BULLET: Jurnal Multidisiplin Ilmu
Volume 03, No. 06, Desember, 2024
ISSN 2829-2049 (media online)
Hal 715-725

A Comprehensive Review of Information Assurance in Cloud Computing Environments

Nahid Neoaz

Wilmington University, USA

nahidneoaz@yahoo.com

Abstract

IA is information that relates to the safety or insecurity of data and service that reside in the cloud computing spaces. Due to the benefits that are enshrined by cloud technologies organizations are using the cloud technologies as solutions to scalability, costs and flexibility while addressing issues of data privacy and security threats and compliance. It is for this reason that in this paper, the following aspects will be addressed; information assurance and cloud computing and other elements of information assurance such as CIA triad, authentication and non-repudiation. It also defines risk at the present time to mean data breach, insider threats, and Distributed Denial of Service (DDoS) attack among others; and how each of these organizations can pursue risk management strategies to such risks. In addition, this paper examines the data privacy aspect and the legal regulation of and concerns with cloud security in the shared responsibility model. By going through the organization information assurance plan, it is asserted that risk identification, assessment and monitoring, and information asset protection such us data encryption, and access should be acknowledged. Thus it becomes possible to implant sound security solution into the cloud computing solutions/ So by emulating on the best practices in support of the security/organizations gain all the benefits of Cloud computing. This paper gives a detailed insight of how Information assurance in cloud environment in a world that is going digital can be handled.

Keywords: I governing IAs, CC, DP, RM, Compliance, Security, CIA, C–Cloud, TL & DP.

INTRODUCTION

Information assurance (IA) was said to refer to the achievement of protecting the confidentiality, integrity, availability, authenticity, and reliability of information in an information system. They are blossoming IT sub discipline that can incorporate components of computer security, security risk management, and information management to ensure the safeguard of data against damaging/accidental utilization/destruction. Information assurance also holds a central position when it comes to developing the desired form of confidence and safeguarding of important information in organizations and protection of valuable data on those systems [1]. Today shift identification shift has moved towards the IT orientated society knowledge has thus become one of the most valuable assets that is required in every individual firm and state. This is why after adopting a cloud computing environment it was realized that securing information had become a challenge and problems are numerous. This complexity is handled by Information assurance’s assertion that all the layers of the system and implements that govern the use of information assets are properly addressed from the physical security of computers’ end user hardware to the security of program structures or software used by the assets. At its core, information assurance focuses on the five pillars of the CIA Triad [2].

Privacy on its part ensures that such information is only provided to those people who have right to that information. This is made by application of the principle of encryption, usage of the access controls as well as other measures within the domain of the protection from unauthorized access. The unique selling point of using them is they cannot be given wrong data – they will not corrupt, lose or alter the data in any way while in use. This includes protection from manipulation or in fact any change on the data without the right authorization [3]. These are situations when information as well as systems are operationally on line in the time required for their use. This is necessary so as to avoid interruptions and thereby sustaining business and operation in regimes whereby a business organization is plagued with loss because of interruptions. In addition to the CIA Triad, information assurance incorporates two other critical aspects:

It is the way of checking whether the user or the system which requests the data or service listed above is allowed to interact with the system. Of non –repudiation it is simply clears and evident that a claimant cannot be in a position to deny that he performed a specific function. Surprisingly, it proves to be more accurate in legal and financial systems that demand occurrence of the actions that took place in the system be demonstrative and a hundred percent provable [4]. Information assurance is no other systems and information protection alone but the concept is larger than that. It means the processes for identifying norms has changed for protecting risks of information in an organization. The institutional purpose of IA is to ensure that an organization is able to determine risks that exist for an Information system, and manage the risks. It also consist of proactive monitoring, hoping to identify risks and threats and respond to these is as fast as can be [5].

As will be illustrated at cloud computing environment, the ASD information assurance process is not an open and shut case. Security problems are still considered sensitive questions for an organization particularly when it is a question of distributed systems, third party service providers and common resources. As such, the main advantages including scalability, low cost, flexibility mean that cloud computing has specific risks that are associated with the data and the level of control and security. The clouds are thus acknowledgement that the information assurance in the cloud Latest Sampled embraces the conventional security control methods in addition to those which are novel for the risks unique to the cloud model of the cloud [6]. Thus, information assurance is recognized as a security science which in any way, be it traditional or cloud information transfer media, has to safeguard usability, confidentiality, and integrity of the carried information. It includes a broad perspective, which encompasses the technological aspect of the issue, existing policies pertaining to security and the solutions to rectify several security issues through risk management. In this regards, it is impossible to underestimate the importance of the powerful information assurance Framework as its importance rose with enhanced organizational digitalization processes [7].

OVERVIEW OF CLOUD COMPUTING

The advancement of cloud computing is one among the most disruptive technologies today at least when it comes to computing environments. This is the managed use of computing resources and services for storage, computation, applications, networks, and services reachable over the Internet or other networks but not physically located in a company, a campus, or a remote site [8]. In this regard, cloud computing also present a rich and effective way of accessing software packages for computational uses via the www without significant physical commitment in machinery; hence organizations and individuals who may not be heavily invested in machineries can efficiently obtain optimal computation systems for a short while. The methods of the application across the cloud is one of the meticulous solution that drove the elastic, easily extendable, comparatively inexpensive over the means of the IT service delivery mod [9].

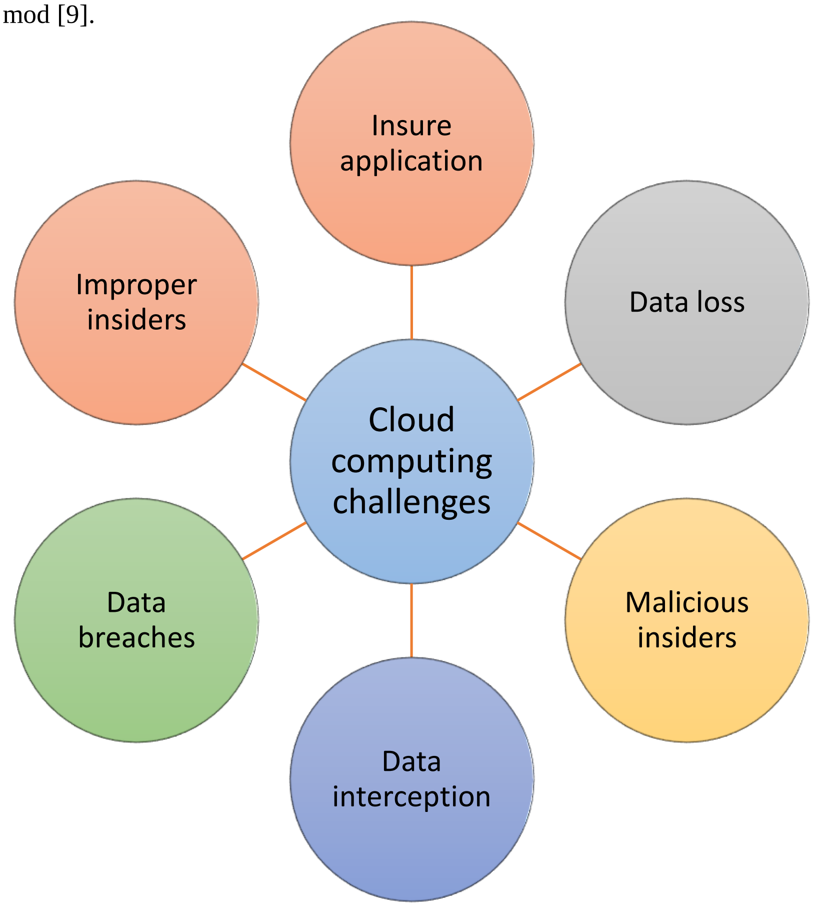

Figure: 1 showing cloud computing challenges

Infrastructure as a Service (IaaS): IaaS is simply the rental of computing infrastructure, equipment and software such as servers, storage, networks, etc over the internet. It allows business organizations to lease the virtualized structures at some fixed fee for use and still be in a position to offer a broader usage or, on the other hand, limit the usage if the situation warrants it. The most recognized known IaaS vendors at present are Amazon Web Services, Windows Azure, and Google Cloud Services [10].

Platform as a Service (PaaS): PaaS give developers a platform on which to build applications & services without having to undertake the rigorous of establishing the support systems. It supports pre-developed professional development suites, databases besides applications and frameworks [11]. Of course, it comes as a massive blow for organizations that have to solely worry about development and do not have to bother with the infrastructure at hand. Some of the notable PaaS services are as follows; Heroku, Google app engine and so on [12].

Software as a Service (SaaS): SaaS is one of the distribution models through which the software is accessed by the customer over the internet and mostly on a contract basis on permissioned access. These applications can be run and provided thru a hosted web browser where no application has to be installed or supported by the user [13]. SaaS is probably the most demanded type of cloud computing services and model and comprises the traditional services like office 365, google workspace and salesforce among others. In addition to these service models, cloud computing can be deployed in various models based on the level of ownership and control [14].

Public Cloud: Public cloud referred to a situation where ‘computing resources’ are procured from a third party and can be used by the public and or other organizations. There are AWS, Google cloud and Microsoft Azure and the multi-tenant public cloud services is comparatively cheap because many consumers use it [15].

Private Cloud: And it can therefore be defined as the selective cloud environment that is only available and accessible from and within a given firm. It could be run inside the organization or could be tendered out to an outside contractor such public storage comes with different compliancy or regulate requirement that are all beneficial to enabling organizations work independently on data security and privacy [16].

Hybrid Cloud: Hybrid cloud is indeed the aggregate of the private cloud and the versatility of the public cloud, & gives a choice for loads to be transferred or worked in either. They afford the capacity as movement among one cloud structure to another one or internal status or to gain extra resources as needed [17].

Cost, Scale and Flexibility: This therefore means that organizations can always scale up or, likewise, scale down their capacity depending on the requirement thus it is unprofitable to buy many resources that are rarely used or buy a small capacity, only to be overwhelmed by usage. Further, the cloud providers also avail their services on a usage or subscription basis further on top of eliminating high capitals of investments on the realization and implementation of data centers. But it has its bowlful of problems especially on the security, data privacy and compliance problems that goes hand in hand with cloud computing [18]. However, if this information is backed up in another location then organizations will have to consider the security that offered by cloud computing partners. Talks involving data leak or loss, violation of data privacy and split responsibility demands precise measures for the protection of information. By being effective, elastic and inexpensive public and private cloud have revolutionized the manner in which public and private organizations tackle the delivery of services through IT. But when compute moves its activity and location in to the cloud for data and applications, concerns about security and governance of this model of computing are sprung in organizations to realize Information assurance in the cloud. The fundamental principle that users need to understand is on information assurance in cloud systems [19].

IA in cloud computing environments, therefore, is primarily concerning protection of data, systems, and networks using the flexibility and scalability features provided by cloud technologies. In the cloud, IA comprises several key principles accruing mainly from CIA Triad (Confidentiality, Integrity, Availability) with others such as authentication and non-repudiation being as important in protecting information. Confidentiality makes sure that data that is of sensitive nature you can only be accessed by the authorized users or computers [20]. In Cloud computing environments, there is high probability data leakage due to the fact that the data is hosted off site and at times transferred through different network. In order to keep information a secret, many use encryption methods in their data communication. Some of the data protection requirements which must be met include data transport protection, for stored data, access control by applying more enhanced data encryption and managing access them the identity and access management or IAM systems [21].

Integrity ensures that data is not changed in any way other than is intended or permitted by an authorized agent. In the cloud, lack of centralized infrastructure where data can be managed, data integrity requires the use of checksum, hash functions or digital signatures to validate data integrity. It is common that the providers of cloud services maintain the versions of the files and possess the backups to restore the primary files if they get corrupted, or if someone changed them maliciously [22]. This makes sure that cloud services and the data are available on call.

One of the benefits of the distributed architecture of cloud computing is high availability, on the other hand the essence of distribution increases the vulnerability to incidents such as service disruption or unavailability. These risks are controlled through redundant facilities; load balance methods; and auto-failover that keeps core applications and processes active despite problems with hardware or hackers [23].

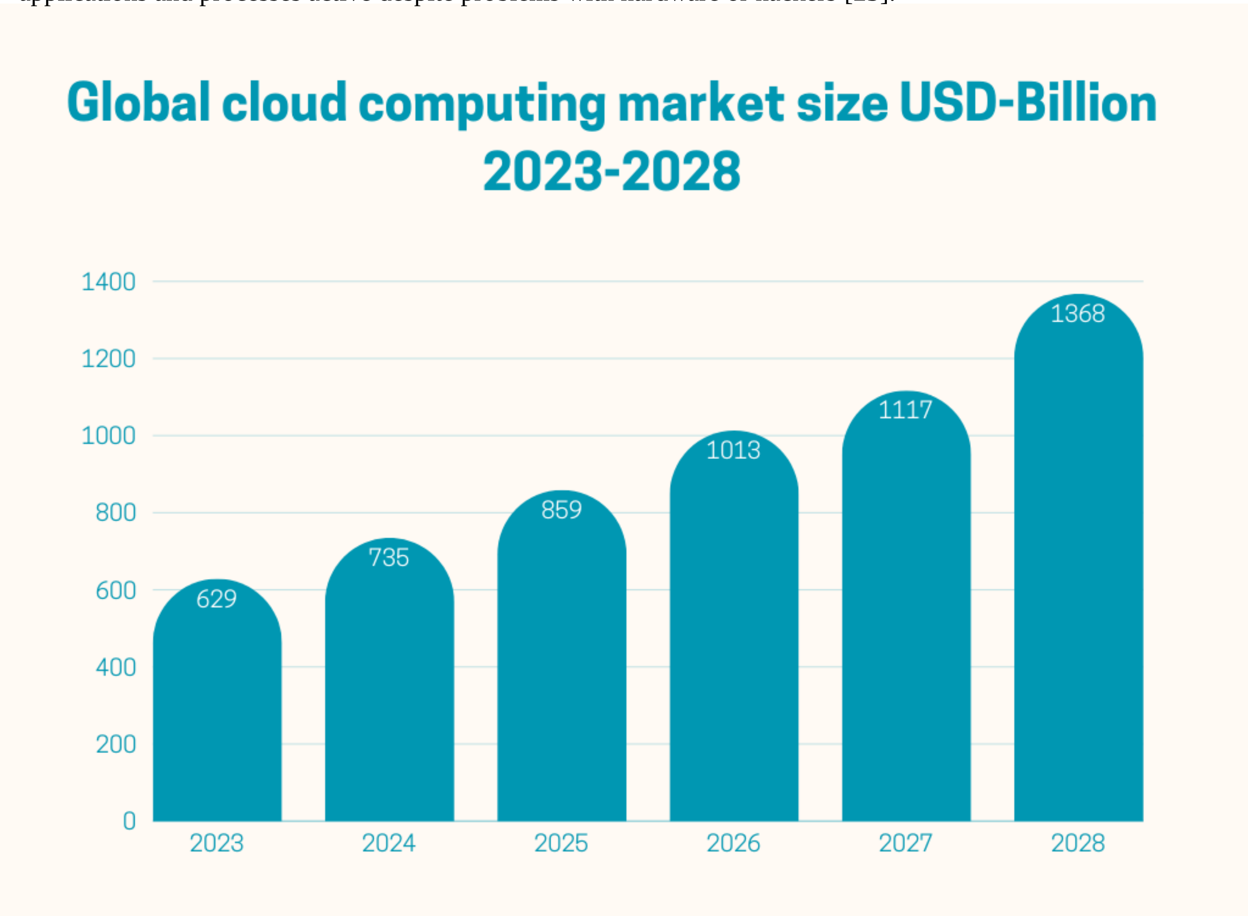

Figure: 2 showing cloud computing market size

CIA Triad is important in cloud computing, but so is user identity confirmation (authentication) and ensuring that actions cannot be denied (non-repudiation). Justification of the users' identity and effective cloud accountability strongly requires the application of proper multi-factor authentication approaches and digital logs. Thus, when these principles are followed to the later, cloud environments can be more assured of their information protection from unauthorized personnel, and service availability [24].

SECURITY THREATS ASSOCIATED WITH CLOUD COMPUTING

Cloud computing risk differs in threats that organizations are bound to encounter sometimes in their cloud computing operations because cloud operations pose serious risks to the privacy, integrity, and accessibility of data and services. Self-Learning is the process by which an individual learns by adapting new knowledge or skills due to the increased use for cloud services, it is crucial to understand and counter these threats in order to provide reliable information assurance [25].

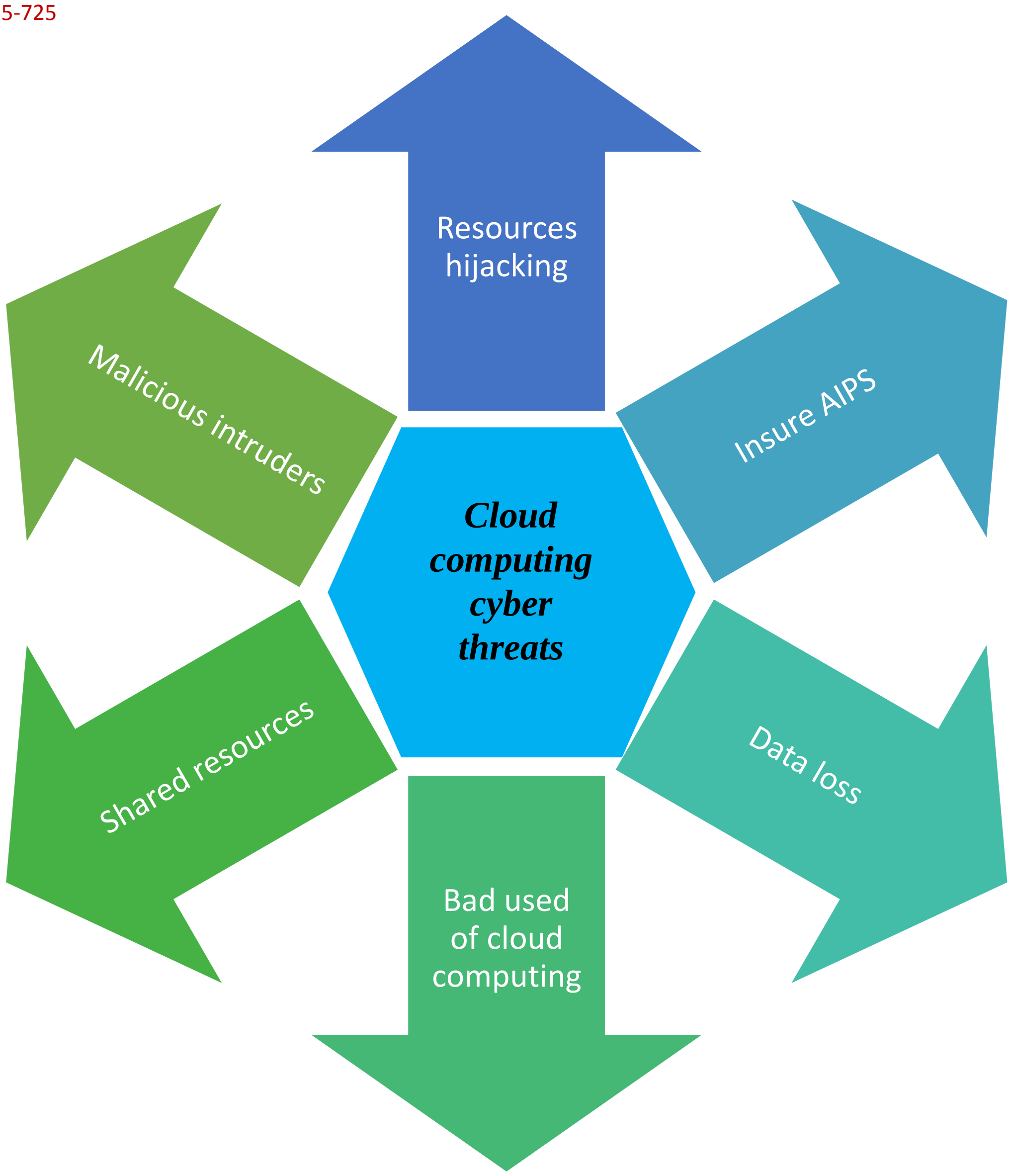

Figure: 3 showing cloud computing cyber threats

Data Breaches: Among the greatest risks that exist in cloud computing is that it is prone to hacking. Data that is stored in the clouds is one of the most vulnerable that can be attacked by cybercriminals. Without proper safeguard, the unauthorized party can gain access, steal or publish personal, financial or intellectual information. That means encryption, the proper implementation of access controls, and solid methods of authentication are needed to prevent such cyber-attacks [26].

Insider Threats: Cloud providers, along with their partners, ensure high levels of security, but internal attacks are always a real threat. Employees are well aware of an organization’s resources and therefore it is relatively easier for them to circumvent security measures in the cloud environment. Some of the control procedures include monitoring, auditing, and the use of role-based access control (RBAC) to minimize insider threats [27].

Denial of Service (DoS) Attacks: Another severe danger of the cloud environments is Distributed Denial of Service (DDoS) attacks. These attacks saturate the cloud services with traffic so as to deny the services to other legitimate users. In order to protect from DDoS attacks providers use such techniques as load balancing, traffic filtering, and rate limiting [28].

Data Loss: This is a result of loss of data or deletion, corruption of data or having insufficient backup systems in place. This means that in cloud computing environments where the data is distributed in different geographic regions or data centers, it’s important to ensure that there are procedures for backup and recovery to prevent total data loss [29].

Misconfigurations: Lack of proper setting or protection for cloud services that are necessary for an organization's functioning might provoke the appearance of several weaknesses that can be used by attackers. It can also be seen that misconfigurations are a potential cause of leakage of structured information or excess access to cloud-related services [30]. Great care should be exercised to avoid misconfiguration, and the security team ought to periodically scan for misconfigurations and set up auto-configuration tools.

Shared Responsibility Model: Cloud security inherently follows the shared responsibility model where some responsibilities are borne by the cloud provider and the other by the customer. Lack of or confusion regarding role definition and deployment results in security vices. Both the providers and the customers need to understand each other and have well-articulated policies regarding security in order to combat this problem [31]. In summary, cloud computing itself has presented various new security threats, thus business organizations have to apply integrated security measures in order to protect their cloud systems. This includes 'being ahead of the game' when it comes to alerting for risks, constant vigilance and the familiarization with best practices to ensure cloud infrastructure and data resistant to attack [32].

RISK ASSESSMENT ON THE CLOUD COMPUTING ENVIRONMENT OPPONENT

Hence, one may regard it as the model through which assessment of risks and opportunities attached to data, application, and structures, as hosted in cloud technologies, measurement, management and monitoring thereof can be understood. New threats originate with cloud since the later has to be managed through specific strategies and measures that will be beneficial for cloud implementation to meet the standard requirement for data protection and other assurance and regulation requirements [33]. A comprehensive risk management approach in the cloud involves several key elements: Risk is either measured/assessed it is controlled and finally monitored always within the line of the process.

Risk Assessment: Risk assessment or more correctly the assessment of threat opportunities is thus the initial and fundamental level of risk management in the context of the discussed cloud environment. This risk includes the organizational risks and the risk that may be related to cloud infrastructural, risk that could be related with third party service provider and split risk between the organizations that want to shift data to cloud and the cloud provider [34]. A large part of problems in cloud environments are identifiable and comprise of loss, unauthorized access, availability and compliance losses. Risk assessment should also consider the legal and the regulatory and the privacy since some of the data and information required for effective risk management are stored in various parts of the world which is legally bound by other laws [35].

Risk Mitigation: However, as soon as risks have been identified the next step has to be taken to ensure those risks are either managed or minimized. For IT gc, some of measures are; implementing security standard like: Cloud storage and data retrieval procedures, access locked down procedure in the data, two factor authorization mechanism of data, and patching up of rights data. In addition, measures that are required to prevent disruption of any service, disaster recovery and business continuity should have set pillars Security services also support tools and services products through which customers of cloud can minimize risks and an intruder for example of detection, firewall, and others protocols. But they said, it is good for the organizations themselves that they have embraced a number of tools and governance which is not always the case [36].

Continuous Monitoring: As pointed out in the literature review the cloud risk has many avatars and needs to be handled preventively and in complementary ways as well as in emergent and as complex and thus requiring a multiple methods approach. Real-time monitoring does contain features that will allow the status of the security of an organizations cloud environment to be tracked to assist inv the identification of breaches as they occur. It can include NL processing tools that analyze unconventional sporadic processes, provide signals and may be useful for further appropriate actions, electronic access tools which operate in close connection with the above mentioned tools [37]. The second one is the supervision of the information security situation to ensure that once started, the risk management process corresponds to classification of cyber threats. Cloud computing risk management is an activity that may also be on-going, with four processes could include risk identification, risk control, current risk assessment and risk treatment. In this way the risk management approach shall guarantee both assurance as well as compliance of the data of an organization as well as eliminating the risk of security threat if which likely to occur may lead to halt or a poor of the image of the organization [38].

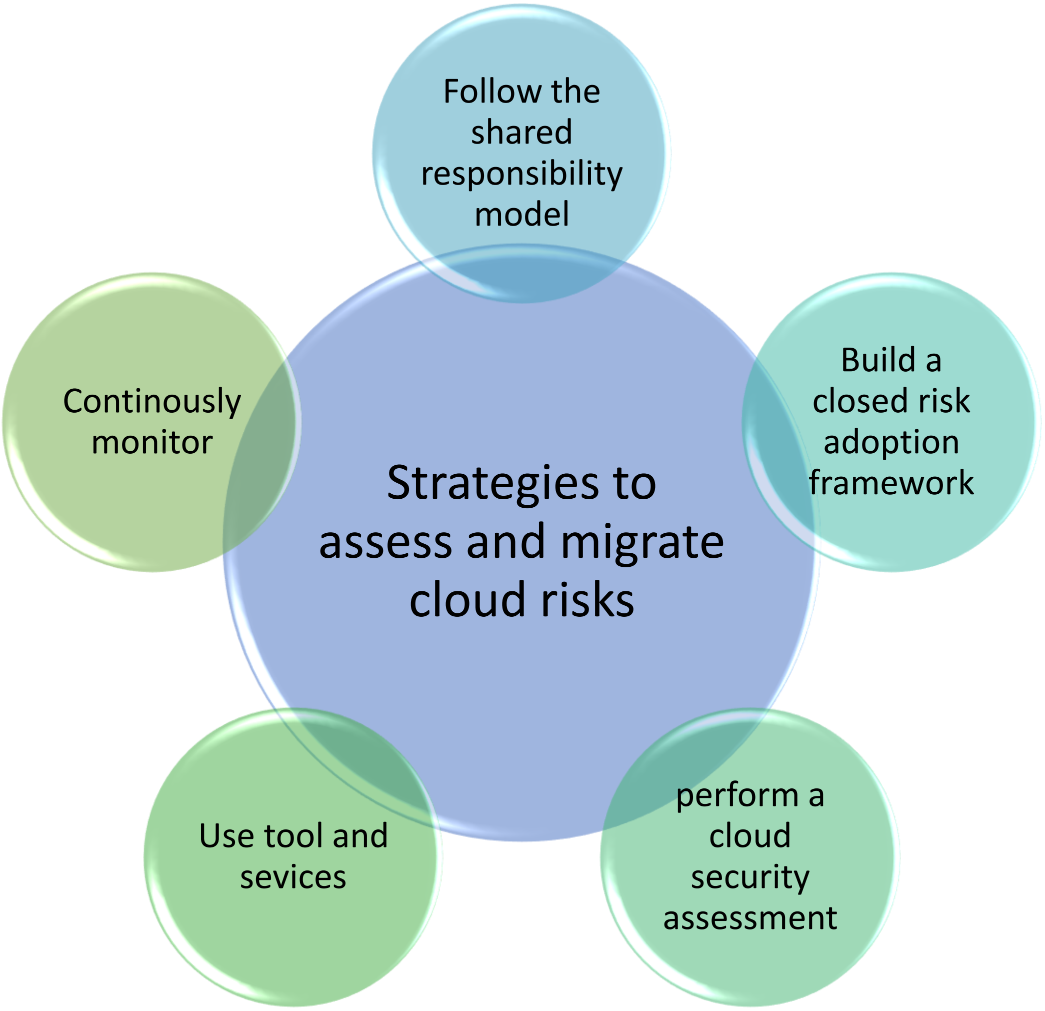
Follow the shared responsibility model
Build a closed risk adoption framework
perform a cloud security assessment
Use tool and sevices
Continosly monitor
Strategies to assess and migrate cloud risks

Figure: 4 Strategies to assess and migrate cloud risks

PII AND ITS MANAGEMENT SEEMS TO BE THE TWO LARGEST PHENOMENA

It is the facts that have to be looked at whenever the organization is engaging the cloud computing services some of which are the security compliance. Since organizations have adopted the cloud services to store simple data let alone personal, sensitive or confidential data the need to protect such data effectively against loss, misuse or cyber–attacks is imperative [39]. At the same time they have to sort through a vast amount of the international legal acts governing circumstances of storage, processing and transfer of the data. If, from the technical and legal perspective, the cloud computing duties are accomplished, the questions related to data protection and compliance can be achieved by the organizations irrespective of the data and application outsourcing through the cloud [40].

Data Privacy Concerns: The cloud solution is normally implemented by different third party service and data providing firms; hence the question of data ownership and protection arises. They become a concern for cloud providers, because data may be distributed in several geographical regions which raises questions on ownership, and privacy to data. Cloud customers must be guaranteed that their cloud service provider has at least a very high standard on data privacy, for example, this must ensure that the cloud service provider uses very strong protection on the customer's data as they move around and also when they are idle. Also, if successful; fundamental principles such as data anonymity and data restriction reduce likelihood of privacy violation through reducing physical volume of data [41].

Regulatory Compliance: Security of data is legal dependent on the nature of the company and the area where the company operates. Among these there is General Data Protection Regulation (GDPR) in European Union which concerns the collection of individual's data and the Health Insurance Portability and Accountability Act (HIPAA) in United States which concerns with the privacy and security of health data [42]. Although recognizing that some particular cloud service providers have to abide with such regulations, the organizations that obtain cloud services host improper cloud service illegitimately or are probably unaware of legal consequences of data storage, access, and transfer [43].

Data Sovereignty: Hence, data ownership relates to the same idea as according to which data is regulated by the laws of the country of residence. When asked how the cloud providers can meet the data localization the answer could be that cloud providers could spread the data in several locations and every such location may also have its own rules on how the data should be dealt with. Some rules in legal regulation limit locations where data can be stored and organizations price themselves against where their cloud providers have factored those rules [44]. Other two subcategories of information assurance in the cloud include data protection, and compliance. With this in mind, organizations require cloud providers that can articulate how these providers are secured, and the sound and appropriate policies that are in place as embraced by the cloud providers alongside compliance to laws governing some of these cloud services in the country/region and other parts of the globe [45]. Therefore, this paper is an attempt to provide some concept and analysis of the legal problems emerge in cloud computing and while implementing the data security measures organization can safeguard its legal problem to avail the benefit which cloud computing provides it.

CONCLUSION

Cloud computing information assurance is an essential and complex process of safeguarding cloud environment both reliability and individuals' privacy. They are; the emerging threats, mitigation strategies, data protection, and consequent legal requirements that accompany the ever-growing cloud adoption among organizations. New challenges are adjusting to the cloud computing environment into which the principles of protection of confidential information, its integrity, and availability come into their own, along with the requirements for strong authentication and non-repudiation. These principle, inherent in the cloud environment and the security requirements are outlined as follows, provide the framework of a good information assurance practice. However, threats like data breaches, insider threats and DDoS attacks do not take pause and require consistent and integrated approach on risk management including risk identification, risk management and ongoing monitoring.

From a data privacy and compliance perspective, cloud computing presents a new set of difficulties and concerns because cloud services are by their nature, international. Cloud customers need to understand how to meet data residency laws, sector-specific rules, and regulations, and the specifics of the shared responsibility model that exists between the provider and the user. Just legal implications of having sensitive data such as GDPR, HIPAA restrictions, good encryption practices and privacy measures need to be met in order to stay safe from malicious actors. Corporations relying on the CC are only capable of effective information assurance if they incorporate a risk management strategy. Using conceptual models to illustrate the types of threat and risk that may exist in a cloud environment, it is argued that when organizations adopt suitable security measures, perform risk analysis, follow legislation requirements, and carry out routine surveillance of cloud architectures, incredible opportunities will arise for organizations to protect their immense data assets. Put simply, the cloud can bring out its best while protecting the company data when key tools, policies and measures are in place.

REFERENCES

1. Radwan T, Azer MA, Abdelbaki N. Cloud computing security: challenges and future trends. Int J Comput Appl Technol. 2017; 55(2):158–72. Doi: 10.1504/IJCAT. 2017.082865
2. Sharma P, Jindal R, Borah MD. Blockchain technology for cloud storage: a systematic literature review. ACM Comput Surv. 2020; 53(4):: 89:1–32. Doi: 10.1145/ 3403954
3. Alkadi O, Moustafa N, Turnbull B. A review of intrusion detection and blockchain applications in the cloud: approaches, challenges and solutions. IEEE Access. 2020; 8:104893–917. doi:10.1109/ACCESS.2020. 2999715.
4. Patel P, Patel H. Review of blockchain technology to address various security issues in cloud computing. In: Kotecha K, Piuri V, Shah H Patel R, editors. Data science and intelligent applications. Singapore: Springer; 2021. p. 345–54. Lecture Notes on Data Engineering and Communications Technologies.
5. Xie S, Zheng Z, Chen W, Wu J, Dai HN, Imran M. Blockchain for cloud exchange: a survey. Comput Electr Eng. 2020; 81:106526. doi:10.1016/j.compeleceng.2019. 106526
6. Gai K, Guo J, Zhu L, Yu S. Block chain meets cloud computing: a survey. IEEE Commun Surv Tut. 2020; 22 (3):2009–30. doi:10.1109/COMST.2020.2989392.

7. Pavithra S, Ramya S, Prathibha S. A survey on cloud security issues and blockchain. In: 2019 3rd International Conference on Computing and Communications Technologies (ICCCT); 2019 Feb. p. 136–40.
8. Memon R, Li J, Ahmed J, Nazeer I, Mangrio MI, Ali K. Cloud-based vs. Blockchain-based IoT: a comparative survey and way forward. Front Inform Technol Electron Eng. 2020; 21(4):563–86. Doi: 10.1631/FITEE. 1800343.
9. Murthy CB, Shri ML. A survey on integrating cloud computing with Blockchain. In: 2020 International Conference on Emerging Trends in Information Technology and Engineering (Ic-ETITE); 2020 Feb. p. 1–6.
10. Xu H, Cao J, Zhang J, Gong L, Gu Z. A survey: cloud data security based on blockchain technology. In: 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC); 2019 Jun. p. 618–24.
11. Prianga S, Sagana R, Sharon E. Evolutionary survey on data security in cloud computing using blockchain. In: 2018 IEEE International Conference on System, Computation, Automation and Networking (ICSCA); 2018 Jul. p. 1–6.
12. Mohammadian V, Navimipour NJ, Hosseinzadeh M, Darwesh A. Comprehensive and systematic study on the fault tolerance architectures in cloud computing. J Circuits Syst Comput. 2020; 29(15):2050240. Doi: 10. 1142/S0218126620502400.
13. Isharufe W, Jaafar F, Butakov S. Study of security issues in platform-as-a-service (paas) cloud model. In: 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). IEEE; 2020. p. 1–6.
14. Shyam GK, Theja RSS. A survey on resolving security issues in SaaS through software defined networks. Int J Grid Util Comput. 2021; 12(1):1–14. Doi: 10.1504/ IJGUC.2021.112475.
15. R. Bonifazi, J. Vandenplas, J. ten Napel, K. Matilainen, R. F. Veerkamp, and M. P. L. Calus, “Impact of sub-setting the data of the main Limousin beef cattle population on the estimates of acrosscountry genetic correlations,” Genet. Sel. Evol., vol. 52, pp. 1–16, 2020.
16. D. A. Van Dyk and X.-L. Meng, “The art of data augmentation,” J. Comput. Graph. Stat., vol. 10, no. 1, pp. 1–50, 2001.
17. K. Houkjær, K. Torp, and R. Wind, “Simple and realistic data generation,” in Proceedings of the 32nd international conference on Very large data bases, 2006, pp. 1243–1246.
18. D. Evans, “Systematic reviews of interpretive research: interpretive data synthesis of processed data,” Aust. J. Adv. Nursing, vol. 20, no. 2, 2002
19. Z. Zhang, “Missing data imputation: focusing on single imputation,” Ann. Transl. Med., vol. 4, no. 1, 2016.
20. K. Weiss, T. M. Khoshgoftaar, and D. Wang, “A survey of transfer learning,” J. Big data, vol. 3, no. 1, pp. 1–40, 2016.
21. M. A. Bouke, A. Abdullah, J. Frnda, K. Cengiz, and B. Salah, “BukaGini: A Stability-Aware Gini Index Feature Selection Algorithm for Robust Model Performance,” IEEE Access, vol. 11, pp. 59386–59396, 2023, doi: 10.1109/ACCESS.2023.3284975
22. M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, “Feature extraction for machine learning-based intrusion detection in IoT networks,” Digit. Commun. Networks, 2022, doi: 10.1016/j.dcan.2022.08.012.
23. M. A. Bouke, A. Abdullah, S. H. ALshatebi, M. T. Abdullah, and H. El Atigh, “An intelligent DDoS attack detection tree-based model using Gini index feature selection method,” Microprocess. Microsyst., vol. 98, no. March, p. 104823, 2023, doi: 10.1016/j.micpro.2023.104823.
24. A. J. Izenman, “Introduction to manifold learning,” Wiley Interdiscip. Rev. Comput. Stat., vol. 4, no. 5, pp. 439–446, 2012.
25. P. B. Udas, M. E. Karim, and K. S. Roy, “SPIDER: A shallow PCA based network intrusion detection system with enhanced recurrent neural networks,” J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 10, pp. 10246–10272, 2022, doi: 10.1016/j.jksuci.2022.10.019.
26. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). The Most Recent Advances and Uses of AI in Cybersecurity. *BULLET: Jurnal Multidisiplin Ilmu*, *3*(4), 566-578.
27. Y. Himeur, K. Ghanem, A. Alsalemi, F. Bensaali, and A. Amira, “Artificial intelligence based anomaly detection of energy consumption in buildings: A review, current trends and new perspectives,” Appl. Energy, vol. 287, no. November 2020, p. 116601, 2021, doi: 10.1016/j.apenergy.2021.116601.
28. S. Rao, A. K. Verma, and T. Bhatia, “A review on social spam detection: Challenges, open issues, and future directions,” Expert Syst. Appl., vol. 186, no. August, p. 115742, 2021, doi: 10.1016/j.eswa.2021.115742.

29. R. K. Deka, D. K. Bhattacharyya, and J. K. Kalita, “Active learning to detect DDoS attack using ranked features,” Comput. Commun., vol. 145, no. June, pp. 203–222, 2019, doi: 10.1016/j.comcom.2019.06.010.
30. T. Hamed, R. Dara, and S. C. Kremer, “Network intrusion detection system based on recursive feature addition and bigram technique,” Comput. Secur., vol. 73, pp. 137–155, 2018, doi: 10.1016/j.cose.2017.10.011
31. N. Pilnenskiy and I. Smetannikov, “Modern Implementations of Feature Selection Algorithms and Their Perspectives,” Conf. Open Innov. Assoc. Fruct, pp. 250–256, 2019, doi: 10.23919/FRUCT48121.2019.8981498.
32. B. Subba, S. Biswas, and S. Karmakar, “Enhancing performance of anomaly based intrusion detection systems through dimensionality reduction using principal component analysis,” in 2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2016, pp. 1–6
33. D. C. Can, H. Q. Le, and Q. T. Ha, “Detection of Distributed Denial of Service Attacks Using Automatic Feature Selection with Enhancement for Imbalance Dataset,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2021, pp. 386–398. doi: 10.1007/978-3-030-73280-6_31.
34. M. Di Mauro, G. Galatro, G. Fortino, and A. Liotta, “Supervised feature selection techniques in network intrusion detection: A critical review,” Eng. Appl. Artif. Intell. vol. 101, no. October 2020, p. 104216, 2021, doi: 10.1016/j.engappai.2021.104216.
35. I. H. Hassan, M. Abdullahi, M. M. Aliyu, S. A. Yusuf, and A. Abdulrahim, “An improved binary manta ray foraging optimization algorithm based feature selection and random forest classifier for network intrusion detection,” Intell. Syst. with Appl., vol. 16, no. November 2021, p. 200114, 2022, doi: 10.1016/j.iswa.2022.200114.
36. L. D’hooge, M. Verkerken, T. Wauters, B. Volckaert, and F. De Turck, “Hierarchical feature block ranking for data-efficient intrusion detection modeling,” Comput. Networks, vol. 201, no. February, p. 108613, 2021, doi: 10.1016/j.comnet.2021.108613.
37. E. Mushtaq, A. Zameer, and A. Khan, “A two-stage stacked ensemble intrusion detection system using five base classifiers and MLP with optimal feature selection,” Microprocess. Microsyst., vol. 94, no. December 2021, p. 104660, 2022, doi: 10.1016/j.micpro.2022.104660.
38. Z. Halim et al., “An effective genetic algorithm-based feature selection method for intrusion detection systems,” Comput. Secur. vol. 110, p. 102448, 2021, doi: 10.1016/j.cose.2021.102448.
39. Khan, M. I., Arif, A., & Khan, A. R. A. (2024). AI-Driven Threat Detection: A Brief Overview of AI Techniques in Cybersecurity. *BIN: Bulletin of Informatics*, *2*(2), 248-261.
40. I. F. Kilincer, T. Tuncer, F. Ertam, and A. Sengur, “SPA-IDS: An intelligent intrusion detection system based on vertical mode decomposition and iterative feature selection in computer networks,” Microprocess. Microsyst. vol. 96, no. December 2021, p. 104752, 2023, doi: 10.1016/j.micpro.2022.104752.
41. R. Panigrahi et al., “Intrusion detection in cyber–physical environment using hybrid Naïve Bayes—Decision table and multiobjective evolutionary feature selection,” Comput. Commun. vol. 188, no. September 2021, pp. 133–144, 2022, doi: 10.1016/j.comcom.2022.03.009.
42. M. Artur, “Review the performance of the Bernoulli Naïve Bayes Classifier in Intrusion Detection Systems using Recursive Feature Elimination with Cross-validated selection of the best number of features,” Procedia Comput. Sci., vol. 190, no. 2019, pp. 564–570, 2021, doi: 10.1016/j.procs.2021.06.066.
43. V. Herrera-Semenets, L. Bustio-Martínez, R. Hernández-León, and J. van den Berg, “A multi-measure feature selection algorithm for efficacious intrusion detection,” Knowledge-Based Syst., vol. 227, p. 107264, 2021, doi: 10.1016/j.knosys.2021.107264.
44. S. M. Kasongo and Y. Sun, “Performance Analysis of Intrusion Detection Systems Using a Feature Selection Method on the UNSWNB15 Dataset,” J. Big Data, vol. 7, no. 1, 2020, doi: 10.1186/s40537-020-00379-6.
45. R. A. Disha and S. Waheed, “Performance analysis of machine learning models for intrusion detection system using Gini Impuritybased Weighted Random Forest (GIWRF) feature selection technique,” Cybersecurity, vol. 5, no. 1, pp. 1–22, 2022, doi: 10.1186/s42400-021-00103-8.
46. D. Kshirsagar and S. Kumar, “Towards an intrusion detection system for detecting web attacks based on an ensemble of filter feature selection techniques,” Cyber-Physical Syst., vol. 00, no. 00, pp. 1–16, 2022, doi: 10.1080/23335777.2021.2023651.