TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 19, No. 4, August 2021, pp. 1152~1161
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v19i4.16875 ❐ 1152

From cloud computing security towards homomorphic encryption: A comprehensive review

Saja J. Mohammed[1], **Dujan B. Taha**[2]
[1]Department of computer science, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq
[2]Department of software, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq

Article Info

Article history:

Received Jun 4, 2020
Revised Dec 25, 2020
Accepted Jan 3, 2021

Keywords:

Cloud computing
Cloud computing security
Cloud computing threats
Cloud data security/privacy
Homomorphic encryption

ABSTRACT

"Cloud computing" is a new technology that revolutionized the world of communications and information technologies. It collects a large number of possibilities, facilities, and developments, and uses the combining of various earlier inventions into something new and compelling. Despite all features of cloud computing, it faces big challenges in preserving data confidentiality and privacy. It has been subjected to numerous attacks and security breaches that have prompted people to hesitate to adopt it. This article provided comprehensive literature on the cloud computing concepts with a primary focus on the cloud computing security field, its top threats, and the protection against each one of them. Data security/privacy in the cloud environment is also discussed and homomorphic encryption (HE) was highlighted as a popular technique used to preserve the privacy of sensitive data in many applications of cloud computing. The article aimed to provide an adequate overview of both researchers and practitioners already working in the field of cloud computing security, and for those new in the field who are not yet fully equipped to understand the detailed and complex technical aspects of cloud computing.

Corresponding Author:

Saja J. Mohammed
Department of Computer Science
University of Mosul
Alkafaat Althaanyaa, Mosul, Ninavah, Iraq
Email: Sj_alkado@uomosul.edu.iq

1. INTRODUCTION

Nowadays the world is facing a new model of computing, on-demand computing, it is a cloud computing, where everything that a computer system can provide is provided as a service in a cloud model when connected to a network [1]-[3]. The National Institute of Standards and Technology (NIST) put a proper description to cloud computing: "Cloud computing is a model for supporting, convenient, on-demand network access to a shared group of configurable computing resources, like servers, networks, storage, services, and applications, that can be quickly provisioned and released with least management work or service provider contact" [4]-[8]. Cloud computing offers many advantages over the traditional computing systems, such as (but not limited): cost and time saving, scalability and flexibility, backup and recovery, resource maximization, mobile access, multi sharing and collaboration, customization and it removes initial capital investments and other pre-operational expenses (pay-as-per-use) [1], [4], [6], [9]-[12].

2. The (5-4-3) CLOUD COMPUTING CONCEPTS

As it explained above, the definition of cloud computing refers to different models and characteristics in it [5]. The 5-4-3 concepts put by NIST describe: (a) the five essential characteristics that boost cloud computing, (b) the four deployment models that are used to narrate the cloud computing opportunities for customers while looking at architectural models, and (c) the three important and basic service offering models of cloud computing [4], [5]. The (5-4-3) concepts are explained as followes:

2.1. The five-essential characteristic

The cloud computing has five essential characteristics, these characteristics are [2], [5], [7], [13]-[17]:

- On-demand self-service: This characteristic enables the user to access cloud capabilities automatically at any time he/she wants if the connection to the network is available.
- Broad network access: The cloud computing abilities are remaining available over the network. Every type of client platform may use them, if it has connected to the network.
- Elastic resource pooling: All required resources (physical and virtual resources) are pooled dynamically according to the customers' demands.
- Rapid elasticity: According to the existing demands, the accessed capability can be quickly provision and released.
- Measured service: Any usage of a cloud resource is measured. This may include monitor, control, and report providing transparency of resources for the consumer and provider together.

2.2. The four models of deployment [6], [7], [13], [17], [18]

- Private cloud: Also called internal cloud [19]. The infrastructure is provisioned for special usage by a distinct organization involving multiple consumers (eg. business units) [5], [20]. This type of cloud may be managed, owned, and operated via the organization or a third party, sometimes via several of their combination [2], [14], [19], [21]-[23]. The private cloud can be classified into two types: on-premise private cloud (also called internal cloud) and externally hosted private cloud. The two types differ in hosted place. The first one is hosted within its own data center where the second is hosted within the cloud provider respectively [19], [22], [23].
- Public cloud: Here, the cloud provides its services to general users [23]. The public cloud provides its infrastructure for open usage [2], [5], [14]. It may be managed, owned, and operated by an academic, government organization, or business or several of their combination [4], [19]-[22].
- Community cloud: A cloud infrastructure that is shared by some organizations and supports a specific community, such as healthcare. The main target of this model of cloud deployment is to share the organization realizes the advantages of public and private clouds together [2], [4], [5], [14], [19]-[21].
- Hybrid cloud: here, the cloud infrastructure is a combination of two or more different cloud infrastructures (i.e. private, public, or community) that keep single entities, but are restricted with each other by standardized technology that allows application and data portability "at the same time the two kinds of clouds is used together to achieve specific job" [2], [4], [5], [14], [20]-[22]. Table 1 illustrates the advantages and disadvantages of the four modes of deployment with existing examples.

2.3. The three important service models

- SaaS model: Software as a service, it defines a cloud service where customers can access any software applications executed on a cloud infrastructure [8], [16], [19]-[21]. SaaS has no primary setup cost, no cost of infrastructure maintenance, all updates are done automatically. On the other side, SaaS has the minimum consumer control on security that because the infrastructure and execution platform placed remote of the user [2], [4], [5], [14], [16].
- PaaS model: Platform as a service, it is a supplying of a computing platform via the network. PaaS is an integration of a cloud-based computing environment that assists the running, management, and development of applications control on the cloud infrastructure like network, servers, and storage. In [8], [14], [16]. Where the customers are allowed to have controls over the deployed applications. PaaS model present high extensibility with greater consumer control on security compared with SaaS but less than IaaS [2], [4], [5], [16], [19]-[21].
- IaaS model: Infrastructure as a service, is the virtual allocation of computing resources (hardware, networking as well as storage services). The infrastructure is controlled completely by the cloud service providers (CSP) [2], [5], [8], [21]. Therefore, IaaS give a greater security control in the client's if compared with SaaS and PaaS models [4], [14], [16], [19], [20].

NIST also defines reference architecture which is intended to simplify the understanding of the operational complexity in cloud computing. Its target is to describe, discuss, and develop a system-specific architecture [5]. The reference architecture defines five main actors in the relation to the responsibilities and roles. These actors are: cloud consumer, cloud provider, cloud auditor, cloud broker, and cloud carrier [5], [24]. Table 2 illustrates the responsibilities of each actor [24].

Table 1. The advantages/disadvantages of cloud deployment models

Cloud model	Advantage	Disadvantage	An example
Private cloud	More customization. Higher security/privacy. Enhanced reliability Greater control over the server. Higher performance.	High costs that devoted in a private cloud infrastructure On site maintain. Capacity ceiling	Eucalyptus Ubuntu Enterprise Cloud Amazon VPC VMware Cloud Infrastructure Suite Microsoft ECI data center
Public cloud	Reduces time to develop new products Cost effectiveness No contract (Pay-as-you-go) Ensures scalability/ reliability No user maintenance effort	Higher security risks Network performance may be suffering instabilities. Slow speed depending on internet quality. Lack of customization. Lack of investment	Google App Engine Microsoft Window Azure IBM smart cloud Amazon EC2
Community cloud	Compromise data security and privacy. Flexibility and Scalability Improved Services Available and Reliable Cheaper than private cloud	Costs higher than public cloud. Share fixed amount of bandwidth/data storage among all members.	PaaS includes Microsoft Azure Platform Google App Engine
Hybrid cloud	Optimal utilization Flexibility Control the resources allocated Cost-effectiveness Data center consolidation	More maintenance High initial costs Challenging on data and application integration	Microsoft Hybrid Cloud (Azure) VMware Hybrid Cloud Amazon Web Services (AWS) Cloud Rackspace Hybrid Cloud EMC Hybrid Cloud, HP Hybrid Cloud

Table 2. The cloud computing actors with their responsibilities

The actor	Definition	Responsible to secure:
Cloud Consumer	Who (person/organization) preserves the business relations with Cloud Providers, and utilizes service from him.	– Cloud Consumption Management. – Cloud Ecosystem Orchestration. – Functional Layers.
Cloud Provider	A (person/organization/entity) ensures an available service for interested parties.	– Cloud Service Management. – Cloud Ecosystem Orchestration.
Cloud Auditor	A party who can conduct a separate estimation of cloud services, performance, information system operations, and security of implementation in the cloud.	– The Auditing Environment.
Cloud Broker	A party who control the usage, performance and delivery of services in the cloud, and negotiates relationships between cloud consumers and cloud providers.	– Cloud Service Management. – Cloud Ecosystem Orchestration. – Service Intermediation. – Service Arbitrage.
Cloud Carrier	An intermediate party that supplies connectivity and transmission of cloud services (from CPS to Cloud Consumers).	– The data transmission to/ from a cloud environment.

3. SECURITY IN CLOUD COMPUTING

Security is a major requirement of many researchers, anyone how interested in can find a lot of papers that focus on this field, for example see [25]-[31]. At the same time, security and privacy concerns are the main issues that prevent wide acceptance of cloud concepts [3], [32] where switching to a commercial public cloud reduces direct control of systems that manage reliable data and applications [7]. Figure 1 illustrates the differences between traditional security and cloud security.

According to a survey by Gartner, 70% of users do not use cloud computing services because of data security and privacy concerns [6]. These users are not ready to dump their infrastructure and move to the cloud, where their data is kept remotely. They know that their sensitive data remains under cloud control only and not by them [6], [7], [12], [21], [33]. For this reason, cloud security and privacy should be a major concern in the cloud scenario. It is worth noting that cloud computing has many essential security issues when using its services, such as outsourcing, system monitoring and access control, massive data, and intense computation and multi-tenancy issues [9], [15].

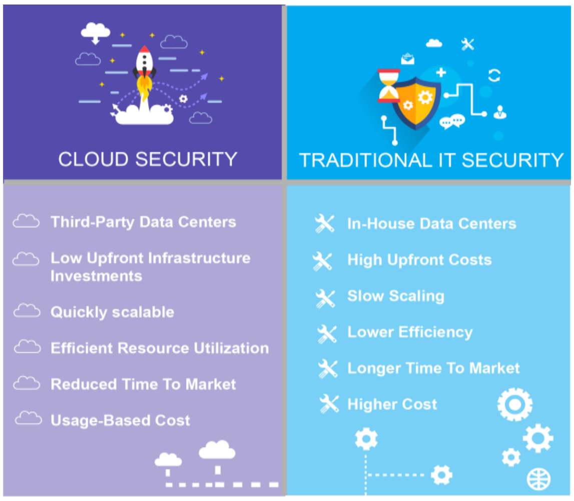

Figure 1. The differences between traditional security and cloud security

4. TOP CLOUD SECURITY THREATS

The Cloud Security Alliance (CSA) defines a list of the topmost organizations of security threats that face when trying to use cloud services. As this list defined, the top security threats summarized the concerns which can be taken into consideration (by cloud security organization) in order to utilize the advantage of cloud computing as more as possible, without falling in the drawbacks that cloud-based systems have [11], [33], [34]. The top cloud security threats explained in Table 3 [2], [6], [7], [34]-[36] where Table 4 explains the analysis of them [34].

Table 3. The top cloud security threats

Threats	Description	Protection
Data breaches	Caused by authentication weakness	Use more than one factor of encryption and authentication
Broken authentication and credentials	Appears when trying to assign suitable permissions for user's job role	Using multi-factor authentication systems
Hacked interfaces and APIs	An attacker utilizes a cloud API to grant access to the resources of cloud	Interfaces must be designed to protect against both accidental and malicious attempts to circumvent policy
Exploited system vulnerabilities	Exploitable bugs in programs are used to penetrate a computer system to damage service operations, steal data or take control of the system	Using the best practices in order to discover potential vulnerabilities and manage the discovered problems rapidly
Account hijacking	Attackers may occupy the control of legitimate users' account	Using multi-factor authentication with evasion of account credentials sharing
Malicious insiders	An insider can manipulate data or damage the whole infrastructures of cloud	Control the encryption operation and keys, separate jobs and reduce access given to users, Active logging and auditing administrator activities
Advanced persistent threat (APT)	Penetrates cloud systems and remain hidden and persistently doing their activities for a long-time interval	Advanced security controls, frequent infrastructure monitoring and rigid process management
Constant data loss	delete data constantly	Different levels of backup and data distribution key management
DoS attacks	Effects the availability of a system consumes processing power and up the bandwidth	Detection is needed, prepare the key of DoS mitigating, access resources which can be used as mitigation immediately.
Shared Technology Vulnerabilities	As a result of resource sharing in the cloud, one vulnerability can produce a compromise across an entire provider's cloud.	Keeping shared resources patched, multi-factor authentication on all hosts, Intrusion Detection System, and segmentation
Cloud service abuses	Malicious actors can use cloud computing resources to target fashion, organizations, or other CSP	A CSP must have a response scope to handle misuse of resources, a means for consumers to report any abuse produced from a CSP.
Inadequate due diligence	Caused by a weak technical efficiency of the development group	Enterprises should review accreditations and standards gained by CSPs including ISO 9001, DCS, PCI, and HIPAA.

Table 4. The cloud threats analysis

Threat	Spoofing Identity	Tampering with data	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege
Data Breaches				√		
Broken authentication and credentials	√	√	√	√	√	√
Hacked interfaces/ APIs		√	√	√		√
Exploited system vulnerabilities	√	√	√	√	√	√
Account hijacking	√	√	√	√	√	√
Malicious insiders	√	√		√		
APT				√		√
Constant data loss			√		√	
DoS attacks					√	
Shared Technology Vulnerabilities				√		√
Cloud Service abuses					√	
Inadequate Due diligence	√	√	√	√	√	√

5. CLOUD DATA SECURITY AND PRIVACY

5.1. Cloud data security

The security of data in the cloud is more complex than traditional systems [4]. However, any cloud must be in a trustworthy environment in order to gain user confidence to adopt this technology [2], [21]. There're lots of security concerns related to cloud computing, these issues collapse into two types [37]:

- Cloud service provider's security issues.
- The customer's security issues.

However, in order to offer reliable services, the cloud providers should confirm the security of their infrastructure, so their clients' applications and data are secured and stay integrated. Simultaneously, the user should apply measures to reinforce their application and use robust passwords/authentication methods [37]. In the environment of cloud computing, data security is a combination of three concepts, called the CIA triangle which consists of: confidentiality, integrity, and availability [3], [14], [38].

5.1.1. Cloud data confidentiality

The main concerns respected with cloud computing is cloud confidentiality. In cloud computing, it can be defined as "the process of keeping the computation jobs and customer's data private to both cloud provider and other customers" [2], [15], [18], [21], [38]. Confidentiality must be assured in the cloud environment, because of the fact that the data of a user are saved remotely and all computations which applied to them are controlled by the cloud provider, [15], [21], [38]. Various approaches proposed to keep data confidentiality in cloud computing environment such as RSA, DES, SDES, SSL 128-bit encryption, mixed encryptions algorithms, RC5, RBE, and AES [39].

5.1.2. Cloud data integrity

Integrity in the cloud environment involves both of integrity of data and integrity of computations [2], [18], [40]. Where data integrity guarantees that user's data are stored inside the cloud providers in a fidelity way without any modification and any violations if occur must be detected [15], [18], [40]. On another side, computation integrity is a concept of executing the programs without being deformed by cloud providers, malware, or any else of malicious users and detect any incorrect computing [21], [38]. One of the most important methods used to achieve cloud data integrity is the hash algorithm [41].

5.1.3. Cloud data availability

The term data availability means the degree to which user's data can be recovered or used (if there is an event of any hard disk damage or failure) and how to confirm user data by technology rather than relying on the credit guarantee via the CPS only [2], [21], [42], [43]. Availability is a very important concern since the essentiality task of cloud computing is providing on-demand service at different levels. If a particular service isn't available or its quality can't meet the service level agreement (SLA), any customers may forfeit trust in the cloud systems [15], [21], [42], [43].

Usually, cloud providers achieve delivering highly available services, but outages and failures are something they have to face at any time. Failures that might happen include, but are not bound, to the following: human mistakes, network vulnerability, server, storage, or power failures. The suggested solutions to recover from some of the outages are high quality and the organized maintenance of the hardware component, data redundancy, failure detection, backup, infrastructure scalability, and redundant architecture [44].

5.2. Cloud data privacy

Privacy is the capability of individuals or groups to isolate themselves or their information from their selves then reveal them in a selective way [6], [21]. In cloud systems, when users want to see sensitive data, privacy has appeared here obviously. The cloud services must have the ability to inhibit possible adversaries from deducing the behavior of the user by the user's visit model [6], [21]. The meaning of privacy in cloud computing is divided into two categories: data privacy and computation privacy [15].

There are many cryptography procedures which are utilized to keep the privacy of the information in order to secure huge information examination in the cloud, such as, homomorphic encryption (HE), verifiable computation (VC), multiparty computation (MPC) [45]. Table 5 explains the main data security aspects in cloud computing, with their possible threats and Defense strategies (for more details see [15]). Where Figure 2 shows the number of noticed research papers written about cloud security and privacy topics in the last five years.

Table 5. The main data security aspects in cloud computing

Security aspect	Threats	Defense strategies
Confidentiality	– Cross VM attack – Malicious sysAdmin	– Placement Prevention – Co-residency Detection – NoHype – Trusted Cloud Computing Platform – retaining data control back to customer
Integrity	– Data loss/manipulation – Dishonest computation in remote servers	– Provable Data Possession (PDP) – Third Party Auditor – Combating dishonest computing
Availability	– Flooding Attack via Bandwidth Starvation – Fraudulent Resource Consumption (FRC) attack	– defending the new DOS attack – FRC attack detection
Privacy	Same of cloud confidentiality threats	– Information centric security – Trusted computing – Cryptographic protocols (Homomorphic Encryption (HE))

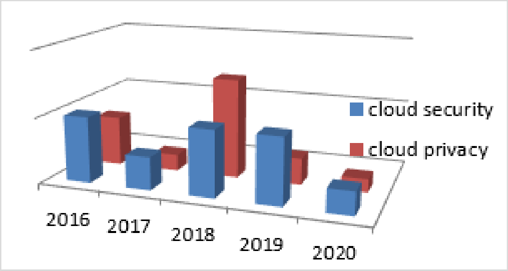

Figure 2. A statistic of the number of published researches in the last five years

6. HOMOMORPHIC ENCRYPTION

Homomorphic encryption (HE) gives a great asset to ensure users' privacy in a cloud computing environment. It is a mathematical model, developed in 1978 from the privacy homomorphism concept [46], [47]. It is one of the most popular schemas which are currently focused by computer science researchers in order to achieve the confidentiality of data [47]. Its importance came due to allowing transfer, store, and process the encrypted data securely because it permits encrypted data to be calculated without being decrypted [46], [48], [49]. It converts plaintext to cipher one which can be used and analyzed as if it were in its original form yet [38].

6.1. Definition

Like any encryption schema, HE includes four functions when applying it, these functions are key generation, encryption, evaluation, and decryption [49], [50]. Mathematically, HE means translation of one data set to an alternative one, without losing its relation between them [17].
Let (P; C; K; E; D) be an encryption method, where [46]:
P& C are the plaintext and ciphertext, respectively
K is the key (secret or public key depending on the type of cryptosystem)
E&D are the encryption and decryption algorithms. Suppose that the plaintexts compose a group (P;$_o$), and the ciphertexts produce a group (C; ◊), consequently, the encryption algorithm E is a map from the group P to

the group C [46], [51]. An encryption schema is Homomorphic encryption if [46]. For all a and b in P and k in K:

$$E_k(a)^\circ E_k(b) = E_k(a \lozenge b) \quad (1)$$

Last years, HE usage in a cloud computing environment is spread widely due to its ability to perform arithmetic operations on encrypted texts without the need for a decryption key so that the results are exactly the same as if they were performed on the explicit text. Now, the provider can apply any computation operation on stored decrypted data of the user without any need for the key. This will gain both of consumer trust and ensure data privacy [8], [46], [52]. Figure 3 illustrates how dealing with encrypted data in cloud computing using homomorphic encryption [8], [49], [53].

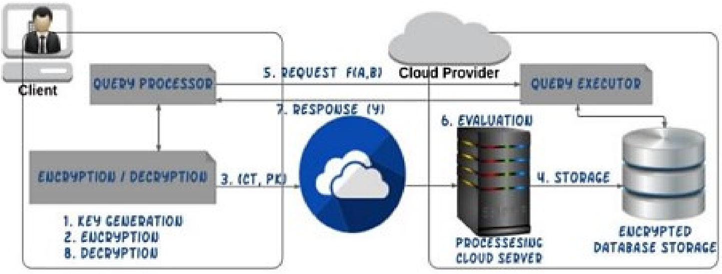

Figure 3. Applying homomorphic encryption to the cloud computing

6.2. Categories

HE has been classified into three types depending on the number of mathematical operations that can be performed. These types are [46], [49], [50], [53], [54]:

- Partial HE: Performs addition or multiplication operation (not both).
- Somewhat HE: Performs a bounded number of addition and multiplication operations.
- Fully HE: Can perform both addition and multiplication operations together.

Table 6 explains the difference between partial and fully homomorphic encryption [54].

Table 6. The difference between partial and fully homomorphic encryption

Parameter	Partial HE	Fully HE
Type of operation	Either addition or multiplication	Both
Computation	Limited number of computations	Unlimited
Computational efforts	Requires less effort	Requires more effort
Performance	Faster and more compact	Slower
Versatility	Low	High
Ciphertext size	Small	Large
Example	Unpadded RSA, ElGamal	Gentry Scheme

6.3. Properties

In general, HE has two properties that appear when applying its schemas. According to these properties, HE can classify into two categories [49], [51], [54], [55]:

- Additive homomorphic encryption: HE is classified as an additive if:

$$\text{Enc}(x\oplus y)= \text{Enc}(x) \otimes \text{Enc}(y) \quad (2)$$

$$Enc(\textstyle\sum_{i=1}^{1} m_i) = \prod_{i=1}^{1} Enc(m_i) \quad (3)$$

- Multiplicative Homomorphic Encryption: A Homomorphic encryption is a multiplicative, if:

$$\text{Enc}(x\otimes y)= \text{Enc}(x) \otimes \text{Enc}(y) \quad (4)$$

$$Enc(\textstyle\prod_{i=1}^{1} m_i) = \prod_{i=1}^{1} Enc(m_i) \quad (5)$$

According to the above definitions, many encryption algorithms classified as HE schema. Table 7 illustrates some of them with their related Homomorphic property [47], [49], [53].

Table 7. Homomorphic encryption schemes

Scheme	year	Properties	Type	Algorithm	Security Assumption
RSA	1978	Multiplicative	Partial	Asymmetric	Factorization
Goldwasser Micali	1982	XOR	Partial	Asymmetric	Quadratic residuosity problem
Elgaml	1985	Multiplicative	Partial	Asymmetric	Diffi-Hellman problem
Okamoto uchiyama	1998	Additive	Partial	Asymmetric	P-subgroup assumption
Paillier	1999	Additive	Partial	Asymmetric	Decisional Composite Residuosity Assumption
Boneh–Goh–Nissim	2005	Additions (Unlimited) Multiplication (only one)	Some what	Symmetric	Subgroup decision problem
Gentry	2009	Fully	fully	Asymmetric	Sparse Subset Sum (SSSP) assumption

7. CONCLUSION

Currently, cloud computing became the most important thing for many people. They use it in their daily lives and businesses to ensure they get the time, effort, cost, and keep data in a place that they can access from their device anywhere if a network connection is possible. With all of the facilities provided by cloud computing, except it faced many security challenges in different directions, which made the security of the cloud one of the most significant things associated with it in order to gain people's trust and attract them to the use of the cloud services continuously. Therefore, the cloud must be more and more secure in many directions (such as data storage, network). One of these important requirements is preserving privacy in the cloud. Homomorphic Encryption is a famous method that used to ensure the privacy of cloud data due to its feature which makes it easy to perform arithmetic operations on encrypted data without the need for a decryption key.

ACKNOWLEDGEMENTS

The authors are very grateful to the University of Mosul/College of Computer Science and Mathematics for their provided facilities, which helped to improve the quality of this work.

REFERENCES

[1] P. J. Sun, "Security and privacy protection in cloud computing: Discussions and challenges." *Journal of Network and Computer Applications*, vol. 160, 2020, doi: https://doi.org/10.1016/j.jnca.2020.102642.

[2] S. Aldossary and W. Allen., "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions," *International Journal of Advanced Computer Science and Application,* vol. 7, no. 4, pp. 485-498, 2016, doi: 10.14569/IJACSA.2016.070464.

[3] R. D. Labati, A. Genovese, V. Piuri, F. Scotti, and S. Vishwakarma, "Computational Intelligence in Cloud Computing," In: Kovács L., Haidegger T., Szakál A. (eds) Recent Advances in Intelligent Engineering. *Topics in Intelligent Engineering and Informatics, vol 14. Springer, Cham.* 2020, https://doi.org/10.1007/978-3-030-14350-3_6.

[4] *K. Chandrasekaran, "*Essentials of cloud computing*," Taylor & Francis Group LLC, CrC Press,* Dec*. 2015.*

[5] W. Stallings, "Cryptography and Network Security Principles and Practice," 7th edition, *Pearson Education Limited,* 2017, ISBN 10: 0-13-444428-0.

[6] K. V. Nasarul, "Review on Benefits and Security Challenges of Cloud Computing," *International Journal of Computer Science and Information Technologies*, vol. 8, no. 2, pp. 224-228, 2017.

[7] R. Krishnan, "Security and Privacy in Cloud Computing," Master Thesis, Graduate College, *Western Michigan University*, 2017, doi: 10.1109/SURV.2012.060912.00182.

[8] P. V. Patel and H. D. Patel., "A Survey of the Homomorphic Encryption Approach for Data Security in Cloud Computing," *International journal of engineering development and research (IJEDR),* pp. 20-23, 2013

[9] S. Kh. Abd, S. A. R. Al-Haddad, F. Hasim, and A. Abdullah, "A Review of Cloud Security Based on Cryptographic Mechanisms," *International Symposium on Biometrics and Security Technologies (ISBAST), Kuala Lumpur, IEEE*, pp. 106-111, Aug. 2014, doi: 10.1109/ISBAST.2014.7013103.

[10] M. Haghighat, S. Zonous, and M. A. Mottaleb, "CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification," *Expert Systems with Applications*, vol. 42, no. 21, pp. 7905-7916, 2015, doi: 10.1016/j.eswa.2015.06.025.

[11] T. Galibus, V. Krasnoproshin, R. de Oliveira Albuquerque, and E. Pignaton de Freitas, "Elements of Cloud Storage Security, Concepts, Designs and Optimized Practices," *Springer* ebook, 2016, doi: 10.1007/978-3-319-44962-3.

[12] L. Yan, X. Hao, Z. Cheng and R. Zhou, "Cloud computing security and privacy," *Proceedings of the 2018 International Conference on Big Data and Computing*, pp. 119-123, 2018, doi: 10.1145/3220199.3220217.

[13] I. Ahmed, "A brief review: security issues in cloud computing and their solutions," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol.17, no. 6, pp. 2812-2817, Dec. 2019, doi: 10.12928/telkomnika.v17i6.12490.

[14] S. Basu, A. Bardhan, K. Gupita, and P. Saha, "Cloud Computing Security Challenges & Solutions-A Survey," *IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, pp. 347-356, 2018, doi: 10.1109/CCWC.2018.8301700.

[15] Z. Xiao and Y. Xiao, "Security and Privacy in Cloud Computing," *IEEE communications surveys & tutorials*, vol. 15, no. 2, pp. 843 -859, 2013, doi: 10.1109/SURV.2012.060912.00182.

[16] T. Kaur, "Cloud Computing: A Study of the Cloud Computing Services," *international Journal for Research in Applied Science & Engineering Technology (IJRASET),* vol. 7, no. VI, pp. 1933-1938, 2019, doi: 10.22214/ijraset.2019.6325

[17] O. Omotosho, "A Review on Cloud Computing Security," *International Journal of Computer Science and Mobile Computing (IJCSMC)*, vol. 8, no. 9, pp. 245-257, Sept. 2019, doi: 10.14257/ijgdc.2015.8.5.21.

[18] M. Mushtaq, U. Akram, I. Khan, and S. Khan, "Cloud Computing Environment and Security Challenges: A Review," *International Journal of Advanced Computer Science and Applications(IJACSA),* vol. 8, no. 10, pp. 183-195, 2017, doi: 10.14569/IJACSA.2017.081025.

[19] KE Narayana, S Kumar, K Jayashree , "A Review on Different types of Deployment Models in Cloud Computing", *International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE),* vol. 5, no. 2, pp. 1475-1480, 2017, doi: 10.15680/IJIRCCE.2017. 0502029.

[20] F. Suthar, S. Khanna, and J. Patel, "A Survey on Cloud Security Issues," *International Journal of Computer Sciences and Engineering (IJCSE)*, vol. 7, no. 3, pp. 120-123, Mar. 2019, doi: 10.26438/ijcse/v7i3.120123.

[21] Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, "Review Article: Data Security and Privacy in Cloud Computing," *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks*, vol.10, no. 7, Jul. 2014, doi: 10.1155/2014/190903.

[22] B. K. Rani, B. P. Rani, and A. V. Badu, "Cloud Computing and Inter-Clouds - Types, Topologies and Research Issues," *2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)*, *Elsevier*, vol. 50, pp. 24-29, 2015, doi: 10.1016/j.procs.2015.04.006.

[23] O. Y. Saygili, "The Introduction to Private Cloud using Oracle Exadata and Oracle Database," *Taylor & Francis*, 2020, doi: 10.1201/9780429020902.

[24] F. Liu *et al*., "NIST Cloud Computing Reference Architecture", *Recommendations of the National Institute of Standards and Technology, NIST SP* 500-292, 2011, doi: 10.6028/NIST.SP.500-292.

[25] Z. N. Al-Kateeb and, S. J. Mohammed "Encrypting an audio file based on integer wavelet transform and hand geometry," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 18, no. 4, pp. 2012-2017, Aug. 2020, doi: 10.12928/TELKOMNIKA.v18i4.14216 .

[26] S. J. Mohammed, "Using biometric watermarking for video file protection based on chaotic principle," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, no. 12, pp. 201-206, Dec. 2017.

[27] Z. N. Al-Khateeb and, S. J. Mohammed, "A Novel Approach for Audio File Encryption Using Hand Geometry," *Multimedia Tools and Applications,* vol. 79, no. 15, pp. 19615–19628 Mar. 2020, doi: https://doi.org/10.1007/s11042-020-08869-8.

[28] Gh. Th. Talee, M. J. Jelmeran, and S. J. Mohammad, "A new approach for chaotic encrypted data hiding in color image," *International Journal of Computer Applications,* vol. 86, no 8, pp. 23-26, Jan. 2014, doi: 10.5120/15006-3233.

[29] D. B. Taha, T. B. Taha, and N. B. Al Dabagh, "A comparison between the performance of DWT and LWT in image watermarking," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 3, pp. 1005-1014, June 2020, doi: 10.11591/eei.v9i3.1754.

[30] Z. N. Al-Khateeb, M. Jader, "Encryption and Hiding Text Using DNA Coding and Hyperchaotic System," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 19, no. 2, pp. 766-774, Aug. 2020, doi: 10.11591/ijeecs.v19.i2.pp766-774.

[31] A. Mouafak, M. Jader, and S. J. Mohammed, "Apply new algorithm for chaotic Encryption using CBC&CFB," *Australian Journal of Basic and Applied Sciences*, vol. 7, no. 12, pp. 221-228, Oct. 2013.

[32] A. Albugmi, M. O. Alassafi, R. Walters, and G. Wills, "Data Security in Cloud Computing," *5th international conference on future generation communication technologies (FGCT2016)*, *IEEE*, pp. 55-59, 2016, doi: 10.1109/FGCT.2016.7605062.

[33] N. Amara, H. Zhiqui, and A. Ali, "Cloud Computing Security Threats and Attacks with their Mitigation Techniques," *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, IEEE,* pp. 241-255, 2017,doi: 10.1109/CyberC.2017.37.

[34] CSA member1, "The Treacherous 12-Top Threats to Cloud Computing + Industry Insights," *Cloud Security Alliance (CSA)*, 2017.

[35] Kazim M. and S. Y. Zhu, "A survey on top security threats in cloud computing," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 6, no. 3, pp. 109-113, 2015, doi: 10.14569/IJACSA.2015.060316.

[36] A. Javaid, "Top threats to cloud computing security," *SSRN Electronic Journal*, 2013, doi: 10.2139/ssrn.2325234.

[37] R. Gupta and R. Kapoor, "A Review Paper of Data Security in Cloud Computing," *Imperial Journal of Interdisciplinary Research (IJIR)*, vol. 2, no. 8, pp. 501-504, 2016, doi: 10.5120/16338-5625.

[38] L. Kacha and A. Zitouni, "An Overview on Data Security in Cloud Computing," *Conference Paper in Advances in Intelligent Systems and Computing(AISC), Springer International Publishing,* vol. 661, pp. 250-261, 2018, doi: 10.1007/978-3-319-67618-0_23.

[39] A. Soofi, M. I. Khan and F. Amin, "Encryption Techniques for Cloud Data Confidentiality," *International Journal of Grid Distribution Computing*, vol. 7, no. 4, 2014, doi: 10.14257/ijgdc.2014.7.4.02.

[40] S. Sharma, "Data Integrity Challenges in Cloud Computing," *4th International Conference on Recent Innovations in Science Engineering and Management, (ICRISEM-16),* pp. 736-743, 2016.

[41] O. Harfoushi, R. Obiedat, "Security in Cloud Computing Using Hash Algorithm: A Neural Cloud Data security model, " *Canadian Center of Science and Education,* vol. 12, no. 6, 2018, doi: 10.5539/mas.v12n6p143.

[42] P. T. Endo *et al.*, "High availability in clouds: systematic review and research challenges*," Journal of Cloud Computing: Advances, Systems and Applications*, *Springer*, vol. 5, no. 16, pp. 1-15, 2016, doi: 10.1186/s13677-016-0066-8.

[43] M. R Mesbahi., A. M. Rahmani, and M. Hosseinzadeh, "Reliability and high availability in cloud computing environments: a reference roadmap," *Human centric computing and information science (Cent. Comput. Inf. Sci.)*, *Springer*, vol. 8, no. 20, pp. 6-16, 2018, doi: 10.1186/s13673-018-0143-8.

[44] W. Bajaber, M. Alqulaity, and F. Alotaibi, "Different Techniques to Ensure High Availability in Cloud Computing," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 6, no. 11, pp. 1-16, November 2017, doi: 10.17148/IJARCCE.2017.61102.

[45] C. Nalini and A. Arunachalam, "A study on privacy preserving techniques in big data analytics," *International Journal of Pure and Applied Mathematics,* vol. 116, no. 10, pp. 281-286, 2017.

[46] X. Yi, P. Russell, and E. Bertino, "Homomorphic Encryption and Applications," *Springer*, (eBook) ISBN 978-3-319-12229-8, 2014.

[47] M. Zhao and Y. Geng, "Homomorphic encryption technology for cloud computing," *Procedia Computer Science 154*, *Elsevier,* pp. 73–83, 2019, doi: 10.1016/j.procs.2019.06.012.

[48] M. Ogburna, C. Turner, and P. Dahal, "Homomorphic Encryption," *Procedia Computer Science,* vol. 20, pp. 502-509, 2013, doi: 10.1016/j.procs.2013.09.310.

[49] M. Alkharji and H. Liu, "Homomorphic Encryption Algorithms and Schemes for Secure Computations in the Cloud," *Proceedings of 2016 International Conference on Secure Computing and Technology*, March 2018.

[50] M. Derfouf and M. Eleuldj, "Cloud Secured Protocol based on Partial Homomorphic Encryptions," *4th International Conference on Cloud Computing Technologies and Applications (Cloudtech), Brussels, Belgium*, 2018, doi: 10.1109/CloudTech.2018.8713353.

[51] M. Tebaa and EL Haji S., "Secure Cloud Computing through Homomorphic Encryption," International *Journal of Advancements in Computing Technology (IJACT,)* vol. 5, no. 16, pp. 29-38, December 2013.

[52] Y. Bensitel and R. Romadi, "Secure Data Storage in the Cloud with Homomorphic Encryption," *2nd International Conference on Cloud Computing Technologies and Applications (CloudTech),* Marrakech, 2016, doi: 10.1109/CloudTech.2016.7847680.

[53] K. El Makkaoui, A. Ezzati, and A. B. Hssane, "Challenges of Using Homomorphic Encryption to Secure Cloud Computing," *International Conference on Cloud Technologies and Applications (CloudTech), Marrakech,* 2015, pp. 1-7, doi: 10.1109/CloudTech.2015.7337011.

[54] B. Seth, S. Dalal, and R. Kumar, "Hybrid Homomorphic Encryption Scheme for Secure Cloud Data Storage," *In: Kumar R., Wiil U. (eds) Recent Advances in Computational Intelligence. Studies in Computational Intelligence,* vol 823. *Springer, Cham,* 2019, doi: 10.1007/978-3-030-12500-4_5.

[55] V. Dhananjaya, R. Balasubramani, K. S. Jagadeeshgowda, and N. Ghorpade, "A Survey of the Homomorphic Encryption Approach for Data Security in Cloud Computing," *International Journal of Combined Research & Development (IJCRD)*, vol. 6, no. 3, pp. 731-736, March 2017.