المجلة الدولية لتكنولوجيا التعليم والمعلومات
International Journal of Education and Information Technology
مجلة علمية – دورية – محكمة – مصنفة دولياً

# اتجاهات الثغرات في البنية التحتية السحابية: دراسة تجريبية لسجلات CVE في Azu و AWS

**أ. رنا كابلي** (١)
١- كلية الأعمال والابتكار والتقنيات الرائدة (BILT)، جامعة ماريماونت، أرلينغتون، الولايات المتحدة.
**د. ميشيل شيانغ ليو**(٢)
٢- كلية الأعمال والابتكار والتقنيات الرائدة (BILT)، جامعة ماريماونت، أرلينغتون، الولايات المتحدة.

تاريخ استلام البحث: ٢٠٢٥/٥/٢٠م تاريخ قبول نشر البحث: ٢٠٢٥/٦/٣م

**E-mail: Rhk57098@marymount.edu**

**الكلمات المفتاحيّة:**
الثغرات الأمنية، الحوسبة السحابية، أمازونAWS، مايكروسوفت Azure

**مستخلص البحث:**

أصبحت الحوسبة السحابية عنصرًا أساسيًا في التحول الرقمي الحديث، لما توفره من مرونة وقابلية للتوسع وكفاءة في التكاليف. وعلى الرغم من مزاياها، فإن تبني الحوسبة السحابية يجلب تحديات أمنية جديدة، خصوصًا في ظل نموذج المسؤولية المشتركة. أجرى هذا البحث تحليلًا تجريبيًا لسجلات الثغرات والتهديدات الأمنية (CVE) الخاصة بمنصتي أمازون ويب سيرفيسز (AWS) ومايكروسوفت أزور (Azure) خلال الفترة من ٢٠١٩ إلى ٢٠٢٥، بهدف الكشف عن الأنماط المرتبطة بتكرار هذه الثغرات وشدتها وأنواعها. وبالاعتماد على بيانات من قاعدة البيانات الوطنية للثغرات(NVD) ، تم تطبيق تقنيات تصفية باستخدام بايثون لعزل الثغرات المتعلقة بـ AWS و.Azure تشير النتائج إلى أن الثغرات مثل البرمجة عبر المواقع-CWE) (79، والتزوير في طلبات الخادم(CWE-918) ، وضعف التحكم في الوصول (CWE-284) من بين الأكثر شيوعًا، وغالبًا ما ترتبط بسوء إعدادات المستخدم أو ممارسات التطوير غير الآمنة. يبرز البحث تزايدًا في ثغرات SSRF ومشاكل التحكم في الوصول، مما يعكس فجوات مستمرة في تنفيذ سياسات IAM وأمن واجهات البرمجة. كما تكشف التحليلات الزمنية عن تذبذب في نمط الإفصاح عن الثغرات، مع عودة ملحوظة لثغرات XSS في السنوات الأخيرة، وهو ما يرتبط بتعقيد التطبيقات السحابية الحديثة.
بالإضافة إلى مساهماته التقنية، يولي هذا البحث اهتمامًا خاصًا بآثار أمان الحوسبة السحابية على المؤسسات الأكاديمية في المملكة العربية السعودية، والتي تعتمد بشكل متزايد على منصات AWSو Azureلدعم التعلم الإلكتروني والبحث والعمليات الإدارية. ويكشف التحليل أن سوء الإعدادات وثغرات طبقة التطبيقات تمثل مخاطر حرجة على هذه المؤسسات، التي غالبًا ما تعمل في بيئات هجينة ولا مركزية. واستنادًا إلى النتائج، يقدم البحث توصيات عملية للأمن السيبراني مصممة خصيصًا للبيئات الأكاديمية، مع التركيز على ممارسات التطوير الآمن، والانضباط في التحكم في الوصول، والمراقبة المستمرة للثغرات

# TRENDS IN CLOUD INFRASTRUCTURE VULNERABILITIES: AN EMPIRICAL STUDY OF AWS AND AZURE CVE RECORDS

**Rana Kabli**[1]
1The College of BILT, Marymount University, Arlington, USA.
**Dr. Michelle Xiang Liu**[2]
2The College of BILT, Marymount University, Arlington, USA.

**KEY WORDS:**
Security vulnerabilities, Cloud computing, Amazon AWS, Microsoft Azure.

**ABSTRACT:**

Cloud computing has become a core enabler of modern digital transformation, offering flexibility, scalability, and cost efficiency. Despite its advantages, cloud adoption introduces new security challenges, particularly under the shared responsibility model. This study conducted an empirical analysis of Common Vulnerabilities and Exposures (CVE) records specific to Amazon Web Services (AWS) and Microsoft Azure from 2019 to 2025, with the aim of uncovering patterns in vulnerability frequency, severity, and types. Using data sourced from the National Vulnerability Database (NVD), the research applied Python-based filtering techniques to isolate AWS- and Azure-related vulnerabilities. Findings indicate that vulnerabilities such as Cross-Site Scripting (CWE-79), Server-Side Request Forgery (CWE-918), and Improper Access Control (CWE-284) are among the most prevalent, often linked to user-side misconfigurations and insecure development practices. The study highlights a rising trend in SSRF and access control flaws, emphasizing persistent gaps in IAM policy implementation and API security. A temporal trend analysis reveals fluctuating disclosure patterns, with a notable resurgence of Cross-Site Scripting vulnerabilities in recent years, likely tied to the increased complexity of cloud-native applications. In addition to its technical contributions, this study places a special focus on the cloud security implications for academic institutions in Saudi Arabia, which are increasingly adopting AWS and Azure platforms to support e-learning, research, and administrative operations. The analysis reveals that misconfigurations and application-layer vulnerabilities pose critical risks to these institutions, which often operate in decentralized and hybrid IT environments. Based on the findings, the study provides practical cybersecurity recommendations tailored to academic settings, emphasizing secure development practices, access control discipline, and continuous vulnerability monitoring.

**Introduction:**

Recently, cloud computing has emerged as a transformative information technology that is enabling organizations to achieve scalability, flexibility and cost-effectiveness [1]. Cloud computing is defined by the National Institute of Standards and Technology (NIST) as a model of computing that is characterized by on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service [2]. One of the effective ways organizations can manage, use or deploy their IT resources on flexible and scalable basis is Cloud Computing. There are three service models structured upon Cloud computing, namely Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS). Businesses use the service in varying degrees of flexibility, control and cost efficiency, in which SaaS offers fully hosted applications, PaaS offers a platform on which to develop applications and IaaS offers virtualized hardware.

With benefits of reduced capital expenditure, increased operational efficiency and ease of deployment, there has been a significant shift from traditional IT infrastructure to cloud based systems. Today, cloud providers such as Amazon Web Services (AWS) and Microsoft Azure are the key enabling technologies of modern digital transformation, powering everything from basic web hosting through to complex software such as artificial intelligence and deep learning. Although, there has been a high growth in the level of cloud base services, there has been a steep rise in the number of cyber-attacks aimed at cloud services [3]. As cloud computing continues to evolve, the threat landscape associated to it grows ever more complex. Within this environment, data protection against unauthorized access, ensuring availability of services and maintaining control over sensitive information have become the highest priorities.

The shared responsibility model architecture of cloud computing has been linked with the cloud computing cybersecurity challenges where customers believe that cloud service provider is responsible for certain aspects of cybersecurity of the cloud environment [3]. What is different between on premises architecture where security controls are owned by the user than cloud architecture that has virtualized abstractions that can be quite difficult to control and can monitor the attack surface. Providers such as AWS and Azure protect the underlying infrastructure but customers must still protect their own applications, data and user permissions.

In the context of Saudi Arabia's Vision 2030, academic institutions are increasingly investing in digital infrastructure and cloud-native platforms to modernize education and research services. Universities, in particular, are integrating AWS and Azure solutions to support virtual classrooms, academic databases, and online collaboration. However, the shift to cloud-based infrastructure has also heightened their exposure to cyber threats. Misconfigured services, under-secured APIs, and inconsistent access controls pose significant risks, especially when sensitive student data and intellectual property are stored in the cloud.

To ensure these institutions remain both technologically advanced and secure, it is essential to conduct vulnerability analyses

specific to cloud service usage patterns within academic settings, and to translate these findings into practical, environment-aware security recommendations. In today's landscape, there is a strong need for empirical analysis of cloud vulnerabilities from structured datasets such as the Common Vulnerabilities and Exposures (CVE) records. Standards for identifying disclosed security flaws as well as for the metadata associated with them enable researchers to track trends over time, categorize threats by severity and proficiency and evaluate the strength of security controls. However, as general cloud security research continues to mature, relatively little work has been performed to perform a data driven analysis of AWS and Azure specific vulnerabilities, the largest cloud service providers globally.

The following research paper provides an empirical analysis of recorded CVEs for AWS and Azure cloud infrastructure security which is becoming an increasingly concerning issue. We will seek patterns in vulnerability disclosures, attempt to determine how prevalent any given threat is and how severe and provide actionable insights into what the cloud threat landscape looks like today and where it's going. This study therefore attempts to fill a gap in the literature on CVE data and provide a foundation upon which more resilient and secure cloud computing frameworks can be developed by systematically evaluating CVE data. Understanding these trends in vulnerability will help cloud consumers and providers improve their efforts in security posture as well as contribute to the overall debate of secure digital infrastructure in such a cloud centric world.

**Motivation**

Amazon Web Services (AWS) and Microsoft Azure, as the two leading public cloud providers, now host mission-critical systems and sensitive data for millions of organizations worldwide. While cloud platforms offer numerous advantages such as elasticity, cost-efficiency, and high availability, they also introduce new dimensions of risk. Despite the shared responsibility model promoted by cloud providers, many users lack clarity on where their security responsibilities begin and end. This confusion, combined with misconfigurations and a growing attack surface, has resulted in an increasing number of high-profile breaches, many of which exploit known and sometimes even preventable vulnerabilities.

Although numerous studies have examined general cloud security practices, there remains a notable lack of quantitative, provider-specific analyses that examine the evolution and characteristics of real-world vulnerabilities. The Common Vulnerabilities and Exposures (CVE) records contain a valuable but mostly untapped resource of understanding how security flaws evolve in cloud platforms over time. Analyzing CVE data for AWS and Azure, researchers can derive insights like the trends of vulnerability frequency and severity. These insights are critical to the development of proactive security strategies, the formation of policy and the direction of future research. The trustworthiness of these systems is intrinsically a function of the security of the underlying cloud infrastructure. Vulnerabilities at this level of foundational setup can vector risks across entire

technology stacks and ecosystems if not addressed or understood.

The urgency of this analysis is especially pronounced within Saudi Arabian academic institutions, where the convergence of national digital transformation efforts and increased cloud adoption presents both opportunity and risk. Academic environments often face unique challenges—such as diverse user groups, open-access policies, and complex integration layers—that can amplify the impact of known vulnerabilities. This study therefore aims not only to reveal trends in AWS and Azure vulnerabilities but also to provide practical, context-specific recommendations for securing academic cloud deployments in Saudi Arabia, helping educational institutions proactively manage risks and enhance their cybersecurity resilience.

Accordingly, there is a pressing need to comprehend and evaluate systematically the trends and prevalence of cloud infrastructure vulnerabilities in comparison of AWS versus Azure. This work aims to move beyond anecdotal or theoretical discussions by means of empirical data and answer key questions: what kinds of vulnerabilities are most common? Are there any trends as a function of time? How are vulnerability characteristics differentiated by providers? The aim of this work is to improve collective understanding of cloud security dynamics and promote the creation of more secure, more transparent and more resilient cloud computing environments, by answering these questions.

**Research Objectives**

The aim of this study is to do an empirical analysis of cloud infrastructure vulnerabilities, in particular for Amazon Web Services (AWS) and Microsoft Azure which are the most popular cloud service platforms. The research attempts to investigate and compare Common Vulnerabilities and Exposures (CVE) records linked to each platform in order to identify patterns, trends and security implications over time. Specifically, the research seeks to achieve the following key objectives:

1. To identify and categorize vulnerabilities in AWS and Azure cloud platforms – This will involve collecting and analyzing CVE data with a focus on classifying the vulnerabilities by type, severity, and potential impact.
2. To examine temporal trends in the disclosure of vulnerabilities – The research will seek to evaluate how the most common vulnerabilities have evolved over time.
3. To compare the prevalence and characteristics of vulnerabilities between AWS and Azure – The research will undertake a comparative analysis that evaluates the most common vulnerabilities, their severity, and the affected services and layers.
4. To translate analytical findings into targeted cybersecurity recommendations for academic institutions in Saudi Arabia – This includes mapping prevalent vulnerabilities to common cloud usage scenarios in educational contexts, and recommending practical mitigation strategies aligned with institutional IT policies and national digital security goals.

**Scope and Limitation**

The conclusion drawn from the research are limited to the exclusive public availability of CVE records linked to AWS and Azure cloud services. The analysis relies on a publicly available databases, and there is limited

information related to the interaction of the cloud services with third-party plugins, and open-source tools linked to the cloud-environments. Whereas the NVD database has significantly categorized different vulnerabilities, a majority of the vulnerabilities are often recorded with no-information classification, which has a significant influence in determining the frequency, and severity of specific types of vulnerabilities.

**Literature Review**

The report by Miliefsky [4] identified that cybercrime is no longer just an IT problem, as it has evolved into a global crisis that is estimated to reach a total global cost of $1.2 trillion by the end of 2025. The number of vulnerabilities being captured on different vulnerability databases have been on a rise, with the report by YesWeHack [5] establishing that since 2016, there has been a 520% increase in the number of CVE records, with 2024 recording a 38% jump in new vulnerabilities based on year-on-year basis. More surprisingly, the total number of CVEs published in 2024 accounted for 15.32% of all the CVEs that have ever been published.

The statistics indicate that there is a clear increase in risk threats and cybercrime, and there is need to provide an analytical analysis that identifies the priority areas for Information Technology (IT) administrators. Focusing on the analysis of the CVE records provides an insights on the emerging vulnerabilities, especially with emerging technologies such as Cloud Computing. Aslan et al. [6] identify four key reasons for the increase in the number of cyber-attacks: emerging technologies, cybersecurity knowledge, system errors, and increased adoption of digital technologies.

The shift from on-premise architecture to cloud-based systems has significantly transformed the threats landscape for organizations with unique vulnerabilities. Different studies have identified that cloud security issues are largely related to data ownership issues, multi-tenancy, and lack of access to cloud provider infrastructure [7]. El Kafhali et al. [8] established that because of the limitation with cloud-based systems, organizations have to be well-prepared to tackle cloud-based vulnerabilities, which often require advanced and more dynamic security strategies.

Recent literature have established that the increase in the complexity of cloud-based security risks have led to an increase in the adoption of cloud services. However, the researcher contents that organizations that value flexibility, convenience, and additional support provided by cloud based services have a greater preference for centralized hosted solution [3]. Researchers that have evaluated cloud computing risks have largely categorized vulnerabilities into two primary classes: cloud-specific, and cloud-generic vulnerabilities [9]. Cloud specific risks are based on the cloud service models: i.e. IaaS, PaaS, and SaaS, whereas cloud-generic vulnerabilities are common security challenges that are not linked to the cloud service models.

Cloud Service models are classified into three, IaaS, PaaS, and SaaS, and each service model is associated with different security vulnerabilities. Infrastructure as a Service provides users with access to critical cloud computing resources such as storage, virtual machines, network infrastructure, and

servers [10]. However, the service model is associated with security risks, with the most common security risk being the potential misalignment of security between virtual servers, and the cloud infrastructure. This results from the existence of a difference in the security policies between cloud customers and cloud providers. Butt et al. [11] identified that there are three common security challenges associated with IaaS: data security and isolation, securing IaaS resources from unauthorized access, and protecting VMs and hypervisors.

Chawkia et al. [12] identified that IaaS service model vulnerabilities are associated with virtualization aspects such virtual machine images, hypervisor, virtual network, and hardware. Virtual images are targeted by cybercriminals because they contain configurations and logs. The research by Chawkia et al. [12] identifies that virtualization security issues can be sourced from virtual machine and host OS. The Virtual Machine Monitor, which is also referred to as hypervisor, is a critical layer that enables virtualization, resource isolation, and multi-tenancy. Through attacks such as VM escape, migration, isolation, and rollback, attackers can easily gain full control of the hypervisor [13]. The cloud specific vulnerabilities are linked to the enabling technologies of the cloud environment which include multitenancy structure, and virtualization.

The PaaS service model provides the required software environment that is crucial for application development and management [14]. Although PaaS is crucial in streamlining the application development process, it also introduces vulnerabilities associated with platform components, interoperability challenges, and authentication and authorization challenges. Dawood et al. [14] identified that focus of security in PaaS service model is securing application development and deployment, encrypting and securing sensitive data, and identifying and Securing from vulnerabilities associated with custom-built applications.

Parast et al., [9] argued that the SaaS service model inherits the security vulnerabilities associated with IaaS and PaaS service models. The service model relies on web APIs, which exposes it to web technology security issues such as broken access control, injection, ineffective monitoring and logging, security misconfiguration, cross-site scripting, sensitive data exposure, and broken authentication [15]. The study by Chouhan et al. [16] identified that security issues associated with SaaS can be classified into three main categories: deployment, data, and application, with data security focusing on the security of data in transit, storage, recovery, access control, integrity, and backup.

The research by Shreyas [17] identified that data breaches are the most common risks associated with cloud computing. The research evaluated the data breaches and identified that the most common threats associated with data breaches are cross-consumer exploitation, API compromise, incomplete data wiping, lack of consumer control and visibility over certain operations, stolen credentials, and unauthorized usage. Critically, the research determined that the vulnerabilities associated with the reliance of users on cloud service providers can be largely classified into organizational failure at the user level, and cloud service provider failure. The organizational failure involves

elements such as employee misuse and lack of IT support, whereas cloud service provider failure involve internal failure, API failure, and system vulnerabilities.

The greatest risk associated with cloud services is data breaches, which result from the complexity with access control and multi-tenant structure of cloud services. The study by Yoosuf [18] established that there has been a rise in unauthorized data access, which is associated with the lack of adequate encryption, insecure APIs, and interfaces. Researchers evaluating the cloud environment have recommended stronger encryption authentication, and account monitoring to limit the cyber risks, and protect sensitive data.

Aslan et al. [6] identifies that one of the key reason for the increase in the number of cyberattacks is the high number of software-based vulnerabilities, coupled with the limited knowledge about the digital environment. The study conducted by Aslan et al. [6] is critical because it classifies system errors into three groups: computer network vulnerabilities, hardware deficiencies, and software-based bugs. The research identified that the leading cause of software related errors and vulnerabilities are: improper software security testing, buffer overflow, cross-site scripting, access control limitation, incomplete authentication, incorrect authentication, and directory related problems.

Kumar & Goyal [13] focused his research on identifying the vulnerabilities associated with cloud systems, and focused on the vulnerabilities in terms of cloud computing architectural components. The research categorizes the vulnerabilities six main categories: injection vulnerabilities, platform vulnerabilities, internet protocol vulnerabilities, unauthorized access, application and interface vulnerabilities, and infrastructure weaknesses.

The report by Verizon [19] established that 70% of cyber criminals target application programs. Application and interface vulnerabilities is a key consideration because cloud computing is made possible through network access and remote software management interfaces which allow users to access cloud services over the internet. User authentication is achieved at the application layer, and security vulnerabilities at this layer can significantly affect cloud applications and services. Alquwayzani et al. [20] identified that the vulnerabilities associated with the application layer are security misconfigurations, identification and authentication failures, server-side request forgery, broken access control, software and data integrity failures, insecure design, security logging, and monitoring failures, injection and Cross-Site Scripting, vulnerable and outdated components, and cryptographic failures. Alquwayzani et al., [20] evaluated the vulnerabilities that are associated with cloud services, and established that the inadequate user configuration was a major cyber risk. The study identified that misconfigurations such as improperly set permissions often lead to cybersecurity incidents.

The other major network layer in cloud computing is infrastructure layer, which Alquwayzani et al. [20] described as being critical in achieving virtualization in the cloud environment. The layer is associated with the traditional vulnerabilities of virtualization, alongside the vulnerabilities associated with multi-tenancy, VM images,

VM recall, and VM migration. The vulnerabilities associated with this layer include cloud network and storage vulnerabilities, shared network component vulnerabilities, virtual network vulnerabilities. Alquwayzani et al. [20] identify the data storage vulnerabilities as data encryption, data cleaning, data storage location, data access, backup, and recovery vulnerabilities.

The survey conducted by Netskope [21] identified that the major threats associated with public clouds are misconfigurations, unauthorized access, and insecure application programming interfaces. Yoosuf established that misconfigurations are a result of insufficient oversight of cloud infrastructure, human error, and limited knowledge on cloud security protocols. Misconfigurations provides an effective entry point to cyber attackers as it enables them to bypass defenses, and access critical systems. The researcher identifies that there are additional risks and vulnerabilities that include third-party vulnerabilities, insider threats, and shared vulnerabilities associated with multi-tenancy structure of cloud infrastructure.

**Methodology**

The research relied on the collection of quality data that could be analyzed to determine the latest and significant vulnerabilities associated with AWS and Azure cloud services. The data for the research was collected from the National Vulnerability Database (NVD) which aggregates Common Vulnerabilities and Exposures of different digital services. The database is maintained by the National Institute of Standards and Technology, and the organization actively verifies the vulnerabilities, and assign a unique identifier, Common Weakness Enumeration ID. The unique identifier is critical because it classifies the vulnerability to a specific hardware or software weakness category.

The data was collected from NVD website by downloading the yearly data, focusing on the data from 2019-2025. NVD separates the vulnerabilities into different yearly based files, and thus the first action was to combine the JSON files into one file. The data cleaning and data analysis relied on python-based analysis which relied on Google Colab. The python code used in combining the seven datasets. The downloaded data was uploaded to google drive, and was accessed via the Google Colab Sheet, and as shown in the code 1 in Appendix 1, the combined data was saved as combined_nvd.json.

After combining the JSON data, the analysis then focused on extracting dataset focusing on AWS and Azure cloud services. This was a critical stage that required the development of exclusion criteria that would provide an exclusive database, while ensuring that critical data points were not excluded. To identify the most effective strategy, two strategies were defined: a permissive exclusion, and strict exclusion. The permissive exclusion would just rely on the mention of AWS or Azure on the dataset, whereas a strict inclusion relied on both the mention of AWS or Azure alongside high confidence terms provided in code 2 in Appendix 1.

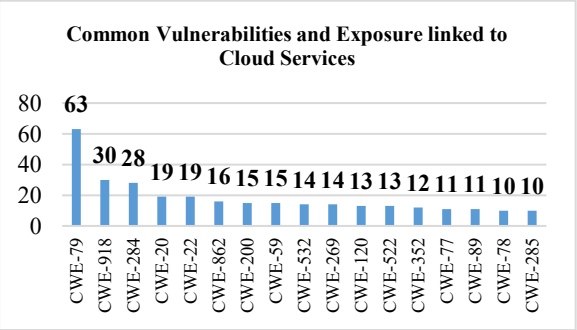
The analysis of the result from the permissive and strict exclusion identified that the strict exclusion was too strict as it excluded a lot of common vulnerabilities and exposure related to AWS and Azure cloud services. The permissive approach was

determined as being the most effective, especially because a majority of the services offered by AWS and Azure are linked to their cloud platforms. Although the permissive approach created a possibility of including vulnerabilities that are not linked to cloud services, it was determined the permissive approach was sufficient to include a significant number of cloud-based vulnerabilities. Code 3 provided in appendix 1 was used to extract cloud-based vulnerabilities, and this was saved on a CSV file. The CSV file was then analyzed using excel to generate graphs capturing the underlying patterns.

**Data Analysis:**

The data analysis of the collected and cleaned data was conducted, and the results are presented in the figure below. Figure 1 below is critical because it provides the frequency of the hardware or software vulnerabilities based on the CWE ID. The figure provides a graphical representation of the vulnerabilities that have a frequency count greater or equal to 10. The figure indicates that the most common hardware or software vulnerability is CWE-79, which has significantly the highest frequency count. The second, and third most common vulnerabilities are CWE-918, CWE-284.

**Figure 1: Frequency Count of the Cloud-based Vulnerabilities**




Using the CWE dictionary developed by MITRE Corporation (2025), the most common vulnerabilities associated with Azure and AWS cloud services was matched. Table 1 below provides a summary table that presents CWE-ID, weakness name, and description was of the software or hardware weakness. The analysis indicates that the most common vulnerability affecting the cloud services is Cross-Site Scripting (XSS), indicates that cyberattacks are able to inject malicious scripts into pages associated with the cloud-services. The second most common vulnerability associated with the services is service-side request forgery, which involves the forcing of a server to make unauthorized internal/external requests. The third most common vulnerability is improper access control, and the fourth most common vulnerability is improper input validation, which both indicates that the cloud services are missing authorization checks for critical function, and that they lack proper validation of input.

**Table 1: Description of the common vulnerabilities linked to cloud services**

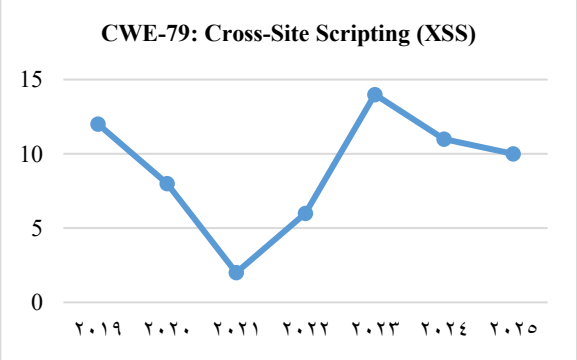
| CWE ID | Weakness Name | Description |
|---|---|---|
| CWE-79 | Cross-Site Scripting (XSS) | Injecting malicious scripts into web pages viewed by others. |
| CWE-918 | Server-Side Request Forgery (SSRF) | Forcing a server to make unauthorized internal/external requests. |
| CWE-284 | Improper Access Control | Missing authorization checks for critical functions. |
| CWE-20 | Improper Input Validation | Failure to properly validate input, leading to injection or corruption. |
| CWE-22 | Path Traversal | Allowing access to files/dirs outside restricted directory. |

| | | |
|---|---|---|
| CWE-862 | Missing Authorization | Complete lack of authorization checks for restricted operations. |
| CWE-200 | Exposure of Sensitive Information | Leaking private data unintentionally. |
| CWE-59 | Improper Link Resolution Before File Access | Symbolic links or shortcuts leading to unauthorized file access. |
| CWE-532 | Information Exposure Through Logs | Sensitive data leaked in logs |
| CWE-269 | Improper Privilege Management | Failing to enforce proper user permissions |
| CWE-120 | Buffer Overflow (Classic) | Writing beyond allocated buffer boundaries, causing crashes/exploits. |
| CWE-522 | Insufficiently Protected Credentials | Storing or transmitting credentials insecurely |
| CWE-352 | Cross-Site Request Forgery (CSRF) | Forcing users to execute unintended actions while authenticated. |
| CWE-77 | Command Injection | Arbitrary OS command execution via malicious input. |
| CWE-89 | SQL Injection | Manipulating database queries via unvalidated input. |
| CWE-78 | OS Command Injection (Shell Injection) | Subverting shell commands via user-controlled input. |
| CWE-285 | Improper Authorization | Incorrectly verifying user permissions before allowing actions. |

In order to identify whether the cloud services vulnerabilities are being resolved, a trend line was generated for the number specific vulnerabilities recorded over the years. The graphical analysis focused on the three most common vulnerabilities: CWE-79, CWE-918, and CWE-284.

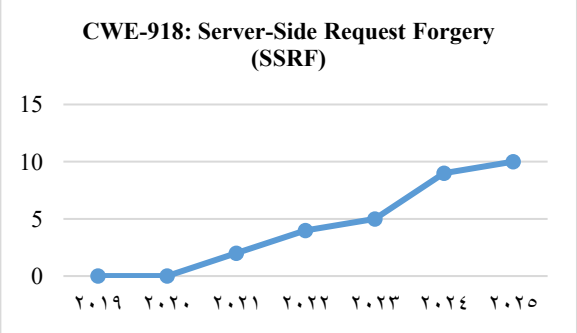
The analysis of NVD records from 2019-2025 reveals that CWE-79 (Cross-Site Scripting, XSS) weakness has a fluctuating, yet insightful trend. The initial trend shows that there was a steady decline in the number of disclosed XSS vulnerabilities from 2019, reaching the lowest point of only 2 disclosed vulnerabilities in 2021. However, the number of disclosed vulnerabilities has been on a sharp rise since 2022, and by May of 2025, there are already 10 disclosed vulnerabilities, indicating that there are likely to be more disclosed vulnerabilities by the end of the year.

**Figure 2: Temporal Analysis of Cross-Site Scripting (XSS) vulnerability**



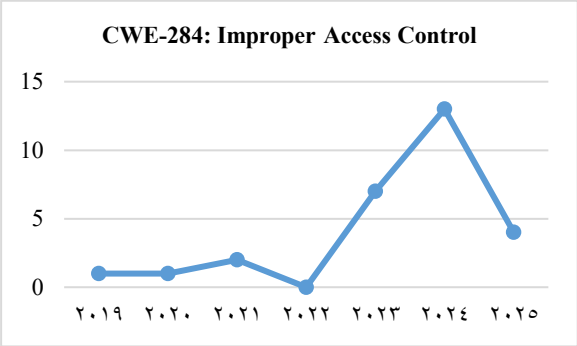

The analysis the server-side request forgery indicates that the vulnerabilities were not recorded on the public database in 2019 and 2020. However, since 2021, there has been a consistent increase in the disclosures of the vulnerabilities, such that the analysis of the data disclosed by mid-year 2025 indicates that there are already the highest number of disclosures in the last 7 years.

**Figure 3: Temporal Analysis of Server-Side Request Forgery (SSRF) vulnerability**



The final graphical analysis focused on the vulnerability that was identified as having the third highest count frequency. The graph presented shows the yearly frequency of CVEs associated with CWE-284: Improper Access Control from 2019 to 2025, based on data extracted from the National Vulnerability Database (NVD). While these counts represent reported vulnerabilities and not direct exploit incidents, the trends is crucial because it provides an indicator of the common vulnerabilities in Azure and AWS service. Taking the assumption that more vulnerabilities will be reported in 2025, the data indicates that improper access control vulnerabilities is being reported at increasing frequency.

**Figure 4: Temporal Analysis of Improper Access Control Vulnerability**




**Discussion**

An analysis of CWE-classified vulnerabilities in the cloud context, with a special focus on AWS and Azure cloud platforms, helps us understand how risk management in the cloud differs from that in traditional enterprise environments—especially when framed through the Shared Responsibility Model. This model defines boundaries clearly: cloud service providers (CSPs) secure the infrastructure and foundational services, while users are responsible for securing the applications, data, and configurations they deploy.

For academic institutions in Saudi Arabia, which are rapidly integrating cloud platforms to support digital learning, research infrastructure, and administrative operations, understanding these boundaries is critical. Misinterpreting or neglecting these roles can expose sensitive student information, research data, and educational systems to avoidable threats. For the purpose of this study, a data-driven review of the most frequently occurring CWEs supports the conclusion that a large number of vulnerabilities are triggered by failures occurring within the user's domain—precisely where academic IT teams must focus their efforts.

CWE-79 (Cross-Site Scripting) is foremost among the vulnerability distribution because XSS flaws are, by their fundamental nature, dependent on the integrity of client-facing web application logic and thus remain within the purview of the user. Dynamic, JavaScript-heavy interfaces are often employed in educational portals to deliver rich, interactive experiences across devices—a core requirement for remote learning platforms. Unfortunately, without proper input sanitization and output encoding, cyber criminals can exploit these same interfaces. A further breakdown of CWE-79 by year highlights that these vulnerabilities persist not due to infrastructural flaws, but due to enduring gaps in secure development practices within user-managed applications. Analysis of other high-ranking CWEs—such as CWE-918 (Server-Side Request Forgery), CWE-284 (Improper Access Control), CWE-22 (Path Traversal), and CWE-862 (Missing Authorization)—reveals clear patterns tied to user-side misconfiguration, insecure coding, and improper privilege

management. For Saudi academic environments, where hybrid cloud deployments may involve multiple stakeholders (administration, IT support, faculty, and students), improper role segmentation and permission sprawl can lead to exposure. Inadequate enforcement of Least Privilege (CWE-266), misconfigured IAM policies (CWE-284), and improper privilege assignment (CWE-269) reflect the complexity of authoring secure access policies—especially in decentralized academic settings. While providers offer granular IAM tooling, negligence or insufficient training often leads to overly permissive access configurations, increasing both the attack surface and the difficulty of maintaining compliance with national cybersecurity guidelines.

Empirical analysis of Common Vulnerabilities and Exposures (CVE) records for AWS and Azure provides insight into the security trends emerging in this dynamic ecosystem. The results show that Cross-Site Scripting (CWE-79) remains the most prevalent vulnerability, with Server-Side Request Forgery (CWE-918) and Improper Access Control (CWE-284) following closely. This distribution supports broader research emphasizing that application-layer vulnerabilities—rather than infrastructure-level flaws—are the primary threat in cloud environments. For universities, this distinction is critical: while the underlying cloud platform may be robust, the applications deployed by the institution (student portals, research databases, e-learning tools) remain vulnerable if not securely coded and regularly audited.

Injection-based vulnerabilities such as XSS and SSRF dominate cloud security issues, pointing to systemic flaws in how cloud applications handle user input and external requests. This is especially dangerous in API-driven academic environments, where integrations between learning management systems (LMS), student information systems (SIS), and third-party educational tools are frequent. One misconfigured endpoint could expose entire datasets or user directories.

A temporal analysis of vulnerability disclosures reveals how cloud security risks have evolved from 2019 to 2025. While Cross-Site Scripting vulnerabilities declined early in the study period—reaching their lowest disclosure in 2021—they have since increased sharply. 2025 is projected to mark the highest number of disclosures during the observed window. This fluctuation may reflect cyclical changes in secure development practices and the increasing complexity of cloud-native academic applications. Even more concerning is the steady rise in Server-Side Request Forgery vulnerabilities, correlating with the adoption of microservices and serverless architectures—technologies that academic institutions are also beginning to explore to reduce costs and improve scalability.

In sum, the findings emphasize that for Saudi academic institutions, cloud risk management must go beyond trusting the provider and instead focus on user responsibility—particularly in securing APIs, hardening IAM configurations, and enforcing development best practices. With increasing digitization of learning and research, academic cloud deployments must be treated as high-value assets deserving of enterprise-grade security oversight.

**References**


[1] E. Fatima, I. Sumra and R. Naveed, "A Comprehensive Survey on Security Threats and Challenges in Cloud Computing Models (SaaS, PaaS and IaaS)," Journal of Computing & Biomedical Informatics, vol. 7, no. 1, p. 537–544, 2024.

[2] P. Mell and T. Grance, "National Institute of Standards and Technology," September 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf. [Accessed 10 June 2025].

[3] S. Ahmadi, "Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies," Journal of Information Security, vol. 15, pp. 148-167, 2024.

[4] G. Miliefsky, "Cyber Defense Magazine," Cyber Defense Magazine, 13 March 2025. [Online]. Available: https://www.cyberdefensemagazine.com/the-true-cost-of-cybercrime-why-global-damages-could-reach-1-2-1-5-trillion-by-end-of-year-2025/. [Accessed 10 June 2025].

[5] YesWeHack. (2025). CVE surge: Why the record rise in new vulnerabilities? Retrieved from: https://www.yeswehack.com/news/cve-surge-record-jump-vulnerabilities.

[6] Ö Aslan, M, Ozkan-Okay, and D, Gupta, "Intelligent Behavior-Based Malware Detection System on Cloud Computing Environment, *IEEE Access*, Vol. 9, 2021.

[7] S. Singh, Y. S. Jeong and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions.," *Journal of Network and Computer Applications,* vol. 75, pp. 200-222, 2016.

[8] S. El Kafhali, I. El Mir and M. Hanini, "Security threats, defense mechanisms, challenges, and future directions in cloud computing," *Archives of Computational Methods in Engineering,* vol. 29, no. 1, pp. 223-246., 2022.

[9] F. K. Parast, C. Sindhav, S. Nikam, H. I. Yekta, K. B. Kent and S. Hakak, "Cloud computing security: A survey of service-based models.," *Computers & Security,,* vol. 114, p. 102580., 2022.

[10] G. Ramachandra, M. Iftikhar and F. Khan, "A Comprehensive Survey on Security in Cloud Computing," Procedia Computer Science, vol. 110, p. 465–472, 2017.

[11] U. A. Butt, R. Amin, M. Mehmood, H. Aldabbas, M. T. Alharbi and N. Albaqami, "Cloud security threats and solutions: A survey.," *Wireless Personal Communications,* vol. 128, no. 1, pp. 387-413, 2023.

[12] B. Chawkia, A. Ahmeda and T. Zakariaea, "IaaS cloud model security issues on behalf cloud provider and user security behaviors," *Procedia computer science,* vol. 134, pp. 328-333, 2018.

[13] R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," *Computer Science Review*, vol. 33, pp. 1-48, 2019.

[14] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas and S. U. Rehman, "Cyberattacks and security of cloud computing: a complete guideline," *Symmetry,* vol. 15, no. 11, p. 1981, 2023.

[15] J. Li, "Vulnerabilities Mapping based on OWASP-SANS: A Survey for Static Application Security Testing (SAST)," *Annals of Emerging Technologies in Computing (AETiC),* vol. 4, no. 3, pp. 1-6, 2020.

[16] P. K. Chouhan, F. Yao, S. Y. Yerima and S. Sezer, "Software as a service: Analyzing security issues.," *arXiv preprint arXiv:1505.01711.,* pp. 1-9, 2015.

[17] S. Shreyas, "Security Model for Cloud Computing: Case Report of Organizational Vulnerability," *Journal of Information Security,* vol. 41, pp. 250-263, 2023.

[18] I. Yoosuf, "Emerging Threats in Cloud Computing Security: A Comprehensive Review," *Iconic Research and Engineering Journals,* vol. 8, no. 4, pp. 199-209, 2024.

[19] Verizon, "Data Breach Investigations Report," 2022. [Online]. Available: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf. [Accessed 27 May 2025].

[20] A. Alquwayzani, R. Aldossri and M. Frikha, "Prominent Security Vulnerabilities in Cloud," (IJACSA) International Journal of Advanced Computer Science and Applications, vol. 15, no. 2, pp. 803-812, 2024.

[21] Netskope, "Cloud Security Report," Cybersecurity Insiders., Santa Clara, California, 2019