Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 16 (2021) pp. 161-168

A Review on Privacy and Security Assessment of Cloud Computing

Khushboo Jain[1], Manali Gupta[2] and Ajith Abraham[3]

[1] School of Computing, DIT University,
Mussoorie Road, Uttarakhand 248009, India
khushboojain2806@gmail.com

[2] GITAM University,
Hyderabad, Telangana 502329, India
manalics0042@gmail.com

[3] Machine Intelligence Research Labs (MIR Labs)
Auburn, WA 98071, USA

***Abstract*: Cloud computing is becoming increasingly common in many businesses. Cloud computing can be described as a distributed system in which a link is formed between the end-user and the cloud service provider's services (CSP). The most popular use is cloud storage, which has been the primary benefit of cloud computing, where the business data get stored in the cloud by the cloud provider. Despite this benefit, cloud computing's security has become much more critical due to numerous security breaches. This article outlines various work related to the threats, flaws, and possible safeguards in cloud computing.**

***Keywords*:** Cloud computing, cloud security, information security, data security, data privacy

I. Introduction

Cloud computing is a distributed system for services hosted by organizations and institutions without the need for maintenance at a very moderate price [1]. This technology is increasingly being adopted, but despite that, the security aspect of cloud computing is still a concern of the end-user in terms of the IaaS security level of the CSP [2]. Due to the flexibility in cloud computing, easy scalability, cost-saving, and high availability, it has been predicted that the cloud market will spread $241 billion by the end of 2020 [3][4]. Nowadays, cloud computing has become an essential aspect of every innovative technology organization, including core business apps, codeless applications, network security, data protection, remote security services, security virtualization, and identity management virtualization security. In all the points raised, data protection is essential in cloud computing, and this needs to be addressed before moving to the cloud [5][6]. This valuation is also reinforced by the 2020 prediction by Forbes that "the hyper-scale global public cloud leaders will form more alliances while refocusing on their core strengths; leading business app vendors will ditch their proprietary infrastructures; high-performance computing will take off; the crowded cloud-native development ecosystem will deliver service meshes and serverless computing; and cloud management vendors will shift focus to security after a well-publicized public cloud data breach" [7][8]. A lack of trained personnel, contradictory best practices, a lack of sophistication, and complex commercial structures tend to be part of the problem. The adoption of the cloud has reached a turning point, and we see today that the usage of cloud service is not only used by the average Internet users but most organizations and institutions have started migrating to the cloud (M2C). Despite all this, the security aspects of cloud computing need to be analyzed and addressed efficiently. One cannot rely on the quality of service (QoS) and the service level agreements (SLA) guaranteed by the host servers. This paper tries to cover a wide range of security flaws and possible solutions [9] [10]. Few questions raised to be addressed: (i) Human and Technology factor, (ii) Data Encryption Method, (iii) Data Location, (iv) Data Transmission, (v) Access rights, (vi) Data Protection, (vii) Protection and Recovery of Data, (viii) Forensic Support, (ix) Long term viability, and (x) Physical Security.

The Nine-Five-Circle [11] ISMS recommends that other factors that need to be considered in a data security perspective in the cloud environment are culture, communication, availability of resources, skilled personals, employees proper training security awareness, and competency.

The main contributions of this review work are as follow:

- To summarize various work related to the threats, flaws, and possible safeguards in cloud computing.
- It also includes details on the most influential cloud architectures and frameworks.
- In addition, the work looks at potential research areas associated with cloud computing security.

The remaining of this work is outlined below: In Section 2, we discuss the Cloud Infrastructure Architecture. In Section 3, we discuss the Security impacts based on deployment and delivery models. The threats and vulnerabilities of cloud computing are presented in detail in Section 4. In Section 5, we present several measures and controls to secure cloud computing. Finally, in Section 6, we offer the conclusion and explore

possible future research fields linked to security in cloud computing.

II. Cloud Infrastructure Architecture

This chapter provides a brief understanding of cloud architecture before diving into the security aspect. Cloud computing is a distributed system for services to be hosted by organizations and institutions. It is seen as a provider of on-demand computing services from applications to storage and processing power [12]. According to US-based National Institute of Standards and Technology (NIST) [13], the Cloud Computing Reference Architecture describes cloud computing and its security implications with four major players: (a) cloud client, (b) cloud auditor, (c) cloud provider, and (d) cloud broker. Figure 1 shows a conceptual model of the NIST cloud computing reference architecture [14], which describes the main actors in cloud computing and their operations and functions. The diagram portrays a generic high-level architecture and is meant to aid comprehension of cloud computing's specifications, uses, characteristics, and standards.

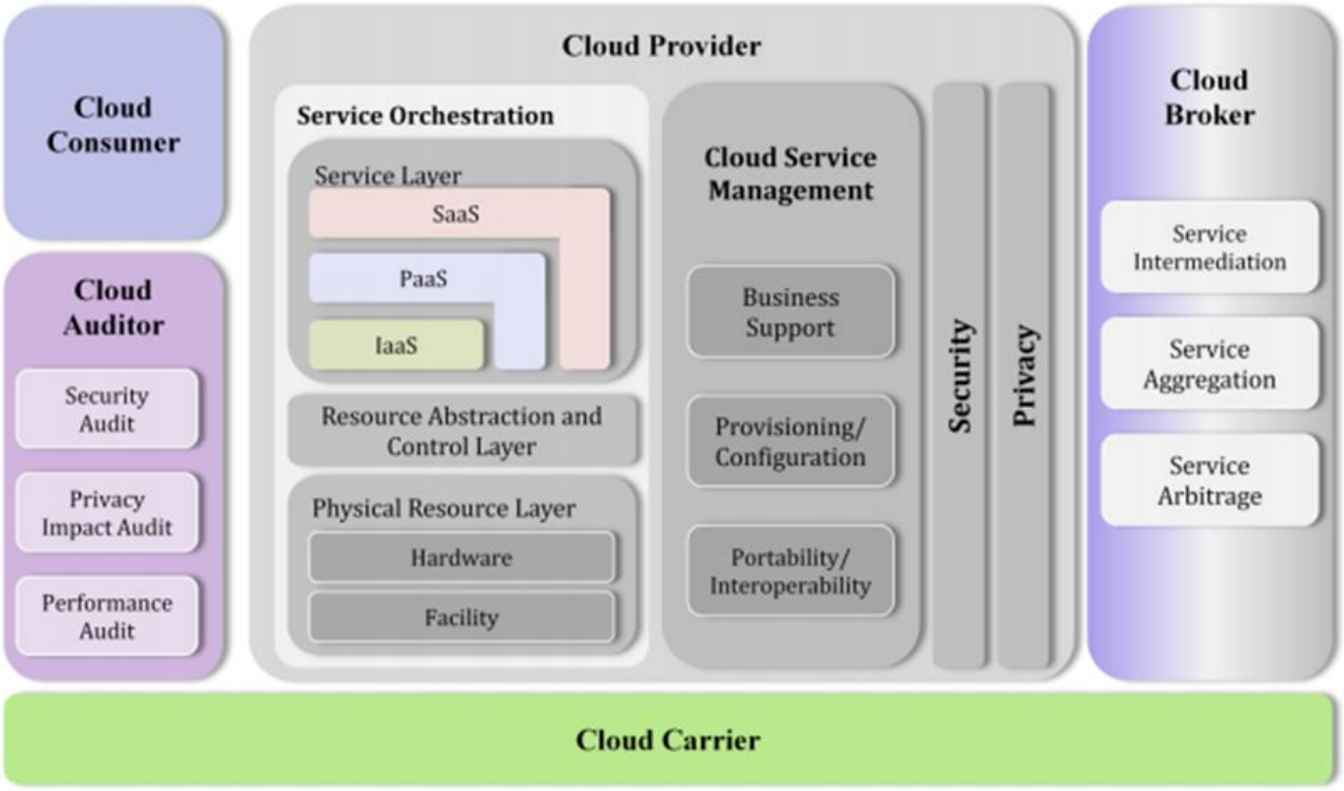

Figure 1. NIST Cloud Computing Reference Architecture

As shown in Figure 1, the cloud provider works over three-layer model which comprises of physical resource layer, resource abstraction and control layer, and service layer. Each layer provides different functionalities while serving the request from the cloud consumer. The physical resource layer deals with the underlying hardware in the cloud architecture. The resource abstraction and control layer provide abstraction to the resources present at different sites as well as controls them. The service layer provides three types of services to its customers which categorized as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) [15]. The cloud auditor, on the other hand, performs various security audits at different sites, privacy-based audit and performance audits to keep check on the performance [16].

The management activities related with cloud services provide business-support, provisioning or configuration and portability or interoperability. The business-support services include managing customers or contracts, managing inventory, accounting and billing, reports and audits, pricing and rating [17][18]. The provisioning or configuration include services like rapid provision, resource change, monitor and report generation, metering and SLA management. The portability or interoperability include services like data portability, copying data to-and-from, transferring bulk data, interoperability of services, providing unified management interface, system portability and migrating VM images/App/Svc [19].

In near future, the cloud and its services will become more complex by integrating more resources and services, it becomes quite difficult for the cloud customers to manage their cloud services by themselves. In such a scenario, instead of directly requesting to the cloud providers, the customers can request cloud brokers to manage the services. The cloud broker can act as service intermediate for enabling value added services to the customers; service aggregator for integrating multiple services for the customers; and service arbitrage for enabling customers to choose services from multiple ones.

The ISO certified Nine-Five-Circle (NFC) presents a framework to secure information at different levels in an organization [20]. It establishes the interrelationship between human security awareness and technology security best

practices and six major factors that also influence cloud computing its security. The NFC conceptual model [21], illustrated in Figure 2, presents an overview of the NFC security reference architecture, which identifies the major factors, their activities, and functions in cloud computing security, namely; (a) Security Intelligence, (b) Cyber threat intelligence, (c) External partners, (d) Organizational commitment (e) Information security misperception (f) Lack of Security Investment (g) Information Security policy.

III. Security impact based on deployment and delivery model

There are currently four different cloud implementation models [22] in use and three different types of integration systems.

A. Cloud Deployment Models

The security consequences of each of these four deployment and provisioning models are different. Both of these models and their security implications are briefly discussed in the subsections below:

Public Cloud [23][24][25]	
Description	This is based on a fine grain of resources. This is the common type of cloud deployment models such as google drive, dropbox, sky drive, and iCloud services. Infrastructure security measures are not known to customers nor the computing mechanism behind these services. Customers can add data and retrieve them at any given period of time when needed. The service provider guarantees the security aspect of this service.
Security Implication	Effects on security are relatively high, and you do not have to take care of them. In this model, your data lived behind an enterprise-class firewall and managed by skills personnel from the service provider. Your data is trusted in the hands of the service provider and its employees.
Security Disadvantages	The huge security challenge of this model is the global granted access. In this model, you will be sharing the server with several other uses. Here, your data security depends on the security measures established by the provider. Other factors include external legislation.
Private Cloud [23] [24][25]	
Description	This is a dedicated system set up for a single organization. Large organizations commonly use this. This comes with a completely private environment where these organizations can apply their security measures. This comes with a high cost.
Security Implication	Effects on safety are relatively high, as the organization controls the physical servers and access to the servers. Some other benefits are that the information lives behind your firewall, and the architecture design is based on your organization's exact needs.
Security Disadvantages	This model has a high implementation cost because it necessitates a large number of resources to maintain protection. Since your workers have physical access and defend against attacks if they occur, high management and administrative skills are needed. As a result, both cost and return on investment are important considerations in this model.
Hybrid Cloud [24][25][26][27]	
Description	A private cloud is connected to one or more external cloud providers in this cloud service technology model. It is seen as a combination of both private and public deployment models. This combination comes with various security strategies, and the cost of this type of model is less as both are integrated into one system.
Security Implication	A positive effect on security is that security can be targeted to the weaknesses, threats, and risks to be evaluated. This makes it cost-efficient and focused.
Security Disadvantages	Security challenges are relatively high due to their complex nature. Additional administrative efforts are required to manage and detect any risk exposure.
Community Cloud [24][25][28]	
Description	More than one single Infrastructure is used in this model type. Several organizations can control a single service deployment model. This kind of model is mostly used when organizations have a shared interest in using a single cloud model.
Security Implication	A positive effect on security is that security concerns are the provider's responsibility. Data is also hosted in several data centers to ensure high uptime, security, and recovery. Visionary financial institutions are adopting this model to make their operations more secure.
Security Disadvantages	You support yourself in any security breach.

Table 1. Cloud deployment model

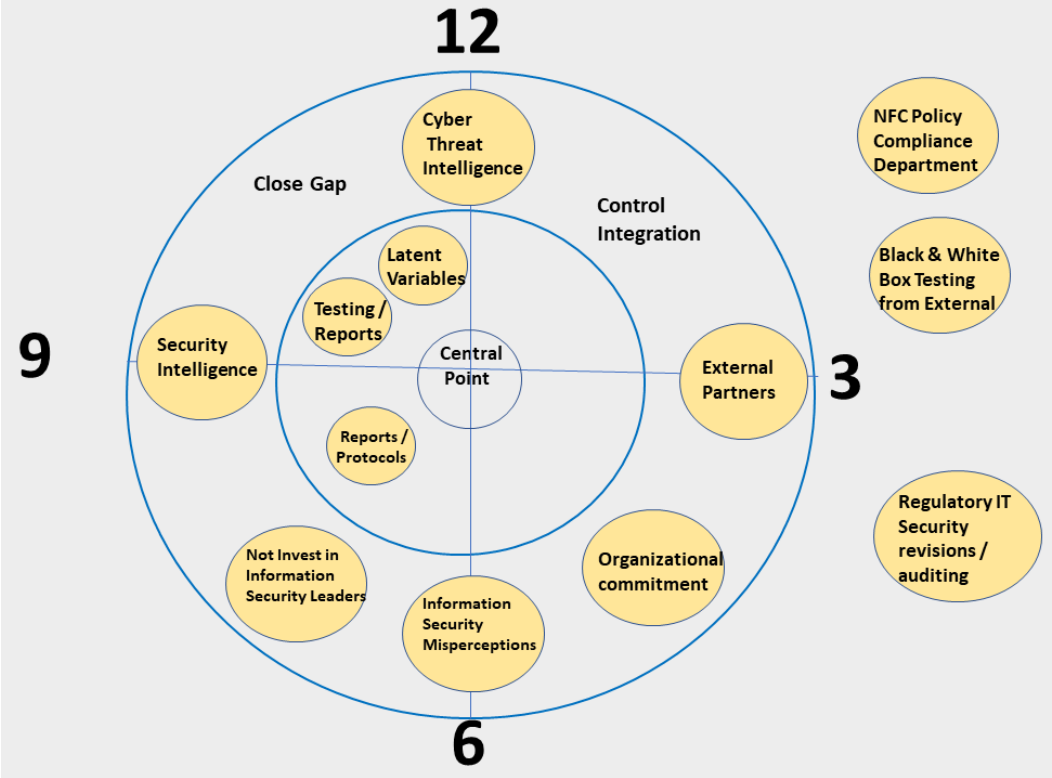

Figure 2. Nine-Five-Circle Cloud Security Reference Architecture

B. Cloud integration model

NIST [29] has proposed three cloud service models, namely, Infrastructure as a Service (IaaS) [30], Platform as a Service (PaaS) [31], and Software as a Service (SaaS) [32]. The service description and associated risk with each cloud service model is presented in Table 2. Further, the mapping of various cloud services provided by the cloud providers to the cloud model is presented in Table 3.

Delivery Model	Description	Risk
Infrastructure as a service (IaaS)	IaaS models are elastic and scalable. This is a cloud-based infrastructure used to maintain and monitor the cloud data and network. This model is based on the consumption of resources by the users. It requires less up-front investment and overhead. The cloud service provider is not responsible for the security of the data but rather the operating system security.	This model has a lot of advantages, but the risk is based on the shared services. Here the security responsibility is shared between the cloud provider and the user. In such scenarios, a misconfiguration in the security aspect, such as the wrong configuration of authentication or security standards from the user side, will leave potentially sensitive information vulnerable to unauthorized access.
Platform as a service (PaaS)	This is a platform used in the development of business applications and for offering cloud components. An example is google-cloud. This model allows organizations to build, run and manage web applications without the requirement of Infrastructure. Both IaaS and PaaS are pay-per-use models.	This model is based on the concept of using shared resources (such as hardware, network, and security measures); security issues typically focus on the business-critical information that hackers can obtain during a data breach. This platform is commonly used for business application development. The security responsibility lies on both the cloud provider and the user. However, the cloud provider takes the higher risk.
Software as a service (SaaS)	SaaS, or on-demand software, is a subscription-based model in which software is licensed and centrally hosted. This is a cloud-based software service used to manage third-party software by the client-side. This kind of application uses web plugins to deliver services. There is no download or installation requirement.	This model comes in handy when the consumer lacks the necessary resources or skills to set up an application ecosystem and manage. The SaaS provider takes the huge responsibility of the services being provided whereby the client ensures the client-side security. Data encryption and other security measures must be adopted here to ensure the security of data.

Table 2. Cloud delivery model

Model	SaaS	PaaS	IaaS
Public Cloud	Amazon Salesforce.com QuickBooks Office 365	Microsoft Azure, VMware, CloudFoundry, Google AppEngine	
Private Cloud		Stackato, Apprenda,	Hyper-V, VMWare, OpenStack, Cloudstack
Hybrid Cloud		Cloud Factory Customized	Customized, Rackspace

Table 3. Categorization of various cloud services

IV. Cloud Computing Threats, Risks, and Vulnerabilities

The same threats exist in the cloud as they do in conventional infrastructures, and they must be handled to the increasing number of cloud users per day, the amount of data stored by the service providers is also increasing rapidly. This has become an attractive target for attackers.

A. Vulnerabilities and open gaps in cloud security

The following are some of the vulnerabilities and open gaps in cloud security.

- **Data Breach:** The major concern arises from data theft due to the numerous numbers of sensitive data these providers keep. This has become a concern to consumers to know which type of security is being provided by providers to protect what type of data.
- **Internet-Accessible Management APIs can be Compromised.** Vulnerable interfaces lead to shortfalls in the confidentiality, integrity, availability, and security of systems and data. A service provider might change API connection, but these are frequently not communicated with the clients about the changes. This brings about a lack of transparency about the kind of vulnerabilities their data might face in the future. Here, we can clarify that the voice of selecting the right cloud model is based on the deployment and delivery model.
- **Shared Technology vulnerabilities:** Because of the increased leverage of resources, attackers now have a single point of attack that can inflict harm well out of proportion to its importance. An excellent example of a technology for sharing is a cloud orchestration or hypervisor.
- **Human Factor:** Companies that migrate to the cloud without a team of experts who are well-versed in cloud technology and the principles of delivering cloud-based applications may face downtime and much more serious operational issues.
- **Insider Threats:** Current or former employees, system managers, vendors, or business associates may all pose a threat, with motivations ranging from data theft to simple vengeance.
- **Misconfigurations and Authentication Bypass:** Misconfiguration of the authentication check is a common cause of data leaks. In combination with a bad encryption key and certificate management, weak passwords are the most common causes of security breaches.
- **Denial of Service (DoS):** Any form of DoS or Distributed DoS will affect all users on the cloud
- **Insufficient Due Diligence Increases Cybersecurity Risk:** Moving to the cloud without sufficient due diligence.
- **Malware Injection Attack:** They are injecting a service implementation or evil virtual machine into the cloud environment.

B. Attack Vector

Regrettably, when it comes to cloud protection, weaknesses in the cloud environment have been discovered, resulting in attacks. The following are a few examples of established cloud-based attacks. According to recent research, there are three main attack vectors: network, hypervisor, and storage hardware. The external, internal, cloud provider and insider attacks are all mapped to these vectors.

V. Security Measures

IaaS and PaaS have progressed beyond the early stages of deployment in the public cloud today. Now that more resources are being migrated to the cloud, confidence has become a critical factor in the relationship between the end-user and the CSP. Cloud security and trust have certain characteristics. The definition of protection in cloud computing is important because it is crucial in protecting user data stored in the IaaS cloud. Trust is linked to security because if the cloud is extremely safe, the data that resides in the cloud is also secure, increasing the degree of trust between users' perceptions of cloud services adoption.

It is important to assess and define the levels of Infrastructure that need attention and safety to reduce the risks associated with information security. The computing layer (hypervisor), data storage layer, network layer, user interface, API layer, etc. This chapter outlines some of the best practices to consider when protecting cloud computing and services, as discussed below. Further, the research work done to provide the different securities to cloud services and computing are presented in Table 4.

- **Data Encryption:** Data must be encrypted at rest and during transmission. Using the out-of-box encryption might not be appropriate for the type of data in question.
- **End to end encryption:** Data being transmitted must be encrypted due to the various geographical locations the data might traverse through.

- **Network Encryption:** Network encryption is also a mandatory.
- **Access Control:** Access control must be addressed by using a state of the act access approach. The use of multi-factor authentication, including OTP, tokens, smart cards, etc., will significantly reduce the risks of unauthorized access to the infrastructure.
- **Validate cloud user:** Screening cloud consumers to prevent the use of any malicious attack purposes.
- **Cloud Access Security Broker (CASB):** Enables administrators to anticipate potential risks of data loss and provides a high level of security.
- **API security:** API security must also be addressed to ensure that any vulnerability is mitigated.
- **Monitoring, Auditing, and Anomalies Identification:** Continuous monitoring and audit of systems allow you to track anomalies.
- **Staff Training:** Continuous security training on technical competence must be provided to enhance the overall level of information security.
- **Business continuity plans:** Security incidents that cause the unavailability of whole or part of a business-critical process must be documented.
- **Insider threats:** cloud providers should screen employees and contractors to prevent any insider attacks.

Protection Technology	Research Study	Description	Advantage	Limitations
Data Encryption	[33]	Applied AES method over Heroku implemented cloud	More secured data with AES	Large-size data takes more delivery time
	[34]	Used Dynamic Data Encryption Strategy (D2ES) for selective data encryption	Lesser time taken for encryption to meet the performance	The risk is bit higher as selective encryption is performed
	[35]	Proposed DNA based security algorithm with 1024 bit key	Resists various security attacks using long-sized key	System overhead increases
	[36]	Proposed a novel attribute-based encryption using limited resource	Lesser computation overhead with better security	Need to design hidden access policies for secure communication
End-to-End Encryption	[37]	Proposed SmartEdge model for secure multi-media communication in Smart cities	Reduces delay and bandwidth consumption	Edge devices need to be registered before starting communication
	[38]	Applied randomness attack model with secure public key	Deals with various randomness-based attacks	Require hardcore functions for encryption
	[39]	Used practical forwarding secrecy for cloud emails	Fine-grain revocation of decryption	Constant size of cipher text
Access Control	[40]	Time-outsourced attribute-based encryption	Reduced cost of access policy and limits the access time	Pairing operation is assigned to the cloud
	[41]	Fine-grained access control over cloud-based multi-server	Works well in heterogeneous environment	Synchronization is required among multiple server
	[42]	Proposed a blockchain based access control framework i.e., AuthPrivacyChain	Protects sensitive data as well as	Bottleneck over centralized access controller
	[43]	Attribute based encryption with threshold-based key sharing and multiple authority access control	Protect from collision attack	Data owner has to divide its users in groups and allot them a secret key
Cloud Access Security Broker (CASB)	[44]	Fuzzy-based CASB for negotiation as well as prioritization	Allows heterogeneity	Requires third-party for CASB
	[45]	Integrate dynamic CASB framework with artificial intelligence	Intelligently securing data adopting dynamic changes	-
	[46]	Identify, evaluate and interpret identity-based CASB	Secure cloud resources to data integrity and accessibility	Limited key capability
Insider Threat	[47]	Anomaly detection framework for intrusion detection	Identifies insider threat by giving warning signals	Works on some patterns only
	[48]	Uses concepts of psychology to analyze the anomalies	Real time system	Requires insiders/employees' technological behaviors

Table 4. Literature review to security measures from various security threats and attacks in cloud computing

VI. Conclusion

Data security remains a major concern, as threats are often discovered too late to be prevented. Despite all of the benefits of cloud computing, its disruptive design, dynamic architecture, and resource utilization pose a specific and severe risk to users and CSPs. The majority of these attacks are the product of the cloud provider's shared data computation and multiple access problems. All stakeholders and actors must consider the risk and take effective measures to mitigate it. To effectively mitigate the risk, security must be built at every level of a cloud computing platform, incorporating best practices and new emerging technologies. Consumers, suppliers, brokers, carriers, auditors, and everyone else in the cloud must take reasonable risk mitigation steps to ensure that the cloud computing infrastructure is truly safe. Otherwise, they will face significant and even business-critical risks. As a result, the user should have a wide range of security options to choose from, allowing them to determine which security measures are best for their data. According to a new study, the best security standards, approaches, and strategies for improving cloud computing security can be found here. It is important to continue this research to apply best practices to a wider range of applications and use cases.

Furthermore, research on the system development life cycle (SDLC) for cloud users should be undertaken to incorporate various models of development and technical advancement and container systems such as dockers to enhance protection on a fundamental level. Other studies have looked into the impact of humans on defense, but their impact on security research is minimal compared to technical factors. The complexities, criteria, and implications of successful security training for both customers and other providers will be the subject of our future work.

Acknowledgment

This research has been financially supported by The Analytical Center for the Government of the Russian Federation (Agreement No. 70-2021-00143 dd. 01.11.2021, IGK 000000D730321P5Q0002).

References

[1] Sabi, H. M., Uzoka, F. M. E., & Mlay, S. V. (2018). Staff perception towards cloud computing adoption at universities in a developing country. Education and Information Technologies, 23(5), 1825-1848.

[2] Ali, K. E., Mazen, S. A., & Hassanein, E. E. (2018). A proposed hybrid model for adopting cloud computing in e-government. Future Computing and Informatics Journal, 3(2), 286-295.

[3] Chihande, M. K., & van der Poll, J. A. (2017, March). Post cloud computing implementation benefits and challenges realised for a South African technology company. In 2017 Conference on Information Communication Technology and Society (ICTAS) (pp. 1-6). IEEE.

[4] Singh, J., Singh, P., & Gill, S. S. (2021). Fog computing: A taxonomy, systematic review, current trends and research challenges. Journal of Parallel and Distributed Computing.

[5] Liu, L., & Han, M. (2019). Privacy and security issues in the 5g-enabled internet of things. In 5G-Enabled Internet of Things (pp. 241-268). CRC Press.

[6] Oppitz, M., & Tomsu, P. (2018). Future technologies of the cloud century. In Inventing the Cloud Century (pp. 511-545). Springer, Cham.

[7] Ashok, A. (2019). Four trends in cloud computing CIOs should prepare for in 2019. Forbes, Jersey City, NJ, USA, Tech. Rep.

[8] Fielding, M. D., Schäfer, S. A., Hogan, R. J., & Forbes, R. M. (2020). Parametrizing cloud geometry and its application in a subgrid cloud‐edge erosion scheme. Quarterly Journal of the Royal Meteorological Society, 146(729), 1651-1667.

[9] Ghahramani, M. H., Zhou, M., & Hon, C. T. (2017). Toward cloud computing QoS architecture: Analysis of cloud systems and cloud services. IEEE/CAA Journal of Automatica Sinica, 4(1), 6-18.

[10] Shirvani, M. H., Rahmani, A. M., & Sahafi, A. (2020). A survey study on virtual machine migration and server consolidation techniques in DVFS-enabled cloud datacenter: taxonomy and challenges. Journal of King Saud University-Computer and Information Sciences, 32(3), 267-286.

[11] Stewart, H. (2021). The hindrance of cloud computing acceptance within the financial sectors in Germany. Information & Computer Security.

[12] Ouedraogo, M., Mignon, S., Cholez, H., Furnell, S., & Dubois, E. (2015). Security transparency: the next frontier for security research in the cloud. Journal of Cloud Computing, 4(1), 1-14.

[13] Altowaijri, S. M. (2020). An architecture to improve the security of cloud computing in the healthcare sector. In Smart Infrastructure and Applications (pp. 249-266). Springer, Cham.

[14] Bohn, R. B., Lee, C. A., & Michel, M. (2020). The NIST cloud federation reference architecture.

[15] Borangiu, T., Trentesaux, D., Thomas, A., Leitão, P., & Barata, J. (2019). Digital transformation of manufacturing through cloud services and resource virtualization.

[16] Mansouri, N., & Javidi, M. M. (2020). Cost-based job scheduling strategy in cloud computing environments. Distributed and Parallel Databases, 38(2), 365-400.

[17] Saadon, G., Haddad, Y., & Simoni, N. (2019). A survey of application orchestration and OSS in next-generation network management. Computer Standards & Interfaces, 62, 17-31.

[18] Al-Sayed, M. M., Hassan, H. A., & Omara, F. A. (2020). CloudFNF: An ontology structure for functional and non-functional features of cloud services. Journal of Parallel and Distributed Computing, 141, 143-173.

[19] Rafique, W., Qi, L., Yaqoob, I., Imran, M., Rasool, R. U., & Dou, W. (2020). Complementing IoT services through software defined networking and edge computing: A

comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 1761-1804.

[20] Hill II, T. P. (2020). Cybersecurity Workforce Issues: A Skills Gap or a Leadership Gap? (Doctoral dissertation, California Southern University).

[21] Hakak, S., Noor, N. F. M., Ayub, M. N., Affal, H., Hussin, N., & Imran, M. (2019). Cloud-assisted gamification for education and learning–Recent advances and challenges. Computers & Electrical Engineering, 74, 22-34.

[22] Khan, A., Hintsch, J., Saake, G., & Turowski, K. (2017, January). Variability management in infrastructure as a service: Scenarios in cloud deployment models. In 2017 International Conference on Computing, Networking and Communications (ICNC) (pp. 724-728). IEEE.

[23] Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in cloud computing. Procedia Computer Science, 125, 691-697.

[24] Tavbulatova, Z. K., Zhigalov, K., Kuznetsova, S. Y., & Patrusova, A. M. (2020, July). Types of cloud deployment. In Journal of Physics: Conference Series (Vol. 1582, No. 1, p. 012085). IOP Publishing.

[25] Bhardwaj, T., Kumar, M., & Sharma, S. C. (2018). Megh: a private cloud provisioning various IaaS and SaaS. In Soft Computing: Theories and Applications (pp. 485-494). Springer, Singapore.

[26] Aryotejo, G., & Kristiyanto, D. Y. (2018, May). Hybrid cloud: bridging of private and public cloud computing. In Journal of Physics: Conference Series (Vol. 1025, No. 1, p. 012091). IOP Publishing.

[27] Helmi, A. M., Farhan, M. S., & Nasr, M. M. (2018). A framework for integrating geospatial information systems and hybrid cloud computing. Computers & Electrical Engineering, 67, 145-158.

[28] Bokhari, M. U., Makki, Q., & Tamandani, Y. K. (2018). A survey on cloud computing. In Big Data Analytics (pp. 149-164). Springer, Singapore.

[29] Simmon, E. (2018). Evaluation of cloud computing services based on NIST SP 800-145. NIST Special Publication, 500, 322.

[30] Amato, F., Moscato, F., Moscato, V., & Colace, F. (2018). Improving security in cloud by formal modeling of IaaS resources. Future Generation Computer Systems, 87, 754-764.

[31] Floerecke, S., & Lehner, F. (2018). Success-driving business model characteristics of IaaS and PaaS providers. International Journal on Cloud Computing: Services and Architecture (IJCCSA), 8(6), 1-22.

[32] Palos-Sanchez, P. R., Arenas-Marquez, F. J., & Aguayo-Camacho, M. (2017). Cloud computing (SaaS) adoption as a strategic technology: Results of an empirical study. Mobile Information Systems, 2017.

[33] Lee, B.H., Dewi, E.K., Wajdi, M.F.: Data security in cloud computing using AES under HEROKU cloud. In: 2018 27th Wireless and Optical Communication Conference (WOCC), pp. 1–5. IEEE, April (2018)

[34] Gai, K., Qiu, M., & Zhao, H. (2017). Privacy-preserving data encryption strategy for big data in mobile cloud computing. IEEE Transactions on Big Data.

[35] Namasudra, S., Devi, D., Kadry, S., Sundarasekar, R., & Shanthini, A. (2020). Towards DNA based data security in the cloud computing environment. Computer Communications, 151, 539-547.

[36] Zhang, L., Cui, Y., & Mu, Y. (2019). Improving security and privacy attribute based data sharing in cloud computing. IEEE Systems Journal, 14(1), 387-397.

[37] Jan, M. A., Zhang, W., Usman, M., Tan, Z., Khan, F., & Luo, E. (2019). SmartEdge: An end-to-end encryption framework for an edge-enabled smart city application. Journal of Network and Computer Applications, 137, 1-10.

[38] Liu, P. (2020). Public-key encryption secure against related randomness attacks for improved end-to-end security of cloud/edge computing. IEEE Access, 8, 16750-16759.

[39] Wei, J., Chen, X., Wang, J., Hu, X., & Ma, J. (2021). Enabling (End-to-End) Encrypted Cloud Emails With Practical Forward Secrecy. IEEE Transactions on Dependable and Secure Computing.

[40] Ning, J., Cao, Z., Dong, X., Liang, K., Ma, H., & Wei, L. (2017). Auditable $\sigma $-time outsourced attribute-based encryption for access control in cloud computing. IEEE Transactions on Information Forensics and Security, 13(1), 94-105.

[41] Roy, S., Das, A. K., Chatterjee, S., Kumar, N., Chattopadhyay, S., & Rodrigues, J. J. (2018). Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications. IEEE Transactions on Industrial Informatics, 15(1), 457-468.

[42] Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K. (2020). AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud. IEEE Access, 8, 70604-70615.

[43] Suresha, K., Vijayakarthick, P., Dhanasekaran, S., & Murugan, B. S. (2021). Threshold secret sharing and multi-authority based data access control in cloud computing. Materials Today: Proceedings.

[44] Ahmad, S., Mehfuz, S., & Beg, J. (2019, November). Fuzzy Cloud Access Security Broker for Requirements Negotiation and Prioritization. In 2019 International Conference on Power Electronics, Control and Automation (ICPECA) (pp. 1-6). IEEE.

[45] Bhattacharya, D., Biswas, A., Rajkumar, S., & Selvanambi, R. (2021). Dynamic Cloud Access Security Broker Using Artificial Intelligence. In Machine Learning for Predictive Analysis (pp. 335-342). Springer, Singapore.

[46] Ahmad, S., Mehfuz, S., & Beg, J. (2021). Enhancing Security of Cloud Platform with Cloud Access Security Broker. In Information and Communication Technology for Competitive Strategies (ICTCS 2020) (pp. 325-335). Springer, Singapore.

[47] Schultz, E. E. (2002). A framework for understanding and predicting insider attacks. Computers & security, 21(6), 526-531.

[48] Ahmad, M. B., Asif, M., Saad, A., & Wahab, A. (2019, May). Cloud Computing: A Paradigm of More Insider Threats. In 2019 4th International Conference on Information Systems Engineering (ICISE) (pp. 103-108). IEEE.