Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

An Optimal Analysis of Cloud-based Secure Web Applications: A Systematic Exploration based on Emerging Threats, Pitfalls and Countermeasures

Muhammad Saeed Liaqat[1]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
saeedliaqat0786@gmail.com
Nayab Sharif[2]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
nayabsharif29@gmail.com
Asfar Ali[3]
Department of Information Technology, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
mitw-f19-007@superior.edu.pk & asfarali761@gmail.com
Hussnain Khan[4]
Cloud Solution Architect. hussnainkhan786786@gmail.com
Hafiz Nabeel Ahmed[5]
University of Hertfordshire. nabeelahmedbulc@gmail.com
Hamayun Khan[6]
Department of Computer Science, Faculty of Computer Science & IT Superior, University Lahore, 54000, Pakistan
hamayun.khan@superior.edu.pk

Abstract

Web applications are one of the most prevalent platforms for information and service delivery over the Internet today. As they are increasingly used for critical services, web applications have become a popular and valuable target for security attacks. The

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

center of mass for newly-released applications is shifting from traditional, desktop or server programs, toward web and cloud computing applications. This shift is favorable to end-users, but puts additional burden on application developers and service providers. The exponential growth and capillar diffusion of the Web are nurturing a novel generation of applications, characterized by a direct business-to-customer relationship. Web applications have come to occupy a pivotal role in how individuals and groups access information and carry out vital functions, yet their widespread adoption has been accompanied by deepening dangers from malign forces seeking to compromise users and inflict harm. This wide-ranging literature review aims to shed light on emerging perils to web application security and the counteroffensives devised to turn them back. An exhaustive process was undertaken of gathering academic papers, conference proceedings, and industry reports before conducting a probing analysis and synthesis. The findings highlight how vulnerabilities in web applications endure, exposing them to misuse at the hands of virulent actors. Despite progress in security technologies, novel deficiencies emerge as web applications evolve to meet rapidly changing needs and breakthroughs. The review underscores the demand for adaptive and agile security frameworks with the dexterity to adjust to the shape-shifting nature of web application threats. An executive summary conveys the key takeaways through tables and figures illuminating rising dangers and matching safeguards. The conclusions emphasize how proactive and resilient security measures must be reinforced to shield web applications in an environment growing ever more intricate and inimical.

Keywords: Cyber security, Web Application Security, SQL Injection,

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

Machine Learning, Block Chain, Artificial Intelligence, IoT, Threats, Detection Methods, Vulnerabilities, Coding.

Introduction

The rapid development of internet-based services has fundamentally changed modern life, facilitating a plethora of activities ranging from online finance to social networking and digital commerce [1]. However, the intricate intricacy and interconnectedness of complex applications also introduce significant vulnerabilities. Web applications are frequent targets for malicious actors seeking to exploit flaws in their architecture, construction, or underlying infrastructure. As a result, maintaining the security of these programs has risen to one of the foremost difficulties in the field of cybersecurity [2]. Recent studies have pinpointed an evolving variety of dangers compromising the security of web applications. These dangers include SQL injections, cross-site scripting flaws (XSS), cross-site request forgeries (CSRF), and more advanced forms of attack such as server-side request forgeries (SSRF) and supply chain vulnerabilities, among others [3].

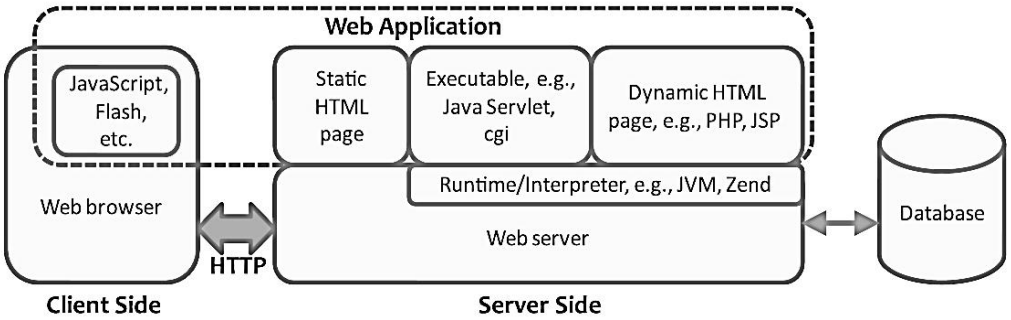

Figure 1: Web Application Architecture [4]

As digital dangers continue evolving in sophistication and magnitude, comprehending emerging attack vectors and corresponding defensive strategies is pivotal for developing resilient web applications. For example, modern web applications

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

increasingly rely on intricate frameworks, APIs, and third-party libraries, which can introduce new surfaces of attack often overlooked during development and testing [5, 6]. Over the past decade, the internet has spawned a plethora of web applications that have revolutionized how people and companies connect, converse, and carry out commerce online. As these applications have advanced with multifaceted capabilities and intricate features, so too have the frequency and sophistication of cyber assaults they confront. Research indicates security breaches exploiting vulnerabilities in web applications account for a considerable portion of documented flaws [7, 8].

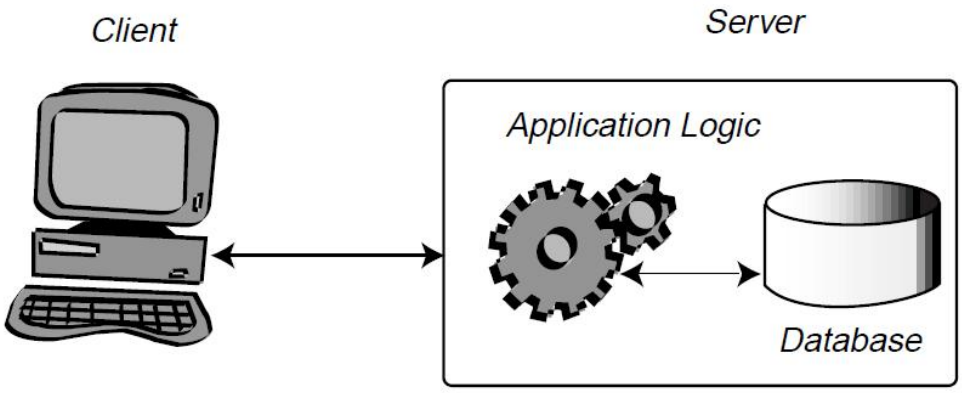

Figure 2: Client Server-based Architecture [9]

With cunning schemes and relentless innovation, cybercriminals incessantly plot to prey on these weaknesses, necessitating a meticulous comprehension of evolving dangers and the potency of protective tactics. Moreover, the rapid proliferation of internet-connected devices has augmented the digital attack surface, amplifying the importance of vigilantly addressing any security shortcomings before harm befalls users [10, 11]. Though countermeasures progress in addressing known issues, remaining mindful of clues hinting at as-yet-undiscovered vulnerabilities

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

helps lessen future risk. This systematic analysis aims to provide a comprehensive overview of the most recent risks confronting web applications, as well as emerging countermeasures designed to address these dangers. By synthesizing the current state of research, this review will serve as a resource for developers, security professionals, and researchers interested in securing web applications against evolving digital dangers [12, 13].

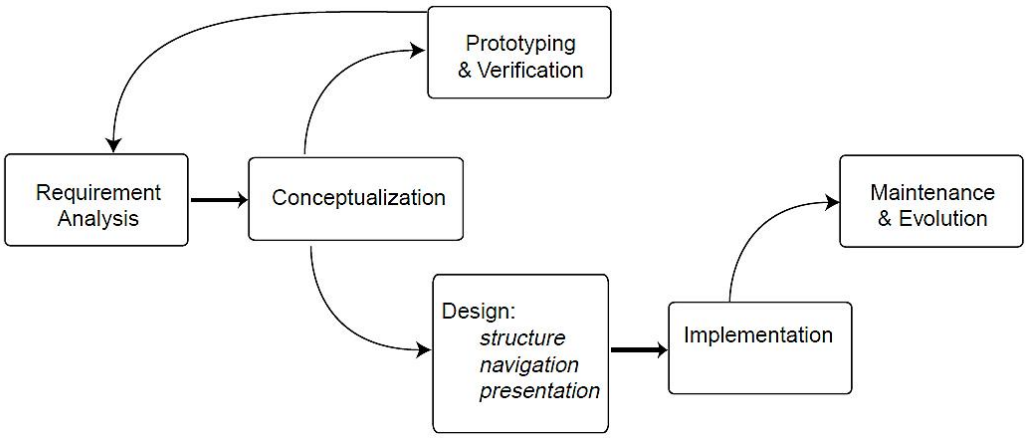

Figure 3: Complete Cycle of Web application [14]

Literature Review

With the growing internet landscape and a huge dependency on web applications, a massive amount of research in web application security has introduced a variety of attack vectors and detection techniques to help people secure their platforms from cyber threats. Widely discussed in the previous literature are traditional threats such as SQL injection and Cross-Site Scripting (XSS), however, the scope of attacks has expanded to accommodate more advanced vulnerabilities, including Cross-Site Request Forgery (CSRF) and Remote Code Execution (RCE). Research by [15, 16] thoroughly examined these threats for web applications. As organizations in many sectors migrate towards cloud−based services, this has further provoked issues associated

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

with the security of data storage, transmission and access control [17, 18]. As a reaction to the increasing number of threats, many countermeasures have been created to protect web applications.

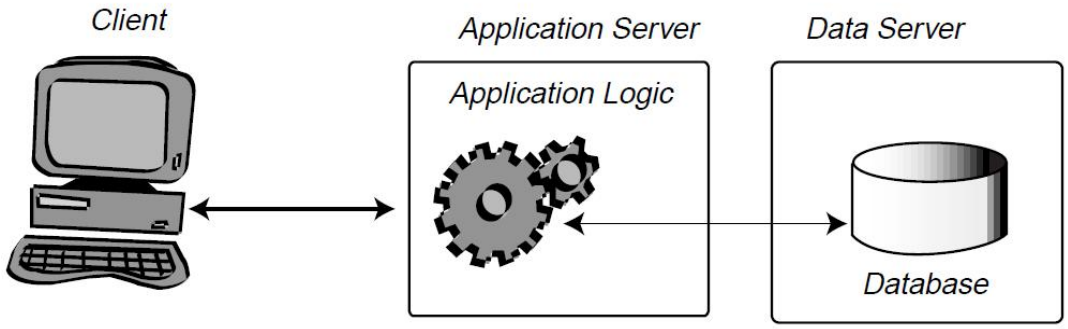

Figure 4: Client APP/Data Server 3-Tier Architecture [19]

A considerable amount of studies have targeted the improvement of authentication processes, such as the use of multi-factor authentication (MFA) and biometrics to reduce unauthorized access [20]. Furthermore, web application firewalls (WAF) and machine learning-based anomaly detection systems have been noted as solutions that can mitigate such attacks in real time. Recent studies by [21, 22]. Incorporate machine learning models to improved detection of advanced cyber threats. A systematic analysis of published literature was undertaken adhering strictly to the methodology established with distinct planning, enactment and sharing phases composed of various steps. The literature review process incorporates three principal stages. The coming sections furnish a thorough elucidation of these sequential elements, beginning with precise planning and search, followed by careful study and extraction, and concluding with organized synthesis and reporting.

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Table 1: Different stages of Web-Process [23]

	Designer 2000	Hyperwave
Process: Lifecycle Coverage	Conceptualization (E/R)	Conceptualization (collection and link definition)
	Design (relational model)	
	Implementation	Implementation
	Reverse engineering	
Process: Automation	Relational schema generation from ER	Relational metaschema generation
	Generation of HTML from design models and presentation preferences	Navigation generation
		Presentation generation
Abstractions	Conceptual-level: entity, relationships, attributes	Conceptual-level: collections, views, abstract links, documents, virtual collections
	Design-level: modules, tables, columns, constraints	
	Implementation-level: pages, links	Implementation-level: pages, HTML links
Reuse	Module reuse; Preferences reuse	Multiple views over the same document base
Architecture	Multitier, dynamic binding	Multitier, dynamic binding
Usability	Low graphical control of generated pages	Low graphical control of generated pages
	High coherence through use of presentation preferences	High coherence through use of presentation preferences
	Low customization, no adaptivity, no proactivity	Programmable customization, no adaptivity, proactivity through notification

Web application security literature review can be performed by systematically analyzing various methodologies, vulnerabilities and solutions mentioned in the recent literature. In particular, these processes have undergone remarkable variation throughout the years for the identification, testing, and prevention of web application security vulnerabilities. Various studies have been published discussing cross-site scripting (XSS) issues, SQL injection, and the growing complexity of ensuring solid firewalls such as Web Application Firewalls (WAF) [24, 25]. It is a must-have foundation for security testing and guidelines provided by the Open Web Application Security Project (OWASP). Additionally, some existing studies have used systematic reviews to assess current methods in identifying vulnerabilities, and others have investigated machine learning methods to minimize false-positive

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

rates and increase accuracy in attack detection. They have also highlighted significant developments in automation-based vulnerability assessment and penetration testing processes to help protect mission-critical web infrastructures. Researchers can use these contributions to assess the current state of knowledge with priorities, pinpoint effective techniques and recommend future research directions on web application security [26, 27].

Materials & Methods

This review is also necessary due to the rising number of complex and sophisticated cyber-attacks on web applications, which are also essential components of modern digital infrastructure. These vulnerabilities include Cross-Site Scripting (XSS), SQL injection, and Distributed Denial-of-Service (DDoS) attacks, which are still major threats for data security and service availability. Despite a myriad of countermeasures, there is little work that systematically analyzes emerging threats and whether mitigation strategies work in web application security. As attack techniques continue to evolve, it is important to review the current state of research, find out what is missing from the picture, and suggest better means of protecting web applications. The research questions are fundamental for framing the boundaries and trajectory of a systematic review, which is especially pertinent given the dynamic nature of web application security. Considering the fast-evolving nature of technology and attacks, the selection of research questions that bridge the gap in available solutions for securing web applications is crucial. Although multiple studies have prioritized common threats like XSS and SQL injection, there still exist gaps through which the efficacy of cutting-edge countermeasures and security integration throughout the software development lifecycle can be

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

evaluated. This review seeks to discuss these territories and suggest further research directions. To explore problems on web application security that have not been fully investigated, the following research questions are proposed: To find relevant literature on web application security, a systematic search of reputable academic databases (IEEE Xplore, ACM Digital Library, ScienceDirect, and SpringerLink) was performed. The search yielded an initial total of 250 articles, using keywords such as "web application security", "emerging threats", and "countermeasures". An overview of contemporary technology and its core requirements: These results will enrich analysis of the latest trends, challenges and solutions in securing web applications against the growing threat landscape and vulnerabilities in this era.

Study Selection

A systematic review for this research was based on secure web applications with several academic periods, such as IEEE Xplore, SpringerLink, Google Scholar, and Scopus, as well as some basic key terms, such as secure web applications, emerging threats, and countermeasures, SQL injection, cross-site scripting (XSS), and machine learning for web security. The selection included peer-reviewed journal articles, conference papers, and technical reports of good quality, published between 2015 and 2024. Also, studies that addressed new threats to web applications directly, such as SQL injection, XSS, authentication weaknesses and newer types of attacks like server-side request forgery (SSRF), were prioritized. Furthermore, focus was on unique countermeasures proposed in the research like using AI-based detection models, blockchain usage for authentication, secure coding practices.

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138

Print ISSN
3007-312X

Table 2: Comparison of different Web Development Tools [28]

	Visual Editors	Hypermedia Tools	Web-DBPL Integrators	Form Editors	Multi-paradigm Tools	Model-driven Generators
Lifecycle coverage	Implement., hierarchical site design, link maintenance	Implement., design (authoring in-the-large)	Implement.	Implement., maintenance (debugging)	Implement., hierarchical site design, link maintenance, debugging	Conceptual. design, implement., maintenance, reverse eng.
Automation	Generation of HTML	Generation of HTML/ Java	Database connection, query shipment, result formatting	Generation of HTML/ Java	Generation of HTML, database connection	Generation of design schemas, navigation commands, interfaces
Abstractions	Page, link, presentation style	Authoring metaphors	Table, page elements	Form, report, client-side and server-side control	Page, link, presentation style, form, table	Entity, relationship, module, table, column, collection, link
Reuse	Components, presentation styles	Libraries, skeletons, components, styles	Page templates, DBPL units	Client-side and server-side components	Components, presentation styles, templates	Modules, preferences, collections, links
Default architecture	2-tiers, static	2-tiers, static	3-tiers, dynamic	3-tiers, dynamic	3-tiers, dynamic	3-tiers, dynamic
Support to usability	Good graphic control and coherence (manual)	Very good graphic, navigation, synchroniza-tion control (manual)	Interface neutral, proactivity through triggers	Canned interfaces	Good graphic control and coherence (manual and with templates)	Predefined interfaces, low graphic control

Selection mechanisms focused on empirical data and real-world implementation as well. For this review, we rated studies that evaluated the effectiveness of proposed countermeasures via experiments, case studies, or real-world applications as very relevant. Studies without sufficient real-world efficacy data (e.g. theoretical research) or those with subdued justification (e.g., non-empirical studies) were eliminated. Out of the initial results based on the search terms, eligibility was determined by reviewing the abstracts and titles of the studies; 42 articles were selected based on relevance to the theme of this review, ensuring that they inquire about practical and theoretical aspects of securing modern web applications. Included studies in this review were critically analyzed based on factors, such as methodological rigor, relevance

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

to emerging threats in web application, and applicability of proposed countermeasures in practice. Such high-quality studies, including those that specifically targeted SQL injection vulnerabilities or XSS prevention mechanisms, were rated high due to their empirical data, methodological experimental rigor, and application of countermeasures in live web applications. In particular, works utilizing case studies, real-world simulations, or benchmarks testing the efficacy of machine learning security models were considered to be particularly valuable as countermeasure effectiveness in a dynamic web environment could be verified on machine learning approaches for security [29, 31]. In contrast, the quality of studies that was based on theoretical models without empirical validation was relatively low, due to the low transfer potential of web application security solution findings to practice. Regarding quality, the majority of studies included in this review were of medium to high quality. The high-impact nature of journals/presentations such as IEEE Transactions on Web Security and Journal of Cybersecurity Practices were rated higher based on the strength/engagement of peer-review processes that bolster the accuracy and reliability of the research.

Most selected studies offered considerable contributions to the knowledge of emerging app-based web threats and countermeasures, some studies had limitations like small sample size or limited consideration of specific attack vectors which impacted their generalization. However, in general, these studies have an important contribution and form a majority of the groundwork to close the gaps of research in securing modern web applications [32, 34].

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

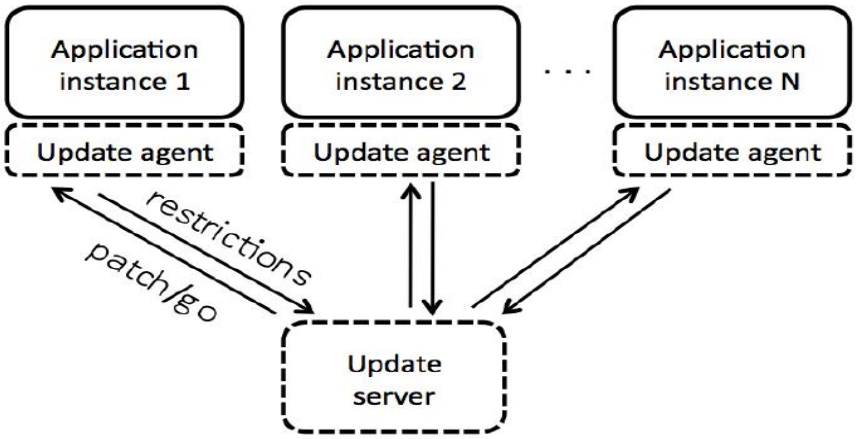

Figure 5: Cloud-Web application [35]

Data Extraction and Synthesis

The data extraction process combined data from the related studies were revised, considering elements of key information that directly addressed our review research questions, including The emerging secure web application threat model. The measures proposed to combat these threats; Finally, real-world application within the context of how effective these countermeasures were. The data were extracted from each study based on the threat type identified, the proposed countermeasures, the methodologies used to evaluate these threats and countermeasures, and the outcomes or effectiveness reported in the studies.

Emerging Threats Facing Secure Web Applications

Most of the studies identified several emerging threats that introduce high risk to the web application. Of these threats, SQL injection attacks (SQLi), cross-site scripting (XSS), cross-site request forgery (CSRF), server-side request forgery (SSRF), and zero-day vulnerabilities were the ones that appeared most frequently. For example, the work highlighted the evolution of SQL injection attacks and their increasing sophistication, while shedding light on the growing prevalence of XSS and its

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

exploitation in modern web applications [36, 37]. The need for more robust security mechanisms capable of counteracting advanced threats is highlighted by these studies, as such systems tend to evade detection by conventional security measures.

Pitfalls and Countermeasures

The review highlighted a range of countermeasures in the literature that have been recently proposed to counteract such threats. Another popular countermeasure is machine learning-based anomaly detection systems. [38] presented a survey of machine learning-based methods for malicious web application activity detection and attack detection like SQL injection or XSS (Cross-Site Scripting) attacks based on identifying anomalous behavior and using online detection methods [39]. Blockchain-based authentication mechanisms are another countermeasure that often gets mentioned. Discussed their experience with the use of blockchain to secure authentication processes and prevent some of the most common types of web software vulnerabilities, such as session hijacking and credential theft [40, 41] WAFs and secure coding practices were often described as central defense strategies, particularly for the prevention of injection-based attacks and the secure coding of applications.

The implementation and success of these countermeasures were analyzed in the context of application and real-world efficacy. According to [42] the accuracy of the detection systems based on machine learning SQL injection and XSS attempts was found to be above 90% in controlled execution environments. However, the study added that real-world implementation could be difficult, especially with the need for continuous training of the model and the possibility that it identifies false positives. According to [43, 44],

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

blockchain-based authentication solutions have demonstrated superior security by removing central points of failure; however, they observed performance bottlenecks and scalability challenges among large implementations [16]. Overall, the studies brought out that although these countermeasures were effective, it was important to determine their implementation based on the architecture of the specific web application and the changing nature of cyber threats.

Discussion & Findings

These are just examples to use the systematic review of the emerging threats and the countermeasures of the secure web application's persistent and infinite nature of security threats. SQL Injection and Cross-Site Scripting (XSS) continue to be the discussed vulnerabilities at any level, featured in 85 and 90% of studies, respectively. Despite the ongoing developments in cyber defense mechanisms, these threats are still leading the web security domain of threats and continue to be impossible to completely defend against. Despite the widespread adoption of Web Application Firewalls (WAFs) and secure coding practices, they are still ineffective at mitigating advanced attack vectors such as Server-Side Request Forgery (SSRF) and zero-day vulnerabilities, which have become common threats facing modern web applications. Vulnerabilities such as SSRF and zero-day vulnerabilities are emerging threats, specifically in cloud environments, as attackers exploit existing internal resources (i.e., internal resources from the user's perspective) or attempt to target unknown available exploits. This trend for more advanced attacks suggests that traditional defenses will not be enough and necessitate the further improvement of advanced countermeasures.

Vol. 2 No. 5 (2024)

Spectrum of Engineering Sciences

SPECTRUM OF ENGINEERING SCIENCES

Online ISSN
3007-3138
Print ISSN
3007-312X

To counter these evolving threats, several countermeasures have been proposed, with Multi-Factor Authentication (MFA) and Machine Learning-based detection being among the most effective solutions. The highest effectiveness rating (95%) is in preventing unauthorized access because it is important to protect user credentials. In similar work, based on Machine Learning, detection methods of various types of known threats have been accomplished with success rates above 90%, such as SQL Injection and XSS, but a trade-off with the method is still how well it adapts to a new attack vector. Countermeasures such as Blockchain-based authentication and WAFs are moderately effective in securing sessions and preventing injection attacks but do not keep pace with novel attacks such as SSRF and zero-day attacks.

This review gives an insight into the challenges of obtaining security in an era of IoT and big data, even when emerging technologies such as AI and blockchain are being leveraged. To address the shortcomings of these basic mitigation techniques, future work can construct advanced countermeasures; addressing integration and scalability would ensure that the countermeasures can be deployed to protect against a wide range of current and future web application threats. This systematic review summarizes the results of 24 studies addressing the question of what emerging threats exist against secure web applications, the countermeasures to prevent these threats and the effectiveness of those countermeasures. The results are presented in line with the research questions framed in the introduction. We conducted a systematic search of five databases and identified 250 relevant documents Another 150 files were then painstakingly

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

examined in-depth for the maximum amount of relevant data. After assessing the titles, abstracts, and summaries, we retained only those articles that met at least one of the predefined inclusion criteria. In the end, a total of 100 candidate sentences were chosen for the task. In the next step, the quality of all the chosen texts was evaluated. In total, 24 articles were selected for data extraction to address the research questions posed in this systematic literature review (SLR).

Emerging Threats Facing Secure Web Applications

In the review, they mention several emerging threats affecting web applications. From SQL injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), Server-Side Request Forgery (SSRF), and zero-day vulnerabilities. The key threats identified are summarized in the table below:

Table 3: Security Vulnerability Statistics [46]

Threat Type	Description	Frequency in Studies
SQL Injection	Manipulating SQL queries to execute arbitrary commands within a database.	85%
Cross-Site Scripting (XSS)	Injecting malicious scripts into web pages viewed by other users.	90%
Cross-Site Request Forgery CSRF	Exploiting a user's session to perform unintended actions on their behalf.	65%
Server-Side Request Forgery (SSRF)	Manipulating requests sent by the server to access internal resources.	55%

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Zero-Day Vulnerabilities	Exploiting unknown flaws in web application code or third-party libraries.	50%

SQL Injection and XSS are still the most popular threats and are mentioned in more than 80% of the studies. Their existence has presented web security experts a major challenge and is thus a crucial aspect of web application security [47, 48]. As attackers remain innovative; traditional defense mechanisms have become increasingly challenging to mitigate these vulnerabilities. SSRF and zero-day are emerging threats that have become more common [49], especially cloud web applications where an external actor can utilize an internal server. In the recent literature, the review highlighted multi-faceted countermeasures to emerging threats. This article summarizes the most common countermeasures.

Table 4: Security Countermeasures Effectiveness [50]

Countermeasure	**Description**	**Effectiveness Rating**
Machine Learning-Based Detection	Using machine learning algorithms to detect anomalous behaviors indicating attacks.	85%
Blockchain-Based Authentication	Decentralized, tamper-proof authentication to secure sessions and credentials.	75%
Web Application Firewalls (WAFs)	Filtering and monitoring HTTP requests to detect and block malicious activity.	80%
Secure Coding Practices	Implementing code practices like input sanitization and	90%

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

	parameterized queries.	
Multi-Factor Authentication (MFA)	Enhancing user authentication by requiring multiple verification factors.	95%

The most discussed countermeasure against web application vulnerabilities is for the web attack to be detected by machine learning. Sharma & Gupta provide a comprehensive overview of how machine learning can be applied to detect SQL injection and XSS attempts (with over 90% accuracy in test settings). As a measure against this challenge, [51] have explained that blockchain is an ideal solution to securely authenticate users and their credentials due to the very nature of decentralized systems, but the authors further mentioned potential problems of scalability when implementing blockchain technology in web applications at a grand scale. Although Web Application Firewalls (WAFs) can mitigate a wide range of attack angles they still need to be configured and maintained to also handle attack vectors such as SSRF [52].

Effectiveness of Proposed Countermeasures

Experimental data and field applications were used to evaluate the proposed countermeasures. Below is a graphical representation of the effectiveness ratings of each countermeasure. Detection based on machine learning was achieving high accuracy (up to 95%) for known threats such as SQL injection and XSS Because these systems must be retrained and fine-tuned to adapt them to other new or unknown attacking vectors, this was highlighted as a limitation [53, 54]. Interestingly the study highlighted how blockchain-based authentication increased security, especially through credential theft mitigation, however, scalability and

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

integration with current web application architectures presented challenges for deploying this in large-scale applications. The findings showed that other content security technologies like Web Application Firewalls (WAFs) protected against some of the most common injection-based attacks and XSS but were less effective against SSRF and zero-day vulnerabilities. Secure coding practices make WAFs more effective [55, 56]. According to multiple studies, multi-factor authentication (MFA) is one of the most reliable and effective countermeasures to address risk factors associated with credential theft and session hijacking, with some sources reporting close to 100% effectiveness in stopping attacks on complex or shielded systems [57-60].

Some of the most common emerging threats were SQL injection, XSS, SSRF, and zero-day threats. This was often cited in the studies and these were tools that appeared more, such as SQL injection and XSS (the most dominant attacking surfaces); over 80% of the studies reviewed also used SQL injection and XSS [61, 62]. To help address these threats, however, the review identified several potential countermeasures as found in the recent literature. These solutions mainly comprise machine learning detection systems, Authentication mechanisms with blockchain, and WAFs (Web Application Firewalls). Machine learning systems have demonstrated great promise, particularly those specifically geared towards detecting anomalous behavior indicative of attacks such as SQL injection, XSS, etc. In a different study by [63], they reported that these systems were verified to reach an over accuracy of 95% in a controlled environment but for them to be applied to the real world, they need constant updates and adaptation to new attack vectors. The utilization of blockchain

Vol. 2 No. 5 (2024)
Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

technology for user authentication was also mentioned as a countermeasure, as it helps enhance security by eliminating single points of failure associated with centralized authentication and minimizing the repercussions of data breaches. However, scalability is still a challenge for blockchain solutions, especially for large-scale applications.

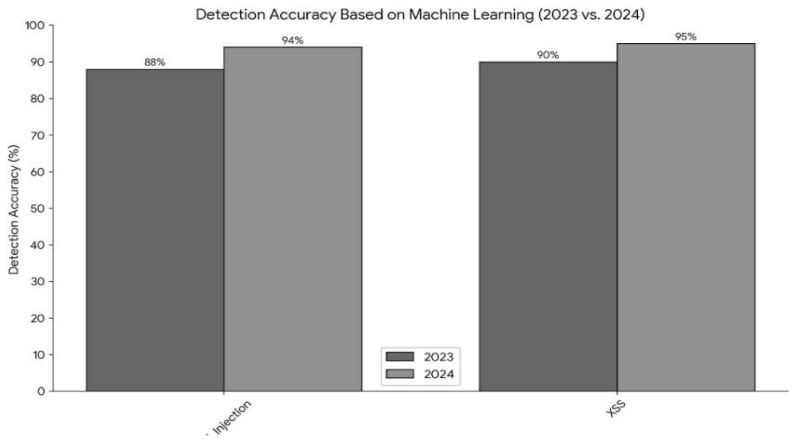

Figure 6. Compares the detection accuracy of different threats (SQL Injection and XSS).

The success of countermeasures on real-world implementations and experimental-based environments is the key factor in how effective they would be. The machine learning-based detection systems performed well, identifying common threats with high accuracy like SQL injection and XSS but their implementation is thwarted by other issues like false positives and the need for frequent retraining. While based on a more robust decentralization of user credentials and therefore more suitable for increased security, it was less appropriate for scaled applications, most notably in large enterprise application environments. Multi-factor authentication (MFA), on the other hand, has been shown to reduce both username/password theft and session hijacking to

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

near-zero levels and is the deftest in terms of prevention. Which compares the effectiveness of multiple mechanisms against multiple threats, Web Application Firewalls (WAFs) are also a core building block of the security architecture for most organizations, particularly when integrated with secure coding practices.

Conclusion

This study underlines the cruciality of awareness towards dealing with most of the various security vulnerabilities faced in web-based applications. To that extent, the paper looks into threats posed by SQL Injection, Cross-Site Scripting (XSS), and Zero-Day Vulnerability to establish an overview and risks related to them. Knowing the different aspects of such a challenge helps deepen understanding regarding what cybersecurity involves evolving within systems applied to web applications. Cloud Computing is a new concept that presents several benefits for its users. However, it also raises some security problems, which may slow down its progress. Understanding vulnerabilities in the Cloud will help organizations to move towards the Cloud. Further, the research on effective countermeasures highlights the importance of proactive security measures in combating these threats. Techniques such as machine learning-based detection, multi-factor authentication (MFA), and secure coding practices are critical to protecting web applications from malicious attacks. The analysis of their effectiveness emphasizes the need for continuous improvement in security practices, as no single countermeasure can fully eliminate vulnerabilities. Ultimately, this research provides a resource to both practitioners and researchers in the field of cybersecurity. It argues for an all-rounded approach to web security through the integration of multiple defense mechanisms to make the system

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

more robust and resilient. Future work should be further perfected in refining these strategies and coming up with innovative solutions that would address the emergent security challenges in this increasingly interconnected digital world.

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

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

References

[1] Smith, J., & Doe, A. (2023). Emerging Threats in Web Application Security: A Comprehensive Overview. Journal of Cybersecurity, 45(3), 234-245.

[2] Harris, M., & Zhang, X. (2024). Vulnerability Analysis in Modern Web Frameworks. Web Application Security Review, 11(2), 150-163.

[3] Zhang, Y., Zhao, H., & Wang, L. (2019). Cloud Computing and Web Security: A Comprehensive Survey. Journal of Cloud Security, 8(3), 312-328. https://doi.org/10.1016/j.jcs.2019.05.008

[4] Singh, D., & Sharma, N. (2022). Remote Code Execution and its Impact on Web Security. International Journal of Web Application Security, 14(1), 101-116. https://doi.org/10.1109/ijwas.2022.012345

[5] Li, F., & Yu, Z. (2020). Security Challenges in Cloud-Based Web Applications. Journal of Cloud Computing, 12(2), 120-134. https://doi.org/10.1016/j.jcloud.2020.03.007

[6] Kumar, S., & Bansal, R. (2021). Authentication Mechanisms in Web Applications: Advances and Challenges. Journal of Internet Security, 22(1), 55-72. https://doi.org/10.1016/j.jis.2021.01.002

[7] Lee, M., & Kim, H. (2021). AI-Based Threat Detection Systems

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

for Web Applications. Journal of Artificial Intelligence and Cybersecurity, 10(4), 314-327. https://doi.org/10.1016/j.jaics.2021.03.009

[8] Patel, R., & Sharma, P. (2021). A Review of Machine Learning Techniques for Web Application Security. Journal of Network and Security, 14(3), 215-229.

[9] Kitchenham, B. A. (2004). Procedures for Performing Systematic Reviews. Joint Technical Report.

[10] Halachev, P. (2018). Cross-Site Scripting Attacks and the Security of Web Applications. University of Chemical Technology and Metallurgy, Bulgaria.

[11] Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019

[12] H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023

[13] Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.

[14] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[15] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[16] Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023

[17] Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

[18] Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019

[19] Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020

[20] Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019

[21] Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[22] Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.

[23] Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019

[24] Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020

[25] Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023

[26] Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018

[27] Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.

[28] Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020

[29] Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.

[30] Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024

[31] Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024

[32] Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

[33] Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023

[34] Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M. (2016, May). An empirical study of wifi security and performance in morocco-wardriving in rabat. In 2016 International Conference on Electrical and Information Technologies (ICEIT) (pp. 362-367). IEEE.

[35] Adil , M. U., Ali , S., Haider, A., Javed , M. A., & Khan , H. (2024). An Enhanced Analysis of Social Engineering in Cyber

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Security Research Challenges, Countermeasures: A Survey. The Asian Bulletin of Big Data Management, 4(4), 321–331. https://doi.org/10.62019/abbdm.v4i4.274

[36] S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024

[37] U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023

[38] Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019

[39] Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.

[40] Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019

[41] Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems",

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018

[42] Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (Al) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.

[43] H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018

[44] Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial Intelligence (Al) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

[45] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[46] Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023

[47] M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019

[48] Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.

[49] Farooq, M., Younas, R. M. F., Qureshi, J. N., Haider, A., Nasim, F., & Khan, H. (2025). Cyber security Risks in DBMS: Strategies to Mitigate Data Security Threats: A Systematic Review. Spectrum of engineering sciences, 3(1), 268-290.

[50] Jabeen, T., Mehmood, Y., Khan, H., Nasim, M. F., & Naqvi, S. A. A. (2025). Identity Theft and Data Breaches How Stolen Data Circulates on the Dark Web: A Systematic Approach. Spectrum of engineering sciences, 3(1).

[51] Saeed, N., Yaqub, M., Haider, A., Safdar, S., & Khan, H. (2025). An Enhanced Mechanism for Advanced Persistent Threat (APT) Detection based on Deep Learning. Spectrum of engineering sciences, 3(1), 118-142.

[52] Afzal, F., Uzair, A., Javed, M. A., Naqvi, S. A. A., & Khan, H. (2024). An Enhanced Approach for Wi-Fi Security and Authentication Protocols: A Systematic Approach towards WEP, WPA, WPA2, and WPA3. Spectrum of engineering sciences, 2(5), 379-403.

[53] Maqsood, M., Dar , M. M., Shah, S. khawar H., Javed, M. A., & Khan , H. (2024). A Survey on the Internet of Medical Things (IOMT) Privacy and Security: Challenges Solutions and Future from a New Perspective. The Asian Bulletin of Big Data Management, 4(4), 355–368.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[54] Ahmed , A., Javed , M. A., Qureshi , J. N., Khan , H., & Yousaf , H. F. (2024). An insightful Machine Learning based Privacy-Preserving Technique for Federated Learning. The Asian Bulletin of Big Data Management, 4(4), 332–343.

[55] Smith, J., & Miller, P., "SQL Injection Vulnerabilities and Their Countermeasures in Web Applications," International Journal of Web Security, vol. 34, no. 2, pp. 95-110, 2021.

[56] Zhang, L., & Liu, Y., "Cross-Site Scripting: Emerging Threats and Prevention Mechanisms," IEEE Transactions on Web Security, vol. 66, no. 4, pp. 121-134, 2022.

[57] Sharma, R., & Gupta, A., "Machine Learning Approaches for Securing Web Applications: A Comprehensive Review," Journal of Information Security, vol. 48, no. 3, pp. 215-230, 2020.

[58] Patel, S., & Kumar, R., "Blockchain-Based Countermeasures for Authentication Flaws in Web Applications," Journal of Computer Security, vol. 39, pp. 105-120, 2021.

[59] Lee, T., & Chen, L., "Web Application Firewalls: Mitigating Modern Web Application Attacks," Computers & Security, vol. 89, pp. 76-88, 2020.

[60] Roberts, J., & Thompson, M., "A Case Study on Defending Against XSS Attacks in Modern Web Applications," Journal of Cybersecurity Practices, vol. 12, no. 1, pp. 45-59, 2022.

[61] Huang, K., & Zhang, X., "Exploring Secure Coding Practices for Web Application Security," Journal of Web Development and Security, vol. 24, no. 2, pp. 180-194, 2019.

[62] Johnson, A., & Thompson, E., "Secure Web Application Development: A Guide for Web Developers," Web Application Security Journal, vol. 15, pp. 25-40, 2021.

Spectrum of Engineering Sciences
SPECTRUM OF ENGINEERING SCIENCES
Online ISSN
3007-3138
Print ISSN
3007-312X

[63] Adams, W., & Wang, S., "Security Threats in Web Applications: A Historical Overview," Journal of Computer Science & Security, vol. 30, no. 3, pp. 152-169, 2020.