International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I10P201

Volume 69 Issue 10, 1-6, October, 2021
©2021 Seventh Sense Research Group®

Cryptography based Techniques of Encryption for Security of Data in Cloud Computing Paradigm

Adel Rajab[1], Sehrish Aqeel[2], Mana Saleh Al Reshan[1], Awais Ashraf[3], Sultan Almakdi[1] and Khairan Rajab[1,4]

[1]*College of Computer Science and Information Systems, Najran University, Najran, Saudi Arabia*
[2]*Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Sarawak, Malaysia.*
[3]*Department of Computer Science, Bahria University Lahore Campus, Lahore, Pakistan.*
[4]*College of Computer Science and Engineering, University of South Florida, Tampa, United States*

msalreshan@nu.edu.sa, adrajab@nu.edu.sa, sehrish.ibit@gmail.com

Abstract - *Cloud Computing (CC) is a cheap and user-friendly compatible platform that aims to provide IT users over the internet to a business organization as well as another internet consumer by a variety of its services. It is also becoming the fastest growing technology that does not need in-stalled hardware or software at consumer's devices. Cloud technology has many advantages in terms of economic cost and IT load. So, currently, the adoption of this emerging technology has increased tremendously. One critical issue in CC is the security of data that is mainly tacked by numerous encryption methods. Based on a systematic literature review, this paper identifies two critical aspects; firstly, the key encryption methods used for securing data in the cloud-based system, and secondly, how encryption techniques are validated in previous research studies? The result of this systematic literature review identified that RSA is a widely used algorithm to ensure security in CC as compared to all existing used algorithms to protect data of the cyber world.*

Keywords — *Cloud-based systems; encryption; cryptography; data security.*

I. INTRODUCTION

Cryptography refers to the securing technique which is used for hiding the desired information. It has originated from the Greek word 'κρυπτός' that means secret. It refers to the science in which information is kept safe and secure. Humans are always curious to secure the information before transmitting it over any communication media. Attack on common communication channel can lead to intercept the sent data and eventually causes serious security issues. That is the reason that cryptography is being practiced for many years to hide the desired data and secure the intended information. Egypt peoples used cryptography in 1900 BC on stones by using ciphertext. Greeks were also familiar with cryptography that used different ways to hide and secure information. [1-3].

NIST defined CC as a framework to facilitate its users by easy-to-use access of network through common shared environment having plenty of resources like storage, servers, devices, services, and applications that could be easily accessed by service provider interaction or minimal management effort. This CC model encourages customers to gain access to the resources from their computer devices such as a laptop or personal computers [4]. Customers use multiple IT services like device storage, computing, and multiprogramming by using a single computer device on the local network that they share [5-6].

As per NIST, Cloud computing has three service models. They are Software as a service model, Platform as a service model, and Infrastructure as a service model. Cloud Computing has five Development Models. NIST also defined five cloud computing development models, which are (1) Public Cloud, (2) Private Cloud, (3) Hybrid Cloud, (4) Community Cloud, and (5) Virtual Private Cloud. Numerous cloud characteristics such as Rapid Elasticity, on-demand self-services, Measured services, location Independent and resource pooling are also discussed in detail [7-9].

Diaa Salama in [10] mentioned some terms which are mostly used in the CC domain. Plain text is called the original message of the user. The user wants to encrypt it. Key is the core object in CC that must be known by both sender and receiver for encrypting and decrypting data [11-12]. Keys can be both public and private. A private key is used in some algorithms for encryption and decryption processes in the cloud-based system, whereas some decryption processes use a private key to just encrypt the data in cloud computing. The ciphertext is the new form of the original text. A ciphertext is a non-readable form of the original text. Decryption is the process in which ciphertext is converted back to the original text by applying different decryption algorithms or techniques.

Abu-Faraj and Osama Discussed various security issues and challenges in [13-15]. Data Breaches, Insider threats, Denial of service attacks, Hijacking of Accounts, Malware injection, and Shared vulnerabilities are the most common security problems observed in a cloud-based system. Consequently, crucial challenges are Security, Privacy, Interoperability, Portability, Performance, and Bandwidth issues that must be handled to implement transmission security over the internet.

Another research related to security issues is [16-19], in which Eesa Alsolami discussed various security concerns related to a cloud-based system. These security issues are User-level Security, Application Infection, Data Theft, Data Loss, privacy issues, and Data Integrity Problems [20].

Three different types of cryptography techniques are used in cloud computing to achieve security at the desired level. The first category is Symmetric key cryptography that shares a common key for the encryption as well as decryption process of data in CC systems. Moreover, it is fast but provides less security because hackers can break it easily [21]. The second is Asymmetric key cryptography that makes use of two keys for each process in CC. In this type, the private key is not shared openly with anyone, and this particular key is used for the process of decryption only, whereas the public key is openly available for everyone to use hence making it more secure as compared to symmetric key cryptography. On the other hand, it utilizes more resources as well in terms of time and effort. The third category is Hash function cryptography that instead of using any key, deals with hash function for encryption and decryption process to secure the data in cloud-based computing systems [22-23].

The rest of the paper is organized as follows: section 2 reports related studies; section 3 describes the outcome of the systematic literature review. Section 8 concludes the findings of the study.

II. RELATED WORK

A systematic literature review is a subtype of literature review that adopts numerous systematic methods to collect secondary data studies in a particular research problem. Qualitative or quantitative data may be used for this purpose. Systematic literature review (SLR) means collecting all previous research studies about a particular research problem, evaluate it properly to understand it well [24]. It also covers comprehensive and unbiased coverage of literature review. To Performed SLR in this research, previous SLR studies have been reviewed and eventually selected our research methodology. 10 stages review process is performed in this regard which is extended from [25]. This paper has concised 10 stages into three-phase steps, and they are: (1) Plan the review, (2) Conduct the review (3) Documentation of the review. Each phase involves several discrete activities. Fig. 1 illustrates all 3 phases with each review stage [26].

In previous studies, researchers mostly focused on the securities problems that are present in clouds-based systems. This study will focus on encryption techniques used by different researchers in their studies to resolve security issues in cloud computing [27-28].

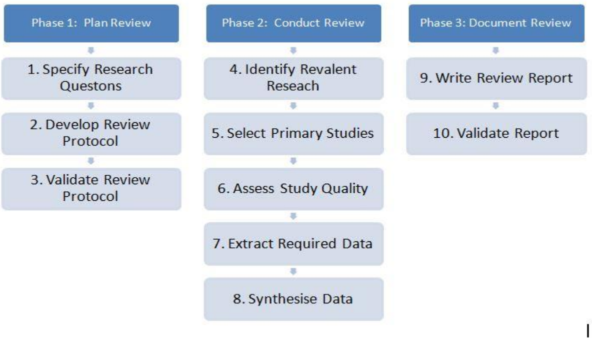


Fig. 1 Systematic Literature Review Process.

A. Research Questions Formalization

Random approaches exist that target new approaches applicable to encryption techniques and validation of those techniques. The main objective of this research is to identify the encryption techniques that are used to tackle security problems in a cloud-based system. These two key questions are tackled in this research which is as follows:

- Question 1: What encryption techniques have been applied to ensure data security in a cloud-based system?
- Question 2: How these encryption techniques are validated and practically deployed?

B. Selection of Sources

In this study, the selection of source criteria is based on certain limitations: (1) Research studies must be related to our research questions that are explored in these databases. (2) Irrelevant studies are not included in these sources. (3) These sources must be freely and easily available on web portals. The review protocol is made up of sources and different keywords. Tab. 1 shows the review protocol for this research study with relevant sources and keywords [29].

TABLE I
REVIEW PROTOCOL

Year	Sources	Keywords
2010-2019	ACM, Google Scholar, Science Direct, IEEE Xplore, Scopus,	Cloud Computing, Encryption Techniques in Cloud Computing, Data Security Techniques in Cloud Computing

It was necessary to define selection and evaluation criteria for conducting the most relevant literature. An inclusion and exclusion criterion is based on our research questions. The evaluation is based on the criteria mentioned in Tab. 2.

TABLE III
INCLUSION AND EXCLUSION CRITERIA

Inclusion Criteria	Exclusion Criteria
Directly related to Cloud Computing and Encryption Techniques. Written in English. Cloud-based Solutions of Data Security issues	Irrelevant to Cloud Computing and Encryption Techniques. Not Written in English Business Analysis Reports Duplicate Articles

C. Review Execution

To conduct this phase, the searching process must be performed on these selected sources. After performing the search process, results are obtained, and these results are evaluated on defined exclusion criteria and inclusion criteria. We will mention the inclusion criteria and exclusion criteria in Tab. 2. After performing the review, a set of 45 research articles was obtained [30-31]. These research articles were filtered by using defined inclusion criteria, and as a result, 35 re-search articles were figured out. These 35 research articles were again filtered based on exclusion criteria. Finally, we obtained 25 most relevant studies about these research questions, as shown in Fig. 2 [32-33].

III. OUTCOME OF SLR

In this section, the results of the review process are represented based upon the year. Tab. 3 illustrates those results. We also categorized results according to research questions.

TABLE IIIII
YEAR WISE SEARCH PROCESS RESULTS

Publication Year	Number of Research Articles
2010	1
2011	2
2012	2
2013	3
2014	2
2015	3
2016	3
2017	3
2018	4
2019	2
Total	**25**

A. *Question 1: What encryption techniques have been applied to ensure data security in a cloud-based system?*

The result of this systematic literature review is shown in Fig. 3, shows that how different encryption techniques are used in cloud computing for data security. The result of this research study is categorized as below

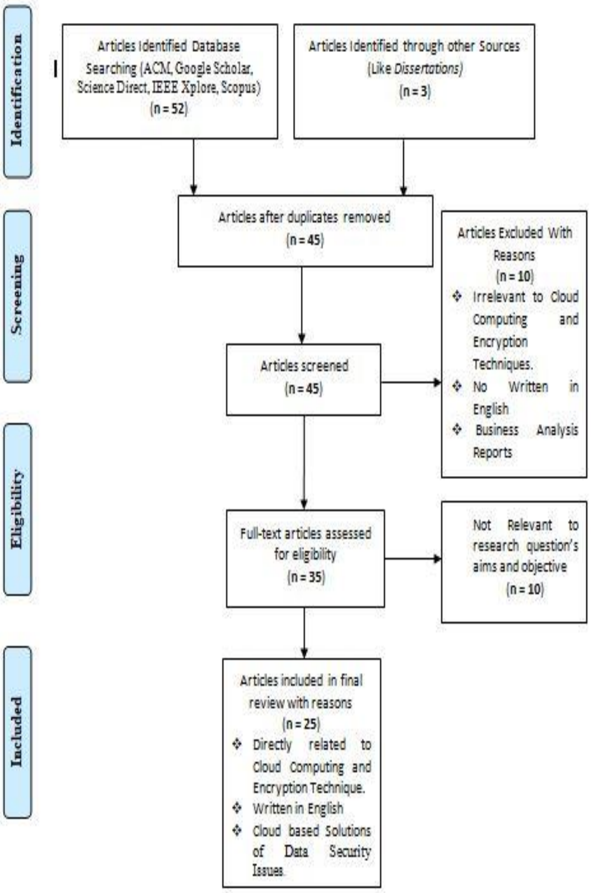

Identification
Screening
Eligibility
Included
Articles Identified Database Searching (ACM, Google Scholar, Science Direct, IEEE Xplore, Scopus) (n = 52)
Articles Identified through other Sources (Like Dissertations) (n = 3)
Articles after duplicates removed (n = 45)
Articles Excluded With Reasons (n = 10)
❖ Irrelevant to Cloud Computing and Encryption Techniques.
❖ No Written in English
❖ Business Analysis Reports
Articles screened (n = 45)
Full-text articles assessed for eligibility (n = 35)
Not Relevant to research question's aims and objective (n = 10)
Articles included in final review with reasons (n = 25)
❖ Directly related to Cloud Computing and Encryption Technique.
❖ Written in English
❖ Cloud based Solutions of Data Security Issues.

Fig. 2 Selection of Research Articles Flow Diagram

1) RSA is widely used to integrate data security in CC. RSA is a famous algorithm that uses two different keys to implement security mechanisms in a cloud computing environment. Adi Shamir and Leonard Adleman proposed the RSA algorithm in 1977. In this algorithm, one key is enabled as a public key and the other one as a private. A private key is used for the encryption process. A public key is used for the decryption process. RSA takes more time to encrypt and decrypt data. RSA has keys of 1024 bit size. Private Key is confidential in the RSA algorithm.
2) Hybrid Approach is the second-largest encryption approach used in cloud computing to ensure and implement data security. In this approach, two different algorithms are used to enforce security in CC. One algorithm may be symmetric, and the other is Asymmetric.
3) Advanced Encryption Standard (AES) is the third-largest most used algorithm to enhance the security of the system. It is an asymmetric algorithm that shares a single common key for the encryption-decryption process. AES can encrypt 128-bit data size, and key length can be 128 bits, 192 bits, and 256bits. AES takes 10 rounds to convert plain text to chipper text or ciphertext to plain text.
4) SHA-512 is a hashing function algorithm that takes 64 bytes or 128 bytes of data for the encryption and decryption process, and digest sizes are 224, 256, or 384 bits. SHA-512 takes 64 or 80 rounds to convert the plain text into ciphertext.
5) DES stands for Data Encryption Standard, which belongs to the symmetric-key algorithm. DES is based on the concept of the Feistel structure. DES has a 56bit key length and 16 rounds in the encryption and decryption process. Moreover, the same algorithm is adopted at the sender and receiver sides while using DES.
6) RC5 is also a symmetric key algorithm that has 12 rounds and takes 128 bits of data for the encryption-decryption process. RC5 transfers the data in the encryption form.
7) RC6 is a symmetric key algorithm that is an extended form of the RC5 algorithm. RC6 was developed by Matt Robshaw and Ray signey. RC6 has 20 rounds and takes 12 bits of data with 128, 192, and 256 bits key length.
8) Geo encryption algorithm is a novel approach to enable security in CC. It uses the user location and geographical position for encryption and decryption of data.
9) Diffie-Hellman is an Asymmetric algorithm used to exchange the public key. It is not an authentication method for users.
10) PRE and ABE is an emerging technology used for data security in cloud computing.
11) CC CUSs can also be utilized actively to achieve security.

Different researchers used it in their research studies. Finally, RSA is one of the Asymmetric methods widely used for the security of data in CC.

The categories of wise review results are summarized in Table IV.

TABLE IVV

CATEGORIZED WISE RESULT OF QUESTION 1

Research Question	Encryption Techniques	No. of Papers	Citations
Question 1: **What encryption techniques have been applied to ensure data security in cloud computing?**	RSA	7	[21],[13],[22], [28],[20],[33],[18]
	Hybrid Approach	5	[27],[10],[25], [24],[23]
	AES	4	[31],[11],[17],[19]
	SHA-512	2	[30],[32]
	DES	1	[14]
	RC5	1	[26]
	RC6	1	[12]
	Geo-Encryption	1	[15]
	Diffie-Hellman	1	[34]
	PRE AND ABE	1	[29]
	CSUs	1	[9]
	Total	**25**	

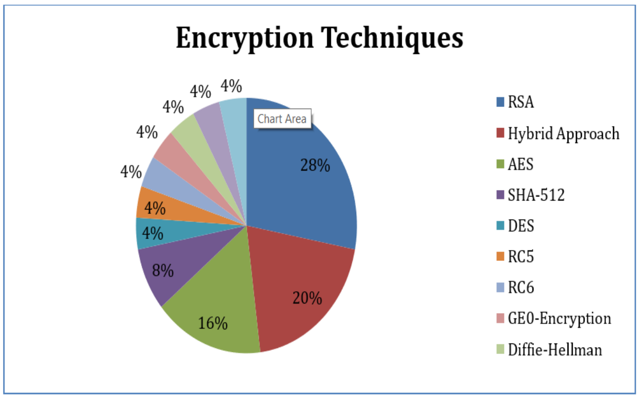


Fig. 3 Proposed Encryption Techniques to Ensure Security of Data in CC Paradigm

B. Question 2: How these encryption techniques are validated in different research studies?

The result of this systematic literature review defined in Fig. 3 shows how these encryption techniques used in cloud computing for data security are validated in different research studies. The result of this research study is categorized as

1) An experiment where researchers conduct different experiments to validate their approaches.
2) Some research studies do not conduct any experiments to validate the encryption approaches.
3) Some research studies compared the result with another scheme of results for validation.

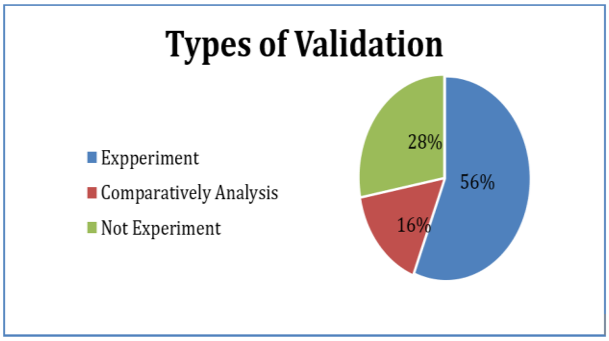


Fig. 4 Types of Validation

The result of this research question 2 about the validation of encryption techniques found that 56% of selected research papers performed experiments to validate the approaches, as shown in Fig. 4. The categories of wise review results are summarized in Table V.

TABLE V

CATEGORIZED WISE RESULT OF QUESTION 2

Research Questions	Types of Validation	No. of Research Articles
Question 2: **How are these encryption techniques validated and deployed?**	Experiment	14
	Comparatively Analysis	7
	Not Analysis	4

A. Forest Plot

The Forest plot illustrates the year-wise combined research effect as shown in Fig. 5. The big block in the forest plot represents that more research studies were conducted in that particular year.

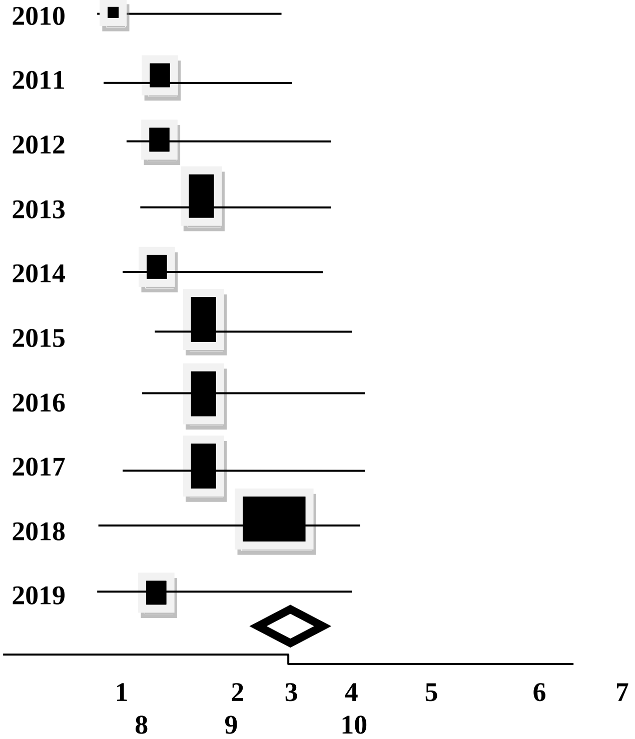
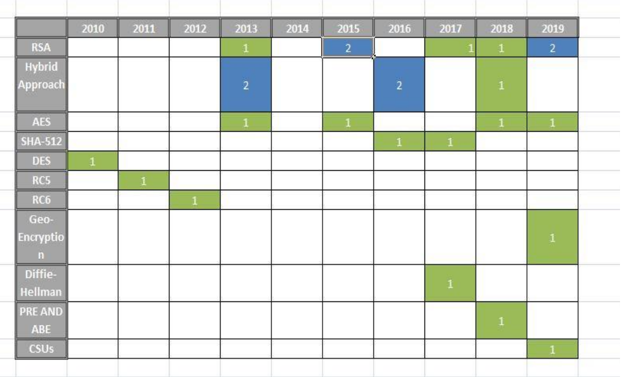


Fig. 5 Forest Pilot Year Wise Research Effect

A heat map is used to poetry the data graphically through the use of color codes schemes. This approach helps to get the better attention of the reader towards analyzing the data set and reach the inference about the most important data values. That is the reason that this approach is used to show the results of the forest plot in the form of a heat map to grab the viewers' sight and conclude about it abruptly, as shown in Fig. 6.



	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
RSA				1		2		1	1	2
Hybrid Approach				2			2		1	
AES				1		1			1	1
SHA-512							1	1		
DES	1									
RC5		1								
RC6			1							
Geo-Encryptio n										1
Diffie-Hellman								1		
PRE AND ABE									1	
CSUs										1

Fig. 6 Heat Map of Systematic Literature Review

IV. CONCLUSIONS

CC is becoming an emerging advanced technology that provides computing resources with better security and less cost. CC provides multiple benefits to end users but at the same time faces various security issues and threats too. This study provides the concept of CC, encryption techniques used in it, and validation of those techniques. The overall result declared that the RSA algorithm is widely used in a cloud-based system for the protection of consumer's data. RSA is an Asymmetric-key algorithm, and 28% out of the total researcher's studies use it for data security in a cloud-based system. On the other end, AES is a symmetric-key algorithm, and 16% out of the total of previous researcher's studies use it in a cloud-based environment. This research study helps business customers to choose an appropriate algorithm for implementing security in cloud-based systems. The optimal option would be the RSA algorithm for data protection and security. Abundant researchers have mostly used RSA encryption techniques in their studies for the protection of data in cloud-based scenarios. Moreover, it was also found out that most proposed approaches are not validated by researchers in their studies. This research study identifies that 16% of approaches have not validated the results. So, this opens a new dimension of discussion where results of the research studies could be well improved by improving validation methods and depicting them in the research studies as well.

REFERENCES

[1] P. Agarwal, Cryptography based security for a cloud computing system, International Journal of Advanced Research in Computer Science, 8(5) (2017) 2193–2197, 2017.

[2] D. Sengupta, Designing of hybrid RSA encryption algorithm for cloud security, International Journal of Innovative Research in Computer and Communication Engineering, 3(5) (2015) 4146–4152.

[3] R. Chatterjee, S. Roy, and U. Scholar, Cryptography in cloud computing: a basic approach to ensure security in the cloud, International Journal of Engineering Science, 7(5) (2017) 11818–11821.

[4] D. AbdElminaam, Improving the security of cloud computing by building new hybrid cryptography algorithms, International Journal of Electronics and Information Engineering, 8(1) (218) . 40–48.

[5] O. Harfoushi, B. Alfawwaz, N. Ghatasheh, R. Obiedat, M. Abu-Faraj, et al., Data security issues and challenges in cloud computing: a conceptual analysis and review, Communications and Network, 06(1) (2014) 15–21.

[6] E. Alsolami, Security threats and legal issues related to cloud computing-based solutions, International Journal of Computer Science and Network Security, 18(5) (2018) 156–163.

[7] P. Brereton, B. Kitchenham, D. Budgen, M. Turner, and M. Khalil, Lessons from applying the systematic literature review process within the software engineering domain, Journal of Systems and Software, 80(4) (2007) 571–583.

[8] K. Hashizume, D. Rosado, E. Fernández-Medina and E. Fernandez, An analysis of security issues for cloud computing, Journal of Internet Services and Applications, 4(1) (2013) 1–13.

[9] Y. Liu, J. Ryoo and S. Rizvi, Ensuring data confidentiality in cloud computing: an encryption and trust-based solution, In 23rd Wireless and Optical Communication Conference (WOCC), Newark, New Jersey, U.S.A, (2015) 1–6.

[10] C. Yang and J. Lai, Protecting data privacy and security for cloud computing based on secret sharing, in the International Symposium on Biometrics and Security Technologies (ISBAST), Chengdu, China, (2013) 259–266.

[11] P. Salim, A. Abbas, and M. Qasim, Improving data storage security in cloud computing using rc6 algorithm, IOSR Journal of Computer Engineering, 19(5) (2017) 51–56.

[12] S. Han and J. Xing, Ensuring data storage security through a novel third party auditor scheme in cloud computing, in the IEEE International Conference on Cloud Computing and Intelligence Systems, Beijing, China, (2011) 264–268.

[13] T. Sathyanarayana and L. Sheela, Data security in cloud computing, International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), 2(1) (2013) 822–827.

[14] M. Abolghasemi, M. Sefidab, and R. Atani, Using location-based encryption to improve the security of data access in cloud computing, in the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Mysore, India, (2013) 261–265.

[15] U. Pius, E. Onyebuchi, O. Chinasa, and E. Adoba, A cloud-based data security system using advanced encryption (aes) and blowfish algorithms, Journal of Scientific and Engineering Research, 5(6) (2018) 59–66.

[16] J. Hamdard, N. Delhi, P. Agarwal, J. Hamdard and N. Delhi, Cryptography based security for cloud computing system, International Journal of Advanced Research in Computer Science, 8(5) (2017) 2193–2197.

[17] S. Talluru, Secure cloud storage using homomorphic encryption, International Journal for Research in Applied Science & Engineering Technology, 6(4) (2018) 2194–2203.

[18] U. Somani, K. Lakhani and M. Mundra, Implementing digital signature with rsa encryption algorithm to enhance the data security of cloud in cloud computing, in the First International Conference On Parallel, Distributed and Grid Computing (PDGC), Solan, India, (2010) 211–216.

[19] P. Kalpana, Data security in cloud computing using rsa algorithm," International Journal of Research in Computer and Communication Technology, 1(4) (2012) 143–146.

[20] A. Sharma, R. Kumar and V. Mansotra, Proposed stemming algorithm for hindi information retrieval, International Journal of Innovative Research in Computer and Communication Engineering, 3297(6) (2016) 11449–11455.

[21] S. More and S. Chaudhari, Third party public auditing scheme for cloud storage," Procedia Computer Science, 79(1) (2016) 69–76.

[22] L. Tawalbeh, N. Darwazeh, R. Al-Qassas and F. AlDosari, A secure cloud computing model based on data classification," Procedia Computer Science, 52(1) (2015) 1153–1158.

[23] J. Singh, B. Kumar and A. Khatri, Improving stored data security in cloud using rc5 algorithm, in Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, India, (2012) 1-5.

[24] M. Rewagad and M. Pawar, Use of digital signature with Diffie-hellman key exchange and aes encryption algorithm to enhance data security in cloud computing, International Conference on Communication Systems and Network Technologies, Gwalior, India, (2013) 437–439.

[25] M. Sulochana and O. Dubey, Preserving data confidentiality using multi-cloud architecture, Procedia Computer Science, 50(1) (2015) 357–362.

[26] Q. Liu, G. Wang and J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Information Sciences, 258(1) (2014) 355–370.

[27] M. Hossain, A. Ullah, N. Khan and M. Alam, Design and development of a novel symmetric algorithm for enhancing data security in cloud computing, Journal of Information Security, 10(4) (2019) 199–236.

[28] S. Delfin, R. Sai, J. Meghana, L. Kundana and S. Sharma, Cloud data security using aes algorithm, International Research Journal of Engineering and Technology, 5(10) (2018) 1189-1192.

[29] S. Thokchom and D. Saikia, Privacy preserving and public auditable integrity checking on dynamic cloud data, International Journal of Network Security, 21(2) (2019) 221–229.

[30] E. Ramadan and M. Djamilou, Using cryptography algorithms to secure cloud computing data and services, American Journal of Engineering Research (AJER), 6(10) (2017) 334–337.

[31] P. Bandal, A. Dhane, S. Chavan and P. Nikam, Key exchange privacy preserving technique in cloud computing, International Research Journal of Engineering and Technology, 5(3) (2018) 3113–3117.

[32] M. Junaid, A. Shaikh, M. Hassan, A. Alghamdi, K. Rajab, M.S. AlReshan and M. Alkinani, Smart Agriculture Cloud using AI based Techniques, Energies,l. 14(16:5129) (2021) 1-15.

[33] R. Ratra and P. Gulia, Privacy Preserving Data Mining: Techniques and Algorithms, International Journal of Engineering Trends and Technology, 68(11) (2020) 56-62.