OPEN ACCESS Freely available online

Journal of Information Technology & Software Engineering

Perspective

An Overview on the Different Privacy Threats to Cloud Based Application

Latham Ruto*

Department of Telecommunication and Information Technology, Kenyatta University, Nairobi, Kenya

DESCRIPTION

Cloud computing is a novel approach for delivering computer services through the Internet, where computation is given as a service. Because computing services are given at considerably lower prices than their own IT infrastructure, cloud computing is a popular alternative among SMEs. Computing and data storage are outsourced to cloud service providers in the cloud computing model. Customers do not have complete control over their data and applications. As a result, security risks are added to the equation, and data security becomes the key worry for cloud consumers when selecting cloud services. The most serious threats to cloud-based apps are data breaches, data loss, poorly built APIs, denial of service, and misconfiguration or inefficient design.

Data breaches

An attacker or hacker tries to get unauthorized access to data under this type of danger. The most well-known data breach attack is SQL injection. One of the most dangerous threats is data breach.

Data loss

Another concern is data loss, which occurs when a malevolent user or software destroys data on purpose. Permanent data loss has a significant negative impact on both cloud service providers and customers. Malicious assaults are not the only cause of data loss; other causes of failures and calamities, such as fires, floods, or earthquakes, can also harm a CSP's infrastructure. Cloud clients, on the other hand, are responsible for establishing and maintaining data security solutions. If a cloud customer encrypts data before uploading it to the cloud and subsequently loses the private/public keys, the encrypted data is useless because it can't be decoded.

Insecure interfaces and APIs

CSPs give APIs to cloud customers so they can engage with cloud services. These APIs provide a wide range of management, monitoring, and CRUD functions.

All of these APIs' security is dependent on the API's good design and proper usage by customers, which means cloud clients, should follow CSP's API rules and best practices.

If the API authentication and access control are not done effectively, attackers may be able to utilize the APIs for their own purposes.

Organizations or third parties may use the cloud service's basic APIs to build their own services on top of the basic cloud APIs, which provide users with more complicated services. These additional services are viewed as a new API layer that, like the underlying base layer, must be secured.

Denial of service

The goal of a denial of service attack is to prevent cloud customers from accessing their apps or data. In this situation, the service uses a lot of system resources, such as memory, disc space, and network bandwidth.

If the attackers/hackers succeed in their goal, the system will slow down, and cloud customers will be unable to use the service correctly as a result of the DoS assault. Known as distributed denial of service, denial of service assaults can be launched simultaneously by multiple attackers or attack sources (DDoS).

Denial of service attacks can also be carried out via exploiting a flaw in a web server, database, or other cloud resource. If such vulnerability exists, an attacker may be able to take down the system by launching an attack with a very little payload, resulting in a denial of service.

Insufficient design, planning, and misconfiguration

Many businesses are rushing into cloud computing without fully comprehending the situation. An organization may face various problems if it lacks appropriate knowledge of the cloud service ecosystem. Applications that are not suited or capable of cloud service, for example, can be pushed into the cloud.

Internal cryptography, network monitoring, and incident response data are sometimes transferred to the cloud. Otherwise, storing such data in the cloud might not be a good idea.

Correspondence to: Latham Ruto, Department of Telecommunication and Information Technology, Kenyatta University, Nairobi, Kenya, E-mail: 556784ruto@edu.ke

Received: 04-Apr-2022, Manuscript No. JITSE-22-17567; **Editor assigned:** 08-Apr-2022, PreQC No. JITSE-22-17567 (PQ); **Reviewed:** 26-Apr-2022, QC No. JITSE-22-17567; **Revised:** 03-May-2022, Manuscript No. JITSE-22-17567 (R); **Published:** 11-May-2022, DOI: 10.35248/2165-7866-22.12.299.

Citation: Ruto L (2022) An Overview on the Different Privacy Threats to Cloud Based Application. J Inform Tech Softw Eng. 12:299.

Physical security threats

Data and application security are equally crucial in the cloud. A data center is a location in the cloud where actual data is stored. To manage computing service demands, it consists of processing, storage, networking, power, and cooling infrastructure.

Physical security ensures that a data center's tangible resources are protected from all types of incidents that could damage the infrastructure. Physical security comprises safeguarding against all potential sources of physical harm, such as fire, flood, and natural catastrophes. Data center physical security is a layered strategy that follows a well-defined security framework.

CONCLUSION

With the growing demand for cloud computing services, data security and privacy are critical. To keep client data safe and secure, security is a continual and continuing process that must be audited and altered on a regular basis.

Before migrating their data and apps to the cloud, consumers must evaluate the cloud service. Security solutions should be able to combat current threats as well as foresee future ones, according to both CSPs and cloud clients.