DESCRIPTIVE STUDY ON SECURITY AS A SERVICE IN CLOUD COMPUTING

Safura Patel and Somaiya Haseeb Shaikh
Assistant Professor, Shree LR Tiwari Degree College and Pace Junior Science College, Thane, Maharshtra

ABSTRACT

Cloud computing is data storage and computing environment that uses the Internet to share resources. Cloud computing allows users to "pay as they go," lowering their costs and allowing individual users to access data in the cloud while focusing on the growth of their enterprises. Data integrity is a must in today's environment since users exchange private corporate information. Enterprises now require third-party services to manage and deliver software applications to extend their IT infrastructure. The recent usage of the cloud computing paradigm leads to new challenges towards securing Cloud services. The new concept of Security as a Service (SECaaS) enables the integration of security services into corporate infrastructure, leading to cost-effective business. The Security as a Service (SECaaS) architecture in the cloud is required due to the complexity of business applications. This paper discusses the numerous aspects of the SECaaS Model in cloud computing and the advantages in terms of corporate growth.

Keywords: Security as a Service, cloud computing, data integrity

INTRODUCTION

Cloud computing refers to applications and services providing reliability, low cost, high availability and flexibility for the end-user. Cloud computing, which runs on various distributed networks, has changed the way businesses store information. The cloud environment is provided with (Infrastructure as a Service (IaaS), software as a Service (SaaS), Platform as a Service (PaaS) in a new computing paradigm. The three basic model works only for storage. In contrast, if the data is sensitive, there is an emergence of the security as a Service model for security and data protection. Security as a Service is a way to outsource security-related services via the cloud over traditional methods. Security as a Service (SECaaS)opens up new opportunities to obtain innovative technically and economically flexible security solutions to fulfil the increasing demands. According to the recent working pattern in the changing world, corporate information and resources have to be protected. Many industries use the software as a service (Saas) tool and need to maintain permission and access for the devices. The security services often include authentication, anti-virus, anti-malware, intrusion detection, security event management. Outsourced security has paved the way in booming the IT industry. Security as a Service provides users with internet security services from various malicious threats and attacks as users are more vulnerable to attacks due to accessing the Internet access points. However, several issues are faced while developing Security as a Service (SECaaS) for cloud infrastructures. Due to this, users are vulnerable to attacks. Hence, there is a need for the cloud service provider to offer Security as a Service (SECaaS) to such users. Security as a Service (SECaaS) is being provided in several forms: subscription, Payment for utilized services, Freeware, and free of charge services. Below are the various forms of services

- **Usage-based** -The provider tracks how often the services they provide and charges accordingly. For example, if a user uses a service for two hours, the costs will be applied for the same.
- **Per usage** - The provider examines the number of authorized users from the company to use the services "Pay for each user". The provider keeps track of the number of employees in an organization availing the service, and accordingly, the organization is charged; this enables reduction cost of the business.
- **Tiered** – The provider provides several packages according to the user requirements. The more features or capabilities included, the higher the price. Huge companies opt for tiered packages as they have a complex business structure, such type of development is difficult for the providers since each user have a different requirement. Businesses have to pay heavy capital on the counterpart's security as a Service (SECaaS) models.
- **Flat** – A single version of the product is available and provided at the same price to the customers. Small scale business avails this service, but the same set of functionalities is not needed by the industry as the structure of the business and security requirement related to various threats differ.
- **Per features** – The user pays for each service the organization offers. The more features user need, the more user has to pay. The provider focuses on specific features as required by the user. The provider

has to pay more attention to various vulnerabilities and safety regulations.

- **Free of charge service** -The provider provides free of cost services with limited functionalities. This service model has a massive chance of intrusion detection as providers focus on paid services.

SECURITY AS A SERVICE

The widespread popularity of cloud computing has given rise to cloud security platforms and providers with Security as a Service (SECaaS). Data protection is an essential aspect of SECaaS. Data protection includes maintenance and access management of services. The security as a Service (SECaaS) model is delivered in the form of cloud services through standardized and comprehensive security functionality. Security as a Service (SECaaS) provides On-demand security services to shared and multi-tenant resources. The security of software services plays an important role in the cloud as various methods and tools for modelling security concerns are needed. Security as a Service (SECaaS) gives solutions to users to access devices. It allows security provisions to manage threats so that IT teams can focus on other vital factors of the organizations. Security as a Service (SECaaS) free up resources, gives total visibility to users with fast provisioning and greater agility in working because of ease management user's data are secure

The following are important aspects of Security as a Service.

1. **Device security** – The client's security policies and configuration devices are a significant concern for users as sensitive information must be protected. Tools that aggregate log and event information are to use to analyze real-time devices that help to detect possible anomalies
2. **Device Monitoring**-Security devices monitor and anticipate potential problems of users. Device monitoring enables the collection and analyzing information to detect suspicious behaviour or unauthorized system changes on your network, defining which types of behaviour should trigger alerts and appropriate action to be performed.
3. **Network security**-Network security protects your network and data breaches and other threats. In Security as a Service, network security deals with confidentiality, integrity and authentication. Tools and services that help you manage network access and distribute, protect, and monitor network services
4. **Software security**- Business-critical applications and data migration are trusted third-party cloud services providers (CSP), which require standardized authentication policies across all Software as a Service (SaaS) applications that enable policies such as single sign-on (SSO) and multi-factor authentication (MFA).
5. **Safety Regulations**-Security as a service focuses on safety regulations to manage backups and resume operations with little impact on the customer. Workplace ensures that local regulations for safety and security of an application. Tools that help you ensure that your IT and operations are back in no time when disaster strikes.
6. **Disaster recovery** –In case of unexpected Tools that help you ensure that your IT and operations are back in no time when disaster strikes. Tools that aggregate log and event information are analyzed in real-time to detect anomalies and intrusion

ADVANTAGES OF SECURITY AS A SERVICE

Security as a Service (SECaaS) can be described as cloud providing model for outsourcing cybersecurity services. Security as a Service (SECaaS) is highly recommended in cooperate infrastructure as a path for ease in security teams handling the responsibilities and business development.

- **Expertise** - The maintenance of security requires a high level of skills that businesses prefer to hire, and the market faces a shortage of cyber security specialists. A security skills gap can leave businesses with vulnerable attacks. With cloud service providers, companies are no longer have to worry about expert staff to provide network security.
- **Low Cost** - Cost is considered an important factor since on-premise maintenance requires enormous capital. The advanced IT security services can fulfil the business demands as no capital expenses on setting up hardware, software, and license than traditional security frameworks. This enables cost ownership for security platforms as the cloud supports Pay-As-You-Go Model or subscription.
- **Scalability** - Security management simply becomes another service as businesses pay providers for bills. Including and removing services becomes easier in SECaaS as vendors update the settings based on the requirement. This advantage of SECaaS has enabled businesses to work evenly while working from home.

- **Easy Management -** Traditional security frameworks generally have a complex management system. The response time is high on cloud-based services as it ensures that damage sustained to a network is more diminutive. The businesses focus on the development rather than management of services. Security as a Service (SECaaS) free up resources, gives total visibility through management dashboards and develops confidence that IT security is being managed competently by a team of outsourced security specialists.

CHALLENGES FACED IN SECURITY AS A SERVICE

As more organizations continue to adapt and move to the public cloud, it becomes even more critical to secure those environments, applications and services. Security as a Service (SECaaS) providers continues to enhance their offerings to add specific security services to their portfolios. Many organizations dive into cloud computing without sufficient knowledge and resources for furnishing their own security. As Security as a Service (SECaaS) matures, it becomes an even more viable option for securing enterprise public and hybrid cloud deployments. Security poses a significant challenge to the widespread adoption of cloud computing. Security as a Service (SECaaS) has various issues that make it diffident for many software applications to maintain reputation and superiority among cloud services.

Below are the few challenges faced in Security as a Service (SECaaS).

- **Increased Vulnerability-**In Security as a Service faces security vulnerability to withstand the effects of the hostile environment. Moving of businesses information to the cloud holds the responsibility for data security. Establishing a security architecture that forms trust boundaries with the businesses without vulnerability can be challenging unless support is provided from both ends.

- **Vendor Lock-in-Vendor** Lock-ins are restrictions that prevent users from switching from one service provider to another. In an IT environment, users can shift providers freely. Due to competition among vendors and various regulatory restrictions, businesses face the difficulty of switching, which impacts the loss of flexibility and loss of access to data.

- **Data Leakage-**Various Data Loss Prevention (DLP) tools that protect, monitor and verify the security measures are taken still services providers come across data leakage. Data leakage affects the effectiveness, reliability of the service providers, and performance. Within the cloud, Data Loss Prevention (DLP) services are provided as part of the build, such that all servers built for that client get the data loss prevention software installed with an agreed set of rules deployed.

RESEARCH CONTEXT

This research paper is theoretical in nature. The data has been collected through various sources of Secondary data. Secondary data has been collected through journals, research papers, books and websites. Secondary data collected from other researchers have served as a good source for collecting the required data to analyse the objectives.

LIMITATION OF STUDY

The research study is limited to understanding and the requirement of Security as a Service (SECaaS) to be introduced in the cloud computing model and to acknowledge the benefits and challenges faced while adopting SECaaS.

CONCLUSION

In this paper, we proposed Security as a service in the cloud. We thoroughly studied various research papers and other articles related to cloud computing and various security areas where the vulnerability of services is required. We have identified that multiple security services are provided. We discussed different categories of security services in the cloud, and we identified the major security issues in cloud computing and the reason for the same. We have also identified the advantages of Security as a service and challenges faced in cloud computing. We also described the term cloud and its services. Our ongoing work is to analyse the security issues in Security as a service (SECaaS) and to analyse the various security as a service models.

REFERENCES

1. http://www.ijiere.com/FinalPaper/FinalPaperTransparent%20Data%20Loss%20Prevention%20as%20Security-as-a-Service%20from%20Cloud170922.pdf/
2. https://jisajournal.springeropen.com/articles/10.1186/1869-0238-4-11#Sec28
3. https://cloudcomputing-news.net/news/2017/jun/06/deeper-dive-cloud-security-service-advantages-and-issues/

4. https://www.liquidweb.com/blog/security-as-a-service-SECaaS/
5. https://www.crowdstrike.com/cybersecurity-101/security-as-a-service-SECaaS/
6. https://www.academia.edu/32053180/Security-as_a_service_in_Cloud_Computing_SECaaS/
7. https://www.okta.com/identity-101/security-as-a-service-SECaaS/