Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606

Volume 07 Issue 01
2024

Research Article
https://doi.org/10.56979/701/2024

A Comprehensive Survey on Security Threats and Challenges in Cloud Computing Models (SaaS, PaaS and IaaS)

Ezzah Fatima[1*], Irshad Ahmad Sumra[1], and Rania Naveed[1]

[1]Department of Information Technology, Lahore Garrison University, Lahore, 54000, Pakistan.
Corresponding Author: Ezzah Fatima. Email: ezzahfatima186@gmail.com

Received: November 09, 2023 **Accepted:** May 01, 2024 **Published:** June 01, 2024

Abstract: Cloud computing has fundamentally transformed data access, storage, and processing for individuals and businesses alike, offering unparalleled scalability, flexibility, and cost-effectiveness through Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) models. However, as with any revolutionary paradigm shift, cloud computing is not without its challenges and concerns, cybersecurity being chief among them. This research article examines security challenges and attacks in each cloud computing model, with SaaS SQL injection and deceitful QR code attacks highlighted, PaaS facing vulnerabilities like unauthorized access addressed through the Multi-Perspective PaaS Security Model, and IaaS confronting issues such as data breaches by emphasizing shared responsibility. To address these challenges and concerns, this study proposes and explores potential solutions, such as integrating machine learning and encryption techniques to mitigate vulnerabilities and enhance the security posture of cloud platforms. By discussing relevant literature and conducting comparative analysis of existing works, this study also identifies research gaps and trends that need to be addressed in the future, including emerging threats and standardization of cloud security measures that would contribute to the establishment of industry-wide standards and effective countermeasures in cloud computing. The findings of this study underscore the critical importance of collaborative efforts between users and Cloud Service Providers (CSPs) in addressing cybersecurity concerns, as well as the need to enhance user awareness and adopt robust longitudinal studies to mitigate future security risks. Ultimately, this research aims to provide a comprehensive understanding of evolving security landscapes in cloud computing, and contribute to the establishment of industry-wide standards and effective countermeasures in cloud computing.

Keywords: Cloud Computing; Software as a Service (SaaS); Platform as a Service (PaaS); Infrastructure as a Service (IaaS); SQL Injection; Deceitful QR Code Attacks; Multi-Perspective PaaS Security Model.

1. Introduction

Cloud computing has transformed the way organizations access, store, and process data, enabling unparalleled scalability, flexibility, and cost-effectiveness. However, this transformative shift comes with its unique challenges, particularly in the realm of cybersecurity. In this paper, we aim to examine the security challenges and attacks that each cloud computing model, namely Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), is facing. By doing so, we intend to identify potential vulnerabilities, recommend solutions to mitigate them, and propose a comprehensive guide for making cloud services safer and mitigating risks associated with cloud adoption. Our study emphasizes the critical role of collaborative efforts between users and Cloud Service Providers (CSPs) to ensure the security of cloud computing. Additionally, we highlight the importance of enhancing user awareness and establishing industry-wide standards in cloud security. Through our research, we aim to contribute to a more comprehensive understanding of evolving security landscapes and effective countermeasures in cloud computing.

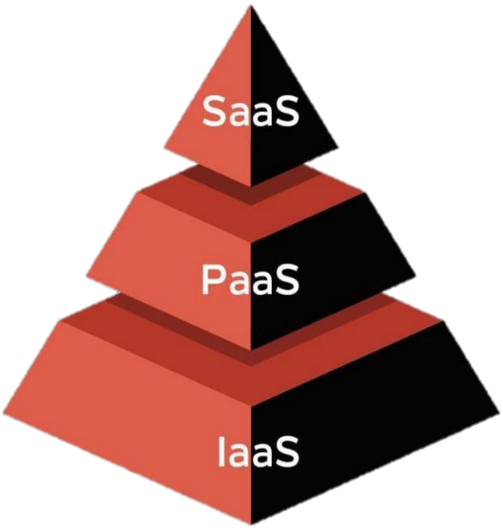

Figure 1. Cloud Models

As organizations increasingly adopt SaaS solutions for their cost-effectiveness and ease of implementation, Tripathy et al.[1] highlight the often-overlooked vulnerabilities that accompany such products. The focus on SQL injection attacks exposes a critical facet of SaaS security, emphasizing the importance of understanding and mitigating potential threats to safeguard sensitive information. Moving beyond SaaS, the review delves into the intricacies of PaaS security. Isharufe et al. [5] underscore the benefits of PaaS, such as scalability and faster time-to-market, but concurrently identify critical security issues. The proposal of a security model, the Multi-perspective PaaS Security Model (MPSM), suggests a holistic approach to mitigate vulnerabilities and enhance the overall security posture of PaaS platforms. The exploration extends to IaaS, where Chawki et al. [10] discuss security challenges inherent in the virtualized IT resources provided by the IaaS model. The study emphasizes the shared responsibility model, acknowledging the collaborative efforts required by both users and Cloud Service Providers (CSPs) to ensure the security of IaaS.

The motivation behind this literature review is to comprehensively explore the security challenges and attacks faced by SaaS, PaaS, and IaaS models. By understanding the nuances of these issues, organizations can make informed decisions, implement robust security measures, and mitigate potential risks associated with cloud adoption.

While cloud services have many benefits, not everyone knows enough about the security risks. This review of existing studies shows that organizations need to focus on problems like SQL injection and collusion attacks that are specific to different types of cloud services. A key contribution from this research is that it sorts out the attacks based on how cloud services are delivered. There are three main ways: IaaS, PaaS, and SaaS. By understanding the unique security issues with each, organizations can better protect themselves against problems in the cloud. This study aims to give a clear guide for making cloud services safer and helping people make smart choices about using them.

The structure of the paper is as follows: A thorough survey of the literature is given in Section 2, exploring the security challenges and attacks associated with SaaS, PaaS, and IaaS models. Section 3 conducts a comparative analysis of the existing works, highlighting the key focuses, methods employed, major findings, and types of attacks discussed in each study. Following the comparative analysis, Section 4, conclude the research paper with some detail discussion with future direction of research study.

2. Literature Review

This literature review explores the security challenges and attacks, targeting SaaS, PaaS, and IaaS models respectively. Tripathy et al. [1] discussed that organizations often adopt low cost and easy implementing SaaS products that comes with their own set of vulnerabilities. Because the organization is unaware of these, they do not know how to protect them. Also, cloud's APIs are available on the internet making the customers using it more prone to those vulnerabilities. The authors focused on SQL injection attacks, that is of different types such as error-based in which attacker can retrieve the table names and information residing in them, Boolean-based where the attacker inserts a condition in the SQL query and command the database to sleep for a set amount of time, if the page quickly loads it is not vulnerable and if the page takes longer to load it is vulnerable ,in time-based, the attacker change the function to make it execute with a time delay and in out-of-band SQLi, the attacker directly sends data (often time username and passwords) from the database to an attacker- controlled machine. The authors used different classifiers such as random forest classifier, AdaBoost classifier, deep ANN, decision tree and TensorFlow. The machine learning algorithm are trained on different malicious and benign payloads. They take the payload as input and decide whether they are malicious or not, from which random forest classifier gives the highest accuracy with an accuracy result more than 98% approximately 99.8%. The major challenge was the dataset, that the researcher created their own dataset by combining small datasets from the internet.

Sahay et al. [2] discussed the detection and prevention of deceitful QR code attacks in SaaS and various security risks, such as data leakage, malicious code injection, unauthorized access and service disruption. They also review the existing methods to mitigate these risks. This paper centers on two specific types of attacks in SaaS applications and databases, SQL injection, where attacker injects malicious code in SQL queries that could result in data loss or theft and collusion, which is when the attacker uses a fake id to access or share information. This study introduces a new approach to detect and prevent SQL injection and collusion attacks for deceitful QR code. This method combines machine learning (similarity algorithm), encryption (PBE with MD5 and DES), and role-based access control techniques through four modules: data uploading, encryption and decryption, data sharing, and access control and revocation. The method utilizes a similarity-based algorithm to identify SQL injection patterns, a password-based encryption scheme to ensure data confidentiality, and a role-based access control algorithm to manage data access and revocation. This paper achieves an accuracy rate for SQL injection 98.57% and for collusion an accuracy of 99.33%.

Soufiane et al. [3] discussed that SaaS is a promising cloud service that have extensive benefits, but faces plenty of security challenges and attacks like, DoS attack, authentication issues like MITM, key logger, phishing, SQL injection and XSS, side channel attacks, brute force and password reset attacks. The proposed solution of authors to enhance the security of SaaS involves using SSL, OTP, encryption, anonymization, classification, SOTA, CTB, IDS, and web application security scanners. The article also examines the security measures taken by major cloud providers like Google, Amazon, and Microsoft. It suggests authentication using one-time passwords (OTPs), encryption, and anonymization as effective security measures. The article concludes by emphasizing the significance of data security in SaaS and the need for reliable and flexible solutions.

Guillén et al. [4] offered a thorough analysis of SaaS security risks and defenses. The authors employed the SALSA framework for a systematic review to identify threats, attacks, and countermeasures aimed at mitigating security issues in a SaaS environment. The authors discuss various security threats that arise in SaaS environments, such as data breaches, unauthorized access, and denial of service attacks etc. They also examine different countermeasures that can be implemented to mitigate these threats, including encryption, access controls, and intrusion detection systems. The study presents a categorization of threats, attacks, and countermeasures based on the literature review of different selected papers. The research study so provides some general recommendations for improving the security of SaaS applications, such as using encryption, authentication, monitoring, and auditing. The figure 1 below lists down the attacks and their countermeasures mentioned in this paper.

Table 1. Summary of Attacks and their Countermeasures

Attack Type	Countermeasures
ARP Spoofing	Maintain an accurate ARP table, employ detection techniques, use encryption, and filtering.
Backdoor and Debug Options	Ensure that debugging options are disabled during software development.
Broken Authentication	Implement robust authentication and session management controls, and automate verification processes.
Buffer Overflow	Mitigate buffer overflow risks using instruction set randomization techniques.

Code Injection	Use content filtering and regularly update web application security measures.
Cookie Poisoning	Regularly clear cookies to prevent malicious cookie manipulation.
Cross- Site Request Forgery (CSRF)	Protect against CSRF attacks using secret tokens and validating referrer and origin headers.
DNS Poisoning	Utilize encryption and robust filtering mechanisms to safeguard against DNS attacks.
Dumpster Diving	Establish and enforce policies for secure disposal of sensitive documents.
Eavesdropping	Implement IPsec and comprehensive security policies, including antivirus solutions.
Economic Denial of Sustainability (EDoS)	Employ EDoS protection mechanisms and graphical Turing tests as recommended by experts.
Google Hacking	Avoid disclosing sensitive information and regularly scan for vulnerabilities.
Hash Value Manipulation	Develop and implement protocols to ensure the integrity of hash values.
Hidden Field Manipulation	Refrain from using hidden parameters for sensitive operations.
Malware Injection and Steganography	Deploy solutions like StegAD to detect and prevent malware and steganography attacks.
Man-in-the-Middle Attack	Strengthen security measures and employ tools like Dsniff, Cain, Ettercap, Wsniff, and Airjack.
Metadata Spoofing Attack	Encrypt critical service details and maintain robust authentication mechanisms.
Phishing Attack	Implement adaptive encryption algorithms, TLS, and HTTPS with valid certificates.
Port Scanning	Use port blocking techniques to restrict unauthorized access.
Race Condition	Apply predicate refresh techniques to prevent race condition vulnerabilities.
Replay Attack	Implement stochastic coding schemes for secure data transmission.
Reused IP Address	Regularly clear cached IP addresses to prevent reuse conflicts.
Service Injection Attack	Ensure strong isolation, reliable identification methods, and service integrity.
Shared Architectures	Conduct thorough binary code analysis to identify and fix vulnerabilities.
Sniffing	Utilize SSL, TLS, and IPsec to enhance communication security.
Social Engineering	Focus on comprehensive security policies and continuous staff training.
Sybil Attack	Implement symmetric key cryptography solutions to mitigate Sybil attacks.
User to Root Attack	Enforce strong password policies and robust authentication mechanisms.
XML Signature Wrapping Attack	Use automated scanning tools and manual verification to detect XML signature wrapping attacks.
Zombie Attack	Employ robust authentication, IDS/IPS systems, regular system scans, and packet filtering.

Isharufe et al. [5] discussed and provide overview of Platform-as-a-Service (PaaS) benefits like scalability, self-service, cost of ownership and faster time to market. But they also identify and analyzes critical security issues associated with PaaS such as unauthorized access, data segregation, securing hypervisor, account hijacking SAML attack etc. Along with mapping the relevant control criteria from the CSA cloud control matrix to the particular problems, the article offers recommendations based on administrative, operational, and technical considerations. In order to safeguard front-end functionalities such as management control, this study suggests that the CSP adopt (IAM) Identity Access Management controls such as IAM 2, IAM 5, and IAM 9. The authors also recommend that login credentials be sent using the most recent security measures and that CSPs offer multifactor authentication.

Yasrab [6] discussed that PaaS in cloud computing is vulnerable to security issues and vulnerabilities. To mitigate these vulnerabilities, the study proposes a security model called the Multi-prospective PaaS Security Model (MPSM). The MPSM includes tools and techniques, such as marble, secure torpors and IDS and guidelines to enhance the security of PaaS platforms. The security model addresses challenges such as data location, privileged access, DoS, MITM, ARP spoofing, information leakage, multi-tenancy, heterogeneity, and shared responsibility. The proposed security model focuses on protecting data in transmission, stored data, and data in processing. It also suggests the implementation of autonomic security, trusted cloud computing, IAM and virtualization security management presented in figure 2, to detect and mitigate intrusion attacks. The study highlights the unique nature of PaaS architecture that makes it more vulnerable to security and privacy attacks. Overall, the study provides insights into the security concerns of PaaS and offers solutions to ensure a more secure PaaS environment.

Table 2. PaaS Security Threats, Requirement and Mitigation Strategies

PaaS Security Threats	PaaS Security Requirements	Mitigation Strategies
Programming errors Software modifications Impersonation Session hijacking Traffic flow analysis Network Exposure Defacement Connection flooding Denial of Service Attacks Impersonation Communication disruption	Access control Application protection Data security Cloud management control security Secure pictures Protection for Virtual Clouds Communication Security	Reliable Cloud Computing Trusted hardware and software Encrypting devices Environment for Secure Execution and Communication Symmetric and homomorphic encryption Secret socket layer Protection of data in transmission, storage and processing Identity and Success Management (IAM) Authentication Authorization Traceability Virtualization Security Management Harding the VM Harden the Hypervisor Firewall additional VM ports Root Securing Monitor Service level agreements for cloud security Autonomic Security

Zhang et al. [7] discussed a new attack methodology for exploiting cache-based side channels in PaaS clouds, where multiple tenants share the same host operating system. The study demonstrates three attacks that can extract sensitive information from co-located tenants, such as user credentials, encryption keys, and application data. The study demonstrates how an adversary can exploit the shared executables and the FLUSH-RELOAD technique to trace the execution path of a victim instance and extract sensitive information across tenant boundaries. The challenges and strategies for achieving and detecting the co-location of an attacker instance with a victim instance in PaaS clouds is also discussed. The study proposes a co-location detection method that leverages the attack NFA and a rare execution path in the victim application. It also validates the co-location detection method using IP address comparison and reports the results of co-location experiments on two public PaaS clouds, Dot Cloud and OpenShift. The study also presents three examples of how the attack framework can be applied to achieve different attack goals, such as inferring user data, hijacking user accounts, and breaking XML encryption schemes [23] [25].

Dinakar [8] presented a survey of the concept of virtualization and its different types such as application, hardware, network, and storage virtualization in cloud computing. The study also discusses the role of hypervisor or virtual machine monitor (VMM) in cloud computing, which is a software that allows multiple virtual machines (VMs) to run on the same physical hardware. The study identifies some of the security challenges and attacks on cloud infrastructure and VMM, such as co- residential attacks, cache-based side-channel attacks, VM escape, and SQL injection. The study concludes that virtualization is a key enabling technology of the cloud, but also poses potential security risks that need to be addressed.

Almadhoor et al. [9] discussed the detection of malware infections on infrastructure hosted in IaaS (Infrastructure as a Service) cloud environments using cloud visibility and forensics. The paper classifies malware attacks into four categories: resource abuse, data theft, data tampering, and denial of service. The paper proposes the best methods to collect, analyze, and correlate data from various sources, such as API calls, host logs, network flows, and cloud resources, to detect malicious activities and indicators of compromise. The paper also suggests the best practices to perform digital forensics on cloud- hosted assets, such as capturing disk and memory images, event data and logs, and network packet captures. The paper evaluates the existing technologies and methodologies for monitoring and forensics in the cloud and identifies the challenges and limitations of each approach. It also discusses the importance of cloud visibility and the use of tools such as SIEM (Security Information and Event Management) software and SIFT (SANS Investigative Forensic Toolkit) for effective detection and response to malware attacks in the cloud.

Chawki et al. [10] discussed about security issues and solutions in the IaaS cloud model, which provides virtualized IT resources as on-demand services. The study explores the security challenges and vulnerabilities in different components of the IaaS model, such as virtualization, data storage, networking, cloud software, utility computing, and SLA. The study also discusses the CSA Top 12 threats, data breaches, system vulnerabilities, account hijacking, insecure APIs, DoS, malicious insiders, abuse of cloud services, insufficient due diligence, shared technology issues, insufficient identity, credential and access management, data loss, advanced persistent threats, to cloud computing and their impact on the IaaS model security, as well as some proposed cryptographic and security techniques to mitigate them. The study concludes that IaaS model security is a shared responsibility between the user and the CSP, and that several researches have been proposed to achieve a certain level of security in the IaaS model [24].

3. Comparative Analysis of Existing Work

The Table 3 contains a comparative analysis of existing work for SaaS, PaaS and IaaS of cloud models.

Table 3. Comparative Analysis of Existing Work

Authors	Cloud Model	Major Findings	Attacks	Proposed Solution	Dataset
Tripathy et al. [1]	SaaS	SQL injection vulnerabilities, ML accuracy ~99.8%	SQL Injection (Various Types)	ML for Payload Analysis, Random Forest classifier	Combined small GitHub datasets
Sahay et al. [2]	SaaS	ML Similarity algorithm, Encryption, Role-based Access Control	SQL Injection, Collusion Attacks	High accuracy in detection and prevention (98.57% and 99.33%)	Normative training set
Soufiane et al. [3]	SaaS	SSL, OTP, Encryption, Anonymization, ML	DoS, MITM, Key Logger, Phishing, SQL Injection, XSS, Brute Force, Password Reset	Enhanced security using SSL, OTP, encryption	HIDS and NIDS analyzed network packets
Guillén et al. [4]	SaaS	Systematic review with SALSA Framework	Data Breaches, Unauthorized Access, DoS	Encryption, authentication, monitoring	Selected 47 out of 6723 articles
Isharufe et al. [5]	PaaS	IAM Controls, Multifactor Authentication, SAML	Unauthorized Access, Data Segregation, SAML Attacks	IAM controls, multifactor authentication	Literature review
Yasrab [6]	PaaS	Autonomic Security, Trusted Cloud	Data Location, Privileged Access, DoS, MITM, Information	Multi-perspective PaaS Security Model	Tools: marble, secure tropos, IDS

		Computing, IAM	Leakage, Multi-Tenancy		
Zhang et al. [7]	PaaS	Exploitation Techniques, Co-location Detection	Cache-Based Side Channel Attacks	Co-location detection methods	Demonstrated on commercial clouds
Dinakar [8]	IaaS	Survey of Security Challenges	Co-Residential, Cache-Based Side-Channel, VM Escape, SQL Injection	Discusses virtualization and security challenges	Multiple literature sources
Almadhoor et al. [9]	IaaS	Classification of Malware Attacks, Forensic Techniques	Resource Abuse, Data Theft, Data Tampering, DoS	Cloud visibility, forensic practices	API call logs, host log, CloudWatch logs
Chawki et al. [10]	IaaS	Exploration of IaaS Security Challenges	Data Breaches, System Vulnerabilities, Account Hijacking, Insecure APIs, DoS, Malicious Insiders	Shared responsibility, cryptographic solutions	Reviewed CSA top 12 threats

The literature review reveals a diverse range of security challenges across SaaS, PaaS, and IaaS models, showcasing an integration of multifaceted approaches, including machine learning and encryption. Notably, the studies emphasize a shared responsibility model, particularly in IaaS, underscoring the need for collaborative efforts between users and Cloud Service Providers (CSPs) [19] [20]. However, research gaps emerge, such as a limited exploration of emerging threats, the absence of standardized security measures, insufficient focus on user awareness, and a scarcity of longitudinal studies. Future research should address these gaps to provide a more comprehensive understanding of evolving security landscapes and contribute to the establishment of industry-wide standards and effective countermeasures in cloud computing [23].

4.Conclusion and Future Work

In this review paper, it has been provided the understanding and mitigation of security challenges in cloud computing models by making several key contributions. We conducted an extensive review of the existing literature on security challenges and attacks specific to SaaS, PaaS, and IaaS cloud models, identifying key areas of vulnerability and common attack types such as SQL injections, cross-site scripting (XSS) [22] [24], and data breaches. By analyzing high-quality papers, we provided a consolidated view of the current state of cloud security. Additionally, we performed a detailed comparative analysis of various security solutions proposed in the literature, categorizing them based on their applicability to different cloud models and assessing their effectiveness using key metrics. This analysis highlighted the strengths and weaknesses of each approach, providing a clear picture of the most promising techniques for each cloud model. Based on the gaps identified in the literature review and comparative analysis, we proposed a set of advanced security solutions integrating modern technologies such as machine learning for anomaly detection, advanced encryption techniques for data protection, and robust authentication mechanisms to prevent unauthorized access. These solutions are designed to be scalable and adaptable to the evolving threat landscape. We also identified several critical research gaps that need to be addressed to enhance cloud security, including the need for standardized security measures across different cloud models, the development of more effective threat detection techniques, and the importance of addressing emerging threats. Our study provides a roadmap for future research, emphasizing areas that require further exploration and development. Moreover, our research has practical implications for cloud service providers, developers, and users, offering actionable recommendations that can be implemented to enhance the security of cloud-based applications and services. These recommendations aim to help stakeholders better understand and mitigate the risks associated with cloud computing. Overall, the contributions of this study provide a comprehensive understanding of the security challenges in cloud computing and propose advanced solutions to address these challenges, synthesizing existing knowledge and paving the way for future research and practical implementations to improve cloud security across SaaS, PaaS, and IaaS models.

References

1. Tripathy, D., Gohil, R., & Halabi, T. (2020, May). Detecting SQL injection attacks in cloud SaaS using machine learning. In 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS) (pp. 145-150). IEEE.
2. Sahay, M., Vanjale, S., & Mane, M. (2024). Software As Service Attack Detection and Prevention for Deceitful QR code. International Journal of Intelligent Systems and Applications in Engineering, 12(4s), 454-462.
3. Soufiane, S., & Halima, B. (2017). SaaS Cloud Security: Attacks and Proposed solutions. Transactions on Machine Learning and Artificial Intelligence,
4. Díaz de León Guillén, M. Á., Morales-Rocha, V., & Fernández Martínez, L. F. (2020). A systematic review of security threats and countermeasures in SaaS. Journal of computer security, 28(6), 635-653.
5. Isharufe, W., Jaafar, F., & Butakov, S. (2020, June). Study of security issues in platform-as-a- service (paas) cloud model. In 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE) (pp. 1-6). IEEE.
6. Yasrab, R. (2018). MPSM: Multi-prospective PaaS Security Model. arXiv preprint arXiv:1804.04731.
7. Zhang, Y., Juels, A., Reiter, M. K., & Ristenpart, T. (2014, November). Cross-tenant side- channel attacks in PaaS clouds. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 990-1003).
8. Dinakar, K. R. (2019). A survey on virtualization and attacks on virtual machine monitor (VMM). Int. Res. J. Eng. Techn., 6(3), 6558-6563.
9. Almadhoor, L., bd El-Aziz, A. A., & Hamdi, H. (2021). Detecting Malware Infection on Infrastructure Hosted in IaaS Cloud using Cloud Visibility and Forensics. International Journal of Advanced Computer Science and Applications, 12(6).
10. Chawki, E.B., Ahmed, A., & Zakariae, T. (2018). IaaS cloud model security issues on behalf cloud provider and user security behaviors. Procedia computer science, 134, 328-333.
11. Halfond, W. G., & Orso, A. (2005, November). AMNESIA: analysis and monitoring for NEutralizing SQL-injection attacks. In Proceedings of the 20th IEEE/ACM international Conference on Automated software engineering (pp. 174-183).
12. Ross, K., Moh, M., Moh, T. S., & Yao, J. (2018, March). Multi-source data analysis and evaluation of machine learning techniques for SQL injection detection. In Proceedings of the ACMSE 2018 Conference (pp. 1-8).
13. Jemal, Ines, et al. "Sql injection attack detection and prevention techniques using machine learning." International Journal of Applied Engineering Research 15.6 (2020): 569-580.
14. Chowdhury, Shreya, et al. "A Comprehensive Survey for Detection and Prevention of SQL Injection." 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS). Vol. 1. IEEE, 2021.
15. Mettildha Mary, P.V.Kavitha, Priyadharshini M, Vigneshwer S Ramana. Secure Cloud ComputingEnvironmentagainst DDOS and EDOS Attacks. 2014
16. Ajey Singh, Dr. ManeeshShrivastava. Overview of Attacks on Cloud Computing. 2014
17. Swain, S., & Tiwari, R. K. (2020). Cloud security research-a comprehensive survey. Int. J. of Electronics Engineering and Applications, 8(2), 29-39.
18. PADMA, M. A. P., & BHOI, R. Attacks on cross-tenant spatial multiplexing in PaaS clouds.]
19. Abbas, F., Iftikhar, A., Riaz, A., Humayon, M., & Khan, M. F. (2024). Use of Big Data in IoT-Enabled Robotics Manufacturing for Process Optimization. Journal of Computing & Biomedical Informatics, 7(01), 239-248.
20. Ammar Ahmad Khan , Muhammad Arslan , Ashir Tanzil , Rizwan Abid Bhatty , Muhammad Asad Ullah Khalid , Ali Haider Khan. (2024). Classification Of Colon Cancer Using Deep Learning Techniques On Histopathological Images. Migration Letters, 21(S11), 449–463
21. Muhammad Kaleem , Muhammad Azhar Mushtaq , Uzair Jamil , Sadaqat Ali Ramay , Tahir Abbas Khan , Siraj Patel , Rizwan Zahidy , Sayyid Kamran Hussain. (2024). New Efficient Cryptographic Techniques For Cloud Computing Security. Migration Letters, 21(S11), 13–28. Retrieved from https://migrationletters.com
22. Ahmed, F., Sumra, I. A., & Jamil, U. (2024). A Comprehensive Review on DDoS Attack in Software-Defined Network (SDN): Problems and Possible Solutions. Journal of Computing & Biomedical Informatics, 7(01).
23. Shah, A. M., Aljubayri, M., Khan, M. F., Alqahtani, J., Sulaiman, A., & Shaikh, A. (2023). ILSM: Incorporated Lightweight Security Model for Improving QOS in WSN. Computer Systems Science & Engineering, 46(2).

24. Khan, A. H., Malik, H., Khalil, W., Hussain, S. K., Anees, T., & Hussain, M. (2023). Spatial Correlation Module for Classification of Multi-Label Ocular Diseases Using Color Fundus Images. Computers, Materials & Continua, 76(1).
25. Ullah, S., Iqbal, N., Khan, A. H., Sajid, M., Ahmad, Z., Ahmad, H., & Hussain, M. (2023). EMPOWERING AGRICULTURE: A GREEN REVOLUTION WITH INTERNET OF ENERGY-DRIVEN FARM ENERGY MANAGEMENT FOR SUSTAINABLE AND ECO-FRIENDLY PRACTICES. Journal of Population Therapeutics and Clinical Pharmacology, 30(19), 975-992.