World Academy of Science, Engineering and Technology
International Journal of Computer and Systems Engineering
Vol:13, No:05, 2019

Specification of Requirements to Ensure Proper Implementation of Security Policies in Cloud-Based Multi-Tenant Systems

Authors : Rebecca Zahra, Joseph G. Vella, Ernest Cachia

Abstract : The notion of cloud computing is rapidly gaining ground in the IT industry and is appealing mostly due to making computing more adaptable and expedient whilst diminishing the total cost of ownership. This paper focuses on the software as a service (SaaS) architecture of cloud computing which is used for the outsourcing of databases with their associated business processes. One approach for offering SaaS is basing the system's architecture on multi-tenancy. Multi-tenancy allows multiple tenants (users) to make use of the same single application instance. Their requests and configurations might then differ according to specific requirements met through tenant customisation through the software. Despite the known advantages, companies still feel uneasy to opt for the multi-tenancy with data security being a principle concern. The fact that multiple tenants, possibly competitors, would have their data located on the same server process and share the same database tables heighten the fear of unauthorised access. Security is a vital aspect which needs to be considered by application developers, database administrators, data owners and end users. This is further complicated in cloud-based multi-tenant system where boundaries must be established between tenants and additional access control models must be in place to prevent unauthorised cross-tenant access to data. Moreover, when altering the database state, the transactions need to strictly adhere to the tenant's known business processes. This paper focuses on the fact that security in cloud databases should not be considered as an isolated issue. Rather it should be included in the initial phases of the database design and monitored continuously throughout the whole development process. This paper aims to identify a number of the most common security risks and threats specifically in the area of multi-tenant cloud systems. Issues and bottlenecks relating to security risks in cloud databases are surveyed. Some techniques which might be utilised to overcome them are then listed and evaluated. After a description and evaluation of the main security threats, this paper produces a list of software requirements to ensure that proper security policies are implemented by a software development team when designing and implementing a multi-tenant based SaaS. This would then assist the cloud service providers to define, implement, and manage security policies as per tenant customisation requirements whilst assuring security for the customers' data.

Keywords : cloud computing, data management, multi-tenancy, requirements, security
Conference Title : ICNSCC 2019 : International Conference on Network Security and Cloud Computing
Conference Location : London, United Kingdom
Conference Dates : May 23-24, 2019