Hindawi
Security and Communication Networks
Volume 2023, Article ID 9810125, 1 page
https://doi.org/10.1155/2023/9810125

Retraction

Retracted: Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions

Security and Communication Networks

Received 10 October 2023; Accepted 10 October 2023; Published 11 October 2023

This article has been retracted by Hindawi following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of one or more of the following indicators of systematic manipulation of the publication process:

(1) Discrepancies in scope

(2) Discrepancies in the description of the research reported

(3) Discrepancies between the availability of data and the research described

(4) Inappropriate citations

(5) Incoherent, meaningless and/or irrelevant content included in the article

(6) Peer-review manipulation

The presence of these indicators undermines our confidence in the integrity of the article's content and we cannot, therefore, vouch for its reliability. Please note that this notice is intended solely to alert readers that the content of this article is unreliable. We have not investigated whether authors were aware of or involved in the systematic manipulation of the publication process.

Wiley and Hindawi regrets that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our own Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] D. K. Saini, K. Kumar, and P. Gupta, "Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions," *Security and Communication Networks*, vol. 2022, Article ID 4943225, 9 pages, 2022.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 4943225, 9 pages
https://doi.org/10.1155/2022/4943225

Review Article

Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions

Dinesh Kumar Saini, Krishan Kumar, and Punit Gupta

Department of Computer and Communication Engineering, Manipal University Jaipur, Jaipur, Rajasthan, India

Correspondence should be addressed to Punit Gupta; punitg07@gmail.com

Received 11 February 2022; Accepted 26 March 2022; Published 12 April 2022

Academic Editor: Mukesh Soni

Cloud computing is a new model for providing computing services, where computing is delivered as a service over the Internet. Cloud computing is a very popular choice among SMEs because computing services are provided at much lower prices compared to their own IT infrastructure. In the cloud computing model, computing services and data storage are outsourced to cloud service providers. Customers do not have full control over applications and their data. Therefore, an added overhead of security risks comes along, and the security of data becomes the primary concern for cloud customers when considering cloud services. This paper explores various deployment models of cloud computing services and IoT (Internet of Things), figures out associated data security issues with them, and suggests a metric-based solution to assess security provided by cloud services.

1. Introduction

NIST (National Institute of Standards and Technology) mentions, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [1].

Cloud computing offers many great benefits like agility, scalability, sustainability, reliability, and affordability, yet customers (especially data-sensitive organizations like banks, defense, government, and financial institutions) think critically about opting for cloud services because data security is the main concern behind their reluctance.

Cloud service providers (CSPs) focus on security mechanisms primarily because security is the most important attribute in the deployment and use of cloud computing services [2]. Mostly, available literature talks about different security solutions to encounter existing threats and service-level agreements of security policy implementation, but the challenging part is that data security is a spiral process that must be reviewed consistently, and new security solutions must take place in order to address anticipated future attacks. To implement new security solutions, CSPs and cloud customers must ensure that to-be-implemented security solutions should address two key aspects. First, they should not compromise with the performance; second, they should be able to gauge future attacks.

This paper is organized into six sections.

(i) Section 2 of this paper talks about cloud computing models and services.

(ii) Section 3 sheds light on different threats that occur in the cloud computing environment.

(iii) Section 4 highlights security issues in various computing services.

(iv) Section 5 lists security assessment metrics that help cloud customers to decide upon the data and application security in cloud.

(v) Section 6 proposes a model for cloud security assessment using metrics mentioned in Section 5.

(vi) Section 7 talks about the research conclusion and future prospects.

2. Cloud Deployment Models and Cloud Computing Services

According to NIST, there are five essential characteristics of cloud, "on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service" [3]. All cloud deployment models and services must have these characteristics.

There are two basic types of cloud deployment models: private and public. By mixing these two types, there emerge two more variants: hybrid and multicloud.

According to Armbrust et al., *private cloud* is used to set up internal data centers of an organization. Private clouds are not for public use, whereas *public clouds* are deployed to use by organizations on a *pay-as-you-go* basis [4]. Public clouds offer shared resources; that is why they are the most affordable computing solutions for small- and medium-sized enterprises.

Cloud customers subscribe to public clouds for computing services by paying monthly or annual subscription fees depending upon the services they use and their service contract. Some examples of well-known public cloud providers are Microsoft Azure, Amazon Web Services (AWS), and Google Cloud.

According to NIST, hybrid cloud is "a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together" [3].

According to RedHat, "multicloud is a cloud approach made up of more than one cloud service, from more than one cloud vendor, public or private" [5].

Figure 1 depicts various cloud deployment models.

Cloud deployment models offer four types of cloud computing services. A cloud computing service tells about what resources will be provided as part of the computing service. These cloud computing services are software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), and database as a service (DBaaS).

2.1. IaaS. In infrastructure as a service, CSP manages hardware part like virtual machines (VMs), storage, and networking, while cloud customer manages operating systems and other types of required software for their business needs like middleware, runtime environments, database, and application software [6]. Some IaaS examples are Microsoft Azure, Amazon Web Services (AWS), and Google Compute Engine (GCE).

2.2. PaaS. Platform as a service is one layer above IaaS. In PaaS, CSP manages IaaS along with basic software stack like operating systems, utility and analytics software, development tools, and database management systems, whereas cloud customer manages application software and services [7]. Azure App Service, AWS Elastic Beanstalk, and Google App Engine are some examples of PaaS.

2.3. SaaS. As the name suggests, software as a service delivers application software over the Internet. CSP manages everything in this model of computing service from hardware to application software [7]. Cloud customers access the application software over the Internet without bothering of complex software and hardware management. Microsoft Office 365, Google Drive, Dropbox, and Cisco WebEx are some examples of SaaS.

Figure 2 shows servicewise resource provisioning in various cloud computing services.

3. Security Threats in Cloud

Cloud computing is the preferred computing solution for small- and midsized enterprises because they have to spend less on IT infrastructure management and maintenance [8]. However, the security of data is their main concern when SMEs think of opting for cloud services. Data security in cloud eventually ascertains the safety of data that leads to winning customer's trust in CSP.

According to CSA (Cloud Security Alliance), most notable security issues in cloud are data breaches, misconfiguration of cloud resources, poor security architecture and strategy, poor credential and access management, insider threat, account hijacking, insecure APIs, weak control plane, metastructure failures, cloud usage visibility, and cloud service abuse [9]. Table 1 lists down major security incidents that happened over the last decade.

As we see in Table 1, security issues adversely affect cloud services. Data breaches, loss of data, poorly designed APIs, denial of service, and misconfiguration or inefficient design are the most critical threats for cloud-based applications.

3.1. Data Breaches. In this kind of threat, an attacker or hacker tries to get access to data illegally. SQL injection is the most known attack for data breaches. Data breach is considered one of the serious threats.

In web applications, SQL injection is a common attack for data breaches. In cloud, it is more dangerous than web applications because in cloud many applications share one database. Therefore, vulnerability in one application can potentially expose the data of all applications to the attacker.

3.2. Data Loss. Data loss is another threat, in which malicious user or software destroys data intentionally. Permanent data loss leads to a large negative impact on both CSP and cloud customer. Not only do malicious attacks cause loss of data, but also there could be other reasons for failures and disasters like fires, floods, or earthquakes that affect a CSP's infrastructure adversely.

However, cloud customers are also responsible for implementing and managing data security solutions. If a cloud customer encrypts data before uploading to cloud and loses the private/public keys, then encrypted data will be of no use because it cannot be decrypted back. When it comes to handling and protection of data, it is a shared responsibility between CSP and cloud customer.

In order to mitigate data loss issues, CSP should take a timely backup of data.

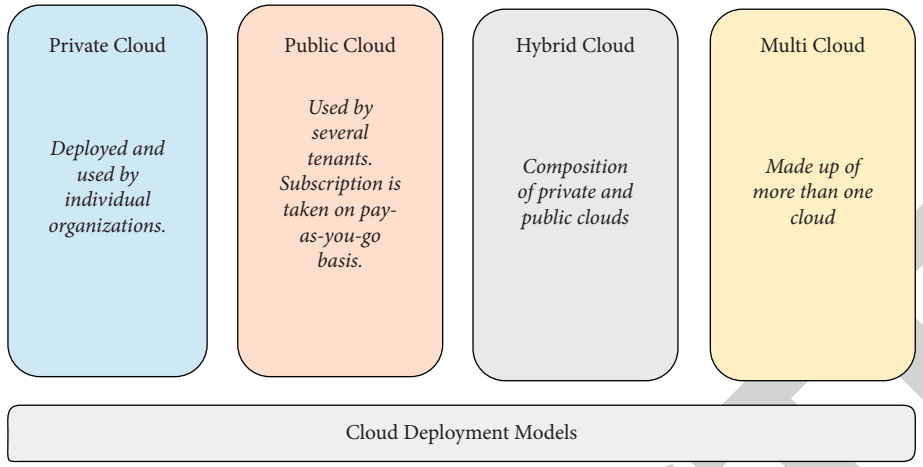

Figure 1: Different types of cloud deployment models.

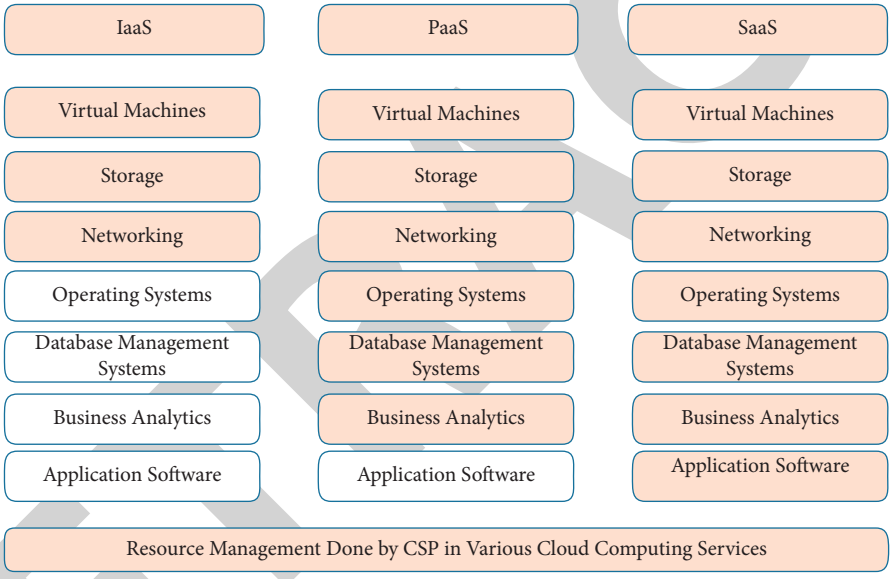

Figure 2: Resource provisioning in cloud computing.

3.3. Insecure Interfaces and APIs. In cloud computing, CSPs provide APIs to cloud customers to interact with cloud services. These APIs offer a wide range of functionality for management, monitoring, and CRUD operations.

Security of all these APIs depends on the correct design of the API and proper usage by customers meaning that cloud customers should follow CSP's instructions and best practices for the API.

If authentication and access control of the API is not implemented correctly, then it is possible for attackers to abuse the APIs for their own purpose.

Sometimes, organizations or third parties use the basic APIs of the cloud service to implement their own services on top of basic cloud APIs, which offer customers services that are more complex. These new services are seen as a new API layer that needs to be secured along with the underlying base layer.

In order to design secure APIs that are safe from malicious data access, CSPs must consider the best following practices for API development:

(i) Proper authentication, encryption, access control, and activity monitoring. All APIs must use API keys to access cloud services, and those keys must not be reused.

(ii) Rely on standard API frameworks like Open Cloud Computing Interface (OCCI) and the Cloud Infrastructure Management Interface (CIMI) [21, 22].

(iii) All APIs must be secured with the API keys. API keys must not be hard-wired in code, and they should not be pushed to GitHub or any other code repository. If any attacker by chance gets the API key, then they can access the data or service on customer's behalf [23].

Table 1: Security issue incidents in cloud.

S. no.	Type of threat	Business impact	Security issue
1	Uber's AWS account was hacked in 2016, which compromised 57 million users' personal information worldwide [10]	Loss of reputation and trust of customers or partners	Data breach
2	Voipo database containing customer call information and credentials became a victim of a data breach in 2019 [11]	Legal and contractual liabilities	Data breach
3	In 2017, AWS S3 misconfiguration caused a data leak of 123 million American households [12]	Confidential information leakage	Misconfigurations and inadequate change control
4	In 2017, Accenture negligently left private data across four unsecured Amazon S3 buckets that exposed passwords and secret decryption keys [13]	Severe business impact like financial loss and reputation damage	Lack of cloud security architecture and strategy
5	In 2017, hackers managed to get OneLogin's AWS keys to gain access to the company's AWS platform via APIs from an intermediate host [14]	Snoop on data in transit and data in rest	Insufficient identity, credential, access, and key management
6	In June 2014, code spaces failed to protect its administrative console with multifactor authentication [15]	Loss of confidential information	Account hijacking
7	In 2018, Tesla suffered a malicious insider attack [16]	Loss of confidential information and intellectual information	Insider threat
8	In 2018, Facebook suffered a significant data breach affecting more than 50 million [17]	Loss of confidential user information	Insecure interfaces and APIs
9	In 2018, more than 120 million unique identification numbers issued by the Brazilian Federal reserved for Brazilian citizens were exposed from S3 bucket because of weak control plane configuration	A weak control plane could result in data loss by either theft or corruption. This could lead to a massive business impact, particularly if data loss includes private user data	Weak control plane
10	In 2018, Microsoft security intelligence report documented that "79 percent of SaaS storage apps and 86 percent of SaaS collaboration apps do not encrypt data both at rest and in transit" [18]	Negative impact on service customers	Metastructure and applistructure failures
11	According to 2018 research conducted by cloud security firm lacework, "more than 22,000 container orchestration and API management systems are unprotected or publicly available on the Internet, highlighting the reality of the risks of operating workloads in the cloud" [19]	Lack of governance, awareness, and security are the major risks involved	Limited cloud usage visibility
12	Spread of Zepto variant of the Locky ransomware via different cloud storage services [20]	Financial loss to customer	Abuse and nefarious use of cloud services

(iv) Add application and domain restrictions to API keys so that if a request comes from a different domain, then the server does not entertain it.

3.4. Denial of Service. Denial of service attack aims to stop cloud customers from accessing their applications or data. In this case, service consumes a large amount of system resources like memory, disk space, or network bandwidth.

If attackers/hackers are able to achieve this goal, then it usually results in system slowdown, where cloud customers are not able to use the service properly after the DoS attack. Denial of service attacks can be executed from several attackers or attack sources at once, which is known as distributed denial of service (DDoS). In February 2020, AWS suffered a DDoS attack, stopping a 2.3 Tbps attack [24].

Denial of service attacks can also be executed by identifying a vulnerability inside a web server, database, or other cloud resources. If such a vulnerability exists, an attacker may be able to take out the system by using an extremely small payload in his attack that would result in a denial of service.

3.5. Insufficient Design, Planning, and Misconfiguration. Many companies jump on cloud computing without understanding the full context of the cloud environment. Without sufficient understanding of the cloud service environment, an organization may run into several issues. Applications, for instance, can be pushed into the cloud, which are not suitable or capable for cloud service.

Sometimes, information about internal cryptography, network monitoring, or incident response is pushed into the cloud. Pushing such information into the cloud may not be advisable otherwise.

In addition, unknown operational or architectural issues arise when developers, designers, or architects are not familiar with cloud development. Therefore, before moving to a cloud environment, it becomes necessary for an organization to understand all risks associated with using cloud

services. For some applications, it may be necessary to redesign core elements of services pushed into the cloud, for example, security functions with respect to key management.

3.6. Physical Security Threats. Physical security in cloud is as important as data and application security. A data center is a location, where actual data is stored in cloud. It consists of computing, storage, networking, power, and cooling infrastructure to handle computing service demands.

Physical security ensures the protection of all tangible resources of a data center from all sorts of events that can cause damage to the data center's infrastructure. Physical security includes protection from all factors that can cause physical damage like fire, flood, and natural disasters.

Physical security in data centers is a multilayer approach that follows a well-chiseled security framework.

Hardware resources (power, cooling, compute, storage, cabling, fire alarms, CCTVs, etc.) and monitoring systems (data center monitoring systems-DCIM) are two main components of physical security.

In a data center, hardware resources are prone to physical damage; therefore, they need physical security. On the other hand, DCIMs are used to monitor various systems like power supplies, cooling unit temperature, and other control units.

Poorly configured DCIMs could be smooth ground for attackers. Exposing these systems without adequate protection may lead to false readings of monitoring systems. Recently, over 20,000 data center management systems have been exposed to attackers [25].

4. Security Issues in Different Cloud Computing Services

The main difference between dedicated and cloud deployments is that when customers set up their own infrastructure, they have their own hardware and software stack, and they are responsible for its security and management, but in cloud, managing resources is a shared and mutual responsibility of CSP and cloud customer. Therefore, data security in cloud is different from conventional security models.

For example, if a customer subscribes to a PaaS computing service, then CSP manages hardware infrastructure along with operating systems and other types of utility software, while cloud customer manages application software and services. In this scenario, customer will be responsible for securing the applications and data, while CSP will be responsible for securing infrastructure and platform [26].

As we have mentioned earlier, in dedicated infrastructure, customers have full control over hardware, software, and data, but in cloud model, data are stored on remote servers (on CSP's datacenters) [27]. Therefore, traditional security solutions will not be just enough, and we will have to take additional security measures.

Securing infrastructure, business applications, and data without compromising affordability, performance, agility, and scalability should be the primary goal of security solutions in cloud.

Security in cloud is a multidimensional approach that should take both physical and software security into account right from secure logins to network access. All applications must be deployed, keeping all security measures in mind [26].

The aim of security solutions should not be limited to addressing existing threats, but they should be able to take preventive measures and actions to combat possible future attacks.

Authentication, authorization, and encryption are the keys to secure data and applications. Authentication ensures that the right person or program is accessing the services, application, and data. Authorization ensures that the person or entity has permission to access the service, application, or data.

Encryption is a mechanism of encoding data into incomprehensible *ciphertext* using a cryptographic key. Encrypting data ensures that even if there is a breach, hackers will not be able to read or understand that data [28].

Authentication, authorization, and encryption have their own purposes for data security. Authentication is used for data access. Authorization is used for operation on data, and encryption is used for secure transportation of data over the network.

Apart from data theft and misuse, there are many other issues that appear in computing services related to resource configuration, network security, and accessibility of service.

Cloud storage is one of the most precious and important resources; therefore, no one is granted direct access to it. Nodes in public cloud are assigned a public IP address to connect to the Internet, but in order to provide secure access to hosts located in the private and public subnets of private virtual cloud networks, bastion hosts are used. Bastion host is used to connect users from specific IP addresses to target resources. Only specific IPs can access resources like cloud storage [29].

4.1. Security Issues in IaaS. When customers use IaaS, they have to take care of all security questions because they only get VMs, storage, and networking from CSP; rest all customers have to manage. Customers have to install, monitor, and operate all software components on their own.

At the IaaS level, virtualization technologies are used to create VMs because many tenants share the same physical hardware in the form of virtual machines.

Data visibility and resource isolation in shared hardware are the most critical issues faced in IaaS. Data confidentiality of guest VMs and denial of service attack by another guest VM are other critical issues [30].

4.2. Security Issues in PaaS. In PaaS, the responsibility of data and infrastructure security falls on both CSP and cloud customer's shoulders.

Most cloud customers use PaaS for their businesses; therefore, it becomes essential to figure out and address security issues in PaaS. A 2019 McAfee Cloud Adoption and

Risk Report mentions that the number of PaaS users is expected to increase in big numbers because organizations are taking their applications to cloud.

Misconfiguration is one of the main security issues in PaaS environments from the CSP side. It often happens when multiple resources are connected, but they are not configured properly. For example, Kubernetes and Docker containers interact with one another without proper permissions [31].

On the other hand, cloud customers are responsible for securing applications, data, and user access. At the application level, proper authentication, authorization, and data encryption must be implemented to secure data and application.

For example, if password-based authentication is implemented, then there must be a strong set of password policies, passwords must be generated with salted password hashes, and they should be stored in an encrypted format. If, by mistake, passwords are stored in plaintext, then malicious system admin can misuse user credentials [32]. Figure 3 shows an example of how to encrypt passwords.

In the public cloud, password-based authentication is not considered good because customers use the Internet to connect to cloud services; therefore, the authentication in the public cloud is more vulnerable than private cloud.

There are other newer and safer methods available for authentication like multifactor, biometric, and YubiKey (hardware authenticator) authentication. YubiKey generates keystrokes that are used along with passwords. It is an extra layer of protection beyond a password [33]. Amazon Web Services (AWS) uses multifactor authentication for identity and access management [34].

In order to keep data secure in cloud, cloud storage encrypts data before writing to storage devices. This encryption happens after customer data arrives at cloud [35]. To be more secure, one additional layer of encryption can be applied, that is, client-side encryption. Client-side encryption is done before data are uploaded to cloud.

Along with authentication and encryption, cloud customer must implement role-based access controls for both data and applications. Role-based access controls enable users to access only those resources, which they have been granted permission for.

4.3. Security Issues in SaaS. In SaaS computing service, except data and application access, CSP manages everything else. Cloud customer is solely responsible for what data they put in cloud and who can access it. In SaaS, CSP takes care of almost all security attributes because all resources right from hardware resources to the entire application software suite are managed by CSP. Theft of data, poor access control, poor or no encryption of data in transit, and poorly managed applications at the cloud side are major security threats in SaaS.

While choosing a SaaS service cloud, customer must look into the cloud provider's security solutions and policies. Timely auditing and security reports increase the confidence level of cloud customers [36].

```php
<?php

$hash = password_hash('Str0ngP@$$word', PASSWORD_DEFAULT);

echo "password hash : ", $hash;
echo "<br>";
if (password_verify('Str0ngP@$$word', $hash)) {
    echo 'Password is valid!';
} else {
    echo 'Invalid password.';
}
?>

OUTPUT
======
password hash : $2y$10$n/gNsv2QqNNlkNdsgHe9MuCF6LdZB8cEzyJRH7g1BzaqrR/Ob3n56
Password is valid!
```

Figure 3: Generation of salted password hash.

5. Cloud Security Assessment Metrics

As more and more customers are taking their applications and data to the cloud, data security becomes a very important factor. Data and applications must be secured in all possible manners.

To achieve a high level of security, data security requirements must be clear enough before transiting to cloud. These requirements should allow the customer to evaluate the security of the cloud environment and help cloud customers to mitigate cloud-specific risks.

Here we are proposing ten cloud security assessment metrics that help customers to assess the security of cloud service. Before moving to cloud, every customer must assess cloud service by following security assessment metrics mentioned in Table 2. Table 2 lists 10 security assessment metrics along with security questions asked as part of each assessment metric.

6. Cloud Security Assessment Using Metric-Based Model

Data security assessment in cloud is not a one-time task. Security threats in cloud environments are constantly evolving; therefore, there must be adequate processes, measures, and technologies in place to prevent cloud infrastructure from all possible threats [37].

For cloud customers, the situation becomes more frustrating and challenging. IoT data have to be moved to cloud in order to leverage cloud storage. IoT network is a personal LAN and carries a lot of confidential data. If IoT data is moved to cloud without proper checks, then it may be risky at times because not all cloud services are appropriately secure.

In order to mitigate security risks, cloud customers should have strong but simple and convenient mechanisms in place to assess the quality of security solutions. Metric-based assessment is worth using because it is easy to implement and provides quantitative results that enterprises can use for deciding whether they should opt for a cloud service or not.

Security assessment metrics and security questions mentioned in Section 5 are taken into account for constituting a security metrics-based assessment model for cloud computing services.

Table 2: Cloud security assessment metrics.

1. Governance, risk, and compliance metrics
   (a) What kind of regulations will be in place for cloud customers in order to protect user's information and privacy?
   (b) Will it be a shared responsibility of CSP and cloud customer to implement governance and compliance processes?
   (c) Will CSP's governance and notification processes match cloud customer's requirements in order to use the cloud services?
   (d) What are the associated risks related to data storage location?
2. Audit metrics
   (a) Are there appropriate mechanisms from CSP's side to report all kinds of audit incidents to cloud customers?
   (b) Is there an appropriate logging mechanism in cloud for recording all kinds of security events and actions?
   (c) Is incident reporting and handling mechanism meeting all cloud customer's requirements?
3. Access control metrics
   (a) What kind of access control is provided by cloud services? Is it matching cloud customer's needs?
   (b) Is MFA (multifactor authentication) in place for all cloud services?
   (c) Is user's access to cloud services being monitored, recorded, and reported properly?
4. Data and information security metrics
   (a) Do CSP and cloud customer know about all the data assets being used in cloud?
   (b) Are all roles and responsibilities clearly mentioned and described for both CSP and cloud customer?
   (c) Do data stored in cloud conform to all security standards and measures?
5. Privacy policy metrics
   (a) What will be the data store and purge policy for personal information stored in cloud?
   (b) Are data protection laws and regulations clearly mentioned for the location of data storage and data usage?
   (c) How is personal information being handled in cloud? Are there appropriate controls in place to keep personal information safe and secure?
6. Security provisions metrics
   (a) Depending on the cloud model, who is responsible for application security? Cloud customer or CSP?
   (b) Are cloud customers' data appropriately encrypted while storing in cloud?
7. Cloud network metrics
   (a) What mechanisms are there in place to deal with DoS (denial of service)?
   (b) Are there enough checks in place for intrusion detection and prevention from CSP's side?
   (c) Are logging and notification mechanisms in place at the network level?
   (d) Is customer network access separate from provider network access?
8. Physical infrastructure metrics
   (a) Is physical infrastructure fully secured? How will CSP ensure cloud customer about it?
   (b) How does CSP ensure availability of service in case of any kind of physical threat or resource failure?
   (c) How does CSP ensure malicious insider attack?
9. Security terms and SLA metrics
   (a) Does SLA mention all the security responsibilities and conditions?
   (b) How does SLA make sure of security management? Are there enough metrics to measure the performance and effectiveness of security?
   (c) How will security incidents be notified and handled? Does SLA contain detailed information about it?
10. Exit process metrics
   (a) Is it clearly mentioned that all customer data will be deleted from the CSP's environment at the end of the exit process?
   (b) What will be the data destroy and purge policy during the exit process?

Table 3: Metric-based security assessment grades.

S. no.	Percent points scored out of 30	Grade	Good for types of data stored
1	91% and above	A	Restricted, confidential, internal, and public
2	81% to 90%	B	Confidential, internal, and public
3	71% to 80%	C	Internal and public
4	Below 70%	D	Public

There are a total of 10 metrics and 30 questions as part of the metrics given in Section 5. Each question carries a weight of one point. While assessing a cloud service, customers have to answer all questions in a yes/no format. At the end of answering all questions, total score is summed up, and a grade is calculated on a percentage basis. There are four types of data/information, restricted or highly confidential, confidential, internal, and public or declassified. A calculated grade helps cloud customers in making a decision about what kind of information they can keep in cloud. According to the grade scored by a cloud service, customers will also be able to decide if they should opt for the given cloud service or not.

Table 3explains the grades and types of data that can be stored in cloud depending upon the grade scored.

7. Conclusion and Future Prospects

With the increasing demand for cloud computing services, security and privacy of the data are very important. Security

is a continuous and ongoing process that must be audited and revised from time to time in order to keep customer's data safe and secure.

Cloud customers must assess the cloud service before moving their data and applications to cloud. Both CSPs and cloud customers should ensure that security solutions are able to address existing threats and able to predict future ones.

It has been observed that intruders and hackers take advantage of glitches in security solutions and poor implementation of security policies (e.g., weak passwords, open ports, and unencrypted data).

New developments in cloud for distributed computing like edge, fog, and Internet of Things (IoT) computing will bring new challenges from data security and user privacy's perspective. Reviewing and updating security solutions and policies should be a consistent process along with the technological updates.

In this paper, we presented a metric-based security assessment model for cloud services, where we took important security metrics that are calculated and are taken into account to make a decision about what kind of data they can move to cloud.

Data Availability

No dataset was used in this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] US Department of Commerce, *NIST Cloud Computing Standards Roadmap*, U. S. Department of Commerce, NW, Washington, D.C., USA, 2013.

[2] C. Vidal and K.-K. R. Choo, "Situational crime prevention and the mitigation of cloud computing threats," *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 239, pp. 218–233, 2018.

[3] P. M. Mell and T. Grance, "The NIST definition of cloud computing," *Sepia*, 2011.

[4] M. Armbrust, A. Fox, R. Griffith et al., "Above the Clouds: A Berkeley View of Cloud Computing," 2009, http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html.

[5] RedHat, "What Is Multicloud?," 2018, https://www.redhat.com/en/topics/cloud-computing/what-is-multicloud.

[6] Microsoft, "What Is IaaS? Infrastructure as a Service | Microsoft Azure," 2021, https://azure.microsoft.com/en-in/overview/what-is-iaas/#overview.

[7] Microsoft, "What Is PaaS? Platform as a Service | Microsoft Azure," 2021, https://azure.microsoft.com/en-in/overview/what-is-paas/#overview.

[8] V. Mike, "Survey Predicts Massive Migration to the Cloud - DevOps.Com," https://devops.com/survey-predicts-massive-migration-to-the-cloud/.

[9] R. Mogull, J. Arlen, F. Gilbert et al., "Security guidance for critical areas of focus in cloud computing," 2021, https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf.

[10] R. Gladys, "Uber Discloses Year-Old AWS Data Breach, Exposing Millions of Users -- AWSInsider," 2017, https://awsinsider.net/articles/2017/11/21/uber-aws-data-breach.aspx.

[11] O. Charlie, "VOIPO database exposed millions of call and SMS logs, system data | ZDNet," 2019, https://www.zdnet.com/article/voipo-database-exposed-millions-of-call-and-sms-logs-system-data/.

[12] B. Thomas, "120 million American households exposed in "massive" ConsumerView database leak," 2017, https://www.forbes.com/sites/thomasbrewster/2017/12/19/120m-american-households-exposed-in-massive-consumerview-database-leak/?sh=2d6b0f837961.

[13] W. Zack, "Accenture Left a Huge Trove of Highly Sensitive Data on Exposed Servers | ZDNet," 2017, https://www.zdnet.com/article/accenture-left-a-huge-trove-of-client-passwords-on-exposed-servers/.

[14] Onelogin, "(1) new messages!," 2022, https://www.onelogin.com/blog/may-31-2017-security-incident.

[15] V. Paul, "Murder in the Amazon Cloud | InfoWorld," 2014, https://www.infoworld.com/article/2608076/murder-in-the-amazon-cloud.html.

[16] Z. Kacy, "Tesla's Tough Lesson on Malicious Insider Threats - Infosecurity Magazine," 2022, https://www.infosecurity-magazine.com/news/teslas-tough-lesson-on-malicious/.

[17] H. Bernard, "Facebook Data Breach Highlights API Vulnerabilities," 2018, https://www.pingidentity.com/en/resources/blog/posts/2018/facebook-data-breach-highlights-api-vulnerabilities.html.

[18] F. Kelly and M. Eric, "Prepare Your Azure Container Technical Assets | Microsoft Docs," 2022, https://docs.microsoft.com/en-us/azure/marketplace/azure-container-technical-assets.

[19] S. Tara, "22K open, vulnerable containers found exposed on the net | threatpost," 2018, https://threatpost.com/22k-open-vulnerable-containers-found-exposed-on-the-net/132898/ (accessed Jan. 29, 2022).

[20] U. Wanve, "Zepto Variant of Locky Ransomware Delivered via Popular Cloud Storage Apps - Netskope," 2016, https://www.netskope.com/blog/zepto-variant-locky-ransomware-delivered-via-popular-cloud-storage-apps.

[21] OCCI, "Open Cloud Computing Interface | Specification," 2011, https://occi-wg.org/about/specification/index.html.

[22] DMTF, "Cloud Infrastructure Management Interface 5 (CIMI) Model and RESTful HTTP-Based Protocol an Interface for Managing Cloud Infrastructure," 2012, http://www.dmtf.org/about/policies/disclosures.php.

[23] G. Morganne, "A Very Expnesvive AWS Mistake," 2018, https://medium.com/@morgannegagne/a-very-expensive-aws-mistake-56a3334ed9ad.

[24] C. Catalin, "AWS Said it Mitigated a 2.3 Tbps DDoS Attack, the Largest Ever | ZDNet," 2018, https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/.

[25] T. Bill, "Over 20,000 Data center Management Systems Exposed to Hackers," 2022, https://www.bleepingcomputer.com/news/security/over-20-000-data-center-management-systems-exposed-to-hackers/.

[26] Ibm Cloud Education, "Cloud security: an essential guide | IBM," 2019, https://www.ibm.com/cloud/learn/cloud-security.

[27] S. Subashini and 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.

[28] J. Hurwitz and D. Kirsch, "Understanding IBM's hybrid and multicloud strategy," 2019, https://www.ibm.com/downloads/cas/EVABY7ZBe.

[29] Oracle, "Bastion Overview," 2022, https://docs.oracle.com/en-us/iaas/Content/Bastion/Concepts/bastionoverview.htm.

[30] F. Sierra-Arriaga, R. Branco, and B. Lee, "Security issues and challenges for virtualization technologies," *ACM Computing Surveys*, vol. 53, no. 2, pp. 1–37, 2021.

[31] CheckPoint Technologies, "What is cloud security posture management (CSPM)?," 2021, https://www.checkpoint.com/cyber-hub/cloud-security/what-is-cspm-cloud-security-posture-management.

[32] J. Anwar, "Microsoft's India Store Hacked, Usernames & Passwords Stolen - Times of India," 2012, https://timesofindia.indiatimes.com/it-services/microsofts-india-store-hacked-usernames-passwords-stolen/articleshow/11865744.cms.

[33] Yubico, "How the YubiKey Works | Yubico," 2022, https://www.yubico.com/why-yubico/how-the-yubikey-works/.

[34] Amazon Web Services, "Archived Amazon web services: overview of security processes," 2020, https://d0.awsstatic.com/whitepapers/aws-security-whitepaper.pdf.

[35] Google Cloud, "Data encryption options | cloud storage | Google cloud," 2022, https://cloud.google.com/storage/docs/encryption.

[36] McKinsey, "Software as a Service and enterprise Cybersecurity | McKinsey," 2019, https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/securing-software-as-a-service.

[37] J. Luna, H. Ghani, D. Germanus, and N. Suri, "A security metrics framework for the cloud," in *Proceedings of the International Conference on Security and Cryptography*, Seville, Spain, July 2011.