European Online Journal of Natural and Social Sciences 2022;
Vol.11, No 3 pp. 816-826
ISSN 1805-3602

Privacy Violation in the Cloud Computing Environment: Challenges and Coping Mechanisms

Fahad Rajallah Aljamei[1*], Majed Muhammad Abusharhah[2], Muhammad bin Ali Musa Khabrani[3]
[1]Hafr Al-Batin University; [2]Ministry of Education - Saudi Arabia; [3]King Abdulaziz University - Saudi Arabia
*Email: aljamei-f@hotmail.com

Received for publication: 21 May 2022.
Accepted for publication: 05 August 2022.

Abstract

Cloud computing is a fertile environment for both organizations and individual users. However, this makes it also a fertile environment for violating the privacy of individuals, hence the importance of drawing attention to the challenges and mechanisms of facing the risks of violating privacy in the cloud-computing environment.

This study aimed at shedding light on privacy data in cloud computing and the user's relationship with it, how that data can be managed, what are the most prominent threats it faces, and identifying the parties that threaten to expose the privacy of such data.

This research provides a clear overview of the most important mechanisms to face data privacy violation or theft in cloud computing. Among the results, the most important ones are that the cloud-computing environment is not a completely secure environment for data privacy, due to the nature of the technology's vulnerability in general to tampering and penetration. Moreover, there are some types of cloud computing based on purely security principles that can be applied in any cloud system such as Security as a Service (SECaaS) and Monitoring as a Service (MaaS).

These findings draw attention to future research on the importance of considering cloud computing technology adoption by large organizations that hold millions of sensitive data.

We hope that the results of the study would contribute not only to draw more attention to the importance of cloud computing but also to adopt more applications that contribute to raising the level of protection for organizations. Indeed, it is worth paying more attention to the development of the cognitive aspect of individuals to adopt awareness ideas that contribute to protecting their privacy on the Internet in general and in the cloud-computing environment in particular.

Keywords: cloud computing, information security, privacy, privacy protection, privacy violation.

Introduction

Nowadays, the cloud information security has become a vital and emerging technology. In fact, many international organizations are interested in cloud computing because of its great advantages, but there is still concern about the protection, privacy and availability of that information as it is located in the cloud. (Shukla, 2021)

This study aims at drawing attention to the importance of educating the user about the existence of his data on special servers of cloud service providers, which are difficult to access, but may be subjected to penetration and therefore the user's data may be violated.

The importance of this study is that it draws attention towards the importance of protecting the privacy of information and data within the cloud-computing environment, because that data is

located in an environment far from the control of the authorized user, so he does not know how his private data is managed on the cloud. In this regard, we have to focus the user's attention on the knowledge of the importance of data privacy and the most important mechanisms used to protect the user from violating his privacy.

On the other hand, and despite the literature covering the study subject, we have found that privacy in cloud computing lacks further studies that ensure the user a good awareness both of the quality of those electronic clouds and of the existence of his private data and preferences in those clouds and how they are protected.

The problem of the study has become clearer when looking at the lack of awareness of individual users or organizations of their use of their private data and their participation in those electronic clouds and the mechanisms for facing privacy threats. This, in fact, may cause them to have greater security problems in the future when that data is leaked, without having mechanisms to maintain their privacy in the Internet environment. Henceforth, we can formulate the problem of the study in the following main question: What are the challenges that users face when sharing their data in electronic clouds, and how do we face them?

Literature review

Cloud computing

Cloud computing is defined as a self-service Internet infrastructure that allows people to access computing resources anywhere around the world (Akhtar et al, 2021), where cloud computing uses a network of remote servers hosted on the Internet to store, manage, and process data. (Coss, D, et al, 2019) However, the fact that the cloud is located in another server away from complete control by the party that put its application on this cloud has raised concerns about the data privacy of this party itself and of its customers as well.

Cloud computing enables the beneficiaries of its services to obtain the required resources such as network, server, storage, application and service through a common set of configurable computing resources and access them anytime, anywhere and on demand (Wu, Z, 2019). These resources are what gave high importance to cloud computing. This means that many areas of daily life have become dependent on it. In fact, it greatly facilitates the process of access through various applications such as cloud storage services and cloud-based web platforms. The main reason for this is the multiplicity of the types of cloud computing services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). (Shukla, 2021. Taha, 2021. Wang, 2020. Abd Al Ghaffar, 2020). The following is a brief explanation of the types of those services in cloud computing:

Cloud computing services

Software as a Service (SaaS)

It provides a complete product that is operated and managed by the service provider, and this can be illustrated by web-based email, where you don't have to think about how to maintain service provision or how to manage the basic infrastructure of the system, you really only need to think about how you will use the software in particular. (AWS, 2021).

Platform as a Service (PaaS)

It eliminates the need for basic infrastructure management, and allows you to focus on deploying and managing your applications, and this helps in achieving high efficiency, especially since you will not have to worry about resource management, capacity planning, software maintenance, debugging or any other heavy burdens. (AWS, 2021)

Infrastructure as a Service (IaaS)

Infrastructure as a Service is the service model upon which cloud technology deployment is built. Thus, you can, on-demand, have access to basic IT resources such as computers, networks and storage through the service provider. This allows you to update and develop your infrastructure to suit the processing and storage requirements of your organization or entity, without being concerned with the burden of managing, developing or monitoring them, as the responsible party for this task is the cloud service provider. (Taha, 2021).

The powers to use the aforementioned services can be summarized in the following figure:

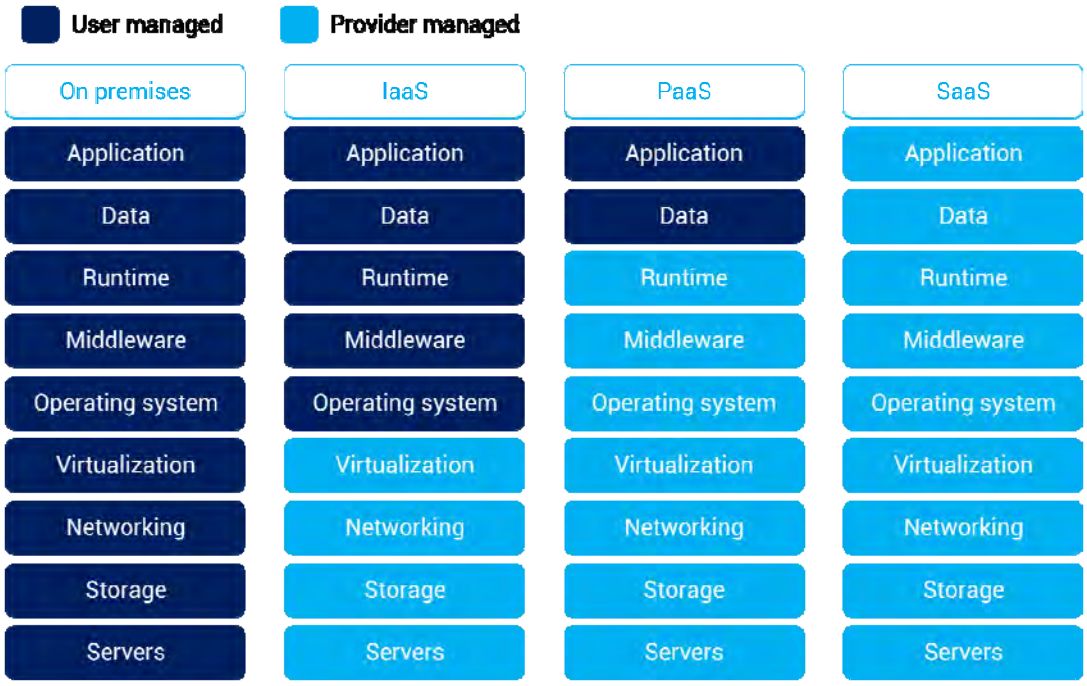

Figure 1. Powers of Cloud Computing Services. Extracted from (alibabacloud.com, 2021)

Observing the ways of providing services in cloud computing gives us an idea about the importance of protecting privacy data for users of those electronic clouds, whether at the level of individuals or institutions. In fact, at the level of institutions, sharing sensitive data of the organization may be subject to breach unless that cloud is reliably secure. As for individuals who may share photos, files or private data, it may also be subject to breach, especially since individuals, unlike organizations, do not have sufficient awareness of the importance of protecting their private data within those clouds. Therefore, we will discuss in the next part data privacy in the electronic cloud environment.

Privacy in a Cloud Computing Environment

Privacy is one of the primary protection mechanisms in the integrity of user records within the cloud, in which user data is encrypted before it is stored in the cloud, and this method protects the information of users or cloud service providers (Shukla, 2021).

The violation of privacy constitutes a security concern at the level of individuals or even governments and organizations that may deposit their data on electronic clouds and rely on them to save and manage their data, as the security problems of service providers pose some concerns for users of those electronic clouds by these providers. Moreover, the service providers themselves are in a constant race to preserve the data of their customers and keep their electronic clouds safe to

achieve more confidence between them and their customers. In the following parts, we will address what is mentioned in the literature about the privacy of individuals in the cloud computing environment, as well as the privacy of governments or organizations in the cloud computing environment:

Privacy Concerns for Individuals in a Cloud Computing Environment

Privacy concerns are increasing seriously in the cloud computing environment due to the nature in which personal information is collected, processed and used by cloud computing service providers. In fact, privacy problems have become a source of concern for users of these electronic clouds, as individuals are exposed to threats of privacy violations when they are persuaded to provide personal information in order to be able to use the electronic clouds. (Coss, et al, 2019) The seriousness of the matter is that data is stored and managed in multiple locations around the world by service providers, where cloud computing consists of hardware and software resources that are provided as an external service managed over the Internet. Thus, users lose effective control over their data in the cloud and delegate this control to a service provider that may not be trustworthy to protect that data (Akhtar, et al, 2021). Moreover, the lack of control of individuals or data owners in the cloud may expose them to the threat of privacy breach either from outside the cloud providers such as hacker attacks to service providers, or even from within the cloud service providers such as threats and intrusion by service providers' employees on individuals' data. (Wu, Z, 2019).

(Oke, A, et al, 2021) stated that users face concerns when using cloud computing, especially in the areas of reliability, availability and integration, particularly that cloud service providers may sometimes hide their shortcomings, in order to gain users' confidence in protecting their data.

It is worth noting that there are three main dimensions of data security within the electronic cloud, which are availability, integration, and reliability (Pawar, et al, 2021). As a result, if these conditions are met for the average user, his concerns about the violation of his privacy will be reduced to minimum levels, and the external threat remains the most prominent element in the threat to users' data in the cloud-computing environment.

Privacy Concerns for Governments and Organizations in a Cloud Computing Environment

The concern of governments and organizations about the violation of their privacy in cloud computing environments is greater than that of individuals. The concerns of governments relate to violating their national security, while commercial organizations, for example, focus on the privacy of their customers' data, which protection is within their responsibilities. The use of cloud computing technologies for governments can reduce costs, but it may increase security concerns in using them as well, especially with regard to securing important information such as intellectual property and personal files. (Ali, et al, 2020), According to the Identity Theft Resource Center, during 2016, the number of data security breaches increased to (1093), an increase of (40%) over the previous year, and only four of these security breaches resulted in the publication of (120) million Social Security IDs which represents 1 out of every 3 Americans. (Coss, D, et al, 2019). This increases governments concerns when using cloud-computing services since personal and sensitive information may be highly vulnerable to intrusion and hacking. However, (Abd Al Ghaffar, 2020) believes that electronic attacks can only pose a threat to national security when the infrastructure is weak, when daily activities depend heavily on remote computer networks, and when governments tend to save data via the Internet. In fact, this is what is happening nowadays due to the shift of governments to cloud computing. Henceforth, governments must balance these risks through robust security systems, active legal frameworks, and proactive measures to secure national infrastructures.

On the other hand, in a study conducted by (Faizi, A, et al, 2021) on a group of organizations in Sweden, the results showed that organizations prefer using (PaaS) platform as a service only be-

cause they do not want to expand their data center to the cloud. Even though, all organizations in that study acknowledged the existence of trust in cloud service providers, but they stressed that it should not be blind trust.

(Abd Al Ghaffar, 2020) states that cloud computing provides not only different levels of security, ranging from the most secure (private cloud) to the least secure (public cloud) but also different cost-saving models such as the cost-saving model (public cloud) and the least cost-saving model (Private cloud). Indeed, most governments that have adopted cloud computing have resorted to the most secure and least cost-effective solutions (private cloud). However, some governments, such as Australia, tend to classify data according to confidentiality and migrate data to different cloud types.

Privacy Concerns in a Mobile Cloud Computing (MCC) Environment

Cloud computing in the mobile environment is one of the recent trends of networks and mobile phone technology that provides computing and storage resources and services to mobile users, including widely spread location-based web sites applications. Protecting the privacy of the user's site is still a focus of attention in protecting users in case of unauthorized access, especially in light of the increasing use of applications such as Google, Instagram, Snapchat and Uber (Almusaylim, & Jhanjhi, 2020).

The results of the study of (Alnajrani, et al, 2020) showed that the threats related to the use of mobile phone applications are unauthorized attacks, data privacy and confidentiality, data misuse and unreliability of the service provider.

It can be concluded that the concerns are common, whether in the mobile phone environment or in the computer environment, and these concerns share a great concern about the user’s privacy of data, which is the subject of the issues in this study, through which we seek to identify the most prominent threats and mechanisms to face those challenges.

Mechanisms for facing the risks of privacy violations in the cloud-computing environment

(Nikkhah, H, 2021) indicated that publishing privacy policies online is an effective tool to increase users' confidence about the security of private information and to encourage users to disclose personal information as privacy policies define the way online businesses store, process and use information that users provide.

On the contrary, (Wu, Z, et al, 2019 & Wu, Z, et al, 2020) see that the enactment of laws and regulations can reduce the problems of privacy violations in the cloud-computing environment. However, the enactment of regulations and laws may not be a basic solution, and accordingly the technical aspect may be a solution or a typical method to solve this problem through the following elements:

• **User authentication:** It is the most common database security technique where the system provides a certain way for users to identify themselves each time they log into the system. The system verifies the user's identity and makes sure that he is authorized to enter the system based on the authentication data he provided, and authentication data can be submitted in several forms, whether with passwords, fingerprint verification, face verification, or a smart card. The user may be asked for one or more authentication ways each time he logs in.

• **The control authority:** This is done through special permissions and licenses for each user, in which it is ensured that users who are logged in access only the data that they are authorized to view or modify.

• **Concealment of the user's identity:** The lack of availability of the user's identity may be one of the good means of protection for that user because his private data is hidden behind an unknown identity from the ground up, which makes access to his data difficult, as it requires first knowing the identity to access the data.

• **Data encryption:** The user's data stored in databases is encrypted, in a way that is difficult to decrypt, even if that data is leaked.

As the study of (Akhtar et al, 2021) referred to the types of services in the cloud computing environment, it mentioned that cloud computing services provide security solutions through their cloud services such as Monitoring as a Service (MaaS), which allows the service provider to provide a security service 24 hours a day, 7 days a week. By constantly monitoring systems, applications, and customers, it also provides security as a service (SECaaS) where the cloud service provider provides managed security services that allow companies to fully-disclaim all responsibilities and hand over responsibility to the service provider to manage and protect their own data of and that of their customers.

However, (Wang, 2020) has mentioned a detailed division of security mechanisms in the cloud computing environment (SECaaS) in ten elements as follows:

1. Identity and Access Management (IAM): It provides trusted identity control and access, granting the right level of access including customers and service providers who have access to enterprise resources.

2. Data Loss Prevention (DLP): It is a strategy to ensure that no data is lost, misused, or no access to sensitive information by unauthorized users is made.

3. Web Security (WS): It provides protection by some process that ensures secure access to the web.

4. Email Security (ES): It provides control over incoming and outgoing email messages to ensure protection from spam, malicious attachments and virus links.

5. Security Assessment (SA): Through which external audits of cloud services are carried out by a third party to ensure that the provided cloud service is working properly.

6. Intrusion Management (IM): It consists of instant messaging involves abnormal event detection and interaction, in which system components are reconfigured in real time to stop or prevent intrusion.

7. Security Information and Event Management (SIEM): It gathers event information from servers, sensors, firewalls, and other systems and routers, then analyzes those event data and makes decisions that ensure the security of the systems and the entire cloud environment.

8. Encryption: It is the process of converting plain text into an encrypted text to make it unreadable. The encryption can be opened with a key to decrypt that encryption when needed.

9. Network Security (NS): It refers to the use of policies and practices to prevent and control unauthorized access, abuse and alteration, and to protect the network and its resources from intrusion.

10. Disaster Recovery: Business Continuity and Disaster Recovery is a flexible and reliable mechanism for bypassing failures when service is interrupted, including natural disasters or disasters caused by human error.

Methodology

This study followed the descriptive approach through the method of content analysis by reviewing the literature to reach the results and recommendations of this study. The research was conducted in the literature published in the English language by looking at the databases of journals and academic search engines such as (IEEE Xplore, Emerald, Research Gate, Google Scholar, and Microsoft Academic). The time limits for this literature ranged between 2019 and 2021. The researcher focused on searching the following phrases: cloud computing security, cloud computing challenges, privacy in the cloud computing environment, information security in cloud computing environment.

The researcher came up with a number of studies related to the subject of the study, with the exclusion of studies that did not discuss the challenges, the security of cloud computing, or the issues related to privacy.

The above concerns about privacy violations and the most prominent coping mechanisms can be summarized in the following table:

Table 1. The main challenges facing cloud computing

Researcher	Study date	Targeted party	The challenge
Coss, et al	2019	Individuals	Forcing the user to provide personal information in exchange for the use and availability of the cloud.
Akhtar, et al	2021	Individuals	Data is managed out of the user's control
Wu, Z	2019	Individuals	Hacker attacks on service providers.
Wu, Z	2019	Individuals	Service providers snooping on data.
Oke, A, et al,	2021	Individuals	deficiencies in data security by service providers
Ali, et al	2020	governments	Violation of the national security of the government.
Ali, et al	2020	trade organizations	Customer data breach.
Abd Al Ghaffar	2020	Governments Commercial Organizations	The amount of damage caused is great.
Faizi, A, et al	2021	governments	Scaling up and adopting cloud computing services (PaaS) without expanding data centers.
Almusaylim, & Jhanjhi,	2020	Individuals	Unauthorized access to a cloud user's website.

Table 2. The most prominent coping mechanisms in cloud computing environments

Coping mechanisms	Application of the mechanisms
Administrative Procedures	Publishing the privacy policy
Technical procedures	User authentication - control authority - user anonymity - data encryption
Service Provider Procedures	The use of MaaS monitoring service as a primary tool by service providers. The use of a Service Provider-Managed Security by SECaaS through its following mechanisms: Identity and Access Management – Data Loss Prevention – Web Security – Email Security – Security Assessment – Intrusion Management – Security Information Management and Event Management – Cryptography – Network Security – Disaster Recovery

Results and Discussion

After surveying the previous parts of the literature review, we noticed that privacy is the biggest concern in the subject of information security in the cloud-computing environment, whether for individuals or organizations, especially since policies, procedures and laws may not be sufficient to protect private information. This is what made organizations in Sweden in the study of (Faizi , A, et al, 2021) gives partial confidence in cloud computing because of the potential privacy risks. The solution was to maintain the level of security, evaluate the data, calculate the importance and cost of the data, whether it is really worth a higher protection cost on a private cloud or keep it public at a lower cost. Depending on (Abd Al Ghaffar, 2020) we represented this importance with a direct relationship in (Fig. 1) between the public feature of the cloud and its security, where the risk to the user or the organization increases whenever the cloud is public or private, and this can be represented in the following figure:

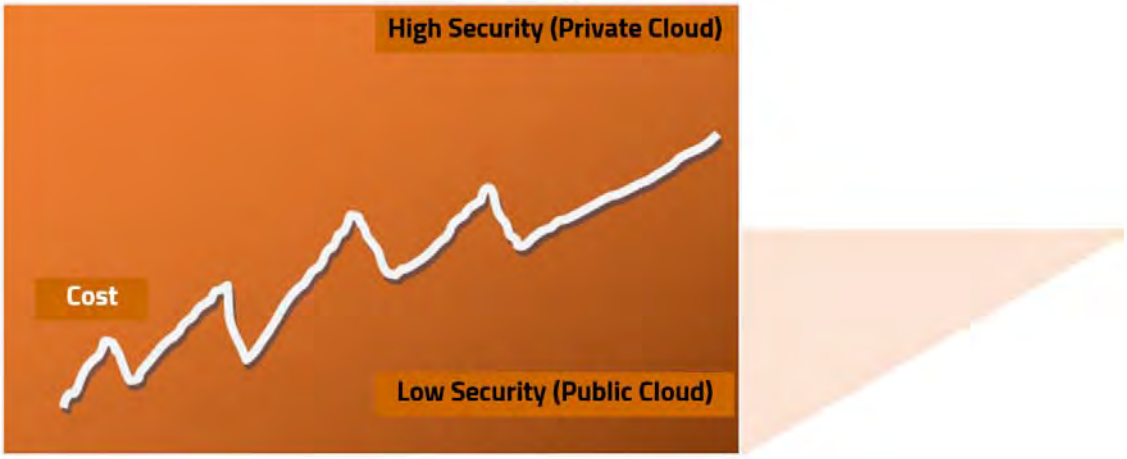

Figure 2. Prepared by the researcher based on what was mentioned in the study of (Abd Al Ghaffar, 2020).

However, there are other non-public or cloud privacy factors that may increase the percentage of privacy and data protection by cloud computing service providers, as service providers may provide additional services such as providing security as a service (SECaaS) or providing monitoring as a service (MaaS) and this would increase The cost too. Nevertheless, governments or organizations that manage a very large volume of data are able to deal with these additional costs in exchange for increasing their guarantees in reducing the threats they may face in the event of leaking their customers' data and violating their privacy. The literature review showed that there is a tendency to switch to cloud computing internationally, and this is evident when looking at the volume of government services that have become fully electronically provided and managed. For example, the Kingdom of Saudi Arabia has shifted to offering the service of obtaining an electronic tourist visa to its visitors from outside Saudi Arabia through a simple electronic system that allows the issuance of an electronic tourism visa in a few minutes, after entering their data, certifying it and ensuring its safety. (Visit Saudi website, 2021) The most prominent mechanisms that have emerged in the protection of data privacy are authentication and control and access management. (Wu, Z, et al, 2020) highlighted data protection by focusing on the user himself largely. Moreover, he stressed the need to authenticate and verify the user’s data, manage the powers so that each user would be given only

specific permissions, and the ability to hide his identity and encrypt his data to make it difficult to be viewed by other parties in the system.

(& Wang, 2020) focused on data protection mechanisms through the same technology. For example, the ability of the system to grant control, access, encryption, to retain data even after its loss for any reason, to recover data from any natural or human disaster that may befall the system, and to protect email and web security.

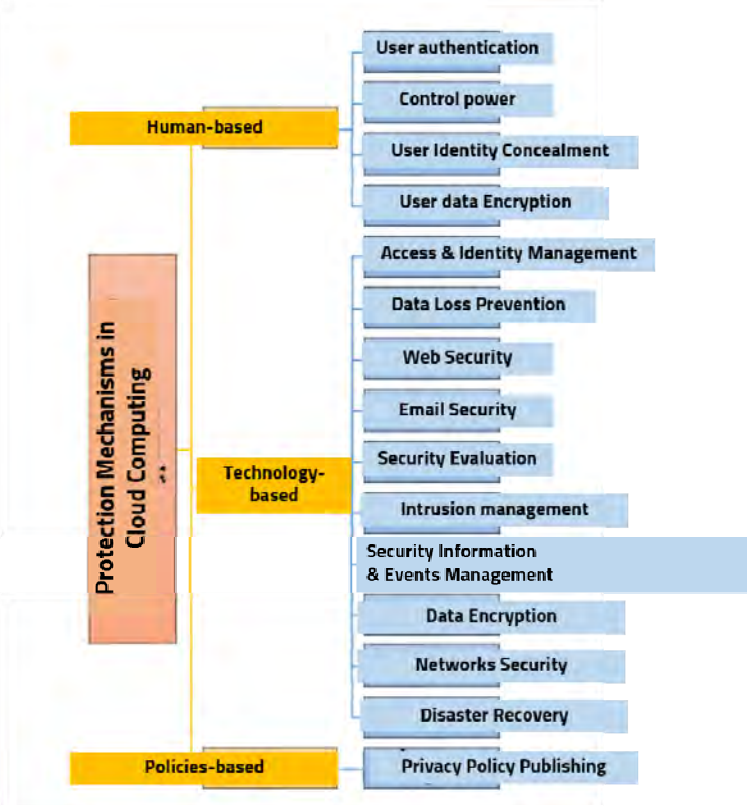

Figure 3. Protection mechanisms in cloud computing prepared by the researcher based on the literature review in this study

Conclusions

The most important conclusions that came out of this study are:

• The cloud-computing environment is not a completely secure environment for data privacy, due to the nature of the technology's general vulnerability to tampering and penetration.

• The most prominent challenge facing users of cloud computing applications is to publish their own data on electronic clouds without the ability to control them while they are in the cloud.

• One of the challenges facing users is their inability to know if service provider employees have violated their privacy data.

• One of the effective mechanisms for gaining the trust of cloud computing users is to publish the service provider's policies and procedures by making these procedures and policies available in the form of a user privacy policy.

• There are three types of data protection mechanisms [human-based type - technology-based type - policy-based type] as shown in Figure (3).

• There are types of cloud computing based on purely security principles that can be applied as an early defending mechanism in any cloud system such as (SECaaS) and (MaaS).

Recommendations

• Organizations should adopt the idea of using a private cloud, even if the cost has increased due to its ability to control more data in the network.

• The privacy policies of cloud computing service providers are to be placed in clear places on their home pages on the Internet, and their awareness of the privacy policy is to be measured through periodic surveys.

• There should be clear restrictions for service provider employees that prevent them from violating customer data by assigning powers or building a tracking record for the employee to ensure that he does not violate the privacy of cloud users.

• There is an obligation for individuals to acknowledge their reading of the privacy policy by answering some random questions related to the privacy policy before finalizing their registration, to ensure that they have actually read the privacy policy and agreed to its terms.

• There should be future studies that contribute to the development of security standards and the dissemination of privacy for cloud computing systems.

• This study suggests that this research should be a basis for launching more future studies in the field of challenges in the cloud computing environment, especially for (SECaaS) and (MaaS) services, and the mechanisms for facing these challenges. This is because these services are provided entirely under the responsibility of service providers and the possibility that these services are the basis for all the uses of cloud computing. Future studies should also compare a number of cloud computing service providers and the most prominent breakthroughs that affected those electronic clouds and indicate their damage to individuals, organizations and governments.

References

Abd Al Ghaffar, H. T. A. N. (2020). Government Cloud Computing and National Security. *Review of Economics and Political Science*.

Akhtar, N., Kerim, B., Perwej, Y., Tiwari, A., & Praveen, S. (2021). A Comprehensive Overview of Privacy and Data Security for Cloud Storage. *International Journal of Scientific Research in Science, Engineering and Technology*, *8*(5), 113–152.

Alibaba Cloude (2021). What Is IaaS? Available at: https://www.alibabacloud.com/knowledge/what-is-iaas seen (25/11/2021).

Almusaylim, Z. A., & Jhanjhi, N. Z. (2020). Comprehensive review: Privacy protection of user in location-aware services of mobile cloud computing. *Wireless Personal Communications, 111*(1), 541-564.

Alnajrani, H. M., Norman, A. A., & Ahmed, B. H. (2020). Privacy and data protection in mobile cloud computing: A systematic mapping study. *Plos one*, *15*(6), e0234312.

AWS (2021). What-is-cloud-computing Available at: https://aws.amazon.com/ar/what-is-cloud-computing/ seen: (09/11/2021).

Coss, D. L., & Dhillon, G. (2019). Cloud privacy objectives a value-based approach. In *Information & Computer Security, 27*, 189–220.

Faizi, A., Padyab, A., & Naess, A. (2021). From rationale to lessons learned in the cloud information security risk assessment: a study of organizations in Sweden. *Information & Computer Security*.

Nikkhah, H. R., & Sabherwal, R. (2021). Information disclosure willingness and mobile cloud computing collaboration apps: the impact of security and assurance mechanisms. Information Technology & People.

Oke, A. E., Kineber, A. F., Al-Bukhari, I., Famakin, I., & Kingsley, C. (2021). Exploring the benefits of cloud computing for sustainable construction in Nigeria. *Journal of Engineering, Design and Technology*.

Pawar, A. B., Ghumbre, S. U., & Jogdand, R. M. (2021). Privacy preserving model-based authentication and data security in cloud computing. *International Journal of Pervasive Computing and Communications*.

Shukla, S., & Agarwal, A. K. (2021). Security Techniques for Data Protection in Cloud Computing: A Review. *IUP Journal of Computer Sciences, 15*(1).

Taha, A. A. D., Ramo, W., & Alkhaffaf, H. H. K. (2021). Impact of external auditor–cloud specialist engagement on cloud auditing challenges. *Journal of Accounting & Organizational Change, 17*(3), 309–331.

Visit Saudi (2021). About Electronic Visa. Available at: https://www.visitsaudi.com/ar/about-e-visa seen: (10/11/2021).

Wang, W., & Yongchareon, S. (2020). Security-as-a-service: a literature review. *International Journal of Web Information Systems, 16*(5), 493–517.

Wu, Z., Shen, S., Lu, C., Li, H., & Su, X. (2020). How to protect reader lending privacy under a cloud environment: a technical method. *Library Hi Tech*.

Wu, Z., Xie, J., Lian, X., & Pan, J. (2019). A privacy protection approach for XML-based archives management in a cloud environment. *The Electronic Library, 37*(6), 970–983.