Available online www.jsaer.com

*Journal of Scientific and Engineering Research***, 2018, 5(5):654-658**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Secure Software Development Lifecycle in the Cloud Era

Mounika Kothapalli

Senior Member Technical at ADP Private Ltd
Email Id: moni.kothapalli@gmail.com

Abstract As enterprise applications increase their adoption of cloud computing, the necessity for security introduction at every stage of the Software Development Lifecycle is apparent in most enterprise applications. It has often been seen that traditional practices of development fail to provide enough security considerations and that vulnerabilities are allowed to be exploited in sophisticated cyber environments. This paper sheds light on the introduction of security measures at each stage of the SDLC and the necessity for tailor and incorporation of existing cybersecurity frameworks like ISO/IEC 27001 and the NIST Cybersecurity Framework. Continual assessment strategies and the integration of security controls will help ameliorate risks, increase compliance, and also ensure the resilience of software products against threats. This paper presents a comprehensive guide to the use of these methodologies in cloud-based development, thereby preparing the ground for developing more secure and robust cloud applications.

Keywords Secure Software Development, Cybersecurity Frameworks, Cloud Security, Risk Management, Data Integrity, Compliance, ISO/IEC 27001, NIST Cybersecurity Framework, Threat Mitigation, Security Best Practices

Introduction

Cloud computing presents users with unprecedented scalability, flexibility, and efficiency. Still, cloud technologies, at the same time, bring new challenges for security. In the context of enterprises embracing cloud technologies, the ability to build robust security measures at every stage of the Software Development Lifecycle (SDLC) becomes paramount. Traditional security practices are mostly reactive and not tailored to the dynamic and distributed nature of cloud computing environments.

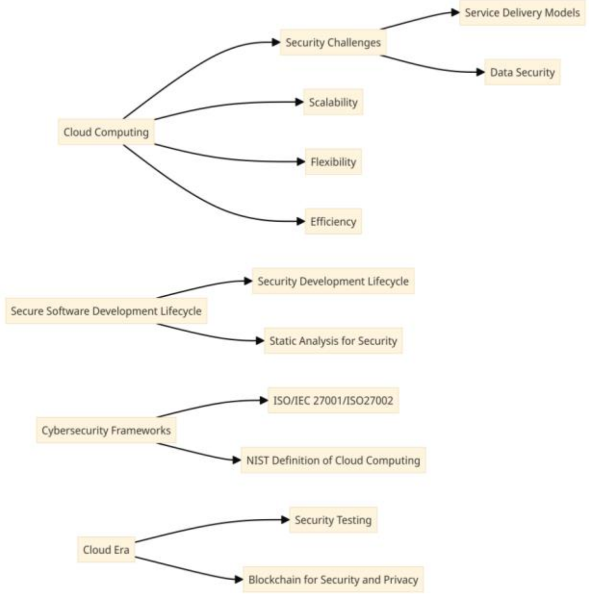

Figure 1: Secure Software Development in Cloud Computing [1, 2, 3, 4, 5, 7, 8, 11]

This makes the idea of a Secure Software Development Lifecycle (SSDLC) very central because it integrates security across the development process, from inception to deployment and maintenance of software. This approach helps in identifying and mitigating security risks early during the development process, which is costly compared to addressing security concerns after the software's deployment. Cybersecurity frameworks such as ISO/IEC 27001 and the NIST Cybersecurity Framework have been instrumental in guiding organizations on how to handle security and risk comprehensively and systematically.

The importance of these frameworks is given a boost in the cloud era when data breaches and cyber threats can have escalated implications because of the shared and interconnected nature of cloud services. This paper explores how security can be a part of software development processes to ensure that security considerations are co-evolving with rapid development cycles and technology innovation in cloud computing.

Literature Review

Security practices in cloud computing environments should be developed in the software development life cycle (SDLC) because of the distributed architecture that makes it possible for vulnerabilities to be exploited throughout the system. This section reviews key literature that underpins the development of secure software methodologies and the application of cybersecurity frameworks in cloud-based systems.

Security in the SDLC: One of the pioneering works by McGraw [1] underscores the importance of integrating security measures from the very early stages of software development. According to McGraw, security should not be treated as an afterthought but as an integral part of development. This helps to minimize vulnerabilities and potential attack vectors.

Cloud Computing Vulnerabilities: Subashini and Kavitha talk that cloud computing, as such, brings a set of specific security concerns mainly related to data confidentiality, integrity, and availability. They talk about a number of threat models and think that adopting a proactive approach to security in the SDLC might significantly abate these risks.

Cybersecurity Frameworks: The work by Mell and Grance [3] on the NIST Cybersecurity Framework provides a structured approach to managing cybersecurity risks. They recommend adoption in cloud computing to ensure consistent and comprehensive security practices covering topics such as identity management to data encryption.

Calder and Watkins analyze how ISO/IEC 27001 is implemented in the software development environments, particularly in establishing, implementing, maintaining, and continuously improving the ISMS in those environments. This standard is of paramount importance for cloud service providers dealing with enormous volumes of sensitive data.

Cost-Effective Security Practices: Bozic and Wotawa: [5] Incorporating security into the SDLC can be efficient and cost-effective, argues Bozic and Wotawa. They claim that the earlier in the development cycle the security problems, the less expensive they are to treat, and this is especially the case with cloud service development, for it moves quickly.

Problem Statement

The adoption of cloud computing has fundamentally changed the way software is deployed and managed. This change, in turn, creates some specific security challenges that classical software development lifecycles cannot efficiently address:

Data Security and Privacy Issues: In cloud environments, data is often distributed, and it's not uncommon for it to be stored in multiple locations. Such a feature significantly complicates conventional data security and privacy measures. Such dispersion of data storage makes it easier to fall into an increased risk of unauthorized access and data breaches.

Deployment Issues: The Ability of Cloud Systems to Scale Fast and Deploy Applications Quickly: Ease of Deploying an application takes a backward slide as far as security measures are in place. This is because most of the time the traditional security measures are too slow or inflexible to dynamically meet the requirements of cloud services. This is one of the challenges that result in the possibility of a security gap increasing.

Compliance and Regulatory Issues: Cloud services are exposed to many regulations that vary with respect to regions and specific industries. Compliance with them while retaining the flexibility and speed of software development is a lasting challenge for cloud service providers.

Solution

An SSDLC designed for cloud environments needs to be integrated into a secure manner to neutralize the risks that appear:

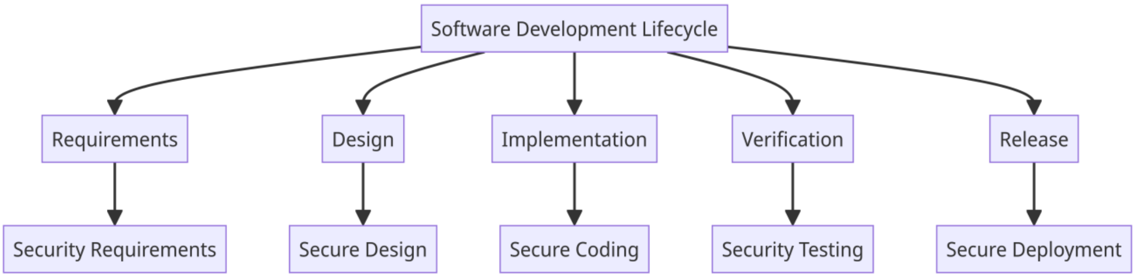

Figure 2: Security Development Lifecycle [7]

Early Integration of Security Measures: At every step of the SSDLC, from planning through to deployment and maintenance, security issues are considered. Only after incorporating techniques such as threat modeling, risk assessments, and security audits can risks be identified and mitigated before the application is put online. [1,8]

Advanced Security Technologies: The implementation of advanced cryptographic techniques and robust access control mechanisms defined for cloud architectures is the main premise. It is the basis for safeguarding integrity and confidentiality in distributed systems. [3,9]

Monitoring and Compliance: The SSDLC incorporates continuous monitoring and automated compliance tools in order to ensure ongoing fulfillment of regulatory requirements and the speedy adaptation to new threats. [2,4]

Impact

The strategic implementation of SSDLC in cloud environments provides significant benefits:

Better Security and Less Breaches: Any organization that deeply embeds security throughout its development process tends to see dramatically fewer security breaches and less data loss or theft.

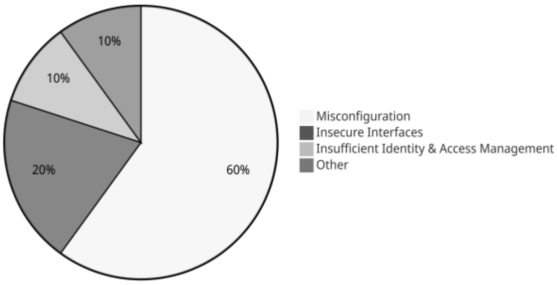

Figure 3: Distribution of Security Incidents in Cloud Environments [12]

Trust and Credibility: By ensuring appropriate security measures, the cloud service provider improves their credibility and builds trust among the end users, an essential factor for retention and satisfaction.

Table 1: Computer Crime and Security Survey [10]

Year	% Of Respondents Experiencing Security Incidents
2011	46
2013	43
2015	48

Cost Effectiveness: Early handling of security issues during development significantly decreases costs for mitigating vulnerabilities, following deployment.

Uses

The Secure SDLC methodologies are applied in all sorts of cloud services as applied below-

Infrastructure as a Service (IaaS): This type of security guarantees the secure state of the base infrastructural units, including virtual machines and storage units, ensuring to prevent unauthorized access and data breaches.

Platform as a Service (PaaS): A secure development platform is provided in this context to ensure application security right from the start of the development cycle, and developers are free to concentrate more on the functionality of the application and less on hidden security problems.

Software as a Service (SaaS): Applications that are run over the internet, which are served in this context, need to meet severe security standards to protect the data of its users from potential threats.

Future Scope

The future development of SSDLC in the cloud will likely witness several developments-

Blockchain for Improved Security: The use of blockchain technology could introduce new ways to manage data integrity and secure transactions across distributed networks.

Adaptation to the Dynamic Threats: As cyber threats evolve, so will the security practices. Future SSDLCs will need to be exceedingly adaptive, ensuring they can learn to respond quickly to new threats and technologies.

Conclusion

The move to the cloud requires significant adaptation on how to integrate security within the software development lifecycle. This paper has illustrated that the application of a Secure Software Development Lifecycle (SSDLC) is critical when dealing with the unique vulnerabilities cloud environments present. Integrating security throughout the development lifecycle and strictly following well-defined cybersecurity standards, such as ISO/IEC 27001 and the NIST Cybersecurity Framework, has proven to be effective in controlling these vulnerabilities. These controls not only ensure data security and privacy but also develop trust in the users and stakeholders, which is an essential component in the success of the clouds.

Recommendations

From the discussions and evidence provided, the following recommendations have been proposed for better security to be integrated in the software development life cycle for cloud computing:

Early and Continuous Integration of Security: The organizations shall integrate security at every stage of the SDLC, starting from the design phase to deployment and maintenance. This shall involve the regular execution of security audits, threat models, and the implementation of security controls designed for cloud architecture.

Adoption and Customization of Cybersecurity Frameworks: Adopting and customizing universally recognized frameworks such as ISO/IEC 27001 and NIST Cybersecurity Framework shall be recommended. Such frameworks shall be customized to meet peculiarities of cloud computing such that a comprehensive approach to security is ensured.

Improved Encryption Methods: Given the distributed data storage methodology of cloud computing, the development and adoption of better encryption methodologies shall play a crucial role. This shall be concentrated on the security of the data both in transit and at rest—particularly where there is sharing of the infrastructure among multiple tenants.

Continuous Education and Training: A lot needs to be done to provide continuous education and training on the new breed of cloud security threats and mitigation techniques for the developers and IT staff. This should include an updated insight into the latest security practices and technologies. It would be a valuable tool in the maintenance of a strong security posture.

Blockchain technology probably will provide new ways of securing transactions and data integrity preservation in distributed systems of the future because it is transparent and does not allow anything to be manipulated.

Compliance with regional and international standards: Compliance with regional and international standards and regulatory requirements are vital to ensure security and privacy. Companies need to use automated tools and maintain regular audits to stay updated with the ever-changing regional and international requirements and adapt their security practices.

Reference

[1]. McGraw, "Software Security: Building Security In," Addison-Wesley Professional, 2006.

[2]. S. Subashini, V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, 2011.

[3]. P. Mell, T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Special Publication 800-145, 2011.

[4]. A. Calder, S. Watkins, "IT Governance: An International Guide to Data Security and ISO27001/ISO27002," Kogan Page, 2016.

[5]. J. Bozic, F. Wotawa, "Security Testing: Approaches and Challenges," in Proceedings of the IEEE International Conference on Software Testing, Verification and Validation Workshops, 2015.

[6]. J. Vacca, "Computer and Information Security Handbook," Morgan Kaufmann Publishers, 2013.

[7]. M. Howard, S. Lipner, "The Security Development Lifecycle," Microsoft Press, 2006.

[8]. E. Chess, G. McGraw, "Static Analysis for Security," IEEE Security & Privacy, vol. 2, no. 6, pp. 76-79, 2004.

[9]. B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C," John Wiley & Sons, 1996.

[10]. L. Gordon, M. Loeb, W. Lucyshyn, R. Richardson, "2015 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, 2015.

[11]. A. Dorri, M. Steger, S. Kanhere, R. Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy," IEEE Communications Surveys & Tutorials, vol. 19, no. 4, Fourthquarter 2017.

[12]. Cloud Security Alliance, "Top Threats to Cloud Computing," 2016.