Migration Letters

Volume: 21, No: S7 (2024), pp. 1100-1109

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Encryption Algorithms For Information Security In Cloud Computing: A Detailed Study And Analysis

Anjana[1], Dr.Ajit Singh[2]

ABSTRACT

Cloud computing has emerged as a prominent paradigm for delivering computing services over the internet. However, cloud data security remains a serious challenge. Protecting sensitive data requires encryption. Cloud computer encryption methods for data privacy, integrity, and authenticity. To improve cloud computing information security, this study reviews and analyzes encryption techniques. The paper examines symmetric, asymmetric, and homomorphic encryption methods. Key management, computational overhead, and scalability are explored for cloud-based encryption. Cloud computing encryption technologies assist practitioners make informed cloud information security judgments. As cloud computing grows, data security is essential. The review paper analyzes cloud computing encryption techniques for data security. It examines cloud computing information security cryptography algorithms. The cloud provides scalable internet services for various devices to access data and applications. Cloud shared resources can cause data breaches, illicit access, and service failures. Cloud security architecture, deployment, and service models. Cloud computing security must be strong and encryption must improve to tackle emerging security threats. Review paper analyses encryption methods for cloud computing information security to help academics, practitioners, and stakeholders secure cloud-based systems and services.

Keywords: *Cloud Computing, Algorithms, Security, Data, Cloud Storage.*

1. INTRODUCTION

Cloud computing, which uses virtualization to provide scalable internet services, is a popular technical issue [1]. Users move files and programs to the "Cloud" via mobile phones, laptops, PCs, etc. and may access them easily online. Many web applications have been added to cloud computing platforms like Hotmail and Gmail in recent years [2]. Cloud computing allows people to access services anywhere. Services and deployment models are cloud computing concepts. They include SaaS, PaaS, and IaaS and four deployment models: Public, Private, Community, and Hybrid cloud. Cloud computing has on-demand, wide network access, quick elast[1]icity, measurement, service, and resource sharing [3]. Chief cloud computing concern Cloud and infrastructure management by third parties always risks sensitive data. Cloud computing suppliers protect accounts with passwords, but a compromise would cost customers and businesses [4].

[1,2]Department of CSE & IT, Bhagat Phool Singh Mahila Vishwavidyalaya, Khanpur Kalan, Sonipat, Haryana, India
ORCID: 0000-0003- 1511-6471

Cloud computing is a major trend in networking systems for users and developers [5]. Cloud computing is beneficial for networked people. Therefore, cloud computing security is a major issue. The cloud shares resources among servers, users, and people. Cloud files become public. All other cloud users can access an individual's files [6,7]. Thus, intruders can simply access, destroy, and misuse original data. Additionally, can disrupt communication. In addition, cloud service providers (CSP) offer crucial applications. Security is equally crucial for the cloud [8]. Cloud storage may not give users control over where their data is stored. Since cloud consumers used the cloud service provider's resource allocation and planning. For this, data or files must be protected through insecure procedures. To solve this problem, we must secure cloud computing platforms. As much as feasible, our recommended security framework considers account breaches. Many security algorithms and models are used in cloud computing. Unfortunately, these approaches have not eliminated all security threats [9-11] E-commerce and other online businesses require a high-capability cloud security [12]. File security models in cloud computing are used to secure files, not communication systems [13]. Additionally, certain security models use secured communication channels [14]. This method is inefficient. Again, combining primary server security, transaction, and so on is rare. Some models try to discuss these, but they're client-driven and don't use machine intelligence to generate key and newer models. Certain models have used hardwire encoding for secure communication [15]. Additionally, hardwire encryption only protects databases. Once again, authorized user detection is crucial but rarely covered in cloud computing security frameworks [16].

1.1 SECURITY ISSUES IN CLOUD COMPUTING

Security risks in cloud computing include data security [17]. Regardless of the technology, it's a huge issue when SaaS users need supplier security [18]. Thus, cloud computing's biggest concern is security leaks, which limit widespread adoption. Cloud servers keep all files, making them available 24/7, giving hackers full time to breach file protection walls like encryption and authentication. Following are cloud service provider security vulnerabilities connected to file storage [19].

- **Secure Data Storage**

Clouds store massive user data. Some parties may value preserved data. Cloud services must strongly combine data encryption and decryption to gain customer trust. All cloud services keep encrypted data in cloud servers. At user request, the decryption key decrypts the data and allows viewing. Such file encryption and decoding prevent unauthorized cloud server access [20].

- **Secure Data Transfer**

Data packages are delivered and received via real-time client networking in cloud computing. These data packages can be traced because the internet is used for communication and can be attacked anytime. Thus, cloud computing companies must secure files or data file chunks for complete safety [21].

- **User permissions**

User access restrictions to other users' data and documents are another cloud computing security aspect. Server login credentials authenticate a user. Other users' private or non-public files are inaccessible. For data management, users should know who has administrative rights in cloud service providers because they can access cloud data [22].

2. ARCHITECTURE OF CLOUD SECURITY

Computing is preloaded and offered as a service over the web, with data, apps, operating systems, storage, and processing capability ready to distribute [23]. Internet-connected data centers (CC) use virtualized infrastructure to provide services [24]. CC uses infrastructure, OS, cloud app development, database management, system and app management software, Internet, and network. Companies that dynamically provide CC resources and services at consumer request follow a business model. Figure 1 demonstrates the interaction between Amazon, Google, Microsoft, and IBM, the top CC service providers.

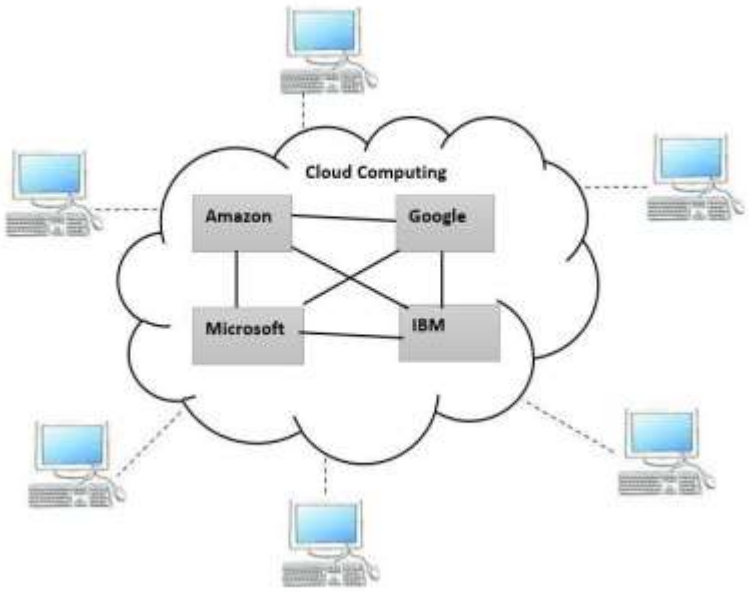

Figure 1: Cloud Computing [29]

2.1 Cloud deployment model

Classifying CC into three categories [25]: private, public, hybrid cloud [26]. Private clouds are operated by a single company and do not use other clients' assets; therefore, they are secure. Organizations and individuals can use public clouds. All clients share assets. Service and asset usage determine client payments to the cloud owner. Physical infrastructure is managed by CSPs apart from clients. Hybrid clouds combine public and private clouds [27].

2.2 Service models

SaaS, PaaS, and IaaS are CC's main services.[28]

IaaS: Computer resources include networks, storage, memory, CPUs to comprise CSP hardware. The virtualized systems are accessible online. CSP controls vital resources.

PaaS: Third parties sell IDEs, middleware, OSes, and platform layer resources online. PaaS only lets clients control cloud apps, not the cloud infrastructure.

SaaS: Online application as a service is available. It can be accessed online without buying, installing, or maintaining software. Use, not ownership, is charged.

The front and back ends of the CC system are separate. Networks, generally the internet, connect them. Cloud customers see the front. Our clients seldom the back-end contains cloud

servers, applications, and network connectivity. Figure 2 depicts CC architecture and cloud service categories [29].

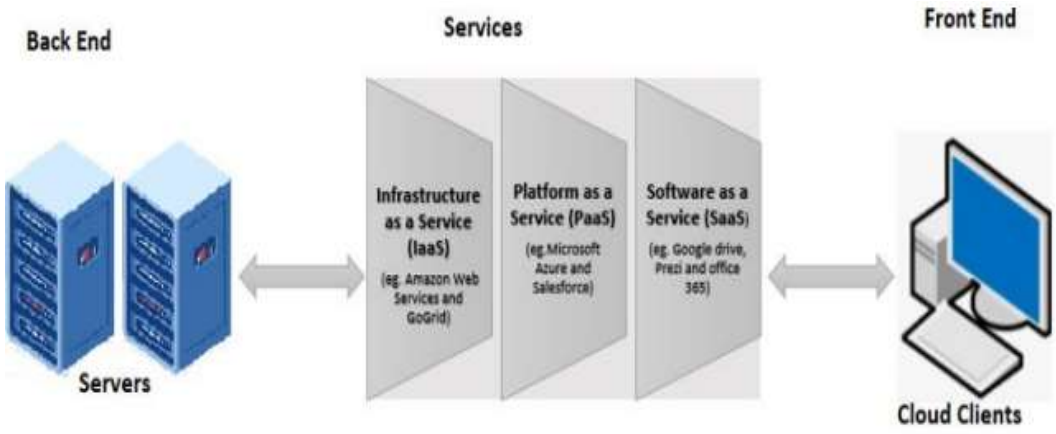

Figure 2: CC service model [29]

3. Encryption algorithm

Encryption uses the public and private keys. The message recipient owns the public key. Message encryptors own private keys. The padding scheme approach converts the message to a number, say m, during encryption.

$$c \equiv m^e \ (\mathrm{mod} n)$$

The encrypted text is calculated via exponentiation by squaring. The receiver receives cipher text c instead of m after the formula is executed.

3.1 Types of encryption algorithm

Data encryption algorithms are divided.

3.1.1 Symmetric

This cryptography uses one key for encryption and decryption. Both sender and recipient should know the same key to encrypt and decrypt. Examples of encryption include DES, Triple DES, AES, RC5, etc [30].

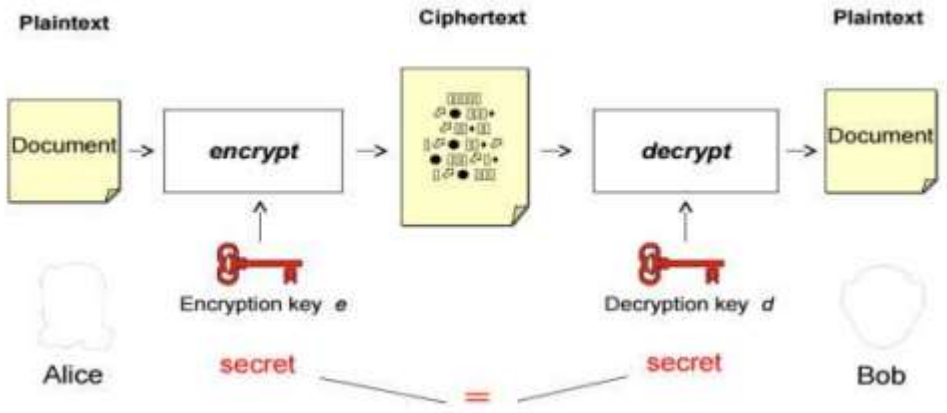

Figure 3: Symmetric Encryption Algorithm [39]

- **DES:** The DES symmetric-key technique was once popular for electronic data encryption. It greatly advanced academic cryptography [31].
- **Triple DES:** DES's 56-bit key size was sufficient when created, but computing power permitted brute-force assaults. Increase DES key size with Triple DES to counter such attacks without inventing a new block cipher algorithm [32].
  - **SHA-I:** Secure Hash Algorithm (SHA)-1 computes data hashes [33]. SHA-1 is more popular than SHA-0 because it fixes SHA hash specification issues that caused weakness.
  - **AES:** AES is a symmetric key encryption/decryption technique that converts plaintext to ciphertext and vice versa [34]. The master key must be hidden or with a trustworthy third party to protect data.

3.1.2 Asymmetric

For encryption and decryption, this cryptographic method uses different keys. A public key is used to encrypt a message or data [35]. The message receiver decrypts with another secret key.

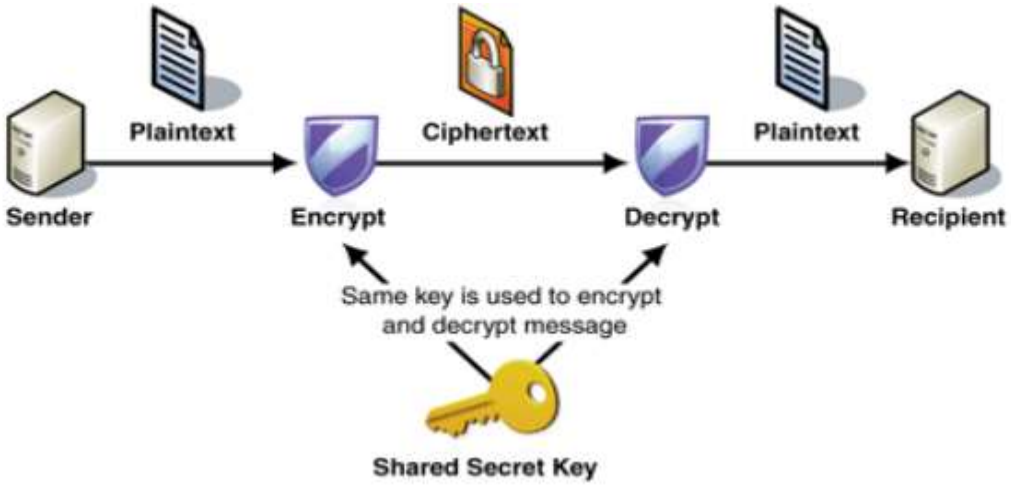

Figure 4: Asymmetric Encryption Algorithm [39]

This encryption limits public and private keys to one use. Such encryption may include RSA, Elliptic Curve, etc. Multi-key encryption and decryption are employed in this cryptographic approach. An encrypted message or data uses a public key. The message receiver decrypts with another secret key. This encryption limits public and private keys to one use. Such encryption may include RSA, Elliptic Curve, etc. [36].

- **RSA:** This web secret authentication method leverages Ron Rivest, Adi Shamir, and Adleman's 1977 algorithm. The most used secret writing algorithm is RSA. It's the only algorithm for private and public key generation and secret writing. Fast encryption [37].
- **Diffie-Hellman:** Diffie-Hellman key exchange [38] may help exchange cryptologic keys. It's one of the first functional cryptography key exchange examples. With Diffie–Hellman key exchange, two parties can share a secret key via an unsecure channel without previous knowledge. In subsequent communications, isobilateral key cipher will be used [39].

Table 1: Comparison of existing literature Review

Author & Year	Algorithm	Focus	Key Findings	Advantage	Disadvantage
Santhi Baskaran, Isaiarasi (2017) [40]	AES Algorithm, RSA algorithm, Triple- DES, Diffie-Hellman Blowfish Algorithm	Improving security in cloud storage environments	To secure cloud storage, discusses encryption methods.	Improved security for cloud environment	Lack of data confidentiality and integrity
Athulya, V. S et.al (2020) [41]	AES (Asymmetric encryption system) algorithm, RSA algorithm	Securing data before uploading to cloud	Covers existing cryptographic approaches to improve security in cloud environments	Enhanced data security for cloud storage	Lack of detailed performance analysis
Mewada, Shivlal, et al. (2015) [42]	AES, DES, Blowfish and RSA Algorithm	Enhancing data security in clouds environments	Discusses cloud data security and presents performance analysis of encryption algorithms	Improved data security in cloud computing	Limited discussion on specific encryption algorithms and their efficacy
Shukla, Dhirendra et.al. (2021) [43]	DES, AES, Blowfish Algorithm	Analyzing performance and comparing with traditional	Proposes an encryption-based cloud computing algorithm and compares its	Better performance compared to traditional algorithms	Lack of comparison with a wide range of encryption algorithms

		encryption algorithms	performance with traditional algorithms		
Rani, Shikha et.al. (2016) [44]	DES, AES, Blowfish, RSA Algorithm	Providing effective security solutions for managing data in the cloud	Emphasizes on various encryption techniques and effective security solutions for managing data in the cloud	Enhanced security solutions for managing data in the cloud	Limited discussion on performance improvement
Ghosh, Papri et.al. (2017) [45]	AES algorithm, Blowfish algorithm, DES algorithm, RSA algorithm	Addressing security and privacy challenges in cloud storage	Presents a comparative study of various security algorithms for addressing security and privacy challenges in cloud storage	Provides insight into various security options for cloud storage	May lack in-depth analysis of individual algorithms

DISCUSSION

Cloud computing platforms must encrypt sensitive data for privacy, integrity, and secrecy. The advantages and downsides of cloud encryption are examined in this thorough study. When considering cloud computing, encryption strength, computational complexity, key management, and cryptographic attack resistance are considered. The encryption mechanism affects system speed, resource use, and scalability. Cloud data can be protected by intelligent encryption method selection using cloud computing security encryption algorithm analysis. New encryption methods and discoveries will test cloud computing security, the research predicts.

Cloud computing dominates networking systems, providing scalable internet services through virtualization. It lets users access "Cloud" data and programs from phones, laptops, and PCs. Integration of Hotmail and Gmail onto cloud systems has increased accessibility. It's popular for Broad Network Access, Rapid Elasticity, Measured Service, On-Demand cloud computing, and Resource Sharing. Despite its benefits, cloud computing raises security risks. Third-party cloud data and infrastructure management puts sensitive data at danger. Cloud service providers use password-protected accounts, but security breaches can harm customers and organizations. Beyond data breaches, cloud computing security considerations include data storage, transport, and user authorization. Cloud data must be encrypted and decoded securely to avoid

unauthorized access. Protecting internet data packets requires secure data transfer mechanisms. Avoiding unwanted access to other users' data and documents requires stringent user access restrictions.

Cloud computing uses numerous encryption techniques and concepts to handle security issues. Asymmetric encryption techniques like RSA and Diffie-Hellman employ separate keys for encryption and decryption, while symmetric algorithms like DES, Triple DES, and AES use a single key. These cloud encryption methods protect data privacy and integrity. Cloud computing security is complex and growing despite encryption methods and security concepts. SaaS users relying on vendors for security face considerable data security threats. To gain consumer trust, cloud service providers must safeguard data storage, transport, and user authorization.

CONCLUSION

In conclusion, the adoption of Cloud computing transformed data and application management for organizations and individuals. However, with the convenience and flexibility provided by cloud computing comes the inherent challenge of ensuring data security and privacy. This study delves into the intricacies of encryption algorithms as a vital component of information security in cloud computing environments. The analysis reveals that while cloud computing offers numerous benefits, it also introduces significant security concerns. These concerns primarily revolve around data security, including secure data storage, secure data transfer, and user permissions. The importance of implementing robust encryption mechanisms to mitigate these security risks and build trust among cloud service users. Furthermore, the study explores the architecture of cloud security, highlighting the different cloud deployment and service models. It elucidates the role of encryption algorithms in securing data transmission and storage within the cloud environment. Moreover, the study provides a comprehensive overview of encryption algorithms, categorizing them into symmetric and asymmetric encryption. It discusses prominent encryption algorithms such as DES, Triple DES, AES, SHA-1, RSA, and Diffie-Hellman, outlining their strengths, weaknesses, and applications in cloud security. In essence, this detailed study and analysis underscore the critical importance of encryption algorithms in safeguarding sensitive data and ensuring information security in cloud computing. The intricacies of encryption algorithms and implementing robust security measures, organizations can reduce hazards with cloud computing and foster a secure and trusted computing environment for their users.

REFERENCE

1. Maryoosh, Amal Abdulbaqi, Rana Saad Mohammed, and Raniah Ali Mustafa. "Subject Review: Cloud Computing Security Based on Cryptography." International Journal of Engineering Research and Advanced Technology-IJERAT (ISSN: 2454-6135) 5.9 (2019): 20-23
2. Jeffrey Voas and Jia Zhang, “Cloud Computing: New Wine or Just a New Bottle?”, IEEE Computer Society, 2009.
3. Sameeh A. Jassim, MSc thesis, “Mediated IBC-Based Management System of Identity and Access in Cloud Computing”, College of Computer, University of Anbar, 2013.
4. SameeraAbdulrahmanAlmulla and Chan YeobYeun, “Cloud Computing Security Management”, Engineering Systems Management and Its Applications (ICESMA), Presented at 2nd IEEE International Conference, 30 march 2010.
5. Ijifr VE. Load Balancing And Security In Multicloud IaaS Using Distributed File System- A Review. International Journal of Informative & Futuristic Research; Volume 2 Issue 4 , December 2014, Page No. 1051-1055.

6. Kumar R, Pandey A. A Survey on Security Issues in Cloud Computing. IOSR J Comput Eng. Volume 3 Number 3:2016,pp506-517
7. Vouk M a. Cloud computing — Issues, research and implementations. ITI 2008 - 30th Int Conf Inf Technol Interfaces. pp:235-246,2008.
8. Hu Y, Wong J, Iszlai G, Litoiu M. Resource Provisioning for Cloud Computing. published 2009 in CASCON (Center for Advance Studies Conference); March 22,2009, pp:101-111.
9. Ahead S. Cloud Computing : Silver Lining or Storm Ahead?.IA News Letter The Newsletter for Information Assurance Technology Professionals Volume 13 Number 2 , Spring 2010.
10. Catteddu D, Hogben G. Cloud Computing.The European Network and Information Security Agency (ENISA);Volume 72 Number 1 , 22 March 2009, pp:2009-2013.
11. Jamil D, Zaki H, Carlin S, Curran K. Cloud Computing Security. Int J Ambient Comput Intell. 2011;Volume 3 Number 1, pp:14- 19,2011.
12. Kumar G, Chelikani A. Analysis of Security Issues in Cloud Based E-Learning. Secur Manag. Universirt of BORAS(School of Business and IT),pp:1-74, 2011.
13. Shan L. Journal Of Computers and math.pdf; Recent Advances in Intelligent Information
14. Technology& Network Security; ISSN 1796-203X Volume 6, Number 10, October 2011.
15. Sadeghi A, Schneider T, Winandy M, Horst G. Token-Based Cloud Computing. TRUST 2010; Springer-Verlag Berlin Heidelberg. Volume 2: LNCS 6101, pp. 417–429;2010
16. Hussain, Abid, Chungen Xu, and Muqadar Ali. "Security of cloud storage system using various cryptographic techniques." International Journal of Mathematics Trends and Technology (IJMTT) 60.1 (2018): 45-51.
17. K.Hashizume, D.G. Rosado, E. Fernandez-Medina, and E.B. Fernandez, “An analysis of security issues for cloud computing,” Journal of Internet Services and Application, 4:5, Feb 2013.
18. JW. Rittinghouse and JF Ransome, “Security in the Cloud,” In: Cloud Computing. Implementation, Management, and Security, CRC Press, 2009.
19. S. Subashini and V.Kavitha, “A survey on Security issues in service delivery models of Cloud Computing,” Journal Network and Computer Applications, vol. 34(1), pp. 1-11, 2011.
20. J Viega, “Cloud Computing and the Common Man,” Journal Computer vol. 42(8), pp. 106-108, Aug 2009.
21. Beckham, The top five security risks of cloud computing, Available on internet: http://blogs.cisco.com/smallbusiness/the-top-5-securityrisks-of-cloud-computing, 2011.
22. Pitchay, Sakinah Ali, et al. "A proposed system concept on enhancing the encryption and decryption method for cloud computing." 2015 17th UKSim-AMSS International Conference on Modelling and Simulation (UKSim). IEEE, 2015.
23. M. N. O. Sadiku, S. M. Musa, and O. D. Momoh, “Cloud computing: Opportunities and challenges,” IEEE Potentials, vol. 33, no. 1, pp. 34–36, Jan. 2014, doi: 10.1109/MPOT.2013.2279684
24. B. S. P. Mishra, H. Das, S. Dehuri, and A. K. Jagadev, Cloud computing for optimization: Foundations, applications, and challenges, vol. 39. Cham: Springer International Publishing, 2018.
25. K. G. Al-moghrabi, A. M. Al-ghonmein, and M. Z. Alksasbeh, “Towards a cloud computing success model for hospital information system In Jordan,” International Journal of Advanced Trends in Computer Science and Engineering, vol. 10, no. 2, pp. 1121–1127, Apr. 2021, doi: 10.30534/ijatcse/2021/891022021.
26. Z. N. Rashid, S. R. M. Zebari, K. H. Sharif, and K. Jacksi, “Distributed cloud computing and distributed parallel computing: A review,” in 2018 International Conference on Advanced Science and Engineering (ICOASE), Oct. 2018, no. June, pp. 167–172, doi: 10.1109/ICOASE.2018.8548937
27. M. Ali, S. U. Khan, and A. V. Vasilakos, “Security in cloud computing: Opportunities and challenges,” Information Sciences, vol. 305, pp. 357–383, Jun. 2015, doi: 10.1016/j.ins.2015.01.025.
28. S. Singh, Y.-S. Jeong, and J. H. Park, “A survey on cloud computing security: Issues, threats, and solutions,” Journal of Network and Computer Applications, vol. 75, pp. 200–222, Nov. 2016, doi: 10.1016/j.jnca.2016.09.002.
29. Alemami, Yahia, et al. "Cloud data security and various cryptographic algorithms." International Journal of Electrical and Computer Engineering 13.2 (2023): 1867.

30. P. Mahajan and A. Sachdeva "A Study of Encryption Algorithms AES DES and RSA for Security" ,Global Journal of Computer Science and Technology Network Web & Security,vol. 13 no. 15 2013.
31. P. Liu H. Chang and C. Lee "A true random-based differential power analysis countermeasure circuit for an AES engine" ,IEEE TRANSACTIONS on CIRCUITS and SYSTEMS-II: EXPRESS BRIEFS,vol. 59 no. 2 pp. 103-107 2012.
32. Q. CHEN Z. TANG Y. LI Y. NIU and J. MO "Research on Encryption Algorithm of Data Security for Wireless Sensor Network" ,Journal of Computational Information Systems, pp. 369-376 2011.
33. O.A. Hamdan and B.B. Zaidan "New Comparative Study Between DES 3DES and AES within Nine Factors" ,Journal Of Computing, vol. 2 no. 3 March 2010
34. M. Yeşiltepe, E. Kaçmaz and M. Kurulay, "Study triple data encryption standart encryption algorithm in windows communication foundation environment," 2016 Electric Electronics, Computer Science, Biomedical Engineerings' Meeting (EBBT), Istanbul, 2016, pp. 1-4.
35. S. Chandra, S. Bhattacharyya, S. Paira and S. S. Alam, "A study and analysis on symmetric cryptography," Science Engineering and Management Research (ICSEMR), 2014 International Conference on, Chennai, 2014, pp. 1-8.
36. H. Hayouni, M. Hamdi and T. H. Kim, "A Survey on Encryption Schemes in Wireless Sensor Networks," Advanced Software Engineering and Its Applications (ASEA), 2014 7th International Conference on, Haikou, 2014, pp. 39-43.
37. G. Padmavathi and D. Shanmugapriya "A Survey of Attacks Security Mechanisms and Challenges in Wireless Sensor Networks",(IJCSIS'09) International Journal of Computer Science and Information Security,vol. 4 no. 1&2 2009.
38. R. Mathur, S. Agarwal and V. Sharma, "Solving security issues in mobile computing using cryptography techniques — A Survey," Computing, Communication & Automation (ICCCA), 2015 International Conference on, Noida, 2015, pp. 492-497.
39. Chinnavedampatti, Saravanamptty. "Comparative Study on Data Encryption Algorithms in Cloud Platform.(2017)"
40. Santhi Baskaran, Isaiarasi A. "Survey on Data Security using Encryption Algorithms in Cloud Environment." (2017).
41. Athulya, V. S., and E. D. Dileesh. "Study on Encryption Techniques Used to Secure Cloud Storage System." (2020).
42. Mewada, Shivlal, et al. "Performance analysis of encryption algorithm in cloud computing." International Journal of Computer Sciences and Engineering 3 (2015): 83-89.
43. Shukla, Dhirendra KR, Vijay KR Dwivedi, and Munesh C. Trivedi. "Encryption algorithm in cloud computing." Materials Today: Proceedings 37 (2021): 1869-1875.
44. Rani, Shikha, and Shanky Rani. "Data Security in Cloud Computing Using Various Encryption Techniques." International Journal of Modern Computer Science, ISSN (2016): 2320-7868.
45. Ghosh, Papri, Vishal Thakor, and Dr Pravin Bhathawala. "Data Security and Privacy in Cloud Computing Using Different Encryption Algorithms." International Journal of Advanced Research in Computer Science and Software Engineering 7.5 (2017).