Cyber Security Experts Association of Nigeria (CSEAN)
Society for Multidisciplinary & Advanced Research Techniques (SMART)
Faculty of Computational Sciences & Informatics - Academic City University College, Accra, Ghana
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA

Proceedings of the Cyber Secure Nigeria Conference – 2023

# Best Practices to Implement and Pitfalls to Avoid in Cloud Application Security

[1]Oyitso, E.J. & [2]Ordia, E.D.
Info Forte Arica
Lagos, Nigeria
**E-mails**: ejoyitso@gmail.com; ebose07@gmail.com
**Phones:** +2349055599819 and +2347015406988

## ABSTRACT

This paper explores the importance of reevaluating the application security posture in the context of modern software development practices and the shift towards cloud computing. It highlights the challenges posed by the evolving threat landscape and emphasizes the need for a comprehensive and proactive security strategy. The paper also discusses various techniques and best practices for securing applications from the code level to the cloud environment, encompassing secure coding practices, and the effective utilization of cloud security services. By adopting a holistic approach to application security, organizations can mitigate risks and protect their applications and data throughout the software development lifecycle.

**Keywords:** Application Security, Software Development, Cloud Computing, Secure Coding, Vulnerability Assessment, Penetration Testing, Cloud Security Services

**Proceedings Citation Format**
Oyitso, E.J. & Ordia, E.D. (2023): Best Practices to Implement and Pitfalls to Avoid in Cloud Application Security. Proceedings of the Cyber Secure Nigeria Conference. Nigerian Army Resource Centre (NARC) Abuja, Nigeria. 11-12th July, 2023. Pp 41-48.
https://cybersecurenigeria.org/conference-proceedings/volume-2-2023/
dx.doi.org/10.22624/AIMS/CSEAN-SMART2023P6

## 1. INTRODUCTION

Over the years, Cloud-based applications have become an important aspect of business operations facilitating cost savings and scalability. The benefits that cloud applications bring are enormous. Recently, a digital asset marketplace,

[1] LLB (Liverpool), LLM (Birmingham.), B.L, CISA, CEH, Security +, Microsoft SC-200, Certified ISO 22301 LI, MCIArb (UK) - https://independent.academia.edu/EserogheneOyitso
[2] BA (Manchester), MSc (Manchester), Certified ISO 9001 LA, Microsoft AZ-900

Patricia announced that its retail trading application (Patricia Personal) was breached, leading to the compromise of Bitcoin (BTC) and Naira assets (Patricia, 2023). This security breach happened in January 2022, costing Patricia $2 million. This incident disrupted operations as the company had to suspend withdrawals on both web and mobile applications to perform adequate incident response (Techloy News, 2023). In today's digital transformation era, almost every company is a software company or is highly reliant on some form of software or application. With most businesses also migrating to the cloud, safeguarding applications in the cloud is an important business strategy for profitability, growth, and sustainability.

In security, prevention is always better and cheaper than cure. Therefore, an excellent way to understand Cloud Security is to understand the best practices and pitfalls to avoid for each concept and implement. One does not need to be a developer or software engineer to understand Cloud Application Security. This article will examine Cloud Development, the pitfalls to avoid, as well as the best practices and recommendations for robust cloud application security.

## 2. CLOUD DEVELOPMENT

In past eras, application security was always an afterthought but with the advancement in hacking technology and the number of software vulnerabilities that exist, the development of applications has to be done securely. The Cybersecurity and Infrastructure Security Agency (CISA) in collaboration with the Federal Bureau of Investigation and 8 other bodies advocate for secure-by-design and secure-by-default approaches. This is to encourage organizations and developers to prioritize the integration of product security as a critical prerequisite over product features and speed to market. (Cybersecurity and Infrastructure Security Agency [CISA] et al., 2023).

Cloud development necessitates the use of Integrated Development Environments (IDEs). An IDE is an application or collection of tools that enable programmers to develop software code effectively and efficiently. Older Generation IDEs are run on a programmer's desktop. Cloud Computing introduced Cloud IDEs shifting the development process to the Cloud. For example, AWS Cloud9 is a cloud IDE that allows programmers to write, run and debug code in a web browser, supporting over 40 languages. (Amazon Web Services, n.d). Cloud IDEs make coding more accessible to developers because all the computing is performed on the server side and all that is required is a computer with internet access.

Before deciding to use a Cloud IDE, a developer must have credible answers to the following security questions:

1. Who will be able to physically access the browser?
2. Who can control the browser remotely? (This is because of Browser Hijacking and Remote Access Attacks).
3. If working within an organization, who can create new cloud IDE instances? (*McDaniel*, 2022).

It is important to remember that threat actors can escalate their privileges and wreak irreversible harm if they gain access to a Cloud IDE. A programmer or product manager should be aware of the following security issues before adopting a Cloud IDE:

1. Safeguard access credentials, keys, and accounts to the IDE- The use of Identity and Access Management, Multifactor Authentication, and Single Sign On (SSO) is an effective measure to prevent attacks.
2. Educate, equip, and train Programmers.
3. Reduce and control the attack surface area.
4. Security by Design and Security by Default.
5. Separate development environments from production environments.
6. Due Diligence and continuous threat monitoring
7. Automated Security Testing (*GuardRails*, 2023).

In most cloud deployments, access is acquired through an Application Programming Interface (API). These APIs use tokens and assertions rather than usernames and passwords. Programmers should be aware of the difference between Representational State Transfer (REST or RESTful API) and Simple Object Access Protocol (SOAP). The best practice from a cloud development perspective is to always choose RESTful API over SOAP, except in situations where REST is not feasible (Gordon, 2016). This is because the RESTful API supports different data formats such as JavaScript Object Notification (JSON), eXtensible Markup Language (XML), and Yet Another Multicolumn Layout (YAML) while SOAP only supports XML.

## 3. COMMON PITFALLS OF CLOUD APPLICATION DEPLOYMENT

"The ability to identify, communicate, and plan for potential cloud-based application challenges proves an invaluable skill for developers and project teams" (Gordon, 2016). Cloud Computing has numerous benefits and has revolutionized the way individuals and organizations store, process and manage data. However, cloud adoption comes with its own set of difficulties and traps, and if they are not avoided, can result in irreversible harm to an application and the organization. Some of the common pitfalls in cloud application deployment include:

1. **Some On-Premises Applications are not transferable to the Cloud and vice versa-** This is because the technological advancements and developments of the cloud were not considered when the on-premises application was initially developed. One possible mitigant is to ensure cloud-based development is tested against on-premises systems or environments (and vice versa).

2. **Not All Applications are Cloud Ready**- A cloud-ready application is a legacy or on-premises software product that has been modified to run on a cloud computing architecture (Siemens Software, n.d.). Cloud development or deployment might be challenging in situations when high-level security measures are applied, or if the application was created using Common Business Oriented Language (COBOL) or an older programming language. As a result, developers need to ensure that contemporary programs are scalable, portable, and interoperable. This is the best practice.

3. **Lack of Documentation and Guidelines-** This is one of the issues this paper aims to resolve. For a very long time, we have witnessed developers and other IT professionals undergo projects without adopting sound guidelines, best practices, planning, and proper documentation. This is a very dangerous practice and can lead to security breaches. The major Cloud Service Providers (CSPs) are mitigating this risk by providing documentation and some level of guidelines, but with the existence of zero-day vulnerabilities and an ever-changing threat landscape, these cannot be always up to date. Organizations like the ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) have established a specialized system for global standardization. When it comes to software development, ISO/IEC has introduced the ISO/IEC/IEEE 12207:2017 (en) Systems and software engineering — Software life cycle processes. This standard "establishes a common framework for software life cycle processes, with well-defined terminology, that can be referenced by the software industry. It contains processes that are applicable during the acquisition, supply, development, operation, maintenance, or disposal of software systems, products, and services"(International Organization for Standardization, the International Electrotechnical Commission, and the Institute of Electrical and Electronics Engineers, (2017).

4. **Lack of Training and Awareness –** Not all IT specialists and software developers have had the required training in cloud computing, which results in increased vulnerabilities, errors, and inefficiencies. Cybersecurity researchers have deduced that the average developer is familiar with Microsoft .NET, SQL Server, Java, and other traditional development techniques. However, cloud-based development environments introduce a different set of challenges to developers. (Gordon, 2016). Mitigants to this pitfall include the following:

    i. Organizations should train employees to ensure that they have adequate expertise, awareness, and skillset to utilize cloud technology effectively. In cases where the developer is self-employed, the developer should equip his/herself with the relevant skills needed for cloud development.
    ii. Choosing a reputable cloud services provider can help speed up the process of upskilling and knowledge transfer in Cloud Computing (Whittaker, 2023).

5. **Integration Challenges-** As we shift towards the era of digital transformation, many IT applications, products, and systems need to be integrated with cloud technology. More often than not, the integration requirements are not adequately considered before cloud adoption. Research has shown that it is crucial to identify the integration requirements and how the integration will occur before going forward. This is because when programmers do not have access to the supporting components, systems, and services, Integration will be complex. Therefore, the best practice to mitigate the challenges of integration is to use the Cloud Service Providers' API.

Cloud application development is transforming the way applications are being developed and managed. Nevertheless, one cannot ignore the pitfalls highlighted above, it is important to note that there are other pitfalls associated with cloud adoption and development, some of which include Vendor Lock In,

Data loss and availability challenges (downtime), and security and compliance risks. It is the best practice to utilize a reputable CSP with a proven track record of addressing the pitfalls explained and listed above.

## 3. THREAT MODELING

Threat Modeling is a well-known practice in software development (Khalil et al., 2023). Threat Modeling is performed on an application once the application is running. It can also be done when an application or system design is created. The objective of threat modeling is to determine and address any weaknesses in the application or application design (as the case may be). Threat Modeling should be a flexible and continuous process because the IT threat landscape is constantly evolving and the overall attack surface is wider because the application is hosted on the cloud. Therefore, constant vigilance is a requirement in cloud application security.

Threat Modelling decomposes the application to better understand the application, especially how it relates to external entities. In doing this, Threat Modeling identifies the entry and exit points as well as the external dependencies of the application such as where the database server will be hosted. According to Open Web Application Security Project (OWASP), the two recommended threat modeling processes are STRIDE and DREAD.

### STRIDE Threat Model

STRIDE categorizes known threats by the types of attacks or the goals of the attackers (OWASP Foundation, n.d.). The STRIDE Threat Model is developer-focused, which implies that it identifies attack vectors that developers and organizations must be aware of. One of the objectives of STRIDE is to nudge the developers to consider security measures during the design phase. This will enable the application to meet the security requirements of confidentiality, integrity, availability, authorization, authentication, and non-repudiation. STRIDE is an acronym for:

- **Spoofing:** This is an exploit where the attacker impersonates the subject. To mitigate this threat, the developer must ensure that the application has adequate identity and Access Management (IAM) controls.
- **Tampering:** This is an exploit where an attacker alters or tampers data, information, or messages. The ideal mitigant for this is proper input validation, this must be implemented by the developer.
- **Repudiation:** Here, an attacker performs his exploits in such a way that they cannot be traced or validated. Therefore, developers must develop applications in such a manner that comprehensive logs of all activities and transactions.
- **Information Disclosure:** This is when an attacker illegally obtains confidential information without authorization and discloses the same. Developers must implement controls to safeguard against information disclosure. Confidentiality is one of the hallmarks of good security.

- **Denial of Service:** This is an exploit where the attacker overburdens the application, preventing it from effectively responding to legitimate requests. Developers and programmers should "minimize how many operations are performed for non-authenticated users. This will keep the application running as quickly as possible and using the least amount of system resources". (Carter, 2017).
- **Elevation of Privileges:** This is where an attacker escalates his/her privilege level above what is allowed. It is advised that applications are developed in such a manner that administrative privileges are re-verified before certain functions are accessed or performed. In other words, implement the principle of least privilege.

### DREAD Threat Model

The DREAD threat model uses quantitative metrics for analyzing and assessing threats. The benefit of this model is that it allows for continuous improvement because performance can be measured over time, due to the usage of numerical metrics. DREAD is based on an algorithm, using a value of 0 to 10, with 10 being the higher risk and 0 being the lower risk. "It involves attaching a numeric score to five risk variables and then calculating another score for a particular threat" (Rizal, 2021). The formula is as follows:

**DREAD SCORE =** Damage Potential + Reproducibility + Exploitability + Affected Users + Discoverability

The higher the dread score, the higher the likelihood that the threat has a greater damage impact on the users. Therefore, high DREAD scores should be prioritized and mitigated urgently.

## 4. SUPPLEMENTAL SECURITY DEVICES

Based on the defense-in-depth architecture, it is the best practice to implement supplemental security devices to increase the level of application security. By using complementary, overlapping, and mutually reinforcing controls, the application's attack surface area will be reduced. Reducing the attack surface area is very essential in cloud computing.

Although some of these devices are used in traditional application security, they are also effective when deployed in cloud computing and cloud software development.

Other Supplemental Security Devices Include XML Appliances and API Gateways. XML Appliances such as XML firewalls are capable of allowing "valid SOAP messages while blocking malicious SOAP messages that contain attacks such as oversized payloads, recursive payloads, and SQL injections" (Y. -s. Loh et al, 2006). In a cloud environment, XML Appliances are used as communication brokers between the cloud services and enterprise applications. XML Appliances implement security measures such as Antivirus and Data Loss prevention, reducing the impact of malware and other threats to the application.

Below is a table of some security devices and the risks, they mitigate:

Table 1: Security Devices and Risks Mitigated

| S/N | SECURITY DEVICE | SECURITY RISK MITIGATED |
|---|---|---|
| 1. | **Cloud Web Application Firewall (WAF) -** This can be a scalable service provided by the CSP or a server plugin that analyzes HTTP traffic by applying rules to an HTTP or HTTP connection. A WAF is a layer-7 firewall. | The WAF filters or mitigates the following attacks:<br>• Cross-Site Request Forgery<br>• Cross-Site Scripting<br>• SQL Injection<br>• Denial of Service<br>• Server Site Request Forgery |
| 2. | **Database Activity Monitoring (DAM) -** This is a layer-7 visibility and monitoring tool that understands SQL commands. A DAM can be Network Based (NDAM) or Agent-Based (ADAM). A DAM has the capability to identify, monitor and report fraudulent, unauthorized, and illegal transactions on data in rest and data in transit. | The DAM identifies and mitigates SQL Injection attacks. |

XML firewalls, which can be physical (in a data center) or virtual machines, understand and process XML communication over HTTP and HTTPS. API Gateways filter API traffic. API Gateways can be installed either as a part of the software/application stack or as a proxy. In Cloud computing, API gateways are used by developers to create, monitor, manage, and secure APIs. As a result, API gateways implement controls such as access control, adequate logging, and security filtering. Best practice dictates that developers and organizations should consider implementing additional security devices for more secure applications hosted on the cloud.

## 5. CONCLUSION

In cloud application security, knowledge is power. If organizations, developers, and cybersecurity professionals, ignore the pitfalls of cloud computing and fail to implement the best practices and security devices, it may lead to a catastrophe and potentially irreparable damage. For cloud applications to be secure and available in the long term, organizations and developers must possess a solid understanding of cloud development, the ability to evaluate cloud service providers, and the ability to analyze the relevant devices and technologies that must be implemented to meet the defense in depth requirement. It must be clearly stated that a good knowledge of APIs and threat modeling is mandatory to secure application development and deployment.

## REFERENCES

1. Carter, D. (2017). *All in One CCSP ® Certified Cloud Security Professional Exam Guide* (1st ed.) [Print]. McGraw-Hill Education.
2. Cybersecurity and Infrastructure Security Agency [CISA], National Security Agency [NSA], & Federal Bureau of Investigation [FBI] et al. (2023, April 13). *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by Design and -Default*. *https://www.cisa.gov/*. Retrieved June 5, 2023, from https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
3. Gordon, A. (2016). *The Official (ISC)2 Guide to the CCSP CBK* (2nd ed.) [Print]. Wiley.
4. GuardRails. (2023). *What is the IDE and What Are the 7 Key Considerations for Implementing Security?* GuardRails. https://www.guardrails.io/blog/what-is-the-ide-and-what-are-the-7-key-considerations-for-implementing-security
5. International Organization for Standardization, the International Electrotechnical Commission, and the Institute of Electrical and Electronics Engineers. (2017) *Systems and software engineering — Software life cycle processes (ISO/IEC/IEEE 12207:2017 (en))*https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:12207:en
6. Khalil, S. M., Bahsi, H., Dola, H. O., Korotko, T., McLaughlin, K., & Kotkas, V. (2023). *Threat Modeling of Cyber-Physical Systems - A Case Study of a Microgrid System.* Computers & Security, 124, 102950. https://doi.org/10.1016/j.cose.2022.102950
7. McDaniel, D. (2022). *Securing The New Frontier in Developer Environments: Cloud IDEs.* GitGuardian Blog - Automated Secrets Detection. https://blog.gitguardian.com/securing-developer-environments-cloud-ides/
8. Patricia [@PatriciaSwitch]. (2023, May 26). *Hello Chief, We have a much-needed update for you. #patriciatechnologies #cryptocurrencies* [Tweet] Twitter. https://twitter.com/PatriciaSwitch/status/1662049215772516352
9. Rizal, D. H. F. (2021, December 13). *How to Calculate Web Security Risk - The Legend* - Medium. *Medium*. https://medium.com/the-legend/how-to-calculate-web-security-risk-27bc6a3e5c5b
10. Techloy News. (2023). Nigerian Crypto Marketplace Patricia Faces $2 Million Loss in Breach. Techloy. https://www.techloy.com/crypto-marketplace-patricia-faces-2-million-loss-in-breach/
11. *Threat Modeling Process* | OWASP Foundation. (n.d.). https://owasp.org/www-community/Threat_Modeling_Process#stride
12. *What are Cloud-Ready Applications?* | Siemens Software. (n.d.). Siemens Digital Industries Software. https://www.plm.automation.siemens.com/global/en/ourstory/glossary/cloud-ready-applications/63229
13. W*hat is an IDE? - Integrated Development Environment Explained* - AWS. (n.d.). Amazon Web
14. Services, Inc. https://aws.amazon.com/what-is/ide/
15. Whittaker, B. (2023, February 22). *Common Pitfalls with Cloud Adoption and Getting it Right.* Medium. https://medium.com/version-1/common-pitfalls-with-cloud-adoption-and-getting-it-right-e504e11152
16. Y. -s. Loh, W. -c. Yau, C. -t. Wong and W. -c. Ho, "*Design and Implementation of an XML Firewall,*" 2006 International Conference on Computational Intelligence and Security, Guangzhou, China, 2006, pp. 1147-1150, doi: 10.1109/ICCIAS.2006.295443.