40&md5=05cf954369a3ea194a6ac5ab380d74de
[27] O. Wahab, J. Bentahar, H. Otrok, and A. Mourad, "Resource-aware detection and defense system against multi-type attacks in the cloud: Repeated bayesian stackelberg game," IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 605–622, 2021. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85063671623&doi=10.1109%2fTDSC.2019.2907946&partnerID=40&md5=b969c836382f22d6826f52d5f7cdb117
[28] O. Wahab, R. Cohen, J. Bentahar, H. Otrok, A. Mourad, and G. Rjoub, "An endorsement-based trust bootstrapping approach for newcomer cloud services," Information Sciences, vol. 527, pp. 159–175, 2020. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85082999402&doi=10.1016%2fj.ins.2020.03.102&partnerID=40&md5=68b4a84ac765928e259ed2bcdd8aabe5
[29] S. Tripathi and et al., "Hadoop based defense solution to handle distributed denial of service (ddos) attacks," 2013.
[30] A. Dahiya and et al., "A reputation score policy and bayesian game theory based incentivized mechanism for ddos attacks mitigation and cyber defense," Future Generation Computer Systems, vol. 117, pp. 193–204, 2021.
[31] M. Hammad and et al., "Myocardial infarction detection based on deep neural network on imbalanced data," Multimedia Systems, vol. 28, no. 4, pp. 1373–1385, 2022.
[32] M. H. Bhatti and et al., "Soft computing-based eeg classification by optimal feature selection and neural networks," IEEE Transactions on Industrial Informatics, vol. 15, no. 10, pp. 5747–5754, 2019.
[33] B. B. Gupta, D. P. Agrawal, S. Yamaguchi, and M. Sheng, "Advances in applying soft computing techniques for big data and cloud computing," pp. 7679–7683, 2018.
[34] B. B. Gupta and et al, "Soft computing techniques for big data and cloud computing," Soft Computing, vol. 24, no. 8, pp. 5483–5484, 2020.
[35] C. L. Stergiou and et al., "Secure machine learning scenario from big data in cloud computing via internet of things network," in Handbook of computer networks and cyber security. Springer, 2020, pp. 525–554.
[36] K. Alieyan and et al., "Dns rule-based schema to botnet detection," Enterprise Information Systems, vol. 15, no. 4, pp. 545–564, 2021.
[37] B. B. Gupta and S. T. Ali, "Dynamic policy attribute based encryption and its application in generic construction of multi-keyword search," International Journal of E-Services and Mobile Applications (IJESMA), vol. 11, no. 4, pp. 16–38, 2019.
[38] A. Tewari and et al., "A mutual authentication protocol for iot devices using elliptic curve cryptography," in 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2018, pp. 716–720.
[39] ——, "A lightweight mutual authentication protocol based on elliptic curve cryptography for iot devices," International Journal of Advanced Intelligence Paradigms, vol. 9, no. 2-3, pp. 111–121, 2017.
[40] J. Peng and et al., "A biometric cryptosystem scheme based on random projection and neural network," Soft Computing, vol. 25, no. 11, pp. 7657–7670, 2021.
[41] 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.
[42] B. B. Gupta and M. Quamara, "Decentralised control-based interaction framework for secure data transmission in internet of automated vehicles," International Journal of Embedded Systems, vol. 12, no. 4, pp. 414–423, 2020.
[43] F. Mirsadeghi and et al., "A trust infrastructure based authentication method for clustered vehicular ad hoc networks," Peer-to-Peer Networking and Applications, vol. 14, no. 4, pp. 2537–2553, 2021.
[44] A. Tewari and et al., "An analysis of provable security frameworks for rfid security," in Handbook of computer networks and cyber security. Springer, 2020, pp. 635–651.
[45] K. T. Chui and et al., "An mri scans-based alzheimer's disease detection via convolutional neural network and transfer learning," Diagnostics, vol. 12, no. 7, p. 1531, 2022.
[46] M. Chhabra and et al., "A novel solution to handle ddos attack in manet," 2013.
[47] 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.
[48] A. M. e. a. Manasrah, "An optimized service broker routing policy based on differential evolution algorithm in fog/cloud environment," Cluster Computing, vol. 22, no. 1, pp. 1639–1653, 2019.
[49] I. Cvitić and et al., "Ensemble machine learning approach for classification of iot devices in smart home," International Journal of Machine Learning and Cybernetics, vol. 12, no. 11, pp. 3179–3202, 2021.
[50] 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.
[51] 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.
[52] J. Lu and et al., "Blockchain-based secure data storage protocol for sensors in the industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 18, no. 8, pp. 5422–5431, 2021.
[53] Z. Zhou and et al., "Coverless information hiding based on probability graph learning for secure communication in iot environment," IEEE Internet of Things Journal, 2021.
[54] R. Al Sobbahi and J. Tekli, "Comparing deep learning models for low-light natural scene image enhancement and their impact on object detection and classification: Overview, empirical evaluation, and challenges," Signal Processing: Image Communication, vol. 109, 2022. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137757142&doi=10.1016%2fj.image.2022.116848&partnerID=40&md5=d34d6b239fd6a62eaef7d72259f1119e