Cloud Computing and Data Science
http://ojs.wiserpub.com/index.php/CCDS/

UNIVERSAL WISER
PUBLISHER

Research Article

Insights on Cloud Security Management

Rachel John Robinson

Cybersecurity, Department of IT, IU University of Applied Sciences, Berlin, Germany
E-mail:info@rachel-johnrobinson.de

Received: 28 June 2023; **Revised:** 13 July 2023; **Accepted:** 18 July 2023

Abstract: The technology known as cloud computing makes it possible to provide computing services over the Internet. Because it allows users to access and manage information and applications through a network of remote servers, this service model has been quickly adopted due to its numerous benefits, including cost savings, scalability, and accessibility. The global market for cloud computing is expected to reach $732 billion by 2023, according to a report from International Data Corporation (IDC). A first-hand survey of approximately sixty (60) cloud companies will be used to provide an overview of cloud computing technology, its architecture, and Security, Privacy, and Trust (SPT) concerns. Privacy concerns for users, data theft, unauthenticated access, and hacker attacks are just a few of the cloud computing problems. These perplexing security issues of validation protection, information assurance, and information check are the primary impediment to cloud transformation for future developments, which are being addressed to recognize the sufficiency and adequacy of cloud security through subjective review based on techniques.

***Keywords*:** NIST, cloud architecture, security, privacy and trust (SPT), virtualization, sustainable data centers

1. Introduction

Cloud storage is widely used today because it offers unlimited, low-cost storage of data that can be accessed from a variety of devices, including smartphones, laptops, tablets, and so on. In addition to well-known cloud service providers like Google, Microsoft, and Amazon, which provide Amazon Web Service (AWS), other distributed storage specialist organizations give more accessible and practical capacity administration to clients. Examples; Dropbox, Box.net, Idrive, IBackup, Sync.com, and Shimmer Share. Some of the most important features of these cloud service providers include a straightforward user interface and storage service, file and folder synchronization between various machines, file-sharing versioning, and automatic backups. The way users manage data has changed thanks to cloud service; Multiple users can work and share data without worrying about consistency, availability, or reliability with cloud service.

Since the data stored in these services are under the authority of the service providers, there are concerns about the confidentiality and security of the data. Therefore, using cloud service to store essential data depends mainly on whether the service provider can offer efficient protection to meet the client's requirement. From how the cloud system is constructed, the cloud providers do not supply the client with adequate levels of security which leads to the risk of clients' data from external and internal attacks. These attacks can be in the form of; data exposure (lack of data security), data tempering (lack of data privacy) and denial of data (lack of data trust) from the cloud providers themselves. In this case, the cloud providers should ensure data confidentiality when data is in motion (while transmitting over the network)

Copyright ©2023 Rachel John Robinson.
DOI: https://doi.org/10.37256/ccds.4220233292
This is an open-access article distributed under a CC BY license
(Creative Commons Attribution 4.0 International License)
https://creativecommons.org/licenses/by/4.0/

and when information is at rest (when stored at providers' disks) before it is outsourced to these services. A client can rely on cloud providers to use encryption software tools to encrypt their data on the cloud service. However, many cloud providers fail to achieve data confidentiality. For instance, Box.net do not encrypt clients' data within the Box servers and, as a result, exposes it to confirmation of files attacks.

As mentioned above, the cloud system has several data security issues and is motivated by these issues; in this research, we pose the following questions.

- Analysis of effective way of cloud architecture.
- Is there a secured Cloud system for companies?
- What are the security policies in place to secure the cloud from its SPT claims?

With these research questions in hand the three main objectives or the aims driving the work would be:

- Adequacy of Security in place for SPT claims.
- Policies available to curtail suspected Security Violation.
- Effective security strategies in Trend.

In other words, we want to know if the company is using a Cloud system, what are measures in place to make sure that the security, privacy and trust of the data are kept.

2. Literature on cloud architecture design-NIST

A common framework for comprehending and evaluating cloud computing technologies and practices has been developed by the National Institute of Standards and Technology (NIST) into a reference architecture for cloud computing. The key components and functions of cloud computing, as well as their relationships, are outlined in this architecture. The three service models in the NIST cloud computing architecture depicted in Figure 1 are as follows: Software as a Service, Platform as a Service, and Infrastructure as a Service is the four deployment models: private cloud, community cloud, public cloud, and hybrid cloud, as well as the following five essential components: cloud carrier, cloud auditor, cloud broker, and cloud provider [1].

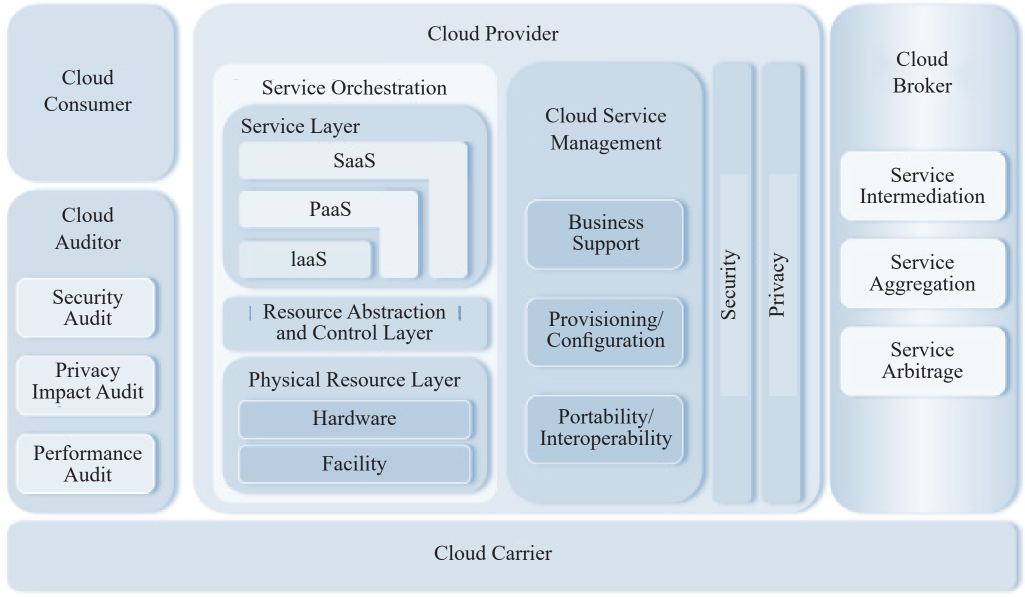

Figure 1. NIST cloud computing architecture [1]

2.1 *Cloud consumer*

It describes the person or business that makes use of cloud computing services to fulfill their computing requirements. They are often the end customers who employ a cloud provider or cloud broker to obtain cloud services. The cloud user has access to a wide range of services through the internet, including infrastructure, platforms, software, and storage. Additionally, they may make use of a variety of resources without having to purchase and maintain their IT infrastructure, like as processing power, storage, and apps.

2.2 *Cloud Provider*

It refers to the organization that offers cloud services to cloud customers, which could be a business, a government agency, or any other organization [2]. It is liable for conveying the framework, stage, programming, or capacity benefits that the cloud customer demands which incorporates keeping up with and refreshing the basic innovation, as well as guaranteeing the security and protection of the cloud purchaser's information. In order to assist the cloud customer in getting the most out of their cloud services, the cloud provider may also offer additional services, such as management and support. To meet the requirements of a variety of cloud customers, they may also provide a selection of pricing options, such as pay-per-use, subscription-based, or metered.

2.3 *Cloud broker*

It alludes to an element that works with the acquirement and the executives of cloud administrations from different cloud suppliers. It serves as a conduit between the cloud customer and the cloud service provider, assisting the customer in selecting the appropriate cloud services to meet their requirements and managing their usage of those services. It offers a variety of services, such as Service Arbitrage, Service Aggregation, and Intermediation [3].

2.4 *Cloud carrier*

It refers to telecommunications companies, internet service providers, and other organizations that provide network connectivity and data transport services as the entity in charge of the physical transportation of data and information between the cloud consumer and the cloud provider [4].

2.5 *Cloud auditor*

It alludes to the element that is liable for inspecting and assessing the security, protection, and consistency of cloud administrations. This can incorporate free outsider associations, government offices, and interior inspecting groups. The cloud examiner is answerable for guaranteeing that the cloud supplier is sticking to laid out security and protection guidelines, as well as any administrative necessities that apply to the information and data put away in the cloud [5].

3. Literature on basic service models

The various ways in which various organizations can receive and use cloud computing services are referred to as "cloud service models". As shown in Figure 2, there are three primary service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

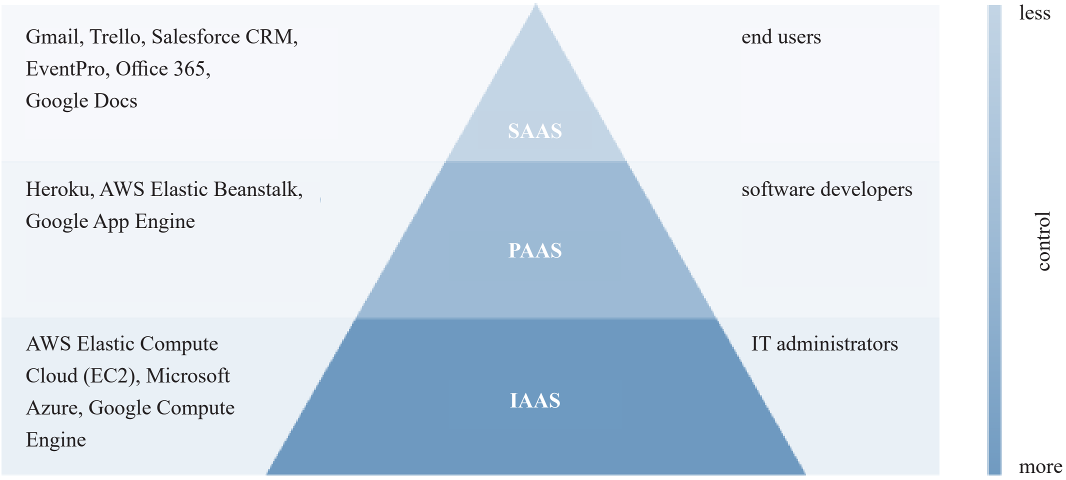
Gmail, Trello, Salesforce CRM, EventPro, Office 365, Google Docs
SAAS
end users
Heroku, AWS Elastic Beanstalk, Google App Engine
PAAS
software developers
AWS Elastic Compute Cloud (EC2), Microsoft Azure, Google Compute Engine
IAAS
IT administrators
less
control
more

Figure 2. Cloud Service Models [6]

3.1 *Infrastructure as a Service (IaaS)*

Here, businesses may use the internet to rent virtualized computer resources, such as servers, storage, and networking. IaaS enables businesses to host their own apps and services just like they would if they were operating them on their own physical infrastructure [7].

Examples of IaaS providers include Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

Advantages of IaaS include:

- It's cost saving.
- It's highly flexible.
- There's reduced IT burden.
- Scalability.

3.2 *Platform as a Service (PaaS)*

It is a model of cloud computing that gives businesses a platform on which they can develop, test, and deploy their applications without worrying about the infrastructure. Databases, middleware, and application development frameworks are typical components of PaaS, which are intended to simplify application development and deployment for businesses [8].

Examples of PaaS models include AWS Elastic Beanstalk, Microsoft Azure App Service, and Google App Engine.

Advantages of PaaS model include:

- Reduced development time.
- Improved collaboration.
- Reduced costs.
- Scalability.

3.3 *Software as a Service (SaaS)*

It is a distributed computing model in which associations can get to programming applications over the web, dispensing with the requirement for programming establishments and support. Users use a web browser to access SaaS applications, which are typically hosted and maintained by the service provider [9].

Examples of SaaS models include Salesforce, Microsoft Office 365, and Google G Suite.

Advantages of SaaS model include:

- Improved collaboration.
- Reduced IT burden.
- Reduced costs.
- Scalability.

SaaS is the cloud service model that is being used the most by businesses because it gives them a cost-effective and flexible way to access a wide range of software applications without having to make a lot of money upfront.

4. Security, privacy and trust challenges in cloud computing (based on literature)

Cloud computing has helped transform organizations in terms of managing and storing data. However, it comes along with security, privacy and trust challenges as described below.

4.1 *Security challenges*

Security is one of the major concerns in cloud computing since organizations use cloud computing to store and manage their data Below are some of the key security challenges in Cloud Computing:

- Data Breaches: Cloud storage systems are often at the risk of being endangered by data breaches which may result in data theft or even exposure to sensitive information since information is stored and managed over the cloud. These data breaches include phishing attacks, malware, and misconfigured systems.
- Cyber Attacks: these are attacks by cyber criminals against computers or networks including the cloud which can result in the loss of sensitive data and disrupt the operation of cloud systems. These include Ransomware attacks, DDoS (Distributed Denial of Service), Man-in-the-middle attacks, and Ransomware attacks [10].
- Unauthorized access: this usually happens when a person gains access to a computer system, network, or data without permission from the owner. This often happens over the cloud too which leads to the misuse of sensitive data [11]. These are some common cases of Unauthorized access, Weak passwords, Unsecured connections, and Unsecured APIs (Application Programming Interfaces).
- Compliance issues: it refers to the adherence to legal and regulatory requirements, industry standards, and organizational policies related to data privacy and security.

Compliance issues in the cloud include Data privacy for example some organizations place strict requirements on how personal data can be collected, stored, and processed as the EU's General Data Protection Regulation (GDPR) does, and Data residency where Some regulations require that data be stored within specific geographic locations [12].

4.2 *Privacy challenges*

Privacy is a major concern to organizations that use cloud systems since it involves the storage and processing of sensitive information by third-party service providers. Below are some of the privacy challenges in cloud computing:

- Privacy Laws: Organizations must comply with various privacy laws and regulations when storing and processing data in the cloud. Cloud computing raises several privacy concerns, as data stored in the cloud may be accessible to a wide range of individuals, including cloud service providers and their employees, other users of the cloud service, and government agencies. To address these concerns, various privacy laws have been enacted, in the European Union, United States and internationally which include Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR).
- Data Sharing: Cloud service providers have access to the data stored in their systems and may share this information with other organizations or even use it for their own purposes. Data sharing challenges include compliance issues, privacy concerns, security risks and Data ownership and control [13].
- Lack of transparency: Cloud service providers may not be transparent about their data handling practices, which makes it hard for organizations to know how their data is being used. Issues involved with Lack of transparency include Limited control over data, Hidden security, and privacy risk, and Opaque pricing models [14].
- Lack of control: Organizations that use cloud computing may have limited visibility into or control over their data and services in the cloud. Issues involved with lack of control include Lack of control over data management,

Limited visibility into service quality, Security, and privacy risks, and Interoperability issues.

4.3 *Trust challenges*

Organizations must trust their cloud service providers to securely protect and manage their sensitive data and applications. However, trust in cloud computing can be difficult to establish and maintain, due to several challenges, which include:

- Limited or no control over data management: Organizations must trust that their data will not be altered, deleted, or tampered with in any manner by the cloud service providers which is difficult to maintain. Challenges associated with this include irregular data backups and recovery as well as irregular data audits [15].
- Security and privacy risks: Organizations are often concerned about the risk of data breaches, theft, and unauthorized access to sensitive information, leading to a lack of trust in the security of the cloud.
- Limited or no visibility into service quality: Cloud providers may not provide adequate information about the quality of their services, such as uptime, latency, and availability, making it difficult for organizations to assess the level of service they are receiving which leads to a lack of trust in the quality of the cloud provider's services.
- Interoperability issues: Not being able to share data over the cloud systems and platforms leads to a lack of trust in the ability to work together by different systems and platforms thus interoperability issues [16].

5. Research process

It attempted to outline the type of analysis used in the data collection of this research, the data analysis and the interpretation of the data. Also, an explanation of the data in graphs and diagrams to know the details on how cloud systems are protected by companies in general will be discussed.

5.1 *Methodology and method*

The Qualitative research is non-numeric data and the Quantitative research is numeric data and these both can be collected in a variety of ways including field notes, surveys and interviews offering deeper insights into topics or experiences. Although less accepted than quantitative research in certain fields such as psychology, the qualitative approach has matured despite "paradigm wars" within this field [17]. Considering this, for the work undertaken the qualitative iterative to form retrospective casual comparisons is undertaken.

It is necessary to experiment with the design for impact assessment through intervention in order to conduct an effective statistical analysis of the received data through these channels [18]. An iterative approach is required for the qualitative method's experimentation. An example is shown in Figure 3.

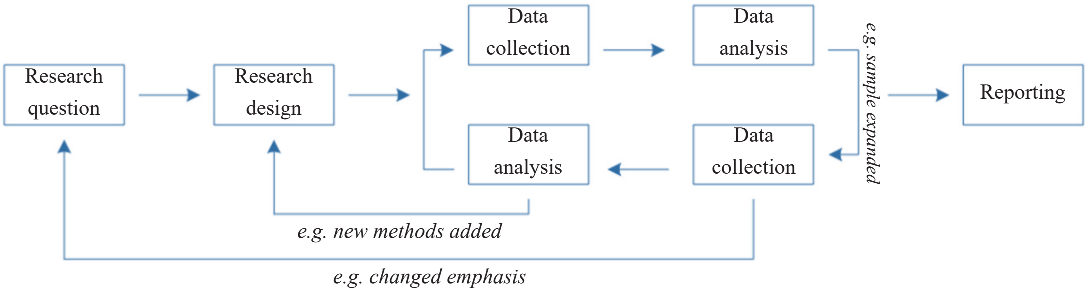

Figure 3. Qualitative Iterative Research Approach [19]

The approach taken in this research is a Qualitative retrospective casual comparative positivism approach using secondary data. This fits the scheme due to primarily utilizing cloud issues performance data.

The importance of research planning cannot be understated as it seeks to align goals and objectives, resource requirements, and expected results delivering focus within the research process [20]. Considering this, the Qualitative retrospective casual comparative is mapped to the research objectives to frame conclusions.

5.2 *Data source*

The graph Figure 4 below shows the categories or the number of companies that were involved in the research. Out of the targeted 100 cloud organization in general, only 10 of the organizations accepted the emails and was involved in this research, approximately 40% of the companies were Window and Glass Companies, 15% were Plumbing Companies, 10% were woodwork Companies, 5% were Clothes Companies, 9% were shoe Companies, 15% were Beverage Companies and 6% were leather Companies. The profile of the organizations involved in this research can be illustrated in the graph below.

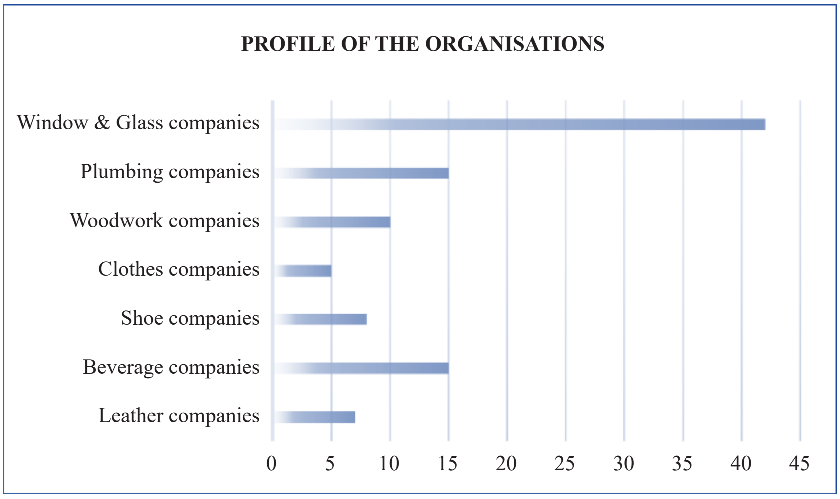

Figure 4. Profile of the Organisations in research

5.3 *Research limitation*

As it is for every study, this research had the following limitation:

- Qualitative research adopted is not allowing the exact measurement of the examined problems.
- In some cases, participants refused to answer with the required exact data requirements for the research.

6. Research findings

The set of tools and methods used by the organization to safeguard cloud-based data will be discussed in this research section. As stated in section 1, this section also sorts to fulfill the second objective of the research. The following are some of the questions that need to be answered here: What measures do some businesses take to safeguard their cloud-based data? Who is authorized to access the cloud's data? What procedures are in place to ensure that only authorized individuals have access to the data? Finally, what procedures are in place in the event of a suspected security breach? What is the calamity recuperation plan?

6.1 *Adequacy of Security in place for SPT claims*

When this question was posed to the respondents, 20 of the respondents answered that data encryption is the action their company uses to protect their data. These describe the group of people and their responses categorized as under P1-P4 representing Beverage companies, P4-8 representing woodwork companies, P9-12 representing window and glass companies, P13-16 representing plumbing companies and P17-20 representing fashion companies (clothes, shoe and leather).

Because it is stored on public servers, most cloud data does not have any security. This makes the data susceptible to attacks from the outside or even from within [21]. As a result, the data itself ought to be safeguarded so that, even in the event that the data are successfully stolen, the contents of the stored data will continue to be protected. Additionally, nine (maximum) of the respondents to the research stated that their company protects its data through data backup. Their customers will be able to easily access the data at any time thanks to this backup, which will always make it available. Six people (average) also stated that they protected their data by using strong passwords. The password will be more difficult to crack if it contains a combination of letters, numbers, and special characters; the rest should be considered to have minimal security measures (Average minimum). these actions as well as the fundamental measures their businesses take to safeguard their data. It is clear from Figure 5 that 70% (14 nos) of the respondents are with Normal Max and Normal Avg controls and just 30% (6 respondents) are with Normal least controls with regards to safety efforts. The histogram, as shown in Figure 5, provides a clear representation of the output.

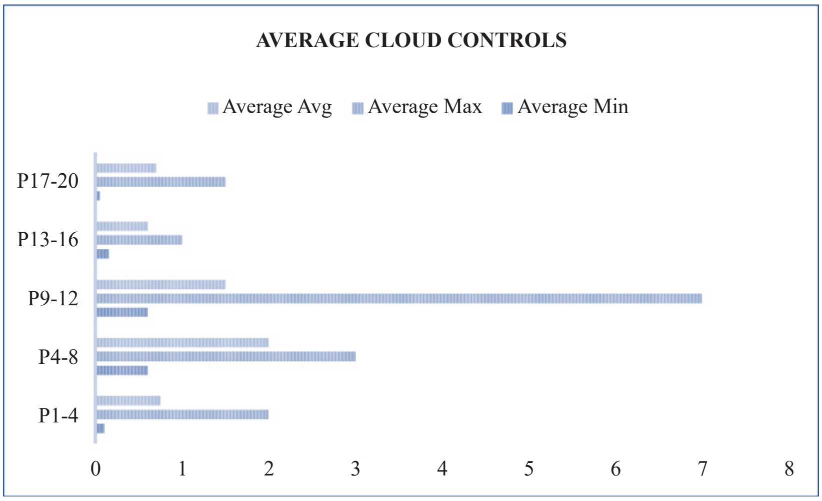

Figure 5. Output of average cloud controls in companies

6.2 *Policies available to curtail suspected Security Violation*

Suspected security occurs when unauthorized individuals gain access to sensitive company information or data stored in the cloud. But when there is a suspected data breach, the company mostly put some actions or measures in place to prevent or solve the problems of the data branch. Some of the responses from our respondents are as follows;

- Vulnerability Management: Regular scanning of vulnerability and privilege-related risks. Practices like penetration testing to determine real-world security resistance should be carried out to audit and test identified vulnerabilities.
- Password Control: There should be a practice of creating a strong password which will be difficult for external or unauthorised individuals to attack the cloud. Password should be changed regularly if possible or suspected of a shared password [22]. Combining passwords with another authentication system for sensitive areas and establishing password management best practices, where respondents stated that practices like encryption, patching, and maintenance could help in the case of a suspected data breach.

- Regular Backup: Backing up data is one of the significant ways to prevent companies' data from disaster. Data are backup when in the cloud and also in transit. By doing this, data in the cloud is secured even when they are tempered; the backup can happen data can replace the lost data [22]. The backup can happen on Home P.C., external hard drives or even cloud-to-cloud as long as two cloud providers cannot share the data.
- Multiple server plant locations: Having multiple server plant locations can also help companies with disaster recovery. Companies' data is stored on multiple servers across multiple locations enabling fault tolerance and bringing in viability and sustainable access. If one server at a particular location is affected by a disaster, the other server will run perfectly in place of the affected server.

6.3 *Effective security strategies in Trend*

Identity & Security Trends insights were gathered from cybersecurity leaders, consulting and systems integration experts, and technology providers. To build a company strategy in an actionable year, they share these actionable steps surrounding each trend to fortify the security posture.

- Rapid Uptake of Cyber Insurance-With an increase in frequency and sophistication of cyber-attacks, damage to organizations can be enormous. Cyber insurance is gaining momentum as a means of protecting against this risk. However, vulnerable enterprises are noticing challenges concering insurance including cost, limited availability, and more stringent security expectations from insurers to policyholders.
- Identity Security Gaps with IDR-Identity Detection and Response (IDR) describes a new enterprise cybersecurity method that can protect an organization's identity infrastructure and other IT systems. IDR uses identity-based risk to identify potentially malicious behaviour occurring within an enterprise and restrict or terminate the identities exhibiting that behaviour. IDR will provide the necessary identity risk context, access patterns, and behaviour analysis in identifying a threat with high fidelity.
- New CISO Leadership Mandate-It's now common for CISOs (Chief Information Systems Officers) to be board members and regularly engage in C-level business discussions. But the technical background of a CISO can become a barrier to communication in this environment. Not surprisingly, disconnects emerge that affect the critical flow of resources and information. To maximize impact, CISOs must evolve their communication style to bridge gaps, improve performance, and even limit professional liability.
- (Shift) to the Left, to the Left-Enterprises are quickly realizing the necessity of "shifting left" and introducing security measures earlier within the software supply chain, particularly as varied code, open-source software, data sets, and cloud-infrastructure get put to use.

7. Conclusions and results

The organization's responses suggest that serious safeguards for cloud-based data are required and are being implemented. However, slow Internet access, cost management, a lack of resources, governance and control, compliance, and performance are still obstacles to the growth of cloud computing. However, with the right strategic approach, Management details can assist in minimizing the cloud's potential risks and challenges and maximizing the cloud's benefits.

Strong passwords and security measures are in place to ensure that only authorized personnel have access to the data, accounts are not logged in public areas, and files, passwords, and other security details are properly shared without leaving any trace [22]. Most associations are likewise utilizing two-factor verification (2fa) or MFA (Multifaceted validation) to lay out admittance to the cloud framework. To convince the cloud system or service that you are who you say you are for the system to determine whether you have the authority to access the cloud's data, the cloud administrator must provide two distinct types of information with 2Fa7 MFA.

Additionally, when viewed from all three objective perspectives, the findings make it abundantly clear that in accordance with Objective 1, 70 percent of security professionals at businesses regard SPT claims as a top priority and have measures in place to mitigate them, as shown in Objective 2. In current parlance, the purpose of Objective 3 is to maintain economic and long-term viability for the sustainability of businesses. The well-known trends that these businesses follow are highlighted.

Distributed computing has turned into a critical innovation for associations across different areas, empowering the conveyance of processing administrations over the web. The rapid adoption of cloud services is due to its advantages, such as cost savings, scalability, and accessibility. The NIST distributed computing engineering gives an extensive structure that assists associations with understanding the different parts that make up a distributed computing framework, from the client layer to the cloud supplier layer. In examination, the cloud design in the virtualized climate, known as cloud-local engineering, exploits the versatility, adaptability, and cost viability of distributed computing through microservices, compartments, and arrangement devices. These give long-haul supportability to organizations. While distributed computing offers many advantages, it additionally presents critical difficulties with regard to security, protection, and trust, which are getting tended to through the solid, successful and moving measures recognized as a feature of the exploration arrangements.

8. Future research

The majority of businesses, in general, approach cloud security issues from an abstractive perspective and capture the security requirements of various stakeholders at various levels to assist them in securing their cloud systems in a time-based rather than a long-term manner. In order to find a solution to this issue, additional research into cloud architecture security patterns, security enforcement, and feedback on these organizations' current security status is needed from a variety of stakeholders at various levels, including internal and external (which is not the focus of this study) but could be extended further for future.

Conflict of interest

The author declares no competing financial interest.

References

[1] Liu F, Tong J, Mao J, Bohn R, Messina J, Badger L, et al. *NIST Cloud Computing Reference Architecture*. National Institute of Standards and Technology, Gaithersburg, MD; 2011. Available from: https://doi.org/10.6028/NIST.SP.500-292.

[2] De Donno M, Tange K, Dragoni N. Foundations and evolution of modern computing paradigms: Cloud, iot, edge, and fog. *IEEE Access*. 2019; 7: 150936-150948.

[3] Zanni A, Bellavista P, Corradi A. Integrating mobile internet of things and cloud computing towards scalability: lessons learned from existing fog computing architectures and solutions. *International Journal of Cloud Computing*. 2017; 6(4): 393.

[4] Rodriguez VKQ, Guillemin F. Performance analysis of resource pooling for network function virtualization. *2016 17th International Telecommunications Network Strategy and Planning Symposium (Networks)*. Montreal, QC, Canada: IEEE; 2016. Available from: https://doi.org/10.1109/NETWKS.2016.7751169.

[5] Vadakkanmarveettil J. *Cloud Auditor: A Brief And Easy Overview (2021)*. UNext; 2021. Available from: https://u-next.com/blogs/cloud-computing/cloud-auditor/ [Accessed 18th July 2023].

[6] Gleb B, Dmitriy G. *Choosing the Right Cloud Service: IaaS, PaaS, or SaaS*. RubyGarage; 2019. Available from: https://rubygarage.org/blog/iaas-vs-paas-vs-saas [Accessed 18th July 2023].

[7] Ernawati T, Febiansyah F. Peer to peer (P2P) and cloud computing on infrastructure as a service (IaaS) performance analysis. *Jurnal Infotel*. 2022; 14(3): 161-167. Available from: https://doi.org/10.20895/infotel.v14i3.717.

[8] Bazm MM, Lacoste M, Südholt M, Menaud JM. Isolation in cloud computing infrastructures: New security challenges. *Annals of Telecommunications*. 2019; 74(3-4): 197-209.

[9] Taufiq-Hail GA-M, Alanzi ARA, Mohd Yusof SA, Alruwaili M. Software as a Service (SaaS) cloud computing: An empirical investigation on university students' perception. *Interdisciplinary Journal of Information, Knowledge, and Management.* 2021; 16: 213-253. Available from: https://doi.org/10.28945/4740.

[10] Zimba A, Chama V. Cyber attacks in cloud computing: modelling multi-stage attacks using probability density

curves. *International Journal of Computer Network and Information Security*. 2018; 10(3): 25-36.

[11] Riad K, Hamza R, Yan H. Sensitive and energetic IoT access control for managing cloud electronic health records. *IEEE Access*. 2019; 7: 86384-86393.

[12] Sudha MR, Sornam M. A revolutionary approach to cloud computing, security and its user compliance. *Indian Journal of Science and Technology*. 2017; 10(1): 1-8. Available from: https://doi.org/10.17485/ijst/2016/v10i1/92560.

[13] Manvi SS, Shyam GK. *Cloud computing: Concepts and technologies*. Boca Raton, FL: CRC Press; 2021.

[14] Marks E. *Seeing Through The Clouds: The Power of Cloud Transparency*. Cloud Spectator; 2019. Available from: https://cloudspectator.com/the-power-of-cloud-transparency/.

[15] Khan MA, Salah K. IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*. 2018; 82: 395-411.

[16] Nogueira E, Moreira A, Lucrédio D, Garcia V, Fortes R. Issues on developing interoperable cloud applications: definitions, concepts, approaches, requirements, characteristics and evaluation models. *Journal of Software Engineering Research and Development*. 2016; 4(1): 7. Available from: https://doi.org/10.1186/s40411-016-0033-6.

[17] Gillham J, Abenavoli RM, Brunwasser SM, Linkins M, Reivich KJ, Seligman MEP. *Resilience Education*. Oxford Handbook Of Happiness; 2013. Available from: https://doi.org/10.1093/oxfordhb/.

[18] Jackson R, Drummond DK, Camara S. What is qualitative research? *Qualitative Research Reports in Communication*. 2007; 8(1): 21-28. Available from: https://doi.org/10.1080/17459430701617879.

[19] Busetto L, Wick W, Gumbinger C. How to use and assess qualitative research methods. *Neurological Research and Practice*. 2020; 2(1): 1-10. Available from: https://doi.org/10.1186/s42466-020-00059-z.

[20] Grant MJ, Sen B, Spring H. *Research, evaluation and audit: Key steps in demonstrating your value*. London: Facet Publishing; 2013.

[21] Charles P. Security issues in cloud computing. *International Journal of Emerging Trends in Science and Technology*. 2017; 5(6): 5253-5256.

[22] Drago I, Bocchi E, Mellia M, Slatman H, Pras A. Benchmarking personal cloud storage. *Proceedings of the 2013 Conference on Internet Measurement Conference*. ACM Digital Library; 2013. p.205-212. Available from: https://doi.org/10.1145/2504730.2504762.