Journal of Information Systems Engineering and Management
2025, 10(11s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Analysis of Machine Learning Security Blockchain Based IoT Enabled Web Platform Applications

Dr.S.Aruna Deepthi [1] , Asha G R [2], Selva kumar S[3] , Saritha A N[4], Syed Akram [5] ,Revathi V [6]
[1]*Assistant professor, ECE, Vasavi college of Engineering, Hyderabad ,https://orcid.org/0000-0001-6751-9913, sadeepthi@staff.vce.ac.in*
[2]*Associate Professor ,Computer Science & Engineering, B.M.S. College of Engineering, Bangalore,Karnataka Orchid id- 0000-0002-9836-4819, asha.cse@bmsce.ac.in ,*
[3]*Associate Professor,Computer Science & Engineering,B.M.S. College of Engineering, Bangalore,Karnataka ,Orchid id- 0000-0002-3342-7161, selva.cse@bmsce.ac.in*
[4]*Assistant Professor, Computer Science & Engineering,B.M.S. College of Engineering, Bangalore,Karnataka , , OrcID: https://orcid.org/0000-0002-2664-3712, saritha.cse@bmsce.ac.in*
[5]*Assistant Professor,Computer Science & Engineering,B.M.S. College of Engineering, Bangalore,Karnataka, OrcID: 0000-0003-2824-5109, syedakram.cse@bmsce.ac.in*
[6]*Professor & Dean R& D, New Horizon College of Engineering, Bangalore. OrcID 0000-0002-8583-1916 srichandrang@gmail.com*

ARTICLE INFO

Received: 15 Nov 2024

Revised: 27 Dec 2024

Accepted: 15 Jan 2025

ABSTRACT

Traditional criminal reporting methods include issues with witness hesitancy, security flaws, and inefficiencies. Even with the introduction of web platforms and mobile applications, there are still issues with data security, transparency, and user anonymity. These include of avoiding unwanted access, preserving confidentiality, and protecting data integrity. This research suggests using smart contracts and blockchain technology to overcome these problems. Improving the anonymity, efficiency, and security of crime reporting procedures is the main goal. In order to guarantee data integrity, transparency, and decentralization, the system makes use of blockchain's decentralized and immutable properties. The reporting process will be streamlined by the automation of tasks like complaint validation and proof verification through smart contracts. The suggested solution aims to transform crime reporting by tackling issues with confidentiality, data integrity, and access control. This will foster transparency, accountability, and confidence.

Keywords— Blockchain, Internet of things, Security, Platforms

INTRODUCTION

The cutting edge technologies to Secure IoT enabled web applications and improve womens safety the way we connect and manage physical objects is being rapidly transformed by the Internet of Things (IoT), which is bringing about enhanced efficiency and financial benefits in a number of areas, including smart homes and smart cities[1]. But the spread of IoT devices also makes security issues more apparent. This paper discusses several methods, including passwords, encryption, authentication, and integrity checks, to secure web applications against unauthorized invasions. It also offers cutting-edge methods for reducing vulnerabilities and putting strong security measures in place[2]. The absence of research on the connections between attack strategies, crucial parameters, and email-based attacks makes web applications especially susceptible to security risks.The paper highlights the need for improved security measures in web applications to close this gap. A companion app is available to empower women and guarantee their protection in emergency situations[3]. Features like continuous position monitoring, offline mode, and safe zone visualization are available through voice commands or SOS alerts in this easy-to-use software. Security in a number of industries, such as surveillance, self-driving cars, and smart homes, is greatly improved by facial recognition technology. In order to evaluate the accuracy and features of sophisticated detection methods such as LBPH, SVM, AdaBoost, and Haar Classifiers in terms of enhancing security, the study compares them. This study adds to the larger conversation about innovation and security in both the digital and physical spheres.

ANALYSIS OF SECURITY AND WEB APPLICATION

The creativity of security breaches and vulnerability exploits rises with technological advancements. These attacks mostly target web applications in an effort to gain access to and misuse user data for malevolent purposes. To protect these data, a secure user login and registration interface was employed. The fig 1 article describes the architecture and security analysis of a web application built with Cloud AMQP's Rabbit MQ message-queuing software and Microsoft's Blazor front-end framework. The study employs industry-standard technologies for threat modeling and static code analysis to assess a Blazor-based online application's vulnerability to typical threats like Cross-Site Scripting and Structured Query Language Injection. The investigation revealed serious flaws, such as the disclosure of Personally Identifiable Information (PII), and Blazor's integrated SQL Injection mitigations strengthen its security posture. To sum up, user privacy is invalidated by the PII Disclosure[4]. This study has shed light on the serious security flaws in contemporary apps and assisted in the creation of more robust security regulations.

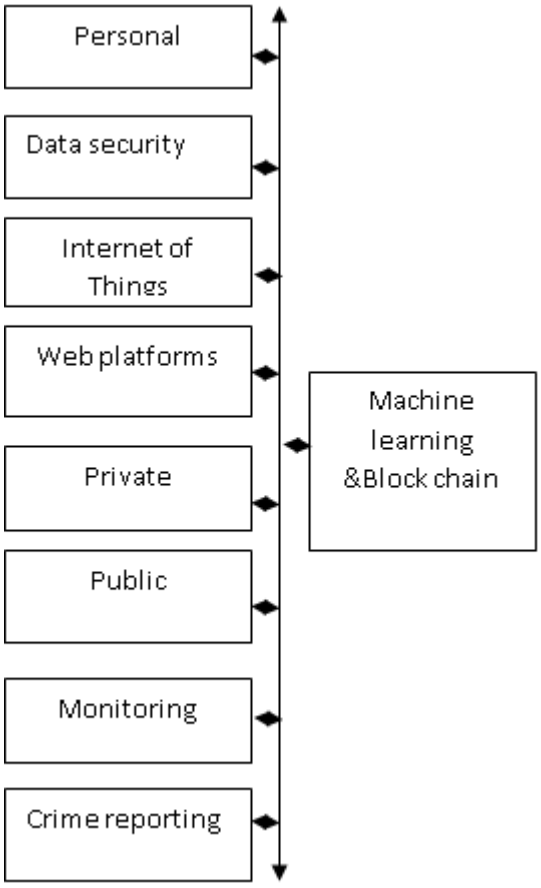

Figure 1. Block diagram

SECURITY AUDITING FOR WEB APPLICATIONS

Concerns about web apps' security are growing as a result of our increased reliance on them. Conventional security auditing procedures frequently have drawbacks like centralized control, manual intervention, and a lack of transparency. To address these difficulties, we offer a unique approach employing blockchain technology and smart contracts to perform security audits for web apps in a decentralized and transparent manner[5]. By enabling users to do security audits on web apps, the web app security audit smart contract streamlines the auditing procedure. The contract makes use of the solidity programming language and the ethereum blockchain. The main features of the contract are the ability to create and retrieve audits, store audit information on the blockchain, and release events in response to audit notifications. The suggested

method is novel in a number of ways. First off, the suggested architecture ensures a transparent and trustless auditing process by doing away with the need for middlemen and centralized authorities through the use of smart contracts. By initiating audits and logging the findings on the blockchain, auditors can work directly with the contract. Owners of web applications can independently confirm the audit details, enhancing accountability and trust. Second, a decentralized audit record system is made possible by the suggested methodology[6]. The storage of audit data is guaranteed to be tamper-proof and unchangeable through the use of blockchain technology. This feature strengthens audit records' integrity by making them more difficult to manipulate or alter without authorization. Thirdly, the agreement establishes the notion of web application addresses and auditor addresses, linking audits to particular organizations.This association makes it possible to trace information in the event of disagreements or queries and efficiently retrieve audit records. To sum up, the suggested smart contract-based security auditing method provides a decentralized, transparent, and unchangeable means of evaluating the security of online apps.

MACHINE LEARNING FOR WEB APPLICATION FIREWALLING

Web apps are essential to many facets of daily life in today's digital world, from social networking to online commerce. But, because of their extensive use, they are also desirable targets for cyber attacks. As a first line of protection, Web Application Firewalls (WAFs) watch over and filter incoming HTTP traffic in order to identify and stop dangerous requests[7]. Even while they are often effective, traditional rule-based WAFs may find it difficult to keep up with new attack strategies and may generate false positives, which could cause needless inconveniences for users who are actually authorized. This research suggests a novel method to improve WAFs with machine learning approaches in order to overcome these issues. Enhancing the WAF architecture with Random Forest and Multinomial Naive Bayes classifiers will help us decrease false alarms and increase detection accuracy. Our test findings using fictitious HTTP request data reveal encouraging results, highlighting the potential of machine learning to improve online application security.

FIREWALLING BLOCKCHAIN DATA SECURITY ON WEB PLATFORMS

A revolutionary method for guaranteeing data integrity, security, and trust in online platforms is provided by blockchain technology. In order to transform data security and privacy, this study investigates the novel use of blockchain as an underpinning layer in ontology management systems[8]. As formal frameworks for information organization, ontologies play a critical role in improving comprehension and interoperability between various web technologies. Recording ontological changes, access, and transactions in an immutable and verifiable manner is a necessary step in integrating blockchain technology with ontology management. By addressing the flaws in centralized, less secure data management systems, this guarantees a transparent and safe process for handling data.

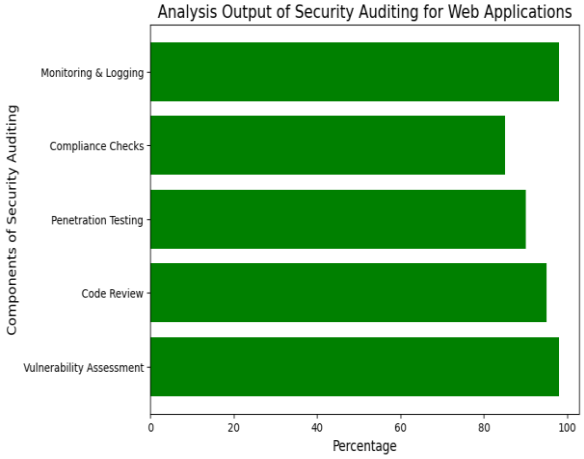

Figure 2. Analysis Output of Security Auditing for Web Applications

The study explores architectural design, describing how cryptographic methods and blockchain's decentralized structure provide strong ontology management. It compares and contrasts current data security methods to show how the blockchain-ontology approach offers better protections. The study also includes case studies of web platforms that have included this approach, showing considerable gains in efficiency, trust, and data security[9]. This integration has consequences that go beyond increased security; these include better data provenance and quality as well as a decrease in fraudulent activity. The fig 2 purpose of this article is to spur additional blockchain innovation and acceptance in web technologies, namely ontology management, in order to build a more reliable and safe digital ecosystem.

ARTIFICIAL INTELLIGENCE NETWORK INFORMATION SECURITY SYSTEM

Artificial intelligence techniques can be used to create a smart and efficient network information security system, which will improve the network's security and information protection capabilities[10]. First, research on intrusion detection, malicious program analysis, cryptography applications, and user behavior analysis was done using artificial intelligence technology in the field of network information security.

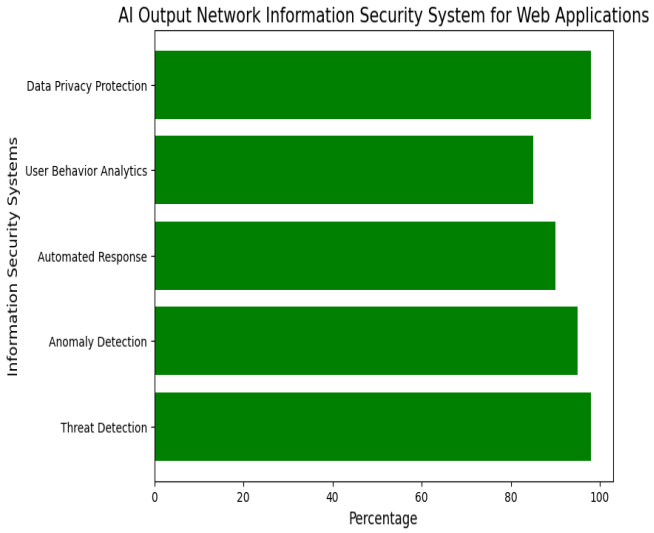

Figure 3. AI Output Network Information Security System for Web Applications

Then, fig 3 network information security was examined from four angles using artificial intelligence algorithms: data collection, model training, intelligent analysis, and emergency reaction. Based on the trial results, the system designed in this article had an average user assessment score of 94.1, greater than the conventional score of 68.2. Ultimately, new avenues for research were suggested, emphasizing the significance of applying artificial intelligence algorithms creatively in order to create a more intelligent and effective network information security system.

CYBERSECURITY

Improving online safety a browser add-on based on machine learning to stop phishing schemes phishing assaults, which target consumers on a variety of online venues, continue to be a serious concern to internet users[11]. To address this widespread problem, we introduce a new strategy that builds on internet security by creating a browser plugin. Our addon offers real-time analysis of URLs to ascertain their vulnerability to phishing attempts by utilizing machine learning algorithms.

CYBERSECURITY

Improving online safety a browser add-on based on machine learning to stop phishing schemes phishing assaults, which target consumers on a variety of online venues, continue to be a serious concern to

internet users[11]. To address this widespread problem, we introduce a new strategy that builds on internet security by creating a browser plugin. Our addon offers real-time analysis of URLs to ascertain their vulnerability to phishing attempts by utilizing machine learning algorithms.

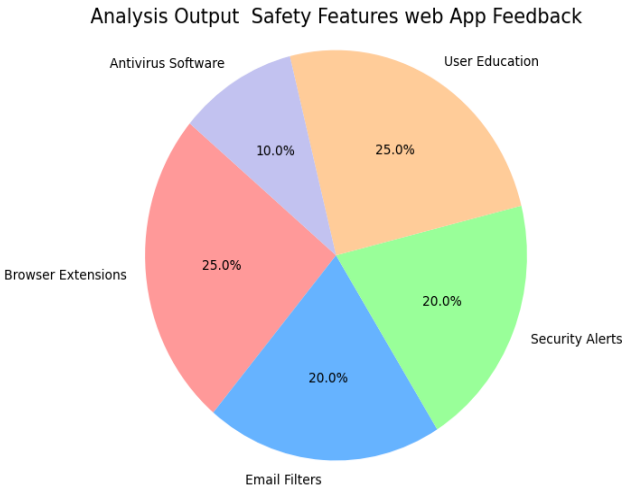

Figure 4 Analysis Output Safety Features web App Feedback

Our technology attempts to reduce the dangers associated with falling for phishing schemes by giving consumers the capacity to recognize potentially hazardous websites[12]. Additionally fig 4, our addon provides a proactive function that lets users add sites to a list of susceptible sites, strengthening defenses against new threats as a group. By putting our browser extension into practice, we hope to give consumers a strong level of security and promote a safer online environment.

MANAGEMENT TECHNIQUES THAT WORK FOR WEB APPLICATIONS

Bad bot traffic is a major problem in a technological age where businesses rely largely on online platforms, such e-commerce sites. Credential stuffing, account takeover, content scraping, disruptions to search engine optimization (SEO), distorted conversion rates, skewed analytics, higher traffic costs, few of the problems that arise from this kind of traffic[13]. Applications that are intended to be accessed via the internet must have a strong and complete end-to-end infrastructure design built on a workable approach that goes beyond conventional Web Application Firewalls and general application hardening[14].The goal of this research is to close the knowledge gap in botnet studies by putting forth flexible, long-lasting architectural designs for effectively controlling bot traffic, including the defense against bot attacks[15]. The architecture's ability to easily upgrade or replace necessary parts guarantees that it will continue to fend off changing threats without requiring major modifications in the future. It provides robust protection against low-volume, covert, and high-volume botnet attacks, secures company operations, and advances cyber security in the digital era[16]. The suggested remedies seek to improve cyber security through the efficient control of malevolent bots on the internet. They ensure that legitimate user traffic is not adversely affected, keep the user experience seamless, lower latency, and outmaneuver adversaries.This protects online applications from dynamic cyberthreats and ensures their integrity, performance, and dependability.

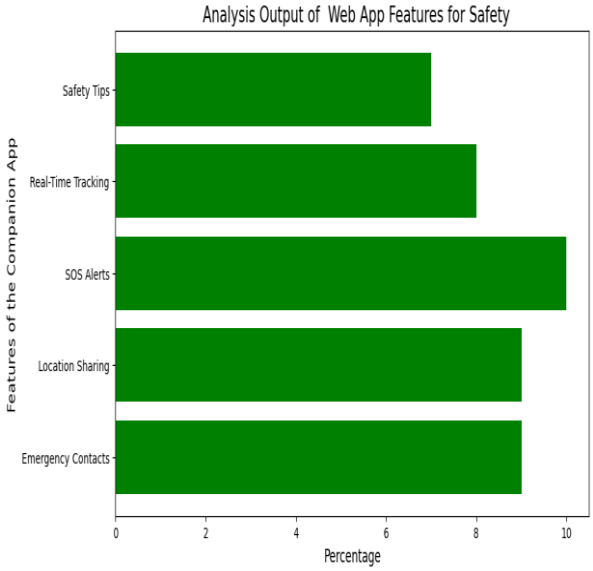

Figure 5 Analysis Output of Web App Features for Safety

WEB APPLICATIONS FOR INDIVIDUALS WITH DIABETES

The gives a broad overview of the spread of diabetes management applications, fig 5 emphasizing the variety and growing accessibility of their features. These applications let users record things like insulin and carbohydrate intake, and some of them also include other features like activity and stress tracking. Basic timestamps and complicated entries with many connected data types are examples of logging capabilities. These apps are improved by the integration of artificial intelligence, which makes decision support and blood glucose prediction models possible. The web application for managing and monitoring diabetic patients is introduced in the summary, with a focus on its predicted blood glucose feature that takes into account patient factors. The significance of secure medical data management is emphasized, and it covers prospective future developments and provides thorough explanations of module usage.

WEB-BASED PLATFORM TO MANAGE AN ONLINE

The creation and deployment of an online platform for managing a virtual university.Due to the internet's growth and popularity, a range of administrative and scholarly duties necessitate dependable and secure management platforms. The purpose of this study is to show the architecture of a web-based platform intended for virtual institution management. The research, which employs the literature review technique, highlights the main obstacles and needs for virtual university administration, focusing on the need to handle security issues, guarantee user-friendliness of interfaces, and boost design flexibility. Among other security measures against cyber attacks, the system design makes use of web application firewalls, access control mechanisms, and secure file storage systems. Adopting responsive design frameworks improves user experience and accessibility by guaranteeing that services work with a variety of devices. Reviews demonstrate that the platform satisfies the requirements for functionality, security, and privacy in addition to basic system usability. The paper concludes with recommendations for future study that include creating more secure systems, customizing the educational experience, and integrating mobile applications to improve the management of the online institution.

ARTIFICIAL INTELLIGENCE UTILIZED IN WEB CONTENT CREATION

Utilizing Artificial Intelligence to Produce Web Content This study explores the use of artificial intelligence (AI) technology in web content development, focusing on the optimization approach of A/B testing. It fig 6 examines the contributions made by technical tools such as Click house, Tailwind, Next.js, and Prisma to the creation and evaluation of online apps. With an emphasis on user behavior analysis, the

value of large language models (LLM) in creating interactive interfaces and offering insights into program performance is also evaluated. The study looks at how artificial intelligence (AI), including tools like GPT-3.5-turbo, could improve the process of producing content for the web. In light of the ongoing advancement of digital communication tactics, the value and promise of AI in text generation are examined.

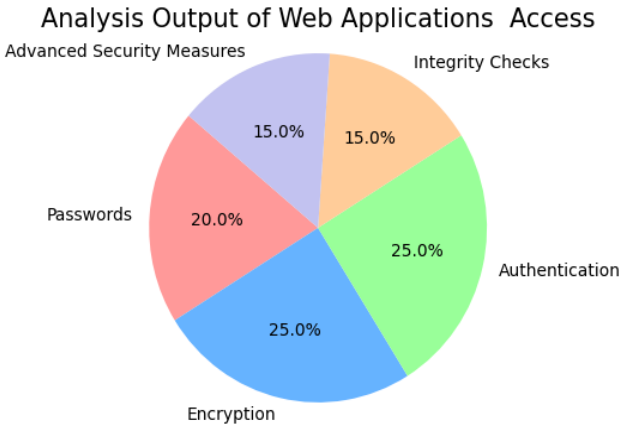

Figure 6 Analysis Output of Web Applications Access

Techniques like performance monitoring and A/B testing are important for assessing how well AI-generated content interacts with viewers. The fig 7 goal of the study is to bring light on how web application development can benefit from the use of AI and modern technologies to boost user productivity and pleasure.

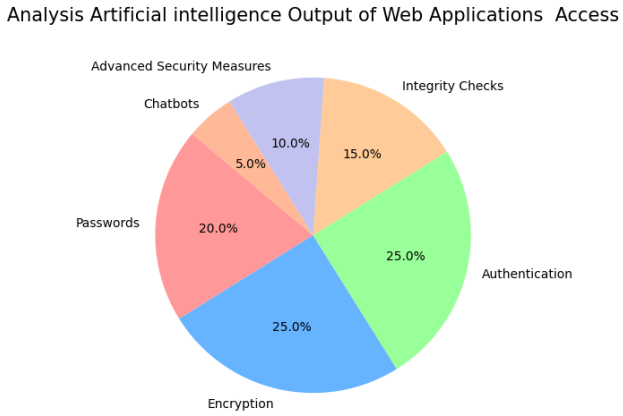

Figure 7 Analysis Artificial intelligence Output of Web Applications Access

The study highlights the significance of artificial intelligence (AI) in influencing the direction of web content by showcasing its potential and limitations in digital communication via theoretical and empirical research.

CONCLUSION

Artificial Intelligence based secured web application with enhanced process artificial intelligence-powered web applications are becoming more and more popular in the marketing sector, and secure, authenticated systems are evolving into new technological frontiers. Using deep learning or cognitive computing technologies makes it possible to implement more reliable, effective, and user-friendly login process implementations. The goal of this research project is to provide an authentication system that improves on current security approaches by integrating artificial intelligence.

REFRENCES

[1] M. Nagy et al., "Web Application Development for Diabetes Patients," 2024 IEEE 18th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara, Romania, 2024, pp. 000573-000580, doi: 10.1109/SACI60582.2024.10619716.

[2] I. F. Sabah, "Design and Implementation of a Web-Based Platform for Administering a Virtual University," 2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 2024, pp. 1-6, doi: 10.1109/HORA61326.2024.10550505.

[3] M. Jovanić and M. Čarapina, "Application of Artificial Intelligence in the Creation of Web Content," 2024 47th MIPRO ICT and Electronics Convention (MIPRO), Opatija, Croatia, 2024, pp. 2063-2068, doi: 10.1109/MIPRO60963.2024.10569691.

[4] R. Jammimanu, G. Joel, S. A. Siddiq, D. Vadlamudi and R. R. Chintala, "Secured Web Application using Artificial Intelligence with Enhanced Methodology," 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 330-334, doi: 10.1109/ICICT57646.2023.10134123.

[5] Z. Zhou, Z. Li, X. Zhang, Y. Sun and H. Xu, "A Review of Gaps between Web 4.0 and Web 3.0 Intelligent Network Infrastructure," 2023 IEEE 9th World Forum on Internet of Things (WF-IoT), Aveiro, Portugal, 2023, pp. 1-6, doi: 10.1109/WF-IoT58464.2023.10539509.

[6] T. Fu, W. Zhen and X. Z. Qian, "A Study of Evaluation Methods of WEB Security Threats Based on Multi-stage Attack," 2020 IEEE International Conference on Information Technology,Big Data and Artificial Intelligence (ICIBA), Chongqing, China, 2020, pp. 1457-1461, doi: 10.1109/ICIBA50161.2020.9276821.

[7] M. Kolárik, J. Paralič, Z. Pella and L. Szalonová, "Web based application for processing cardiology medical records," 2022 IEEE 20th Jubilee World Symposium on Applied Machine Intelligence and Informatics (SAMI), Poprad, Slovakia, 2022, pp. 000053-000056, doi: 10.1109/SAMI54271.2022.9780784.

[8] F. Liu and J. Liu, "A novel teaching model based on Web Mining and Data Mining," 2022 Global Conference on Robotics, Artificial Intelligence and Information Technology (GCRAIT), Chicago, IL, USA, 2022, pp. 488-491, doi: 10.1109/GCRAIT55928.2022.00107.

[9] Y. Huang, C. Leng and L. Zhan, "Application of AI technology in management engineering," 2021 2nd International Conference on Artificial Intelligence and Computer Engineering (ICAICE), Hangzhou, China, 2021, pp. 81-84, doi: 10.1109/ICAICE54393.2021.00024.

[10] Kanade A, “Analysis of wireless network security in internet of things and its applications” Indian Journal of Engineering, 2024, 21, e1ije1675 doi: https://doi.org/10.54905/disssi.v21i55.e1ije1675

[11] A. Sharma, A. Tyagi, P. Khatri and R. Garg, "Enhanced 403 Bypass Mechanism for Web Security," 2024 4th International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2024, pp. 1858-1862, doi: 10.1109/ICACITE60783.2024.10617037.

[12] I. F. Sabah, "Design and Implementation of a Web-Based Platform for Administering a Virtual University," 2024 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 2024, pp. 1-6, doi: 10.1109/HORA61326.2024.10550505.

[13] C. Zheng, J. Wang, S. Si, Z. Li, N. Yu and L. Sun, "MOMR: A Threat in Web Application Due to the Malicious Orchestration of Microservice Requests," ICC 2024 - IEEE International Conference on Communications, Denver, CO, USA, 2024, pp. 3304-3309, doi: 10.1109/ICC51166.2024.10623095.

[14] B. Kannan, M. Sakthivanitha, S. Jayashree and R. Maruthi, "Prediction of Cyber Attacks Utilizing Deep Learning Model using Network/Web Traffic Data," 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2024, pp. 363-367, doi: 10.1109/ICAAIC60222.2024.10575032.

[15] K. Hussain, S. Sah, B. Seth, N. Fatima Rizvi and B. V. Febiyola Justin, "Analysis Application of Big Data-based Analysis of Network Security and Intelligence," *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, Coimbatore, India, 2023, pp. 1481-1485, doi: 10.1109/ICAIS56108.2023.10073823.

[16] A. Padma, M. Ganeshwar Rao and Swatmaram, "An Analysis of Artificial Intelligence and Bigdata Cyber Security its Applications," *2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE)*, Shivamogga, India, 2024, pp. 1-6, doi: 10.1109/AMATHE61652.2024.10582057.