JOURNAL OF AERONAUTICAL MATERIALS
ISSN: 1005-5053

Vol. 43, Issue-01, 2023
pp. 953-960

BIG DATA ANALYSIS: PRESERVING SECURITY & PRIVACY WITH HYBRID CLOUD COMPUTING ENVIRONMENT

Lakshmi B.S.
Guest Lecturer of Computer Science, Department of Computer Science, Sunrise University, Alwar, Rajasthan
Email ID: lakshmibs17@gmail.com

Dr. Nabeena Ameen
Assistant Professor (Sr gr), Information technology, B.s.abdur rahman crescent Institute of science and technology, Vandalur , Chennai
Email ID: nabeena@crescent.education

Abdul Rahiman Shaik Kodavendla
Lecturer, College of Computing and Information Sciences, University of Technology and Applied Sciences, Muscat, Oman
Email ID: abdulrahiman@hct.edu.om

Subir Chakraborty
Assistant Professor, Department of Computer science and engineering, Haldia Institute of Technology, Haldia, East Midnapore, West Bengal
Email ID: subirchak@gmail.com

Imad Salim Rashid AL Barwani
L&D Manager, Muscat, Oman
Email ID: emadbarwani@gmail.com

Mrs. Shikha
Assistant Professor, Department of Computer Science and Applications, Himachal Pradesh University Regional Centre Mohli, Khaniyara, Dharamshala (H.P.)
Email ID: dhimanshikha15@gmail.com

Abstract:

Big data analytics is a crucial technology advancement currently utilized in several commercial domains globally. The storage of big data in cloud environment presents challenges in user privacy & sensitive data preservation in unreliable cloud servers, whereas it is more challenging for the hybrid cloud due to the integrated framework. This investigation's primary objective is to determine a reliable framework for big data security & privacy in a hybrid cloud environment. This research looks to identify & comprehend efficient security & privacy algorithms for big data security & privacy in a hybrid cloud environment. The study has been performed with a contextual analysis followed with a discussion on insights obtained. In the final, according to the insights obtained, Blowfish algorithm has been chosen effective small data sets & Bilinear pairing technique has been identified efficient for all data types.

Keywords: *Hybrid cloud, Privacy, Security, Big data, Blowfish*

1. Introduction:

Cloud computing has emerged as one of the most promising new areas of business in the information technology sector in recent years. The most recent survey indicated that the market share of cloud computing has been 21% more in 2022 than it was in the previous year (Faridi et al., 2022). The cloud offers a variety of services, including infrastructure, platforms, & software; however, the provision of security for huge amounts of data stored in the cloud is the most important challenge. In general, sensitive information is preserved in the cloud environments for medical data, military data, & government data; nevertheless, the user is unsure of the level of security given by the service providers for these environments (Shekhawat et al., 2019).

The concept of hybrid clouds refers to circumstances in which interactions between two separate deployments may be required, however these deployments continue to be linked using appropriate technology. A private environment can be connected to one or more public clouds to create what is known as a hybrid cloud. It is possible to safeguard the confidentiality of user information by separating it into sensitive & non-sensitive categories, & then only sending the non-sensitive data to a public cloud storage location. The sensitive information is kept in the user's own personal cloud storage (Chinnasamy et al., 2021). The cloud is home to a wide variety of resources, including networks, operating systems, database management, & memory management, & all of these components are susceptible to various types of assaults. As a result, safety & privacy are extremely important aspects of cloud computing, attempts to develop security algorithms were evident with intense focus (Sajay et al., 2019).

The research focuses on the safety & privacy of big data stored in the hybrid cloud. The users generally save their data within the cloud; however, they need to possess a privacy & security method to protect their sensitive information, such as health care data, bank details, & military data, from being accessed by unauthorized parties. The objective of the study is to analyse & comprehend a privacy & security prevention method for big data storage environments with hybrid cloud framework.

2. Literature Review:

2.1 Privacy & security for hybrid cloud:

Sheena Hussaini, (2020) reported on a reliable solution that ensures data confidentiality & integrity in cloud storage for transmission & storing responsibilities. The study demonstrated that the suggested optimal blowfish encryption strategy achieved the highest level of cyber security in cloud storage by achieving the fastest key breaking time when compared to the blowfish, Rivest–Shamir–Adleman (RSA), & Advanced Encryption Standard (AES) algorithms. The security framework proposed by Praveena & Rangarajan, (2020) has been implemented, & its adaptability to the hybrid cloud's security level was further investigated. The study emphasized the newly created deduplication processing algorithm for safe storage & retrieval without duplication or redundancy features the great beneficial for the hybrid cloud system privacy.

2.2 Significant frameworks:

Shanmugapriya & Kavitha, (2019) proposed a bilinear pairing cryptography with a session key generation model to safeguard healthcare private data in the cloud utilizing fog computing technology. The study concluded that pairing encryption was more secure than existing approaches & that the suggested method does not require multiplication group operations to use encryption. Shekhawat et al., (2019) discussed on a survey on privacy preservation methods. The study emphasized the need for cryptographically enforced access control & secure communication for big data since big data analysis is commonly utilized to acquire information from outsourced data & is used to make business predictions & decisions. An improved blowfish algorithm has been developed by Gangireddy et al., (2021) to address the problems with existing methods. The suggested Enhanced Blowfish Algorithm reportedly offers greater security than RSA & AES, according to the earlier study, which is similar to this one.

3. Research Method & framework study:

Due to the untrusted nature of clouds, cryptographic & diverse encryption techniques have been employed to preserve the cloud data in a private mode. Several encryption techniques such as Order preserving, Image shuffling, Key management, fog computing for cloud services & conventional techniques such as AES are few among the other proposed techniques. It has also been reported that hybrid encryption methods, such as Blowfish, RSA, AES, Eclipse, Ivanov-Dikov-Arnaudov (IDA) encryption, & Data Encryption Standard (DES), are utilized in order to improve the level of privacy afforded to information that is kept on cloud servers (Thabit et al., 2021). On-site encoding & decoding of data are included in its functionality. This technique achieves a significantly greater level of performance & protection for data files of any size, either large or small. Encryption & decryption using this approach are both straightforward & extremely safe. The aforementioned technique provides a straightforward structure that is suitable for the cloud environment. Camelia, Secure Force (SF), Blowfish, & DES ciphers are only some examples of well-known & widely used ciphers.

3.1 Method:

In focus to establish an effective security & privacy approach for hybrid cloud systems, performance insights reported on three distinct algorithms, notably Bilinear pairing, DSRBACA, & blowfish algorithm, have been analysed & compared. Efficient techniques are discussed followingly. The study has been performed with an insight analysis & discussion-based approach on the security & privacy frameworks for hybrid cloud system. The hypothesis based on the efficient framework will be comprehended.

3.2 Frameworks analysed:

i. *Bilinear Pairing methodology:*

The bilinear pairing is accomplished by employing a variety of application phases, including bilinear maps, complexity implications, & cryptographic techniques, amongst others. This cloud database needs to be protected from assaults & invasions, & it must also be protected from any changes that might be made (Shivani & Sarika, 2021). As a result, there is a requirement for an efficient & helpful mechanism for the detection of a change in integrity, which can be accomplished through the process of bilinear pairing. The data that is kept in the database is subjected to a hash key creation procedure, which enables this task to be completed successfully. This operation of hash key evaluation takes place over the course of a predetermined amount of time, & the hash keys are stored in the database in the form of pairs that are referred to as the Bilinear Pairs. The evaluation of the bilinear pairings is what is used to determine whether or not the data that is being saved on the considered cloud Database has been altered in any way. The evaluation of the bilinear pairings is critical & important to achieving the dependability & security goals for the database. The computational complexity is not overly strained by the implementation of the Bilinear Pairs evaluation, which keeps it within feasible constraints. The framework has been adopted from Shanmugapriya & Kavitha, (2019).

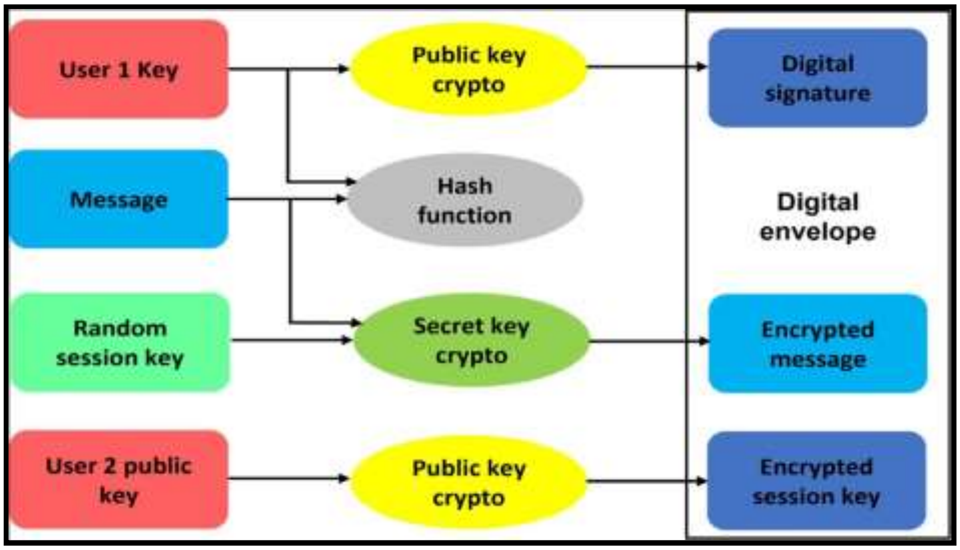
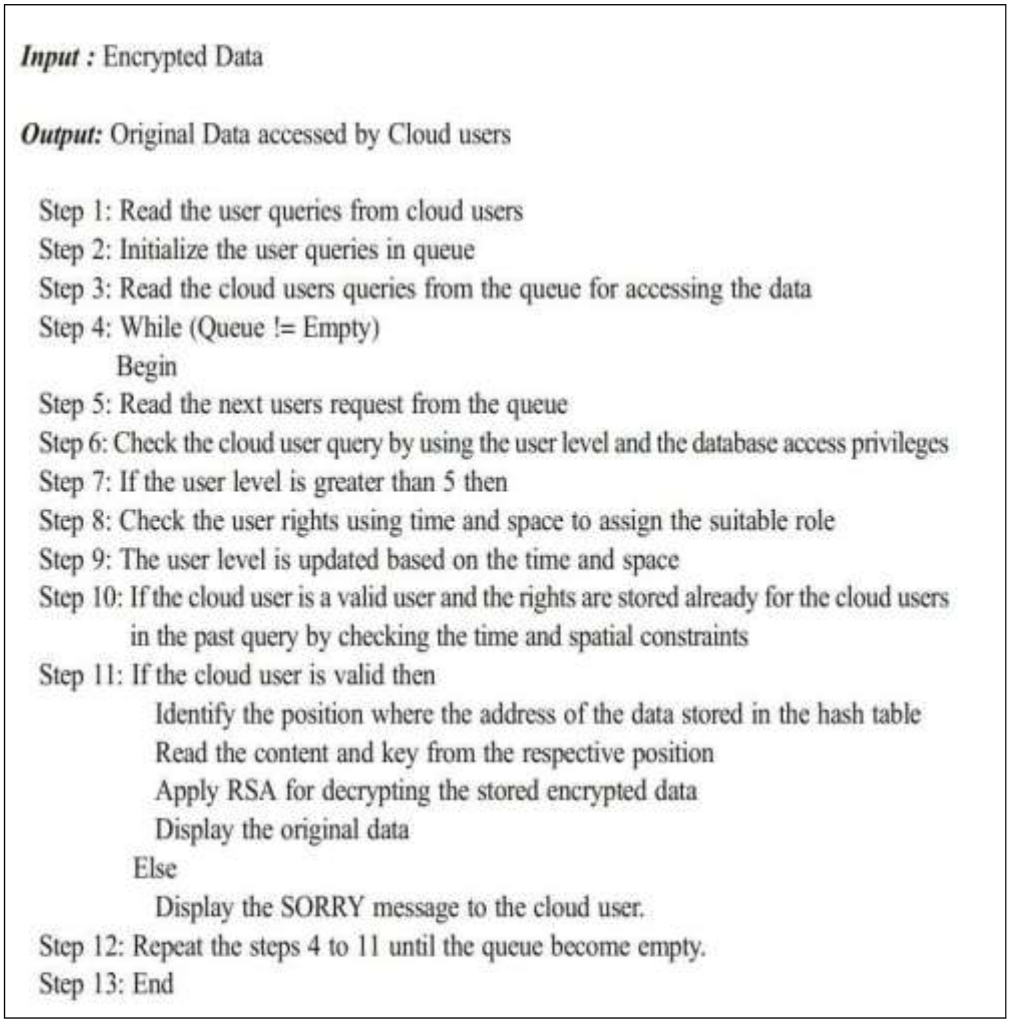


Figure 1: Bilinear Pairing methodology with key generation

ii. Dynamic Spatial Role Based Access Control Algorithm (DSRBACA):

DSRBACA is an algorithm that is utilized for the purpose of restricting the ability of cloud users to access the data or documents stored in the cloud database according to the role in the organisation (Praveena & Rangarajan, 2020). Here, the users have the ability to change their responsibilities in this task on a regular basis, & they can also dynamically manipulate the roles of other users. The DSRBACA that has been proposed has the ability to dynamically assign various roles to the different cloud users depending on the circumstances that are present. The DSRBACA that is being developed has the additional capability of enabling cloud users to access data in a manner that is dynamically dependent on the place from which they originate. The locations of cloud users will be detected & monitored by the proposed DSRBACA in order to finalize the responsibilities those users will play in accessing their own company's data.



```
Input : Encrypted Data

Output: Original Data accessed by Cloud users

  Step 1: Read the user queries from cloud users
  Step 2: Initialize the user queries in queue
  Step 3: Read the cloud users queries from the queue for accessing the data
  Step 4: While (Queue != Empty)
          Begin
  Step 5: Read the next users request from the queue
  Step 6: Check the cloud user query by using the user level and the database access privileges
  Step 7: If the user level is greater than 5 then
  Step 8: Check the user rights using time and space to assign the suitable role
  Step 9: The user level is updated based on the time and space
  Step 10: If the cloud user is a valid user and the rights are stored already for the cloud users
           in the past query by checking the time and spatial constraints
  Step 11: If the cloud user is valid then
             Identify the position where the address of the data stored in the hash table
             Read the content and key from the respective position
             Apply RSA for decrypting the stored encrypted data
             Display the original data
           Else
             Display the SORRY message to the cloud user.
  Step 12: Repeat the steps 4 to 11 until the queue become empty.
  Step 13: End
```

Figure 2: Algorithm for *DSRBACA* framework (Praveena & Rangarajan, 2020)

iii. Blowfish Algorithm:

The blow fish method is employed to develop cloud security & privacy improvements. The security key is generated using the blowfish technique. A symmetric key block is then generated for the technique's encryption & decryption. One of the most reliable cypher algorithms is the blowfish key algorithm (Dinesh & Ramesh, 2021).

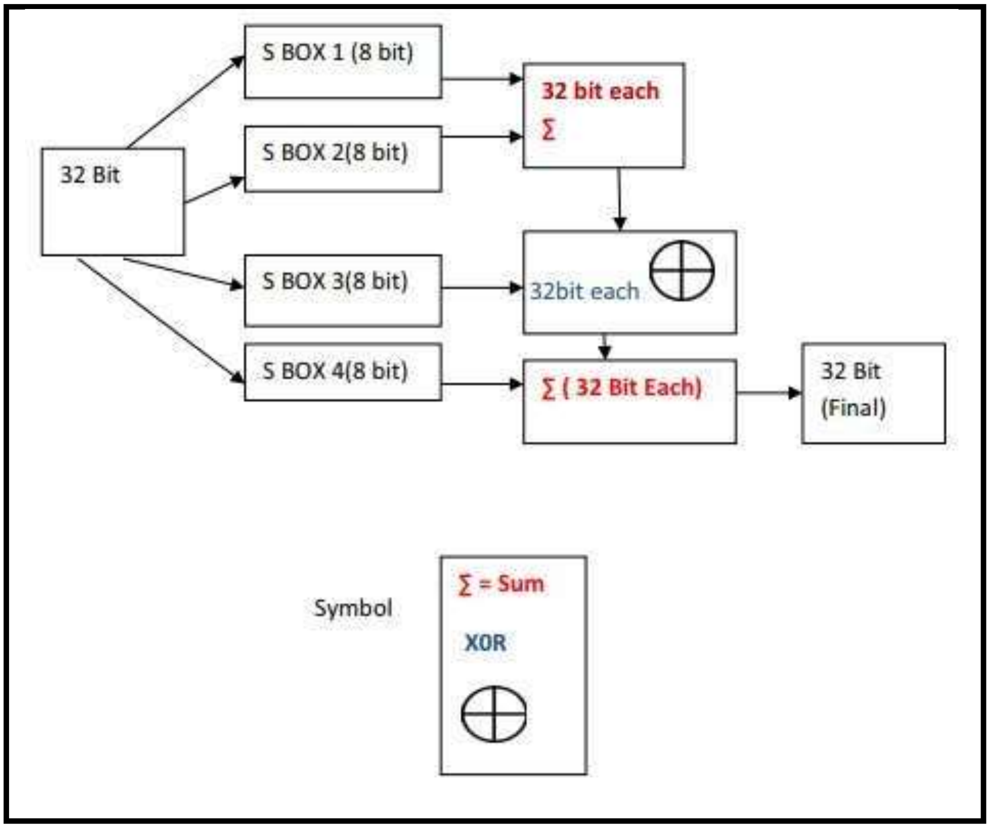


Figure 3: Blowfish algorithm for encryption (Gangireddy et al., 2021)

The secret policy of the username is acquired, along with the user's attributes, to obtain the encryption key for the random data in the name. The real file can be retrieved from the decryption method which was used to access the data by using the random key. Using HTTPS, a secure communication technology, the encrypted message is transferred to the cloud. These give the owner of cloud-based data another level of security using the same cloud infrastructure. Blocks are 64 bits long, & communications longer than 8 bytes are ignored (Sheena Hussaini, 2020).

4. Discussion:

Notably, the suggested DSRBACA is effective in comparison with the standard role-based security model in terms of restricting cloud users' count & providing accuracy in detection & prevention that is greater than 90%. This is because the de-duplication method utilised in this novel security framework is efficient & secure, & decisions are made while taking into account both time & spatial restrictions. In DSRBACA, the private key was reported to be generated as per the role of the user in the organisation & the ability to modify or handle the data in cloud has been allocated, respectively. Whereas the algorithm for blow fish encryption uses a process called key generation to produce a safe key to be utilised for both the process of decoding & the process of encoding.

Blowfish is a symmetric block cipher that may be used for the purpose of protecting the data in a secure manner. The same key is used for the function of decryption as it is for the function of encryption. The advantages of utilizing the blow fish encryption method have been determined to include a block size of 64 bits, the ability to manipulate big data blocks, an effective algorithm, expandable keys ranging from 32 bits to 256 least bits, & the capability to carry out operations in an easy manner. A different name for the blow fish algorithm is variable length cipher of key block. This can be used for a wide variety of applications due to the fact that the key does not change, & it is far faster than the majority of encryption methods.

Shanmugapriya & Kavitha, (2019) had reported the performance of the bilinear pairing approach along with the key size & performance time consumption of the model. The study also included the performance time consumption. By utilizing this strategy, the user was able to obtain both a high rate of data processing efficiency & a satisfactory level of protection using the technique that was suggested.

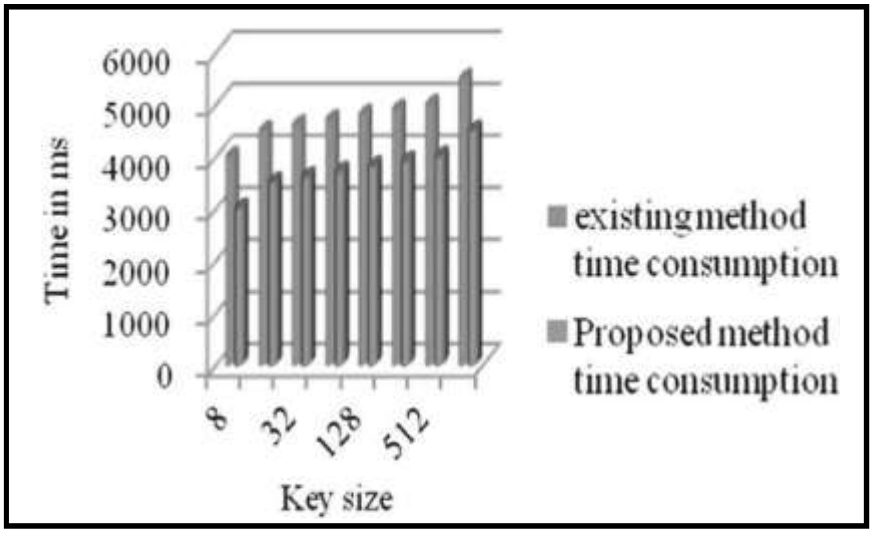


Figure 4: Time consumption analysis of Bilinear pairing algorithm reported in Shanmugapriya & Kavitha, (2019)

The safety & integrity of data saved in the cloud are both improved by using discussed Blowfish & Bilinear pairing algorithms, but the data can still be accessed on demand. Among the discussed algorithms it was evident that Blowfish algorithm is ease of implementation & usage whereas other algorithm has an above average level of complexity. Despite the complexity, Bilinear algorithm showed better time consumption with better key size, which can be considered prominent choice for security purpose for intense & sensitive files. The above discussed algorithm is capable of providing protection against some of the most common types of threats to information security, including related-key attacks, weak key attacks, symmetric characteristics, & differential & linear cryptanalysis.

5. Conclusion:

Computing is still viewed as an on-demand service on the cloud, which is a new & emerging paradigm. As soon as a company decides to move its operations to the cloud, it forfeits control over the data. Hence, authenticated computing & encryption are necessary for cloud security. In this research work, the insights from the contextual analysis on efficient algorithms has been analysed & reported as an intention to preserve the security & privacy for hybrid cloud environments. From the discussion, it is evident that the Blowfish algorithm has been chosen effective small data sets as it has accessibility to 64 KB data sets & Bilinear pairing technique has been identified efficient for all data types due to its adaptability & time consumption reported. In the future work, both the algorithms will be optimized to accomplish advancements in terms of speed, efficiency, & real-time implementation.

6. References:

1. Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient data security using hybrid cryptography on cloud computing. *Lecture Notes in Networks & Systems*, *145*. https://doi.org/10.1007/978-981-15-7345-3_46
2. Dinesh, E., & Ramesh, S. M. (2021). Security Aware Data Transaction Using Optimized Blowfish Algorithm in Cloud Environment. *Journal of Circuits, Systems & Computers*, *30*(1). https://doi.org/10.1142/S0218126621500043
3. Faridi, F., Sarwar, H., Ahtisham, M., Kumar, S., & Jamal, K. (2022). Cloud computing approaches in health care. *Materials Today: Proceedings*, *51*, 1217–1223. https://doi.org/10.1016/J.MATPR.2021.07.210
4. Gangireddy, V. K. R., Kannan, S., & Subburathinam, K. (2021). Implementation of enhanced blowfish algorithm in cloud environment. *Journal of Ambient Intelligence & Humanized Computing*, *12*(3), 3999–4005. https://doi.org/10.1007/S12652-020-01765-X
5. Praveena, D., & Rangarajan, P. (2020). A machine learning application for reducing the security risks in hybrid cloud networks. *Multimedia Tools & Applications*, *79*(7–8), 5161–5173. https://doi.org/10.1007/S11042-018-6339-0
6. Sajay, K. R., Babu, S. S., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using hybrid encryption algorithm. *Journal of Ambient Intelligence & Humanized Computing*. https://doi.org/10.1007/S12652-019-01403-1
7. Shanmugapriya, E., & Kavitha, R. (2019). Medical big data analysis: preserving security & privacy with hybrid cloud technology. *Soft Computing*, *23*(8), 2585–2596. https://doi.org/10.1007/S00500-019-03857-Z
8. Sheena Hussaini. (2020). Cyber Security in Cloud Using Blowfish Encryption. *International Journal of Information Technology (IJIT)*, *6*(5).
9. Shekhawat, H., Sharma, S., & Koli, R. (2019). Privacy-preserving techniques for big data analysis in cloud. *2019 2nd International Conference on Advanced Computational & Communication Paradigms, ICACCP 2019*. https://doi.org/10.1109/ICACCP.2019.8882922
10. Shivani, & Sarika. (2021). Handling big data security & Service through bilinear pairing & parallel computation. *IJARIIE*, *7*(4).
11. Thabit, F., Alhomdy, A. P. S., Al-Ahdal, A. H. A., & Jagtap, P. D. S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. *Global Transitions Proceedings*, *2*(1), 91–99. https://doi.org/10.1016/J.GLTP.2021.01.013