World Journal of Advanced Engineering Technology and Sciences
eISSN: 2582-8266
Cross Ref DOI: 10.30574/wjaets
Journal homepage: https://wjaets.com/

(REVIEW ARTICLE)

Check for updates

Review of the security challenges in web-based systems

Odiaga Gloria Awuor *

Jaramogi Oginga Odinga, University of Science and Technology, Kenya.

World Journal of Advanced Engineering Technology and Sciences, 2023, 08(02), 204–216

Publication history: Received on 21 February 2023; revised on 28 March 2023; accepted on 31 March 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.8.2.0099

Abstract

Web-based systems are vulnerable to security issues similar to any other applications. Due to the characteristics of web-based systems such as their distributable nature and cross platform accessibility, security challenges are predominant. Recently, more focus has been placed on how to handle security concerns in web systems. Current solutions to counteract the web-based system security challenges include web system languages, firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), cryptographic techniques, digital certificates and signatures among others. However, attacks and threats such as cross site scripting (XSS), Distributed Denial of Service (DDoS), cross-site request forgery (CSRF) and structured query language (SQL) injection attacks are still common. This gives the impression that there are still security challenges in this regard, despite the efforts for detection and prevention of attacks. Consequently, due to their dynamism, secure architectures are pivotal for the security of web-based systems. The focus of this paper therefore, is to review the existing security challenges of web-based systems. It is evident from this literature study that most security challenges in web-based systems stem from the threat of unauthorized access and risks from implementing technologies and standards that are under developed as regards security.

Keywords: Security; Web-based system; Risk; Attack; Threat

1. Introduction

Web-based systems are delineated as systems accessible over networks such as Intranet or Internet. According to [1] and [2], web-based systems have mainly been popularized by browser ubiquity. The capacity of updating and maintaining web-based systems without necessarily installing or distributing software on many client computers is the main reason why they have become popular [3], [4]. The authors in [5] add that web-based systems and web applications have been adopted in different scopes such as banking, e-commerce, business operations and various other functions. Considering that the Intranet and Internet are open systems and web systems are utilized in the delivery of services, the primary concern for users is security [6], especially due to the fact that web systems are characterized by interactivity and there is an exchange of personal and sensitive data [7]-[12]. Without security of web systems, there is a high risk for both the database and users being compromised. According to [13] and [14], the prevalence of risk catapulted significant research towards the provision of web systems security, with significant attention being given towards security at network-level for example, port scanning. Nonetheless, while the focus was at this level, it was established that majority of attacks were aimed at systems' application-level, which mainly included web servers [15], [16], [17].

Security in web applications and web systems is an overlooked part in enterprises and it is essential that it be prioritized across all organizations [18], [19], [20]. Hackers have increased efforts and enhanced their concentration on services provided across web systems [21], [22], [23]. Due to the fact that web systems can be accessed at any time and from any location, hackers can easily intrude the backend and carry out illegal actions in corporate databases. As explained in [24], almost 49 percent of reviewed web applications are highly vulnerable and about 13 percent can be easily

*Corresponding author: Odiaga Gloria Awuor

compromised. Consequently, vulnerable web systems can be used in launching criminal actions for example, phishing and transfer of illegal content while the system's bandwidth is abused, which makes the owner accountable for the illegalities carried out in their system [25], [26], [27], [28]. According to [29], majority of attacks are launched at the application level of web systems.

Despite majority of organizations attempting to protect their systems using Secure Sockets Layer (SSL) and firewalls, they do not provide adequate protection against web system intrusion. This is because website access is public [30], [31], [32], [33], [34]. Web-based systems' backend data can always be directly accessed and since majority of them are customized, their degrees of testing are lower compared to off-shelf applications [35]. With compromised systems, hackers are able to completely access organization's back end data, even with proper configurations to firewalls or repeated patching to applications and operating systems [36], [37], [38]. Further, network security defense offers inadequate protection against attacks to web systems because hackers infiltrate web systems through port 80, taking advantage that it remains open for regular operations to be carried out in the organization. This means that it is pertinent for organizations to regularly audit their web-based systems to counter vulnerabilities that can be exploited [39], [40], [41], [42].

Literature reveals that in previous years, vulnerabilities at the application level of web-systems have been greatly consequential, leading to harvesting and leaking of confidential information. Subsequently, studies have been carried out to explore new techniques and tools to counter the issue of application-level security. For instance, the authors in [43], [44], [45], [46], [47], [48], [49] and [50] point out that it is pertinent for security to be the initial step prior to system development. The process should not only be flexible but also independent, containing security aspects customized to the organization. A study in [51] concluded that in the development of web systems, policies on security should be abstracted from other heterogeneous systems which would lead to a resilient system able to counter myriad attacks. The authors in [52 discuss that browsers themselves are insufficiently secure. They therefore concluded that secure browsers are essential in preventing existing vulnerabilities. Other studies such as the ones in [24], [53] and [54] have also emphasized web system hardening in mitigating attacks. According to [55], secure web systems are characterized by three components; input validity, state integrity and logic correctness. Input validity refers to the validation of input prior to utilization by the system. State integrity refers to un-tampered state of the system. Logic correctness refers to the correct execution of the system or application logic as the developer intended.

The contributions of this paper are as follows:

- Presentation of a security framework that guarantees conformity to the six key security requirements when adopting different web-based system security techniques.
- Discussion of the existing security challenges in web-based systems and the counteracting techniques.
- Identification of research gaps and suggestion of areas of intervention with regards to enhancing the security of web-based systems

The rest of this paper is organized as follows: section II presents a security framework that posits the six key security requirements and the corresponding security techniques used in web-based systems. Section III discusses the security challenges in web-based systems and the security threat assessment tools. Section IV shows the identified research gaps. Section V provides the conclusion and direction for future research.

2. Security Framework for Web-Based Systems

The authors in [56] posit that similar to any distributed system or application, it is equally essential for web systems to have adequate mechanisms which ensure that data is transferred securely. When functionality or information is shared through web systems, architectures and programming languages are not relied on. Such interoperability that characterizes web systems where access is granted across platforms necessitates for greater detail when conceptualizing system security [57], [58], [59], [60]. Basically, the requirements of web systems are authentication, authorization, confidentiality, integrity, availability and non-repudiation [61]-[66].

According to [56], authentication refers to the processes through which users of the system are identified. User identity should thus be verifiable in the same manner that they claim. On the other hand, authorization refers to the process where permission is granted to users to perform actions or carry out activities in the system. It is also seen from the standpoint of the administrator setting permission and checking the values of granted permissions after users have accessed the system [67], [68], [69], [70]. However, confidentiality refers to the prerequisites concerned with data in transit such that third parties do not access the data. It is mainly achieved through encryption and Virtual Private Network (VPN) approaches [71], [72], [73]. On the other hand, integrity in the security framework refers to detection

of information that has been tampered with. It is achieved by mathematical algorithms to identify specifically what and to what extent the tampering has occurred [74], [75], [76], [77]. Availability is a requirement that all services and resources of the system need to be accessible at all times to the parties authorized to access them. In cases of vulnerability, attacks occur whereby services and access is denied to the system's authorized users as all system resources have been used up [78], [79], [80]. However, non-repudiation refers to the fact that once a user has sent or received a message, they cannot deny having sent or received it [81], [82], [83], [84], [85].

As explained in [86], the requirements for security in web systems is implemented in a variety of ways. In the authentication requirement, prior to users being able to use the system, usernames and passwords are required. However, whereas they are both validated, there is a drawback in the plain manner in which they are propagated from clients to server. Sniffers can read the packages that are sent in the network. The Security Assertion Markup Language (SAML) is used to enhance system authorization and authentication to limit address sniffing vulnerabilities [87], [88], [89]. Other authentication techniques include the use of certificates which are sent to the server for verification of credentials, albeit it necessitates the use of Hypertext Transfer Protocol Secure (HTTPS) due to the lack of secure communication channels [90], [92]. Alternatively, Kerberos protocols are used to mutually authenticate users in the system using symmetric keys (shared secret between them) [91].

In the authorization requirement, technologies that are used are the SAML and the eXtensible Access Control Markup Language (XACML) [93], [94]. With XACML, decisions are made on whether access to resources can be granted or denied. Decisions are enforced respectively by the Policy Decision Point (PDP) and Policy Enforcement Point (PEP). Authorization through SAML involves two controls, which are the Role Based Access Control (RBAC) and the Context Based Access Control (CBAC) which map the organization's structure to security management and privileges are assigned to users respective to their roles in the organization [95].

According to [70], the availability requirement is a four-fold defense mechanism against Denial of Service (DoS) attacks. Foremost, the mechanism prevents attacks. Secondly, it detects attacks, determining where the attack came from and categorizing the harmful packets. Thirdly, the mechanism reacts to stop the attack, thus countering damages caused, by dropping the harmful packets or alternatively providing services on backup lines.The authors in [70] argue that a comprehensive defense solution against DoS attacks is difficult to achieve. However, techniques include implementation of robust infrastructure, complemented by firewalls, Intrusion Detection System (IDS) sensors, honeypots and Intrusion Prevention System (IPS).

Techniques used in the confidentiality requirement involve Extensible Markup Language (XML) encryption, which is used in instances when information needs to be confidential as it is being sent over a transaction [96]. Furthermore, in instances where encryption of information must be maintained, XML is useful. Algorithms commonly applied in the encryption requirement are Advanced Encryption Standard (AES) and Triple-Data Encryption Standard (Triple-DES)[97].

In the integrity requirement, web system functionality is described by Web Services Description Language (WSDL) files, which selects the web service upon users' request and Universal Description, Discovery, and Integration (UDDI) registry communication. In case of tampering, the service's integrity is destroyed. Integrity may also be ascertained using XML signatures [48]. However, XML signatures while guaranteeing integrity of certain document portions, allows users to edit other portions of the document that remain unsigned.The authors in [98] posit that WS-Security addresses the XML shortfall by enhancing security during end-to-end messaging and allows exchange of encrypted information and messages in the web environment.

Non-repudiation requirement techniques include WS-Security which applies digital signatures that offer non-repudiation guarantees [99], [100], [101]. In this specification, various formats of signatures, multiple trust domains and encryption guarantees are allowed. Additionally, variety of certificates such as X.509, SAML assertions and Kerberos tokens are provided. Security features are also added in the system's application layer and with the X.509, digital certificate information such as serial numbers, private keys, public keys and expiry dates can be formatted [102]. Table 1 gives a summary of the various security requirements and how they can be achieved, together with their challenges.

Table 1 Security framework for web-based systems

Security requirement	Drawbacks/Challenges	Techniques suggested
Authentication	Propagation of authentication information such as usernames and password in a plain manner between clients and servers.	-SAML (security assertion markup language) to limit address sniffing vulnerabilities -Use of HTTPS, Kerberos and digital certificates for verification of credentials
Authorization	Setting right permissions to the right users	-SAML and XACML (Extensible access control markup language) for access control to resources on web based systems -PDP (Policy Decision Point) and PEP (Policy Enforcement Point) for enforcement of access control decisions.
Confidentiality	Unauthorized access to data at rest and in transit.	XML (extensible markup language) and cryptographic algorithms such as AES and Triple DES
Integrity	Detection of information that has been tampered with using mathematical algorithms	-XML signatures with WS (web services) Security -Web-based system functionality is described by WSDL (Web Services Description Language) files, which selects web service upon users' request and -UDDI (Universal Description, Discovery, and Integration) registry communication
Availability	Availability of all web- based system resources and services at all times to authorized users.	-Implementation of robust infrastructure complemented with firewalls, Intrusion Detection System (IDS) sensors, honeypots and Intrusion Prevention System (IPS)
Non-repudiation	Web system users cannot deny having sent or received messages.	-Digital signatures with WS security -Digital certificates such as X.509 -SAML assertions and Kerberos tokens

3. Security Challenges in Web-Based Systems

Web systems and applications are basically an integrated technique with the capacity of being applied in both public (B2B) and internal (EAI) solutions. When adopted in EAI, issues around security are less considered due to the fact that the integrated services are protected and contained within the organization's network [103]. Nonetheless, depending on applications and services used by the organization, there may still be a prevalence of threats and vulnerabilities to the organization both internally and externally, so security concerns should not be disregarded. One of the key issues of security in web systems is when access is widened to the public scope, which essentially puts the organization's internal aspects at risk [104].

Various threats have been identified in literature by different authors. Vulnerabilities and threats variedly impact different roles in the organization and hinder not only system performance but also the performance of users. The authors in [105] posit that unauthorized access is an encompassing threat which includes firewall bypassing and eavesdropping on the network. Additionally, unauthorized access also refers to access of private and confidential data and information be it by internal or external users. Data decryption also presents a threat of unauthorized access, especially in instances where security requirements are not enhanced. According to [106], challenges in unauthorized access can be addressed with cryptographic techniques which counter attempts at accessing information and data.

Malicious manipulation of system parameters refers to instances whereby attackers input unexpected data to the system causing crashes and giving them an opportunity through which they can exploit the erroneous circumstance. Malicious data can be input into the system through various means such as SQL injection, and overflowing the system's buffer [105].

Configuration data disclosure, according to the authors in [105], is another challenge that web-based systems are exposed to. Another type of attack is message replay, which refers to instances when attackers capture messages illegitimately and use the messages to gain access to system resources. On the other hand, eavesdropping on the network allows attackers to intercept messages that are transmitted between parties, especially on public infrastructure. Data has traditionally been protected using SSL or VPN. However, in the case of web systems, these techniques are argued to be inadequate in providing security.

Service denial, results from DoS attacks [107]-[109]. In this case, attackers take advantage of the complexities exhibited by a network and may message bomb the network, aiming a specific service of the system, hampering services depended on by an organization. The authors in [95] adds that DoS attacks pose significant destruction as they limit legitimate resource accessibility and they can pose much difficulty for the organization when guarding against them. As explained in [107], security challenge such as reconnaissance allows attackers to carefully study their targets prior to proceeding with an attack. Attackers take advantage of the web system characteristic which allows users to search for services, which gives them adequate intelligence on their victims.

With regard to firewall bypassing, the authors in [110] argue that firewalls are both a benefit and a threat. Considering that services on web systems use Port 80, firewalls tend to allow data to pass without inspecting the traffic. Attackers can then exploit services that are implemented poorly, compromising other systems that are not protected by the firewall. The authors in [111] argue that the firewall challenge can be addressed by implementing firewalls that can control traffic in and out of the system and establishing mechanisms to allow firewall updates.

The authors in [69] argues that considering that web systems are complex, there is need for a larger scope of knowledge for appropriate industry practices to be defined regarding security. Similarly, the authors in [112] argue that considering the empirical nature of security, there are system vulnerabilities that may be undiscoverable unless the system is actually attacked. In this case therefore, the supposition presented in [112] is that implementing technologies and standards that are underdeveloped presents considerable risk to system security. According to [113], the trajectory of organizations moving towards web based systems and services exposes them to new threats especially at the level of business processes. Security experts have thus been said to focus on the lower end, which leaves many users vulnerable as they do not fathom the security in their systems.

Table 2 Web security challenges in web-based systems

Author	Security challenges identified
[105]	-Threat of unauthorized access including firewall bypassing and network eavesdropping Threats from malicious data such as through SQL injection and buffer overflows Configuration data disclosure
[106]	Unauthorized access from poor security enhancements that lead to data decryption
[69]	Message bombs aimed at specific web based system services. Reconnaissance threats that allow attackers to gather intelligence on their victims
[108]	DoS attacks that limit web resource and service accessibility
[110]	Threat from firewalls that allow data to pass through without inspection through port 80 that is used by web systems Attacker exploitation of poorly implemented services in web based systems
[112]	Threats from undiscoverable system vulnerabilities unless the system is actually attacked. Risks from implementing technologies and standards that are underdeveloped
[99]	Threat from the web-based system user unawareness of security issues and practices
[111]	Threat from multiple web service routing Unauthorized access threat during decryption at the intermediary during exchange of messages in web-based systems.
[114]	Some techniques like SSL only provide security for data in transit, therefore data at rest such as on servers is at risk with these techniques.

The authors in [111] discuss that there is a significant challenge in web systems' capacity to maintain security during multiple web service routing. In instances when intermediaries are involved in the exchange of messages, the concern is that encryption approaches working on lower layers encrypt the whole interaction rather than selecting a specific part. Upon arrival at an intermediary, decryption is carried out such that information is extracted, during which the data and information is vulnerable to unauthorized access. Another issue the authors in [114] identify is that in techniques like SSL, security is provided only for data in transit, which means that data at rest, for example data stored on servers cannot be protected using SSL techniques, hence the security is not persistent and the data is vulnerable when there is least resistance from the security tools. This is the same with HTTP, which is concluded to be a web system's weakest link and the prevalent point through which attackers can exploit the system. Table 2 offers some of the web security challenges that have been identified in literature.

4. Threat Assessment Tools

According to [115], sustainable security has majorly been the focus of organizations utilizing web systems. Consensus exists on the necessity of constant implementation of security models, considering that security in web systems is argued to be overlooked in most cases despite its significance in the design stage. For security professionals, they tend to depend on unreliable frameworks and simple engineering which negatively impact long term security sustainability. Vulnerability assessment respective to empirical studies is shown in the Table 3 below:

Table 3 Security threats, effects and resolutions in web-based systems

Author	Security Threat	Effect	Resolution
[116]	XSS (Cross site scripting)	Phishing Cookie stealing Key logging	-Use of white and black box testing methods -Using security testing [117] approaches in detecting XSS Using firewalls at application level to handle requests between server and clients
[118]	DDoS CSRF XST	It is impossible for all vulnerabilities to be investigated with one tool	-Selection of tool sets in an organized and optimized manner following the phases of identification, analysis, testing and reporting -Combining varied tools for instance Nikto and W3AF
[119]	SQL injection XSS Disclosure of IPs	In industries such as finance, prevalence of effects are encountered with private and sensitive organizational and customer data	-Vulnerability testing and observation, followed by development of a framework to enhance security
[120]	SQL	Leads to administrator credentials disclosure and private information such as credit card details, social security numbers etc.	-Adopting the use of Escrow, specifically in four aspects, thus: link gathering, URL analysis, injection identification and exploration of the database.
[121]	CSRF SQL XSS	Compromises integrity of data, flaws in security lead to unavailable system resources and private data may be stolen	-Adopting automation tools for instance Burp Suit and Acunetix -Manually testing vulnerabilities considering difficulty of finding some vulnerabilities automatically
[122]	CSRF XSS	Both are prevalent and are implemented by breaching user confidence in the application level	-Implementing code patterns for XSS stored in the system -Adopting black and white box testing methods

5. Research gaps

Various solutions have been suggested to counter the identified web system security challenges such as web system languages, proper firewall setups, IDS, IPS, cryptographic techniques, digital certificates and signatures among others. However, there is also need to focus on web system users' security training and awareness programs, as we adopt these technical solutions. Sophisticated hardware and software may be rendered useless if the user does not understand and comply with the security practices and protocols of web-based systems. It is also important to adopt security techniques that integrate all the six aspects of the presented security framework for web based systems.Consequently, policies and standards must be designed to capture all these basic requirements for the security of web based systems. Some of the techniques presented in the literature touch on specific security requirements and leave the other requirements unattended to, hence the onset of a vulnerable system. An attacker may exploit such techniques, to overcome the unshielded security requirements in that specific solution. Further, web system languages are argued to be lacking in the enforcement of security policies and may be in violation of data integrity and confidentiality of the system, posing a threat to the system. Subsequently, in order for safety to be ensured, there is need for comprehensive analysis to be conducted and for reliable and efficient techniques to be developed in the prevention of attacks, thus ensuring data security in web-based systems.

6. Conclusion

The aim of this paper was to review security challenges in web-based systems. From the study, it is evident that a key concern in web systems is the implementation of tools and techniques to test and sustain security. Increase in web systems usage such as in websites and web applications, poses challenges for sustainable security in organizations, which is attributed to crawling methods used in web exploration. Another challenge in web system security is the use of illegitimate inputs which leave a pathway for attacks to occur, leading to significant damages to data integrity. The implementation of insecure storage may also be challenging to web system security. In testing the security of web systems, there is a probability of repudiation attacks occurring, which leaves receivers unable to confirm the source of senders of the data. With autonomous data and information transmission and access in web-based systems, security requirements are paramount and must be maintained. Future research should focus on the performance and scalability challenges of these techniques to improve their security reliability.

Compliance with ethical standards

Acknowledgments

I would like to thank all parties that offered some assistance during the development of this article.

References

[1] Purwati UD, Amalia N. A mathematical model of social media popularity with standard incidence rate. InIOP Conference Series: Materials Science and Engineering 2019 Jun 1 (Vol. 546, No. 5, p. 052086). IOP Publishing.

[2] Humayun M, Jhanjhi NZ, Alsayat A, Ponnusamy V. Internet of things and ransomware: Evolution, mitigation and prevention. Egyptian Informatics Journal. 2021 Mar 1, 22(1):105-17.

[3] Mishra S, Jain S, Rai C, Gandhi N. Security challenges in semantic web of things. InInnovations in Bio-Inspired Computing and Applications: Proceedings of the 9th International Conference on Innovations in Bio-Inspired Computing and Applications (IBICA 2018) held in Kochi, India during December 17-19, 2018 9 2019 (pp. 162-169). Springer International Publishing.

[4] Jiang Y, Atif Y, Ding J. Cyber-physical systems security based on a cross-linked and correlated vulnerability database. InCritical Information Infrastructures Security: 14th International Conference, CRITIS 2019, Linköping, Sweden, September 23–25, 2019, Revised Selected Papers 14 2020 (pp. 71-82). Springer International Publishing.

[5] Gupta BB, Quamara M. An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols. Concurrency and Computation: Practice and Experience. 2020 Nov 10, 32(21):e4946.

[6] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[7] Sicari S, Rizzardi A, Coen-Porisini A. 5G In the internet of things era: An overview on security and privacy challenges. Computer Networks. 2020 Oct 9, 179:107345.

[8] Fauzi AF, Mohamed NN, Hashim H, Saleh MA. Development of web-based smart security door using qr code system. In2020 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS) 2020 Jun 20 (pp. 13-17). IEEE.

[9] Vadla S, Parakh A, Chundi P, Surbamaniam M. Quasim: A multi-dimensional quantum cryptography game for cyber security. InJournal of The Colloquium for Information Systems Security Education 2019 Feb 28 (Vol. 6, No. 2, pp. 19-19).

[10] Li Y, Saxunová D. A perspective on categorizing Personal and Sensitive Data and the analysis of practical protection regulations. Procedia Computer Science. 2020 Jan 1, 170:1110-5.

[11] Christen P, Ranbaduge T, Schnell R. Linking Sensitive Data: Methods and Techniques for Practical Privacy-Preserving Information Sharing: Synopsis by Kerina Jones. International Journal of Population Data Science. 2021, 6(2).

[12] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1, 142:103117.

[13] Xiao Y, Jia Y, Liu C, Cheng X, Yu J, Lv W. Edge computing security: State of the art and challenges. Proceedings of the IEEE. 2019 Jun 19, 107(8):1608-31.

[14] Ghubaish A, Salman T, Zolanvari M, Unal D, Al-Ali A, Jain R. Recent advances in the internet-of-medical-things (IoMT) systems security. IEEE Internet of Things Journal. 2020 Dec 17, 8(11):8707-18.

[15] Sadqi Y, Belfaik Y, Safi S. Web oauth-based sso systems security. InProceedings of the 3rd International Conference on Networking, Information Systems & Security 2020 Mar 31 (pp. 1-7).

[16] Yaacoub JP, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems. 2020 Sep 1, 77:103201.

[17] Zografopoulos I, Ospina J, Liu X, Konstantinou C. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access. 2021 Feb 10, 9:29775-818.

[18] Johns M, Dirksen A. Towards enabling secure web-based cloud services using client-side encryption. InProceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop 2020 Nov 9 (pp. 67-76).

[19] Qureshi SG, Shandilya SK. Advances in cyber security paradigm: A review. InHybrid Intelligent Systems: 19th International Conference on Hybrid Intelligent Systems (HIS 2019) held in Bhopal, India, December 10-12, 2019 19 2021 (pp. 268-276). Springer International Publishing.

[20] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[21] Alenezi M, Agrawal A, Kumar R, Khan RA. Evaluating performance of Web application security through a fuzzy based hybrid multi-criteria decision-making approach: Design tactics perspective. IEEE Access. 2020 Jan 31, 8:25543-56.

[22] Shahid J, Hameed MK, Javed IT, Qureshi KN, Ali M, Crespi N. A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions. Applied Sciences. 2022 Apr 18, 12(8):4077.

[23] Shen G, Wang W, Mu Q, Pu Y, Qin Y, Yu M. Data-driven cybersecurity knowledge graph construction for industrial control system security. Wireless Communications and Mobile Computing. 2020 Dec 26, 2020:1-3.

[24] Yadav D, Gupta D, Singh D, Kumar D, Sharma U. Vulnerabilities and security of web applications. In2018 4th International Conference on Computing Communication and Automation (ICCCA) 2018 Dec 14 (pp. 1-5). IEEE.

[25] Kruthik JT, Ramakrishnan K, Sunitha R, Prasad Honnavalli B. Security model for Internet of Things based on blockchain. InInnovative Data Communication Technologies and Application: Proceedings of ICIDCA 2020 2021 (pp. 543-557). Springer Singapore.

[26] Arogundade OT, Abayomi-Alli A, Misra S. An ontology-based security risk management model for information systems. Arabian Journal for Science and Engineering. 2020 Aug, 45:6183-98.

[27] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1, 133:102763.

[28] Chen H, Pendleton M, Njilla L, Xu S. A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. ACM Computing Surveys (CSUR). 2020 Jun 12, 53(3):1-43.

[29] Albahar M, Alansari D, Jurcut A. An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities. Electronics. 2022 Sep 21, 11(19):2991.

[30] Jemal I, Haddar MA, Cheikhrouhou O, Mahfoudhi A. Performance evaluation of Convolutional Neural Network for web security. Computer Communications. 2021 Jul 1, 175:58-67.

[31] Vidya MS, Patil MC. Reviewing effectivity in security approaches towards strengthening internet architecture. International Journal of Electrical and Computer Engineering. 2019 Oct 1, 9(5):3862.

[32] Riadi I, Raharja PA. Vulnerability analysis of E-voting application using open web application security project (OWASP) framework. International Journal of Advanced Computer Science and Applications. 2019, 10(11).

[33] Alsubaei F, Abuhussein A, Shandilya V, Shiva S. IoMT-SAF: Internet of medical things security assessment framework. Internet of Things. 2019 Dec 1, 8:100123.

[34] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[35] Albalawi M, Aloufi R, Alamrani N, Albalawi N, Aljaedi A, Alharbi AR. Website Defacement Detection and Monitoring Methods: A Review. Electronics. 2022 Nov 1, 11(21):3573.

[36] Tabrizchi H, Kuchaki Rafsanjani M. A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing. 2020 Dec, 76(12):9493-532.

[37] Patel A, Jain S. Present and future of semantic web technologies: a research statement. International Journal of Computers and Applications. 2021 May 28, 43(5):413-22.

[38] Wu Z, Shen S, Zhou H, Li H, Lu C, Zou D. An effective approach for the protection of user commodity viewing privacy in e-commerce website. Knowledge-Based Systems. 2021 May 23, 220:106952.

[39] Altulaihan EA, Alismail A, Frikha M. A Survey on Web Application Penetration Testing. Electronics. 2023 Mar 4, 12(5):1229.

[40] Kodali RK, Rajanarayanan SC, Koganti A, Boppana L. IoT based security system. InTENCON 2019-2019 IEEE Region 10 Conference (TENCON) 2019 Oct 17 (pp. 1253-1257). IEEE.

[41] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In 2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432).

[42] Shukla G, Gochhait S. Cyber security trend analysis using Web of Science: a bibliometric analysis. Eur J MolClin Med. 2020 Sep 1, 7(6):2567-76.

[43] Kanniah SL, Mahrin MN. A review on factors influencing implementation of secure software development practices. International Journal of Computer and Systems Engineering. 2016 Sep 2, 10(8):3032-9.

[44] Wiefling S, Dürmuth M, Lo Iacono L. What's in score for website users: A data-driven long-term study on risk-based authentication characteristics.I nFinancial Cryptography and Data Security: 25th International Conference, FC 2021, Virtual Event, March 1–5, 2021, Revised Selected Papers, Part II 25 2021 (pp. 361-381). Springer Berlin Heidelberg.

[45] Tahsien SM, Karimipour H, Spachos P. Machine learning based solutions for security of Internet of Things (IoT): A survey. Journal of Network and Computer Applications. 2020 Jul 1, 161:102630.

[46] Ali A, Ahmed M, Imran M, Khattak HA. Security and privacy issues in fog computing. Fog Computing: Theory and Practice. 2020 May 5:105-37.

[47] Madden N. API security in action. Simon and Schuster,2020 Nov 20.

[48] Kumar P. Prelude of security dispensation in web technology. Cosmos Journal of Engineering & Technology. 2020, 10(1):1-4.

[49] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[50] Subashini P, Krishnaveni M, Dhivyaprabha TT, Shanmugavalli R. Review on intelligent algorithms for cyber security. InHandbook of Research on Machine and Deep Learning Applications for Cyber Security 2020 (pp. 1-22). IGI Global.

[51] Van Der Linden D, Anthonysamy P, Nuseibeh B, Tun TT, Petre M, Levine M, Towse J, Rashid A. Schrödinger's security: opening the box on app developers' security rationale. InProceedings of the ACM/IEEE 42nd International Conference on Software Engineering 2020 Jun 27 (pp. 149-160).

[52] Reis C, Moshchuk A, Oskov N. Site isolation: process separation for web sites within the browser. InProceedings of the 28th USENIX Conference on Security Symposium 2019 Aug 14 (pp. 1661-1678).

[53] Deepa G, Thilagam PS. Securing web applications from injection and logic vulnerabilities: Approaches and challenges. Information and Software Technology. 2016 Jun 1, 74:160-80.

[54] Javed IT, Copeland R, Crespi N, Emmelmann M, Corici A, Bouabdallah A, Zhang T, El Jaouhari S, Beierle F, Göndör S, Küpper A. Cross-domain identity and discovery framework for web calling services. Annals of Telecommunications. 2017 Aug, 72:459-68.

[55] Agarwal N, Hussain SZ. A closer look at intrusion detection system for web applications. Security and Communication Networks. 2018 Jan 1, 2018.

[56] Aruna S, Vellore VI. Security in web services-issues and challenges. Int. J. Eng. Res. 2016 Sep, 5(09):243-8.

[57] Kashyap N, Malali HR, Gururaj HL. Cyber Attacks and Security—A Critical Survey. InSoft Computing: Theories and Applications: Proceedings of SoCTA 2019 2020 (pp. 895-904). Springer Singapore.

[58] Nyangaresi VO. A Formally Validated Authentication Algorithm for Secure Message Forwarding in Smart Home Networks. SN Computer Science. 2022 Jul 9, 3(5):364.

[59] Paik HY, Xu X, Bandara HD, Lee SU, Lo SK. Analysis of data management in blockchain-based systems: From architecture to governance. Ieee Access. 2019 Dec 23, 7:186091-107.

[60] Yan T, Liu J, Niu Q, Chen J, Xu S, Niu M. Network security protection technology for a cloud energy storage network controller. Global Energy Interconnection. 2020 Feb 1, 3(1):85-97.

[61] Muttaqin K, Rahmadoni J. Analysis and design of file security system AES (advanced encryption standard) cryptography based. Journal of Applied Engineering and Technological Science (JAETS). 2020 May 26, 1(2):113-23.

[62] Popescu A, Bauereiss T, Lammich P. Bounded-deducibility security. In12th International Conference on Interactive Theorem Proving (ITP 2021) 2021 Jun 21 (Vol. 193, p. 3). SchlossDagstuhl--Leibniz-ZentrumfuerInformatik.

[63] Manulis M, Bridges CP, Harrison R, Sekar V, Davis A. Cyber security in new space: analysis of threats, key enabling technologies and challenges. International Journal of Information Security. 2021 Jun, 20:287-311.

[64] Mohamed KS, Mohamed KS. Cryptography concepts: integrity, authentication, availability, access control, and non-repudiation. New Frontiers in Cryptography: Quantum, Blockchain, Lightweight, Chaotic and DNA. 2020:41-63.

[65] Badra M, Borghol R. Long-term integrity and non-repudiation protocol for multiple entities. Sustainable cities and society. 2018 Jul 1, 40:189-93.

[66] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec, 39(10):e13126.

[67] Mohsin AH, Zaidan AA, Zaidan BB, Albahri OS, Albahri AS, Alsalem MA, Mohammed KI. Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. Computer Standards & Interfaces. 2019 May 1, 64:41-60.

[68] Esposito C, Ficco M, Gupta BB. Blockchain-based authentication and authorization for smart city applications. Information Processing & Management. 2021 Mar 1, 58(2):102468.

[69] Sharma A, Singh A, Sharma N, Kaushik I, Bhushan B. Security countermeasures in web based application. In2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) 2019 Jul 5 (Vol. 1, pp. 1236-1241). IEEE.

[70] Nandy T, Idris MY, Noor RM, Kiah LM, Lun LS, Juma'at NB, Ahmedy I, Ghani NA, Bhattacharyya S. Review on security of internet of things authentication mechanism. IEEE Access. 2019 Oct 16, 7:151054-89.

[71] Tyagi AK, Nair MM, Niladhuri S, Abraham A. Security, privacy research issues in various computing platforms: A survey and the road ahead. Journal of Information Assurance & Security. 2020 Jan 1, 15(1).

[72] Al-Turjman F, Zahmatkesh H, Shahroze R. An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies. 2022 Mar, 33(3):e3677.

[73] Alferidah DK, Jhanjhi NZ. A review on security and privacy issues and challenges in internet of things. International Journal of Computer Science and Network Security IJCSNS. 2020 Apr, 20(4):263-86.

[74] Wei P, Wang D, Zhao Y, Tyagi SK, Kumar N. Blockchain data-based cloud data integrity protection mechanism. Future Generation Computer Systems. 2020 Jan 1, 102:902-11.

[75] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[76] Garg N, Bawa S, Kumar N. An efficient data integrity auditing protocol for cloud computing. Future Generation Computer Systems. 2020 Aug 1, 109:306-16.

[77] Fan Y, Lin X, Tan G, Zhang Y, Dong W, Lei J. One secure data integrity verification scheme for cloud storage. Future Generation Computer Systems. 2019 Jul 1, 96:376-85.

[78] Lalropuia KC, Khaitan V. Availability and reliability analysis of cloud computing under economic denial of sustainability (EDoS) attack: a semi-Markov approach. Cluster Computing. 2021 Sep, 24:2177-91.

[79] Qi Q, Tao F. A smart manufacturing service system based on edge computing, fog computing, and cloud computing. IEEE access. 2019 Jun 19, 7:86769-77.

[80] Kumari P, Kaur P. A survey of fault tolerance in cloud computing. Journal of King Saud University-Computer and Information Sciences. 2021 Dec 1, 33(10):1159-76.

[81] Sun J, Yao X, Wang S, Wu Y. Non-repudiation storage and access control scheme of insurance data based on blockchain in IPFS. IEEE Access. 2020 Aug 24, 8:155145-55.

[82] Chen F, Wang J, Li J, Xu Y, Zhang C, Xiang T. TrustBuilder: A non-repudiation scheme for IoT cloud applications. Computers & Security. 2022 May 1, 116:102664.

[83] Hegde N, Manvi SS. Distributed integrity and non-repudiation scheme in the dynamic vehicular cloud environment. International Journal of Information and Computer Security. 2023, 20(3-4):315-48.

[84] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[85] Divya KS, Roopashree HR, Yogeesh AC. Non-Repudiation-based Network Security System using Multiparty Computation. International Journal of Advanced Computer Science and Applications. 2022, 13(3).

[86] Rawat A, Singhal A, Choudhury T. Towards Securing Cloud & Information-Vision & Challenges. In2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence) 2021 Jan 28 (pp. 220-226). IEEE.

[87] Karie NM, Kebande VR, Ikuesan RA, Sookhak M, Venter HS. Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud. InProceedings of the 3rd International Conference on Networking, Information Systems & Security 2020 Mar 31 (pp. 1-6).

[88] La Z, Yu L. SAML Improvement Scheme in Cloud Environment. InInternational Conference on Applications and Techniques in Cyber Security and Intelligence ATCI 2018: Applications and Techniques in Cyber Security and Intelligence 2019 (pp. 1271-1275). Springer International Publishing.

[89] Kodam T. A roadmap for ensuring SAML authentication using Identity server for on-premises and cloud.

[90] Calzavara S, Urban T, Tatang D, Steffens M, Stock B. Reining in the web's inconsistencies with site policy. InProceedings of the 2021 Network and Distributed Systems Security Symposium 2021.

[91] Mutaher H, Kumar P. Security-enhanced SDN controller based Kerberos authentication protocol. In2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence) 2021 Jan 28 (pp. 672-677). IEEE.

[92] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1, 15:100210.

[93] Kousalya A, Baik NK. Enhance cloud security and effectiveness using improved RSA-based RBAC with XACML technique. International Journal of Intelligent Networks. 2023 Mar 21.

[94] Charaf LA, ALIHAMIDI I, ADDAIM A, Abdessalam AI. A distributed XACML based access control architecture for IoT systems. In2020 1st International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET) 2020 Apr 16 (pp. 1-5). IEEE.

[95] Singh DP, Rajpoot S, Singh P. A protection and assurance version for E-authorities Web Services based totally on Cloudlet computing. In2021 International Conference on Technological Advancements and Innovations (ICTAI) 2021 Nov 10 (pp. 146-149). IEEE.

[96] Gupta C, Singh RK, Mohapatra AK. A survey and classification of XML based attacks on web applications. Information Security Journal: A Global Perspective. 2020 Jul 3, 29(4):183-98.

[97] Patel A, Shah N, Ramoliya D, Nayak A. A detailed review of cloud security: issues, threats & attacks. In2020 4th International conference on electronics, communication and aerospace technology (ICECA) 2020 Nov 5 (pp. 758-764). IEEE.

[98] Devi S, Bharti TS. Study of Architecture and Issues in Services of Cloud Computing. In2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N) 2021 Dec 17 (pp. 1578-1581). IEEE.

[99] Khan RA, Khan SU, Khan HU, Ilyas M. Systematic mapping study on security approaches in secure software engineering. IEEE Access. 2021 Jan 18, 9:19139-60.

[100] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[101] Bubaker L, Yousef A, Algariani W. A Systematic Mapping Study on Web services Security Threats, Vulnerabilities, and Countermeasures. AlQalam Journal of Medical and Applied Sciences. 2021, 4(1):91-100.

[102] Adhiguna KA, Rusli FM, Irawan H. Building an ID Card Repository with Progressive Web Application to Mitigate Fraud based on the Twelve-Factor App methodology. In2021 9th International Conference on Information and Communication Technology (ICoICT) 2021 Aug 3 (pp. 544-549). IEEE.

[103] He YM, Yang L. Object-oriented analysis in Enterprise Application Integration using web services. InFrontiers in Enterprise Integration 2020 Oct 28 (pp. 33-38). CRC Press.

[104] Gawin B, Marcinkowski B. IT solutions integration: technical and organizational challenges. InInternational Conference on ICT Management for Global Competitiveness and Economic Growth in Emerging Economies 2018. UniwersytetWrocławski.

[105] Raj G, Mahajan M, Singh D. Trust decision model and trust evaluation model for quality web service identification in web service lifecycle using QSW data analysis. International Journal of Web-Based Learning and Teaching Technologies (IJWLTT). 2020 Jan 1, 15(1):53-72.

[106] Ahmed AI, Gani A, Ab Hamid SH, Abdelmaboud A, Syed HJ, Mohamed RA, Ali I. Service management for IoT: requirements, taxonomy, recent advances and open research challenges. IEEE Access. 2019 Oct 17, 7:155472-88.

[107] Sharma S, Kaushik B. A survey on internet of vehicles: Applications, security issues & solutions. Vehicular Communications. 2019 Dec 1, 20:100182.

[108] Singh A, Sharma A, Sharma N, Kaushik I, Bhushan B. Taxonomy of attacks on web based applications. In2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT) 2019 Jul 5 (Vol. 1, pp. 1231-1235). IEEE.

[109] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[110] Yarygina T. RESTful is not secure. InApplications and Techniques in Information Security: 8th International Conference, ATIS 2017, Auckland, New Zealand, July 6–7, 2017, Proceedings 2017 (pp. 141-153). Springer Singapore.

[111] Al-Qallaf CL, Ridha A. A comprehensive analysis of academic library websites: design, navigation, content, services, and web 2.0 tools. International Information & Library Review. 2019 Apr 3, 51(2):93-106.

[112] RezaeiKalantari K, Ebrahimnejad A, Motameni H. Efficient improved ant colony optimisation algorithm for dynamic software rejuvenation in web services. IET Software. 2020 Aug, 14(4):369-76.

[113] Khan F, Ramasamy LK. Web Services Security Using Semantic Technology. Recent Advances in Intelligent Systems and Smart Applications. 2021:403-27.

[114] Sahoo S, Panda KC. Web content analysis of Indian Institute of Technology (IIT) library websites: An evaluative study. Library Philosophy and Practice (e-journal). 2019, 3949.

[115] Agrawal A, Alenezi M, Kumar R, Khan RA. Measuring the sustainable-security of Web applications through a fuzzy-based integrated approach of AHP and TOPSIS. IEEE Access. 2019 Oct 14, 7:153936-51.

[116] Shrivastava A, Choudhary S, Kumar A. XSS vulnerability assessment and prevention in web application. In2016 2nd International Conference on Next Generation Computing Technologies (NGCT) 2016 Oct 14 (pp. 850-853). IEEE.

[117] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[118] Alghamdi MI. Survey on Applications of Deep Learning and Machine Learning Techniques for Cyber Security. International Journal of Interactive Mobile Technologies. 2020 Dec 6, 14(16).

[119] Goutam A, Tiwari V. Vulnerability assessment and penetration testing to enhance the security of web application. In2019 4th International Conference on Information Systems and Computer Networks (ISCON) 2019 Nov 21 (pp. 601-605). IEEE.

[120] Delamore B, Ko RK. Escrow: A large-scale web vulnerability assessment tool. In2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications 2014 Sep 24 (pp. 983-988). IEEE.

[121] Nagpure S, Kurkure S. Vulnerability assessment and penetration testing of Web application. In2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA) 2017 Aug 17 (pp. 1-6). IEEE.

[122] Farah T, Shojol M, Hassan M, Alam D. Assessment of vulnerabilities of web applications of Bangladesh: A case study of XSS & CSRF. In2016 sixth international conference on digital information and communication technology and its applications (DICTAP) 2016 Jul 21 (pp. 74-78). IEEE.