西 南 交 通 大 学 学 报

第 55 卷 第 1 期
2020年 2 月

JOURNAL OF SOUTHWEST JIAOTONG UNIVERSITY

Vol. 55 No. 1
Feb. 2020

ISSN: 0258-2724 **DOI：10.35741/issn.0258-2724.55.1.11**

Research article

Computer and Information Science

INTEGRITY AND SECURITY IN CLOUD COMPUTING ENVIRONMENT: A REVIEW

云计算环境中的完整性和安全性：回顾

Safa S. Abdul-Jabbar [a, *], Ali Aldujaili [b], Saja G. Mohammed [c], Hiba S.Saeed [d]
[a] Department of Computer Science, College of Science for Women, University of Baghdad
Al-Jadriya, Karrada, Baghdad, Iraq, safa.s@csw.uobaghdad.edu.iq
[b] Department Affairs of Student Accommodation, University of Baghdad
Al-Jadriya, Karrada, Baghdad, Iraq, ali@uobaghdad.edu.iq
[c] Department of Mathematics, College of Science, University of Baghdad
Al-Jadriya, Karrada, Baghdad, Iraq, saj85_gh@yahoo.com
[d] College of Science for Women, University of Baghdad
Al-Jadriya, Karrada, Baghdad, Iraq, hiba.toshi1987@gmail.com

Abstract

Cloud computing is a newly developed concept that aims to provide computing resources in the most effective and economical manner. The fundamental idea of cloud computing is to share computing resources among a user group. Cloud computing security is a collection of control-based techniques and strategies that intends to comply with regulatory compliance rules and protect cloud computing-related information, data apps, and infrastructure. On the other hand, data integrity is a guarantee that the digital data are not corrupted, and that only those authorized people can access or modify them (i.e., maintain data consistency, accuracy, and confidence). This review presents an overview of cloud computing concepts, its importance in many applications, and tools that can be used for providing the integrity and security to the data located in the cloud environment.

Keywords: Data Security, Data Integrity, Cloud Computing, Cloud Security, Cloud Integrity

摘要 云计算是一个新近发展的概念，旨在以最有效，最经济的方式提供计算资源。云计算的基本思想是在用户组之间共享计算资源。云计算安全性是基于控制的技术和策略的集合，旨在遵守法规遵从性规则并保护与云计算有关的信息，数据应用程序和基础架构。另一方面，数据完整性保证了数字数据不会被破坏，并且只有那些授权人员才能访问或修改它们（即，保持数据的一致性，准确性和可信度）。本文对云计算概念，其在许多应用程序中的重要性以及可用于为位于云环境中的数据提供完整性和安全性的工具进行了概述。

关键词: 数据安全性，数据完整性，云计算，云安全性，云完整性

I. INTRODUCTION

Cloud computing offers a flexible and cost-effective solution for many Internet services [1]. By using cloud service, users transfer the burden of software installation, data maintenance, infrastructure, storage space, etc. to the cloud service provider; these facilities give their users the opportunity to store, collect, and share information in a transparent manner with other users [2]. Small and medium-sized organizations are moving to cloud computing, as it supports quick access to their application and reduces infrastructure costs. Therefore, cloud computing is considered as a technical solution and business model that can sell and rent computing energy [3]. Cloud computing is seen as one of today's most successful computing techniques, capable of addressing inherently a number of challenges. A number of key cloud computing features were recognized, such as reliability, broad network access, scalability of infrastructure, flexibility, location independence, economies of scale and cost-effectiveness, and sustainability [4], [5]. In addition, this cloud computing system contains many characteristics, such as [5], [6]:

1. Multiple operating systems run on multiple virtual machines and different underlying hardware.
2. It can share all resources simultaneously to all users at the same time.
3. The cloud system completely depends on virtualization.
4. For networks, clouds are distributed over local area networks (LANs), wide area networks (WANs), and metropolitan area network (MANs).
5. Clouds allow multiple applications or services to run at the same time.
6. Each user or application is provided with a secure virtual machine because the cloud system suffers from many challenges regarding sharing and other characteristics mentioned previously.

The cloud computing business model implies two major key factors [7]:

- The cloud service provider (CSP): deliver applications via the Internet, which are accessed from web browsers and desktops, as well as mobile apps.
- Cloud service user (CSU): such as a consumer or an enterprise that accesses and uses the cloud services, while business software and information are stored remotely on servers.

Three types of clouds can be identified depending on the level of provided service: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), as shown in Figure 1. Cloud computing faces various challenges, such as data security, lack of resources and knowledge, etc. [7]. Security was listed as the biggest challenge from all these challenges. The cloud providers need to make sure that they have appropriate security aspects because if things go wrong, they are the ones who will take the responsibility [8], [9]. Data security is also described as the protection and processing of private data from illegitimate entry, alteration, or interruption [10]. While cloud storage requires security that differs from different users and apps, users share the same three goals as availability, integrity, and confidentiality. To achieve these goals, different types of instruments have been developed, such as audition, access control, authentication, encryption, and digital signature [7].

This paper was organized as follows: Section 2 describes a number of previous works. Section 3 deals with a general description of the cloud computing deployment model, as well as types of services and applications. Section 4 is a description of cloud computing attacks. The security requirements and limitations are presented in Section 5. Furthermore, in section 6, the conclusions are summarized.

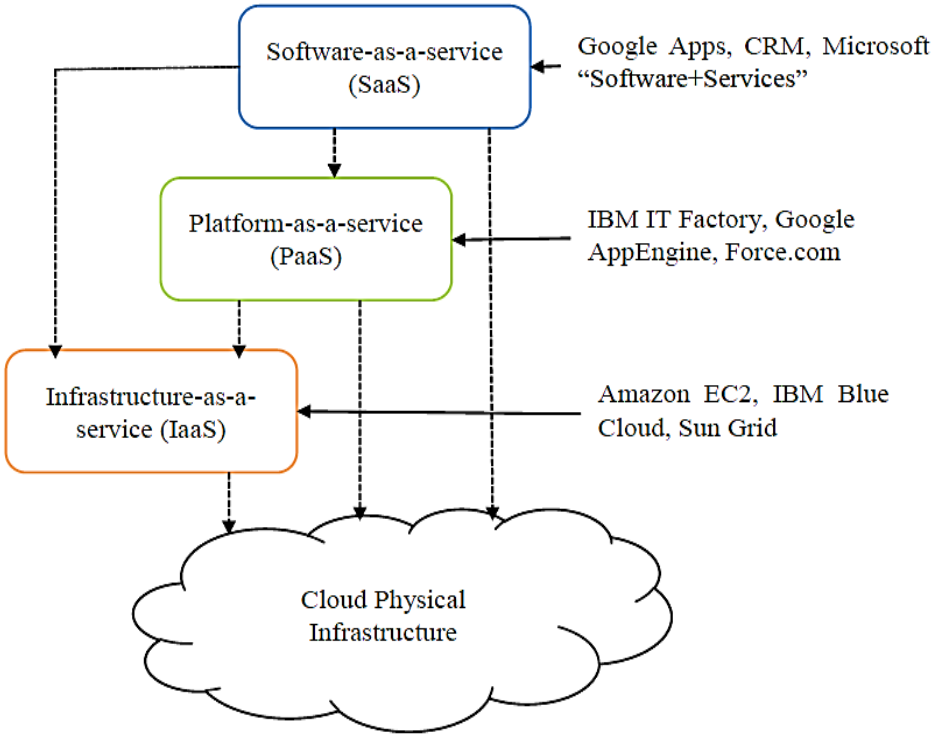

Figure 1. Cloud system model [8]

II. TYPES OF CLOUDS

There are essentially four kinds of clouds, as follows [6]:

A. Public Cloud

This is one of the clouds where cloud services are accessible over the Internet to customers through a service provider. It offers them with a control mechanism. The services might be available free of charge or on a pay-per-use model.

B. Private Cloud

This offers many of the public's advantages, but the primary distinction between the two is that information is correctly managed within the organization alone without the network bandwidth limits.

C. Community Cloud

This kind of cloud is essentially managed by a group of origin servers with a common goal to accomplish. Members share cloud access to data.

D. Hybrid Cloud

This is a mixture of both public and private clouds. It can also be described as multiple cloud systems connected in a way that makes it easy to move programs and data from one system to another.

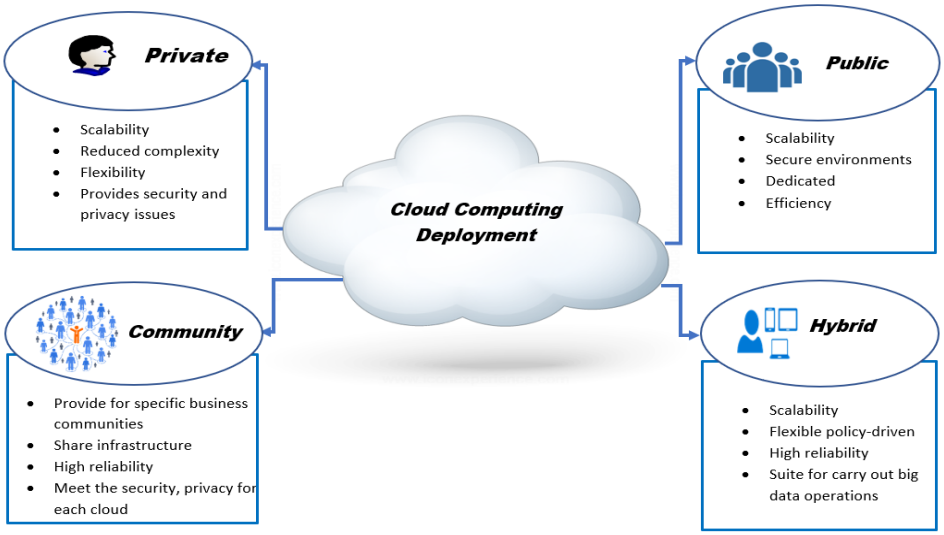

Figure 2. Cloud computing deployment models

Figure 2 describes the four different types of cloud computing deployment models with the most advantages of each type. On the other hand, the most common and widely adopted types of cloud computing services are:

1) Infrastructure-as-a-Service

IaaS is a computer deployment infrastructure model that allows users, who have control over the IT system virtually, to use lease power for processing, networks, and other computer resources from cloud providers [6].

2) Platform-as-a-Service

PaaS is a way to use lease hardware, operating systems, storage, and network capability. The service delivery model enables the client to use lease virtualized servers and related services to run current apps or to develop and test new apps [30].

3) Software-as-a-Service

SaaS ensures clear physical and application-level to separate data from distinct users. This access control architecture can be used in cloud computing for access management. It is better to use qualification or assigned based strategies to detect unauthorized customers [30].

All these three types were illustrated previously in Figure 1. There are many applications for cloud computing (e.g. healthcare, smart home and smart metering, smart energy, smart logistics, smart cities and communities, environmental monitoring, and web applications). Moreover, several web-based services use SaaS, IaaS, and PaaS besides the pervious mentioned application examples (e.g., Gmail, Yahoo, and Skype use SaaS; Google Maps and Microsoft's Azure use PaaS; IBM, Amazon … etc.) [31].

III. Literature Review

Cloud computing security and integrity is the most widely discussed area in both industry and academic researchers. Therefore, in this section, a number of related works will be addressed and discussed as follows:

- Security Concern (Table 1)

Table 1.
Related works in security concern

Year	Author names	The proposed method name	Advantage(s)	Disadvantage(s)	The used technique(s)
2009	Yan et al. [11]	-	- Simplifies the distribution of public keys and reduces the size of SOAP[a] headers. - HIBC[b] approach could limit the key issue of identity-based cryptography.	-	HIBC, SOAP messages, and PKG
2012	Marium et al. [12]	EAP-CHAP[c]	- Using EAP-CHAP and RSA[d] ensure the security of client data in the cloud.	-	RSA algorithm
2013	Hojabri and Venkat Rao [13]	-	- Improves the security of cloud computing through the provision of an authentication service.	Data management and software in the cloud may not be fully confident.	Third party auditor, DES[e], and Kerberos
2013	Arasu et al. [14]	-	- Saves time and computing resources with the user's reduced online burden. - HMAC[g] may provide data stored in the cloud during the audit process, together with homomorphic tokens with data erasure-coded. - One of the key issues is to detect changes and misconduct during TPA[f]'s audit process.	-	TPA and HMAC
2013	Rewagad and Pawar [15]	-	- These three-way mechanisms make it difficult for hackers to crack the security system and thus protect data stored in the cloud. - If the key were hacked through transition, the data confidentiality would be maintained by using AES[h].	-	AES algorithm, Diffie Hellman key, and digital signature
2014	Shereek et al. [16]		- This new method helps users to build trust in the cloud computing environment.	-	RSA algorithm and Fermat's

		-	- It also decreases the disadvantage of RSA encryption; this means that making RSA encryption can be faster than previous.		theorem
2014	Lenka and Nayak [17]	-	- Security for the entire cloud computing environment, where it is provided. - Each algorithm is performed on various servers to overcome the system's slowdown problem. - The used algorithms are executed in altered servers at altered locations; this will affect the intruder performance because he cannot easily access or upload any file.	-	RSA algorithm and digital signature technique (MD5 algorithm)
2015	Shimbre and Deshpande [18]	-	- This system is highly effective against malicious attacks on data modification and collusion on servers.	-	SHA-1[i] and AES algorithms and TPA
2016	More and Chaudhari [19]	-	- It ensures privacy and public auditing for the cloud through the use of a TPA, which performs the audit without retrieving the copy of the data.	The proposed scheme cannot perform all data operations, such as updating data, deletion, and insertion.	AES, TPA, RSA algorithm, and SHA-2
2016	Kaaniche et al. [2]	-	- This system provides confidentiality for encrypted data stored on public servers. - This system provides users with controlled access and sharing of data. - By using IBC-PKG, they can issue their own public elements and keep their resulting IBC[j] confidential. Also, they use a data key that is derived from the data identifier to encrypt.	-	IBC
2016	Singh et al. [20]	-	- Improves security and authentication through the use of RSA algorithms, and only the authorized user can access the data. - If an unauthorized user can access the data and decrypt them, he cannot get back the original data from it.	-	RSA algorithm
2017	Jothy et al. [21]	-	- Provides more confidential data protection. - Provides greater security for residual data (cloud server) and moving data (network channel). - The designed system will not allow anyone that has only a public key to encrypt and decrypt data, which is transmitted across the network.	-	AES, PGP[k] algorithms, and SSL[l]
2017	Raza et al. [22]	VKC[m]	- A collaborative solution. - Avoid time attacks in the cache in the cloud environment.	-	AES and VKC
2018	Akhil et al. [23]	-	- Increases data security during storage and transfer. - By using the TPA technique, the auditor is denied access to the user data. - Since the AES encryption technique is used to transfer data, it excludes the possibility of the system being unavailable at times when huge data arrives.	-	AES Algorithm, and TPA

2018	Jothy et al. [24]	-	- The combination of the used techniques (AES and PGP over SSL) provides security to the confidential data. - The designed system will not allow anyone that has only a public key to encrypt and decrypt data, which is transmitted across the network.	Taking long time duration (time consumption) and a lot of key number generators.	Triple AES and PGP over SSL algorithms
2018	Pius et al. [25]	-	- Provides data (confidentiality, authentication, and verification). - Protects the information from unauthorized users. - Cloud users can manage the privacy and integrity of their cloud-based data securely without relying on the cloud provider's credibility.	Applied on text only.	AES, blow fish algorithm, SMS[n], OOADM[o], and C# programming

[a] SOAP: Simple object access protocol
[b] HIBC: Hierarchical identity-based cryptography
[c] EAP-CHAP: Extensible authentication protocol and Challenge handshake authentication protocol
[d] RSA: Rivest–Shamir–Adleman
[e] DES: Data Encryption Standard
[f] TPA: Third-party auditor
[g] HMAC: Hash message authentication code
[h] AES: Advanced encryption standard
[i] SHA-1: Secure hash algorithm-1
[j] IBC: ID-based cryptography
[k] PGP: Pretty good privacy
[l] SSL: Secure socket layer
[m] VKC: Variable key block cipher
[n] SMS: Short message service
[o] OOADM: Object-oriented analysis and Design method

- Integrity Concern (Table 2)

Table 2.
Related works in integrity concern

Year	Author names	The proposed method name	Advantage(s)	Disadvantage(s)	The used technique(s)
2016	More and Chaudhari [19]	-	- Secure, efficient to use and possesses cloud storage capabilities. - Achieves privacy-preserving and public auditing for the cloud by using TPA, which does the auditing without retrieving the data copy, hence privacy is preserved. - The data is separated into some parts and then stored in the cloud storage in an encrypted format, which keeps the data confidential.	It verifies the data by using data signatures comparison only, which does not deal with dynamic data operations, such as deletion, insertion, ...etc.	Data owner, TPA, cloud server, AES, SHA-2[a], and RSA algorithms
2019	Li et al. [26]		- Public auditability. - The proposed model has a low client cost. - Storage correctness. - Batch auditing. - Lightweight this allows the user to carry out the initialization with the minimum computation overhead to access devices. - Also, the proposed method was designed to support data dynamics and public verifiability.	-	TPA and CSP[b]
2019	Saxena and Dey [27]	-	- A multipower variant of the Paillier cryptography system with a homomorphic tag is the main building component of the proposed approach. - It helps in cloud-based dynamic data operations with less overhead. - The proposed system has better security in the case of the MITM[c] attack.	-	PHC[d] and Hadoop MapReduce framework
2019	Pitchai et al. [28]	AIVP[e]	- Avoids the privacy issues by separating the public and private data. - Reduces the latency (avoids the communication and computation cost). - Increases both the outperforms efficiency and system throughput.	-	CSPs[f]
2019	Mahmood et al. [29]	-	- The proposed system is shown to be secure and highly reliable through extensive analysis of security and efficiency. - The proposed method reduces the assumption of information that is concealed in the image.	-	AES, hybrid steganography scheme SVD-DWT[g], and SHA-2

[a] SHA-2: Secure hash algorithm-2
[b] CSP: Cloud service provider
[c] MITM: Man-in-the-Middle
[d] PHC: Paillier homomorphic cryptography
[e] AIVP: Availability and integrity verification protocol
[f] CSPs: Cloud service providers
[g] SVD-DWT: DWT (Discrete Wavelet Transform) and SVD (Singular Value Decomposition)

IV. Attacks on Cloud Computing Environment

Cloud computing becomes more sophisticated and exposed to many attacks. Several types of attacks, which threaten system security and integrity, are illustrated as follows:

A. Cloud Malware Injection Attack

An attacker attempts to inject malicious service or virtual machines into the cloud. In this attack, the attacker creates its own malicious service implementation module (SaaS or PaaS) or virtual machine instance (IaaS) and attempts to add it to the cloud system [32].

B. Man-In-The-Middle Cryptographic Attack

This type of attack is related to an attack that involves an attacker in the center and accesses the information that is passed between two sides.

This attack is feasible because a Secure Socket Layer (SSL) lacks safety configuration. To illustrate this situation if we have two parties (sender and receiver) that they interact in the cloud, and if there was an intruder currently resides in the center. the intruder can access to the transmitted information if the communication channel is not safe [7].

C. Authentication Attack

Authentication is a major weakness that is often targeted by an attacker in cloud computing services. Most services still use a simple username and password type of knowledge-based authentication today, but some exception is financial institutions that use different forms of secondary authentication (such as site keys, shared secret questions, etc.), which make it harder for popular phishing attacks [32].

D. Attack on Virtualization

Two distinct kinds of attacks are conducted the virtualization attack in the cloud; one is virtual machine (VM) escape, and the other is hypervisor rootkit. In a virtualization attack, VM control will be captured in the virtual environment. The other attack involves a backdoor attack, alteration of VMs, distribution of storage, and multi-tenancy [7].

E. Side-Channel Attack

A side-channel attack (SCA) is a reverse engineering type of attack. Inherently, electronic circuits and software programs are leaky; they generate emissions or a means of interaction as by-products, which allow an intruder to deduce how the circuit operates and what data it processes without access to the circuit itself [33].

F. User to Root Attack

In this type of attack, the attacker intends to obtain administrator access privileges for an unauthorized account [34].

G. Denial of Service Attack

This is a form of attack where the attacker sends the victim a thousand request packets over the Internet. The attacker's primary objective is to exhaust all the victim's resources. An intruder can flood a big amount of demands to waste computational energy, time of execution, and cryptographic activities. This type of attack can affect cloud behavior and cloud services availability [7].

H. Phishing Attack

By phishing attack, the attacker manipulates the web link. As a result, a lawful user is redirected to a false web page, and he believes that the open web page is a secure page for entering credentials (user name and password). After that, the attacker will be able to access his credentials [7].

I. Metadata Spoofing Attack

In this type of attack, the attacker wants to access the Web Services Description Language (WSDL) file and perform the file modification or deletion operation because the features and details of the service are stored in [7].

J. Port Scanning Attack

Port scanning is used to distinguish system parts that are closed, open, and filtered. In port scanning, intruders use open ports, such as services, IP addresses, and MAC addresses, which are parts of a connection to capture information. TCP, UDP, (FIN, SYN, ACK) flag sets, and window scanning are the most common port scanning attack. After scanning the port, the actual attack is performed by attackers [7].

The effects of these attacks on different cloud services are illustrated in Figure 3.

Figure 3. Cloud services effected by each attack

V. Security Requirements and Limitations

A. Confidentiality

This is a concept that protects the information by safeguarding it secure from unauthorized recipients and users. In most instances, the cloud may also contain delicate information that must be kept confidential without any risk disclosure. The only way of keeping the information confidential is by encrypting such information with a secret key that is accessible to the location on its own [35].

B. Integrity

Even if, because of confidentiality, the attacker cannot steal the information, it can still change, add new, or remove some certain fragments before reaching its target. Data in the cloud should be accurate, regular, and reliable. Also, integrity ensures that the transmission of a message through media remains uncorrupted [35].

C. Authentication

This characteristic authenticates the sender with the receiver to guarantee that each obtained data packet comes from the authenticated transmitter, and particularly important packages that add to the decision-making scenario, such as the selection of clusters, and the shortest path (trading of credentials) is necessary to guarantee authentication [36].

D. Freshness

Cloud data must be new and not replaced. The packet must be accompanied by a time stamp choice or time counter to ensure its freshness. It must provide timely and accurate data on critical cases, such as climate or earthquake [35].

E. Availability

It is essential to guarantee that network and Internet service providers are constant and not interrupted. The cloud server information should be available to their customers. A Denial of Service (DoS) assaults, natural disasters, and machinery failures at the end of each service provider because there are major threats that can access to these services, so it will prevent some online service from working properly [3].

F. Time Synchronization

Since power is a critical issue in the cloud, it is essential to synchronize time to save energy. Data synchronization errors will result in data inconsistency. Last but not least, tracking the suitability of data operations is more difficult for CSUs [37].

VI. Discussion

The discussion of the results starts with the various security and integrity studies identified in the literature featuring different case studies of cloud computing. The findings of the current study show twenty-one studies discussed the security and integrity in cloud computing with advantages and drawbacks (if they found) for each study and technique used in each one. The results of this paper are summarized in Table 3 and Figure 4. In this regard, Table 3 illustrates new methods, which were used with the authors' studies, while Figure 4 shows the statistics of turnout for each method based on the researches presented in the literature review section.

In Table 3, there are three novel methods (i.e., extensible authentication protocol and challenge handshake authentication protocol (EAP-CHAP), variable key block cipher (VKC), and availability and integrity verification protocol (AIVP) in different papers; these new methods can be used in order to enhance security and integrity in cloud computing. Figure 4 discusses the number of

repetitions of the techniques used in all presented researches.

Through the potential explanations in this review, six studies discussed the Rivest–Shamir–Adleman (RSA) algorithm. This algorithm is characterized via increases in security capability by increasing the speed of data encryption. Equally important, ten studies discussed the advanced encryption standard (AES) algorithm as a technique. This technique provides security to confidential data.

Another important finding was the third party auditor (TPA). Seven studies used this technique to prevent attackers from accessing data in an easy way. Moreover, three studies focused on secure hash algorithm-2 (SHA-2). This algorithm is used for encryption, which contributes to the complexity of the encryption process and reduces harmful attacks. Besides that, among the possible explanations for these findings, these techniques were used twice, such as pretty good privacy (PGP), digital signature, SSL, and CSP.

Finally, other authors showed the use of different algorithms and methods, such as SHA-1, hierarchical identity-based cryptography (HIBC), simple object access protocol (SOAP) message, PKG, Kerberos, hash message authentication code (HMAC), ID-based cryptography (IBC), and Paillier homomorphic cryptography (PHC). These algorithms and methods are also used to keep data confidential and encrypt it in complex ways. All the mentioned studies were categorized in Figure 4.

Table 3.
New proposed methods among the studies that have been presented

Technique name	Authors
EAP-CHAP	Marium et al. [12]
VKC	Raza et al. [22]
AIVP	Pitchai et al. [28]

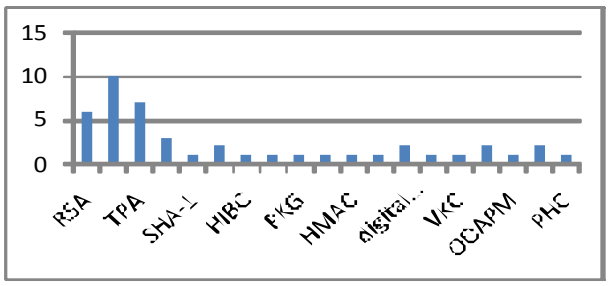

Figure 4. Percentage of turnout for each method

VII. Conclusion

In Cloud Computing Model, computer services (such as servers, databases, storages, networking, analytics, intelligence, and software) over the cloud environment are required to provide rapid development, dynamic resources, and economies of scale. Most of cloud computing services fall into three broad categories: IaaS, PaaS, and serverless and SaaS. These services help to reduce the operating costs and operate your network more effectively and scale up as your business needs change.

Our review paper discussed the security and integrity aspect of the cloud. For example, in sharing of critical data through the cloud environment, data leakage and data theft can be done. In this regard, we found that the biggest and most appalling concern about cloud computing is confidentiality and security (safety). Thus, data security and data integrity are major issues that should be maintained. Moreover, this review paper provides a general view of the problems that can occur with multiple security and integrity issues in a cloud computing system; it also provides some solutions that are suggested by researchers.

The limitation of this research is various studies that show how it has been difficult to study and consider the reliability and security of cloud computing in different ways. Therefore, it took a lot of time and energy to obtain this amount of data, comprehend the topic correctly, and summarize it, as well as take most studies over the last ten years. Furthermore, future work involves adding more references (articles and conferences) to investigate the other security issues in the cloud computing world, as well as developing a security model by using some authentication techniques in order to maintain data integrity and information dissimulation in the cloud environment.

References

[1] NEPAL, S., CHEN, S., YAO, J., and THILAKANATHAN, D. (2011) DIaaS: Data integrity as a service in the cloud. In: *Proceedings of the 2011 IEEE 4th International Conference on Cloud Computing, Washington, District of Columbia, July 2011.* Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, pp. 308-315.

[2] KAANICHE, N., BOUDGUIGA, A., and LAURENT, M. (2013) ID based cryptography for cloud data storage. In: *Proceedings of the 2013 IEEE 6th International Conference on Cloud Computing, Santa Clara, California, June-July 2013.* Piscataway, New Jersey: Institute

of Electrical and Electronics Engineers, pp. 375-382.
[3] MELL, P. and GRANCE, T. (2011) *The NIST Definition of Cloud Computing.* Gaithersburg, Maryland: National Institute of Standards and Technology, U.S. Department of Commerce.
[4] REESE, G. (2009) *Cloud Application Architectures: Building Applications and Infrastructure in the Cloud.* Sebastopol, California: O'Reilly Media.
[5] BUYYA, R., YEO, C.S., VENUGOPAL, S., BROBERG, J., and BRANDIC, I. (2009) Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems,* 25 (6), pp. 599-616.
[6] ABDELBAKI, N., RADWAN, T., and AZER, M.A. (2017) Cloud computing security: challenges and future trends. *International Journal of Computer Applications in Technology,* 55 (2), pp. 158-172.
[7] KUMAR, P.R., RAJ, P.H., and JELCIANA, P. (2018) Exploring data security issues and solutions in cloud computing. *Procedia Computer Science,* 125, pp. 691-697.
[8] CYRIL, B.R. and KUMAR, D.S. (2015) Cloud computing data security issues, challenges, architecture and methods - A survey. *International Research Journal of Engineering and Technology,* 2 (4), pp. 848-857.
[9] VIEGA, J. (2009) Cloud computing and the common man. *Computer,* 1 (8), pp. 106-108.
[10] WANG, C., WANG, Q., REN, K., and LOU, W. (2010) Privacy-preserving public auditing for data storage security in cloud computing. In: *2010 Proceedings IEEE INFOCOM, San Diego, California, March 2010.* Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, pp. 1-9.
[11] YAN, L., RONG, C., and ZHAO, G. (2009) Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In: JAATUN, M.G., ZHAO, G., and RONG, C. (eds.) *Cloud Computing. CloudCom 2009. Lecture Notes in Computer Science,* Vol. 5931. Berlin, Heidelberg: Springer, pp. 167-177.
[12] MARIUM, S., NAZIR, Q., AHMED, A., AHTHASHAM, S., and MIRZA, A.M. (2012) Implementation of EAP with RSA for enhancing the security of cloud computing. *International Journal of Basic and Applied Science,* 1 (3), pp. 177-183.
[13] HOJABRI, M. (2013) Innovation in cloud computing: Implementation of Kerberos version 5 in cloud computing in order to enhance the security issues. In: *Proceedings of the 2013 International Conference on Information Communication and Embedded Systems, Chennai, February 2013.* Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, pp. 452-456.
[14] ARASU, S.E., GOWRI, B., and ANANTHI, S. (2013) Privacy-preserving public auditing in cloud using HMAC algorithm. *International Journal of Recent Technology and Engineering,* 2 (1), pp. 149-152.
[15] REWAGAD, P. and PAWAR, Y. (2013) Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. In: *Proceedings of the 2013 International Conference on Communication Systems and Network Technologies, Gwalior, April 2013.* Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, pp. 437-439.
[16] SHEREEK, B.M., MUDA, Z., and YASIN, S. (2014) Improve Cloud Computing Security Using RSA Encryption with Fermat's Little Theorem. *IOSR Journal of Engineering,* 4 (2), pp. 1-8.
[17] LENKA, S.R., and NAYAK, B. (2014) Enhancing data security in cloud computing using RSA encryption and MD5 algorithm. *International Journal of Computer Science Trends and Technology,* 2 (3), pp. 60-64.
[18] SHIMBRE, N. and DESHPANDE, P. (2015) Enhancing distributed data storage security for cloud computing using TPA and AES algorithm. In: *Proceedings of the 2015 International Conference on Computing Communication Control and Automation,*

Pune, February 2015. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, pp. 35-39.
[19] MORE, S. and CHAUDHARI, S. (2016) Third party public auditing scheme for cloud storage. *Procedia Computer Science*, 79, pp. 69-76.
[20] SINGH, S.K., MANJHI, P.K., and TIWARI, R.K. (2016) Data Security Using RSA Algorithm in Cloud Computing. *International Journal of Advanced Research in Computer and Communication Engineering*, 5 (8), pp. 11-16.
[21] JOTHY, K.A., SIVAKUMAR, K., and DELSEY, M.J. (2017) Efficient Cloud Computing with Secure Data Storage Using AES and PGP Algorithm. *International Journal of Computer Science and Information Technologies*, 8 (9), pp. 582-585.
[22] RIZVI, S.S., ULLAH, M.A., ABBAS, S., and NASEEM, S. (2017) Enhancing Cloud Security Using VKC as a Service. *International Journal of Computer Science and Network Security*, 17 (6), pp. 185-190.
[23] AKHIL, K.M., KUMAR, M.P., and PUSHPA, B.R. (2017) Enhanced cloud data security using AES algorithm. In: *Proceedings of the 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, June 2017*. Piscataway, New Jersey: Institute of Electrical and Electronics Engineers, pp. 1-5.
[24] Prof. V. Sangeetha and D. Jagadeeshwari, "Enhancing the Security of the Cloud Computing With Triple Aes, Pgp Over Ssl Algorithms," *Rev. Res.*, vol. 7, no. 12, pp. 1–9, 2018. http://www.ijesrt.com/issues%20pdf%20file/Archive-2018/February-208/10.pdf
[25] PIUS, U.T., ONYEBUCHI, E.C., CHINASA, O.P., and ADOBA, E.F. (2018) A Cloud-Based Data Security System Using Advanced Encryption (AES) and Blowfish Algorithms. *Journal of Scientific and Engineering Research*, 5 (6), pp. 59-66.
[26] LI, A., TAN, S., and JIA, Y. (2019) A method for achieving provable data integrity in cloud computing. *The Journal of Supercomputing*, 75 (1), pp. 92-108.
[27] SAXENA, R. and DEY, S. (2019) Data integrity verification: a novel approach for cloud computing. *Sādhanā*, 44 (3), 74.
[28] PITCHAI, R., BABU, S., SUPRAJA, P., and ANJANAYYA, S. (2019) Prediction of availability and integrity of cloud data using soft computing technique. *Soft Computing*, 23 (18), pp. 8555-8562.
[29] MAHMOOD, G.S., HUANG, D.J., and JALEEL, B.A. (2019) Achieving an Effective, Confidentiality and Integrity of Data in Cloud Computing. *International Journal of Network Security*, 21 (2), pp. 326-332.
[30] RAO, R.V. and SELVAMANI, K. (2015) Data security challenges and its solutions in cloud computing. *Procedia Computer Science*, 48, pp. 204-209.
[31] BOTTA, A., DE DONATO, W., PERSICO, V., and PESCAPÉ, A. (2016) Integration of Cloud Computing and Internet of Things: A Survey. *Future Generation Computer Systems*, 56, pp. 684-700.
[32] CHOUHAN, P. and SINGH, R. (2016) Security attacks on cloud computing with possible solution. *International Journal of Advanced Research in Computer Science and Software Engineering*, 6 (1), pp. 92-96.
[33] SADIQUE, U.M. and JAMES, D. (2016) A Novel Approach to Prevent Cache-Based Side-Channel Attack in the Cloud. *Procedia Technology*, 25, pp. 232-239.
[34] CARLIN, A., HAMMOUDEH, M., and ALDABBAS, O. (2015) Defence for distributed denial of service attacks in cloud computing. *Procedia Computer Science*, 73, pp. 490-497.
[35] RADY, M., ABDELKADER, T., and ISMAIL, R. (2019) Integrity and confidentiality in cloud outsourced data. *Ain Shams Engineering Journal*, 10 (2), pp. 275-285.
[36] SINGH, A. and CHATTERJEE, K. (2017) Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, 79, pp. 88-115.
[37] LIU, Y., SUN, Y.L., RYOO, J., RIZVI, S., and VASILAKOS, A.V. (2015) A survey of security and privacy challenges in cloud computing: solutions and future directions. *Journal of Computing Science and Engineering*, 9 (3), pp. 119-133.

参考文:

[1] NEPAL，S.，CHEN，S.，YAO，J. 和 THILAKANATHAN，D.（2011）DIaaS：数据完整性作为云中的服务。在：2011年电气工程师学会第4届国际云计算国际会议论文集，华盛顿，哥伦比亚特区，2011年7月。新泽西州皮斯卡塔维：电气与电子工程师协会，第 308-315 页。

[2] N. KAANICHE，A。BOUDGUIGA 和 M. LAURENT（2013）基于鉴定的云数据存储加密技术。在：2013年电气工程师学会第6届国际云计算国际会议论文集，加利福尼亚州圣克拉拉，2013年6月至7月。新泽西州皮斯卡塔维：电气与电子工程师协会，第 375-382 页。

[3] MELL，P. 和 GRANCE，T.（2011）云计算的国家标准技术研究所定义。马里兰州盖瑟斯堡：美国商务部国家标准与技术研究所。

[4] REESE，G.（2009）云应用架构：在云中构建应用和基础架构。加利福尼亚塞巴斯托波尔：奥赖利媒体。

[5] BUYYA，R.，YEO，CS，VENUGOPAL，S.，BROBERG，J。和 BRANDIC，I。（2009）云计算和新兴的它平台：作为第五实用程序交付计算的愿景，炒作和现实。下一代计算机系统，25（6），第 599-616 页。

[6] N. ABDELBAKI，T。RADWAN 和 M.A. AZER（2017）云计算安全性：挑战和未来趋势。国际计算机技术应用杂志，55（2），第 158-172 页。

[7] KUMAR，P.R.，RAJ，P.H. 和 JELCIANA，P.（2018）探索云计算中的数据安全性问题和解决方案。普罗迪亚计算机科学，125，第 691-697 页。

[8] CYRIL，B.R. 和 KUMAR，D.S.（2015）云计算数据安全性问题，挑战，架构和方法-调查。国际工程与技术研究杂志，2（4），第 848-857 页。

[9] VIEGA，J.（2009）云计算与普通人。计算机，1（8），第 106-108 页。

[10] WANG，C.，WANG，Q.，REN，K. 和 LOU，W.（2010）在云计算中为数据存储安全性保留隐私的公共审计。在：2010年会议记录，电气工程师学会INFOCOM，加利福尼亚圣地亚哥，2010年3月。新泽西州皮斯卡塔维：电气与电子工程师协会，第 1-9 页。

[11] YAN L.，RONG，C. 和 ZHAO，G.（2009）使用基于分层身份的加密技术，通过联邦身份管理来增强云计算安全性。于：M.G.的JAATUN，G。的 ZHAO 和 G. RONG，C.（编辑）云计算。云通2009。计算机科学讲义，第1卷。5931。柏林，海德堡：施普林格，第 167-177 页。

[12] MARIUM，S.，NAZIR，Q.，AHMED，A.，AHTHASHAM，S。和 MIRZA，A.M。（2012）通过RSA实施EAP，以增强云计算的安全性。国际基础与应用科学杂志，1（3），第 177-183 页。

[13] HOJABRI，M.（2013）云计算中的创新：在云计算中实施Kerberos版本5，以增强安全性问题。于：2013年国际信息通信与嵌入式系统国际会议论文集，金奈，2013年2月。新泽西州皮斯卡塔维：电气与电子工程师协会，第 452-456 页。

[14] S.E. ARASU，B。GOWRI 和 S. ANANTHI（2013）使用HMAC算法在云中保护隐私的公共审计。国际最新技术与工程杂志，2（1），第 149-152 页。

[15] REWAGAD，P. 和 PAWAR，Y.（2013）将数字签名与迪菲·赫尔曼密钥交换和AES加密算法结合使用，以增强云计算中的数据安全性。在：2013年国际通信系统和网络技术国际会议论文集，瓜廖尔，2013年4月。新泽西州皮

斯卡塔维：电气与电子工程师协会，第437-439 页。

[16] SHEREEK，B.M.，MUDA，Z. 和YASIN，S.（2014）使用具有费马小定理的RSA加密提高云计算安全性。IOSR工程杂志，4（2），第 1-8 页。

[17] LENKA，S.R. 和NAYAK，B.（2014）使用RSA加密和医学博士5算法增强云计算中的数据安全性。国际计算机科学趋势与技术杂志，2（3），第 60-64 页。

[18] SHIMBRE，N. 和DESHPANDE，P.（2015）使用TPA和AES算法增强云计算的分布式数据存储安全性。在：2015年国际计算通信控制与自动化国际会议论文集，浦那，2015年2月。新泽西州皮斯卡塔维：电气与电子工程师协会，第 35-39 页。

[19] MORE，S. 和CHAUDHARI，S.（2016）云存储的第三方公共审计方案。普罗迪亚计算机科学，79，第 69-76 页。

[20] S.K. SINGH，P.K。MANJHI 和 R.K. TIWARI。（2016）在云计算中使用RSA算法的数据安全性。国际计算机和通信工程高级研究杂志，5（8），第 11-16 页。

[21] JOTHY，K.A.，SIVAKUMAR，K. 和DELSEY，M.J.（2017）使用AES和PGP算法通过安全数据存储进行高效云计算。国际计算机科学与信息技术杂志，8（9），第 582-585 页。

[22] S.S. RIZVI，马萨诸塞州阿拉拉，S。ABBAS 和 S. NASEEM（2017）使用VKC作为服务增强云安全性。国际计算机科学与网络安全杂志，17（6），第 185-190 页。

[23] AKHIL，K.M.，KUMAR，M.P. 和PUSHPA，B.R.（2017）使用AES算法增强云数据安全性。于：2017年6月，哥印拜陀，2017年国际智能计算与控制国际会议（一世2C2）会议录。新泽西州皮斯卡塔维，电气与电子工程师协会，第 1-5 页。

[24]

[25] 美国的PIUS，加拿大的ONYEBUCHI，加拿大的CHINASA 和加拿大的ADOBA（2018）一种使用高级加密（AES）和河豚算法的基于云的数据安全系统。科学与工程研究杂志，5（6），第 59-66 页。

[26] LI，A.，TAN，S. 和JIA，Y.（2019）一种在云计算中实现可证明的数据完整性的方法。超级计算杂志，75（1），第 92-108 页。

[27] SAXENA，R。和DEY，S。（2019）数据完整性验证：一种用于云计算的新颖方法。萨达纳，44（3），74。

[28] PITCHAI，R.，BABU，S.，SUPRAJA，P. 和ANJANAYYA，S.（2019）使用软计算技术预测云数据的可用性和完整性。软计算，23（18），第 8555-8562 页。

[29] G.S. MAHMOOD，D.J。HUANG 和B.A. JALEEL。（2019）在云计算中实现数据的有效，机密性和完整性。国际网络安全杂志，21（2），第 326-332 页。

[30] RAO，R.V。和SELVAMANI，K.（2015）云计算中的数据安全挑战及其解决方案。普罗迪亚计算机科学，48，第 204-209 页。

[31] A. BOTTA，W。DE DONATO，V。PERSICO 和A.PESCAPÉ（2016）云计算和物联网的集成：一项调查。下一代计算机系统，56，第 684-700 页。

[32] CHOUHAN，P. 和SINGH，R.（2016）对云计算的安全攻击和可能的解决方案。国际计算机科学与软件工程高级研究杂志，6（1），第 92-96 页。

[33] SADIQUE，美国 和JAMES，D.（2016）一种防止云中基于缓存的侧通道攻击的新颖方法。普罗迪亚技术，25，第 232-239 页。

[34] A. CARLIN，M。HAMMOUDEH 和 O.
ALDABBAS（2015）云计算中的分布式拒绝服务攻击防御。普罗迪亚计算机科学，73，第 490-497 页。
[35] RADY，M.，ABDELKADER，T. 和 ISMAIL，R.（2019）云外包数据的完整性和机密性。艾因·夏姆斯工程杂志，10（2），第 275-285 页。
[36] SINGH，A. 和 CHATTERJEE，K.（2017）云安全问题和挑战：一项调查。网络与计算机应用杂志，79，第 88-115 页。
[37] LIU Y，SUN，Y.L.，RYOO，J.，RIZVI，S. 和
VASILAKOS，A.V.（2015）对云计算中的安全性和隐私挑战的调查：解决方案和未来方向。计算科学与工程学报，9（3），第 119-133 页。