Journal of
Data Acquisition and Processing

ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777958

UTILIZING MULTI-STAGE AUTHENTICATION AND AN OPTIMIZED BLOWFISH ALGORITHM FOR EFFECTIVE SECURE DATE RETRIEVAL ON CLOUD COMPUTING

K. Kanaka Durga[1*], Dr.Venkata Kishore Kumar Rejeti[2], Dr.G.Rajesh Chandra[3], R.Ramesh[4]

[1*]M.Tech Student, Department of CSE, KKR & KSR Institute of Technology and Sciences, Guntur, AP, India.

[2,3,4]Professor, Department of CSE, KKR & KSR Institute of Technology and Sciences, Guntur, AP, India.

***Corresponding Author:** K. Kanaka Durga

*M.Tech Student, Department of CSE, KKR & KSR Institute of Technology and Sciences, Guntur, AP, India.

Abstract

Since cloud computing offers so many benefits, including widespread adoption and low cost, it plays a significant part in today's information technology. Additionally, it offers several areas for various Internet users and enables rapid data storage and transmission across zones. Cloud users can avoid making expensive investments. Put additional storage and IT infrastructure towards your core business. Due of this, a lot of businesses and organisations have moved their work to the cloud. However, due to privacy and security concerns, many consumers are hesitant to use the cloud.

This study uses the multi-level recognition (MSA) and optimisation blowfish algorithm (OBA) to solve the problem and generates useful data. Three steps make up the planning process: MSA, data security, and data recovery. Users of the cloud first saved their data there using a multi-factor authentication system. Data is encrypted using OBA when it is switched off. The binary crow search method is used to carefully choose the keys in order to maintain the system's security. MSA-based information recovery is accomplished following the encryption procedure. This will stop data from being utilised brute force by unauthorised individuals. Python has been used to implement the method's performance, and a demonstration has been conducted.

INTRODUCTION

Scientific community (De la Prieta et al., 2019). Cloud computing (CC) business technology has always been effective and has been used worldwide, even in recent years. Only by usage do they get paid. Pay-as-you-go is the name of this strategy (Kumar et al. 2019). In the digital era, storage is one of the most crucial and expensive financial resources. In the CC sector, it is one of the most well-liked services (Helmi et al., 2018). Due to the simple access to storage, many organisations and corporations store their data in the cloud. A few noteworthy examples of cloud data storage are Apple's iCloud, Amazon Simple Storage Service (S3), and Amazon Elastic Compute Cloud (EC2). However, cloud computing security is a major problem. Several cryptographical algorithms and control arrangements have been established to overcome safety problem. The safety area is strongminded as three points such as confidentiality, reality and serviceability. Cryptography is about the privacy of data in the cloud. Access control procedures are used to access cloud storage data. Administration technology not only assurances successful entree request from valid operators, but also hunks entree by unauthorized operators and solves practical problem against misuse of valid users.

Traditional access control is founded on self-identification technique and work in the field of united security (Vafamehr and Khodayar 2018; Li et al. 2009). A verification, biometric verification and multiple verification are formed for the access control process.
Procedures for one-step authentication can be breached. The paper suggests using biometric identification methods including fingerprint, palm print, face and voice recognition, iris acknowledgment, and retinal authentication. The benefits and drawbacks of any biometric verification method rely on a number of factors, including consistency, individuality, and verification (Kushida and Pingali 2014; Burger 2001). Utilising biometrics might be challenging since it changes how operators behave. Additionally, the majority of biometric systems need specialised equipment and a remote user that is incompatible with the internet to categorise persons. Multi-Factor Authentication (MSA) was developed to solve this issue. There are more than three levels of security at MSA.

(Kang et al., 2015; Dinesha and Agrawal, 2012; Rajani et al., 2016).
Some issues, such the maximum processing time, cost, and information loss, do not go away, though. Metaheuristic techniques have Its goal is to make cryptography algorithms run more efficiently. A new system must be developed to address the security issue in order to prevent this issue from occurring. The major choice of the approach is to use the MSA and Optimised Blowfish Algorithm (OBA) to safely transmit data from the cloud. In order to prevent unauthorised users from storing data in the cloud, MSA uses a three-level security system. Here, the binary crow search algorithm (BCSA) is uses to selected the values. Finally, data is refunded if the user is satisfying with multiple authentication methods. This way, unofficial users are excluded. The main result of the articles are as follows:

• Blowfish algorithm is used to encrypt information. To recover the Blowfish procedure, key ideas are selected using BCSA optimization.
It will hide ancient data from evil.
• It is recommended to uses the MSA transaction to avoid transaction mistakes. This will guard the doctor from bad outbreaks.

PROBLEM STATEMENT

Thanks to the technical growths in the world, people now rely on the internet to send info from one end of the world to the other. Messaging, chat, and other formats are just a few of the ways data is conveyed over the Internet. Data transmission can be done online very quickly, precisely and quickly. However, one of the main problems with sending data over the Net is the "Security risk" it poses; for Example, private or confidential information can be hidden or leaked from various angles. since it is one of the most important matters to be consider while transferring Data in this way, it is needed to considered information safety.

Both symmetric and asymmetric encoding algorithm have advantage and disadvantages. Asymmetric algorithms afford more presentation than symmetric processes, but at lesser price and with more expensive hardware. On the other hand, symmetrical encoding offers a good and financial way to protect data without security and should be consider as the best key and suitable for many arrangements satisfy. in some cases, free admittance to symmetric and asymmetric encryption may be the best option. Hybrid cryptanalysis aim to exploit the assets of both class of processes while avoiding their faults. In Symmetric Encoding Symmetrical encoding uses a key and an encryption algorithm to convert plaintext to ciphertext. The ciphertext is decrypted to disclose the plaintext using the same key and decryption procedure. The authors opinion to the extended history of symmetrical key cryptanalysis. It includes, but is no limit to, different symmetric key encoding algorithms (AES, DES, and Blow-fish).

Several encryption and authentication systems have been announced to overcome this problem, such as biometric verification, but this needs extra apparatus or hardware, and the present AES process will require a lot of calculation. To overcome this problematic, the author is here. Report on a process called the new multi-level verification concept that usages the Blowfish security process improved for data storing and rescue.

LITERATURE SURVEY

S. Vatshayan, et., al , Explain how to keep data from unauthorized access using Vigenere encoding and Polybius Square encoding algorithms. This post does good job of explanation procedure of encrypting and decrypting data using the methods provided. Finally, it provides a way of relating, use a practical map, what data can be encoded and decoded uses the above procedure.

A Research Paper on New Hybrid Cryp- tography Algorithm
Chaudhari, Swapnil. (2018).

The authors converse the design of Hybrid encoding models using symmetrical and asymmetrical encoding procedures. This Article describes the symmetrical and asymmetrical algorithm concepts in detailed, along with their advantages and disadvantages. Explain the design of a hybrid model combination binary RSA and floating ciphers. The report ends with some insights into the advantages of using a mixed methods approach. The article [3] discusses the application of similar hybrid cryptography methods in wireless sensor networks (WSN).

Next, the article briefly discusses the security aspect of WSNs. In this study, the procedure of combination cryptographic rules is conversed. It also assesses the efficiency of the method (encryption and decryption) using a simulation model and monitoring the results of ciphertext size, throughput, and processing time

S. Immaculate et.,al Cloud computing plays an important role in today's business world with its many advantages such as improved performance, widespread access and low cost. It also provides many places for different users to store information and transfer information from one area to another nearby. Cloud customers can save on large investments in IT infrastructure and focus on their core business with more storage. For this reason, many companies or organizations have transferred their work to the cloud. However, many customers are reluctant to use the cloud due to security and privacy concerns. This will prevent unauthorized persons from attacking the data. The performance of the proposed method is achieved in JAVA and the presentation to different metrics."

R. Soundhara Raja Pandian[1] et.,at, Cloud computing has become popular in the IT industries due to its good performance, wide accessibility, little charge and other advantages. It is also a pay-as-you-go method; Therefore, cloud information can be accessed by anyone from anywhere and is used in educational an online learning platform as it is easy to use. However, many schools are reluctant to use cloud learning due to security and privacy concerns. So, in this study, numerous cryptographic algorithms including Elliptic Curve Cryptography (ECC), Advanced Encryption Standard (AES), Pisces, Blowfish, Data Encryption Standard (DES), and Triple Data Encryption Standard (TDES) are reviewed in terms of their effectiveness and accountability. In the NPTEL database, Regulatory Assessment (RBAC) security was examined and contrasted with cloud training protection management. To determine the optimal end-to-end encoding security in network systems, use the encode time, decrypt time, and retrieval time of various data sizes as an assessment topology graph. ElGamal SBO with Delta-competitive NN cryptography has also been constructed, in which the ElGamal Stag flaw optimises ElGamal encryption and quickly creates optimised keys, enabling only access to educational resources and information transmission to other buildings. Use the Delta Competitive NN, a kind of neural network that manages choices to lower the chance of explosions. The outcomes demonstrate that ElGamal SBO was ready using Delta Competitive NN. Coding takes precedence when utilised in security scenarios since cryptography outperforms all other measures in terms of recovery time, encryption time, communication cost, computational overhead, and decision-making time. Encryption can be made better.

Storage also Encoding Files verification for Cloud-Based Data Retrieval.
Mustafa Qahtan Alsudani, et.,al

The amount of data that has to be processed, saved, and updated keeps growing at the same time. Large files coming from many sources must to be kept on a safe platform. It is not required to keep a lot of data on a hard drive or computer. As a result, the cloud is the ideal platform for data storage on a massive scale. The accessibility of data stored in the cloud at any time and from any device is one of its advantages. The security of data kept in the cloud is a significant worry, though. Because of this, most users are hesitant to migrate their data to the cloud despite these benefits. Data must be encrypted before being delivered to the cloud service to prevent this issue. This is a fantastic technique to safeguard your data. Experience with the technique indicates that it is possible to search for information in an encrypted file without endangering the security and privacy of numerous information owners. Data that has been encrypted may be managed without having it decrypted using Pallier homomorphic encryption technology.

Niyanth Guruprasad, et.al, The world is moving forward when it comes to internet connectivity. While this advances connectivity and advances communication, it also comes with disadvantages. The advent of the Internet went hand in hand with the advent of hackers. This makes businesses vulnerable to terrorist attacks by various groups and organizations. To protect their customers and user data, businesses need to protect their servers and data centers, thus improving and ensuring security and closing multiple points of negativity.

Cryptography is a technique that involves encoding information and messages so that only viewers can decipher and understand it. Hybrid cryptography and integrity checks (MD5 hashes) are used to increase security. One Time Pad (OTP - symmetric) and Route cipher (transpositional) encoding methods are used together

Yi Zhang, et.,al, "Mobile devices may transfer tasks to nearby MEC servers for reduced latency and energy efficiency thanks to mobile edge computing (MEC). In a MEC system with several MEC servers, this paper tries to design crucial security activities that will necessitate data encryption and consequently use an increasing amount of power. Planning is done to shorten work completion times as well as the energy consumption of mobile devices. The resultant NP-hard issue is solved by two slow particle swarm optimisation techniques that we provide. To help the product reach the solution, we design a project-based project plan in specific. The approach is based on the best up-to-date solutions and models that work as much as possible to create good solutions that most now originate good models from good solutions. To prevent significant changes in particle activity, we are adding a new particle update strategy that slows down the movement of particles to search for the best solution based on the behavior of personal best products and world best products. Experimental results show that the proposed algorithm is better than the best combination of presentation and efficiency. The presentation of the drawing method and the particle update strategy are also measured.

Nirmaljeet Kaur1, et.,al, Cloud computing is the establishment of computing resources as a service over the Internet. Cloud computing allows the storage of user data and the estimation of applications and services provided by cloud servers. Many files are stored on cloud storage servers. Security is a major problem impeding the development of cloud computation, so cloud computing must have an encyclopedic solution. This article describes the use of Blowfish, RSA, and Hash algorithms to secure data exchange in the cloud, which can solve data security, authentication, and data integrity issues.

Data security is improved via cryptographic techniques. introduce hash technology to validate the accuracy of data. "The performance metrics for the upgraded approach (Blowfish + RSA + Hash) are compared to those for plain RSA and Blowfish, including transmission rate, encryption time, ciphertext, and latency. We developed using coupled, asymmetric, and hash algorithms, which improve on subpar performance. To guarantee the accuracy of user data in the cloud, TPAs must compare hash codes on behalf of the data subjects.

Survey of Blowfish Algorithm for Cloud
Shamil Zaiden , Auday H. Alwattar

Security is the study of encryption and decryption, information hiding, potential attacks, and performance system of measurement. Many algorithms do this. Blowfish is a symmetric block cipher using the Feistel network. Although there are many studies using the Blowfish algorithm for cloud security, there are no previous research traineeships. Cloud computing is the establishment of computer services such as servers, storage, databases, networks, software, analytics and intelligence over the Internet ("the cloud") to enable faster, more flexible computation and save prices.

The most common issues with cloud computing are information security, privacy, privacy, and how cloud providers provide these services. This article comprises a survey of most of the previous work on cloud security using the Blowfish algorithm.

PROPOSED SYSTEM:

"Cloud computing is a service that has grown significantly in recent years in the field of information technology. For both consumers and service providers of the cloud, privacy and security are top priorities. Users cannot remotely control their data in a cloud environment since their data is transferred to a public cloud server. As a result, information security, including information confidentiality, integrity, availability, and dependability, is crucial while using cloud storage. OBA and MSA are recommended in this paper as a solution to this problem.

OBA is designed to improve the privacy of sensitive data in public cloud storage. The plan has three phases: MSA, data safety castoff OBA, also query based data retrieval. Use SaaS like this. This approach protects data from both internal and external attackers. The program has three phases: the enrolment period, the security period, and the recovery period.

During registration, users save their data in the cloud. At this stage, an MSA is created to prevent unofficial persons from accessing the transaction. During security, data is encrypted using the Blowfish algorithm. To install Blowfish, the encryption key is suitably selected using the BCSO algorithm. In the fetch phase, the authorized person makes a request to the server.
Enumerated users mean they will receive information, otherwise the requested will be ignored.

SYSTEM ARCHITECTURE

Architecture is a graphical representation of data from information systems that models its processes. It is used as a preliminary step in the development of the process and does not require further explanation. The architecture specifies how the data is read and output from the system, how the data is processed by the system, and where the data is stored. Unlike standard arrangement, which efforts on flow control, it does not show information about the timing of the process or how well the process is performing or stabilizing. Logical data flowcharts can be drawn using four simple symbols i. for example, it represents process and data storage. We use these symbols as Gain and Sarson symbols. Square boxes indicate external locations, curved boxes indicate processes, rectangular boxes indicate data storage, and arrows indicate data flow.

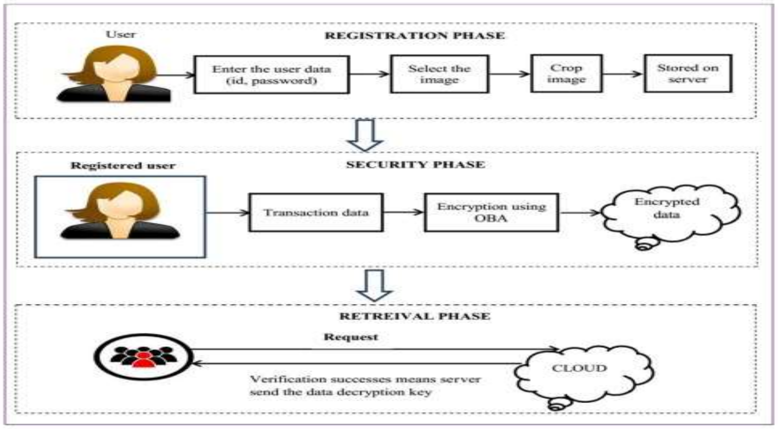


Fig 1 Proposed architecture

MSA PROCESS

"Authentication systems are necessary to stop malicious attacks, data theft, and data loss. Unauthorised users can readily alter data without the administrator's awareness, especially in a government setting, thus there is no security violation. This document mandates that MSAs have access to cloud-based data in order to avoid this problem. By limiting access, it will safeguard the air from unauthorised usage. Registration and access are the two stages of the MSA procedure.

The full description is as follows

Registration process

During registration, customers can access their information in the data center. First, the client generates a user ID UID and a password PID to access all the user's information. After the server gets the UID and PID, it shows N images to the client. User selects I1 image from N images. After that, the selected images are sent to the server and stored.

Then crop the selected image 1 to improve recognition and send the cropped image to the server. This is also stored on the server.

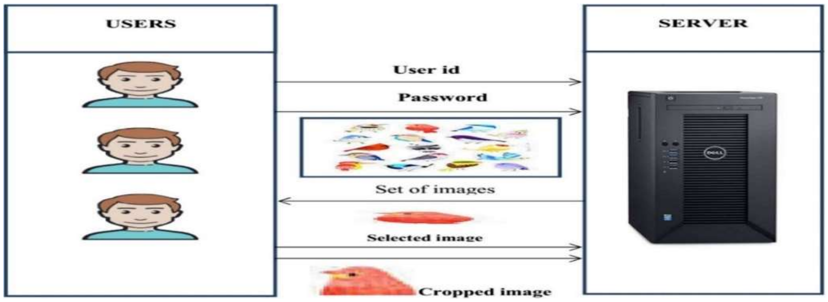


Fig 2 Registration process

Login process

"The login procedure is explained in this section. Customers can download or upload files to the cloud once registration is complete. No one is able to keep data on the cloud without anonymity. This approach will help us avoid data loss. The user must first input their user ID (UID) and password (PID) in order to log in. The server validates the accuracy of the data after receiving it. If the technique is correct, the server displays N pictures right away. The produced image also contains image validation. Customers pick pictures from pictures. The procedure continues with the same picture as the closed image.

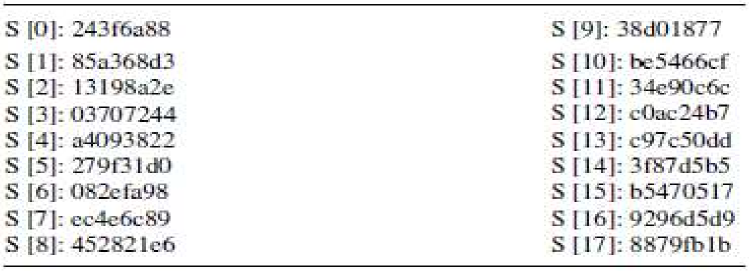
Using the Optimised Blowfish Algorithm for Data Security:

"After registering, Login data is encoded using OBA. An essential encoding technique is the blowfish algorithm (BA). For 64-bit blocks, the key length is 32-448 segments. Four 32-bit S-Boxes and the P-Array are accessible here. S-Boxes send 32-bit output while recognising 8-bit data. Key development and encoding technique are two aspects of BA. A 16-round network service is used for the encryption process. Each round has one key change and one key change. 32-bit messages are added to all functions in XOR and BA. Consider the plaintext value 123456abcd132536. The step-by-step process of the Blowfish algorithm is as follows,"

- Generate master keys
- Initializes substate
- Encrypt
- Decrypt

1: key size generation

Encoding and decoding require 18 subkeys and the same key is used for both operations. The 18 subkeys are stored in the S array, each item is a 32-bit entry. It is Initialized with the number Si[x]. Some examples of the hexangular depiction of subkeys are as follows:



S [0]: 243f6a88	S [9]: 38d01877
S [1]: 85a368d3	S [10]: be5466cf
S [2]: 13198a2e	S [11]: 34e90c6c
S [3]: 03707244	S [12]: c0ac24b7
S [4]: a4093822	S [13]: c97c50dd
S [5]: 279f31d0	S [14]: 3f87d5b5
S [6]: 082efa98	S [15]: b5470517
S [7]: ec4e6c89	S [16]: 9296d5d9
S [8]: 452821e6	S [17]: 8879fb1b

Table 1 key size generation

2: initialize the substitution boxes

four Substitution Boxes { Sb[1], Sb[2], Sb[3], Sb[4] } are needed both the encoding and the decoding process which having 255 entities {Sb[i][0], Sb[i][1], …, Sb[i][255]} with 32 bits.

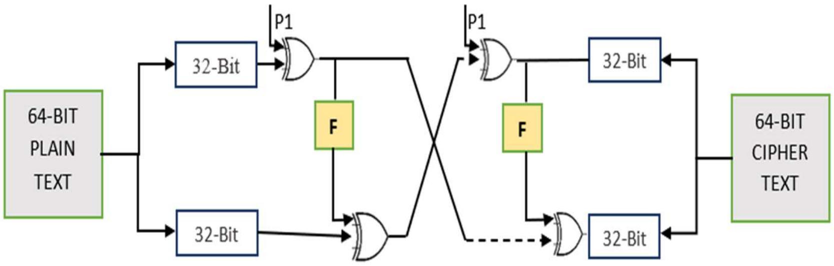


Fig 3 Structure of Blowfish Algorithm

3: encoding

“Blowfish has 16 rounds and the entry contains 64-bit files containing x. Divided x into 64 parts xL and xR. Next, I = 1 to 16.

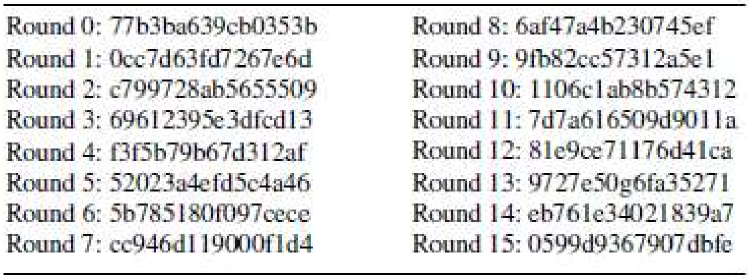
xL = xL XOR Si

xR = F(xL) XOR xR

swaps xL and xR. After the sixteenth, swap xL and xR again to undo the last swap.

Then xR = xR XOR S17 and xL = xL XOR S18. Finally, repeat xL and xR to get the ciphertext.

The Examples of encoding process is given as,



Round 0: 77b3ba639cb0353b	Round 8: 6af47a4b230745ef
Round 1: 0cc7d63fd7267e6d	Round 9: 9fb82cc57312a5e1
Round 2: c799728ab5655509	Round 10: 1106c1ab8b574312
Round 3: 69612395e3dfcd13	Round 11: 7d7a616509d9011a
Round 4: f3f5b79b67d312af	Round 12: 81e9ce71176d41ca
Round 5: 52023a4efd5c4a46	Round 13: 9727e50g6fa35271
Round 6: 5b785180f097cece	Round 14: eb761e34021839a7
Round 7: cc946d119000f1d4	Round 15: 0599d9367907dbfe

Table 2 Encoding”

After encryption we get the ciphertext like "d748ec383d3405f7".

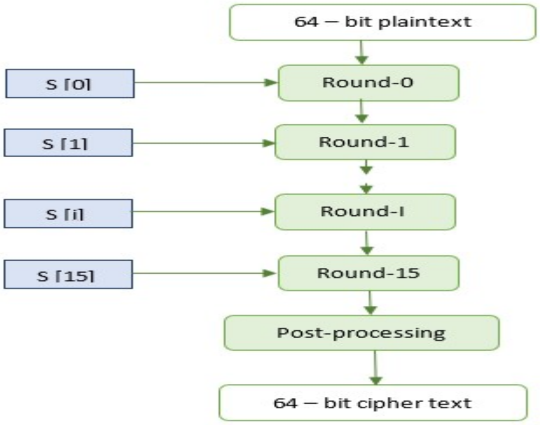
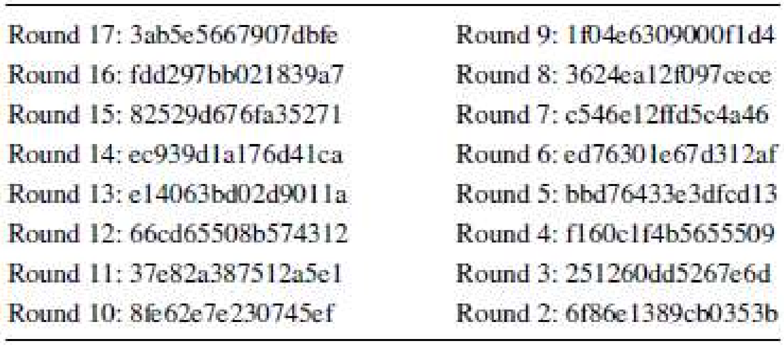


Fig 4 Encryption process of *Blowfish* Algorithm

4: Decryption

The decryption procedure using the Blowfish algorithm is shown in Figure 3. During this process, the encrypted image is decrypted using the same key used for encryption. Decryption is similar to encryption except in the order {S[1], S[2], … , S[18]}is reversed when decrypting. The decrypted value is as follows



Round 17: 3ab5e5667907dbfe	Round 9: 1f04e6309000f1d4
Round 16: fdd297bb021839a7	Round 8: 3624ea12f097cece
Round 15: 82529d676fa35271	Round 7: c546e12ffd5c4a46
Round 14: ec939d1a176d41ca	Round 6: ed76301e67d312af
Round 13: e14063bd02d9011a	Round 5: bbd76433e3dfcd13
Round 12: 66cd65508b574312	Round 4: f160c1f4b5655509
Round 11: 37e82a387512a5e1	Round 3: 251260dd5267e6d
Round 10: 8fe62e7e230745ef	Round 2: 6f86e1389cb0353b

Table 3 Decryption

Finally, we get the sum of "123456abcd132536". This white paper is similar to the original paper. To improve BA, key values are well chosen with the help of BCSO algorithm.

RESULTS

The recommended approaches' retrieval time, file access time, encryption time, decryption time, and memory utilisation are all scrutinised. The main objective of the provided method is to transport data to the cloud securely and without information loss. To accomplish the task, a cutting-edge MSA method and cryptography algorithm are applied. The results of the proposed procedures are depicted in the numbers below. The efficiency of the recommended method is measured in terms of file access time in Fig. 5. In this graph, the x-axis represents file size and the y-axis represents time.

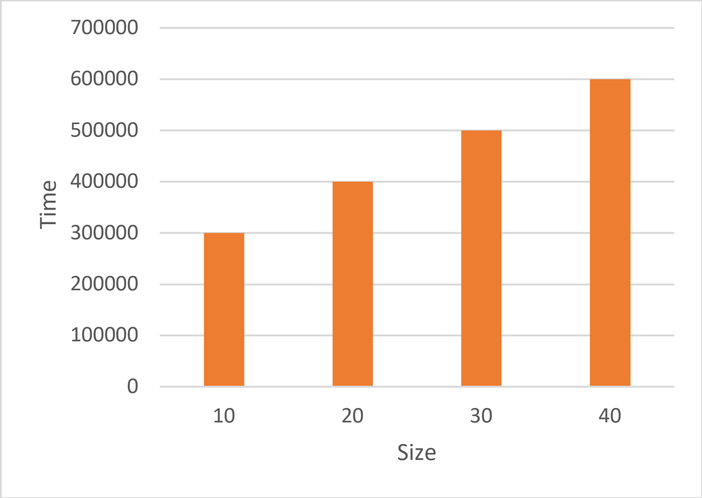


Figure 5: Proposed method performance

The recommended method accesses the 10 kb file while examining Fig. 5 in 75 ms, which is the bare minimum amount of time. Additionally, as the figure clearly illustrates, image access time increases as file size increases.

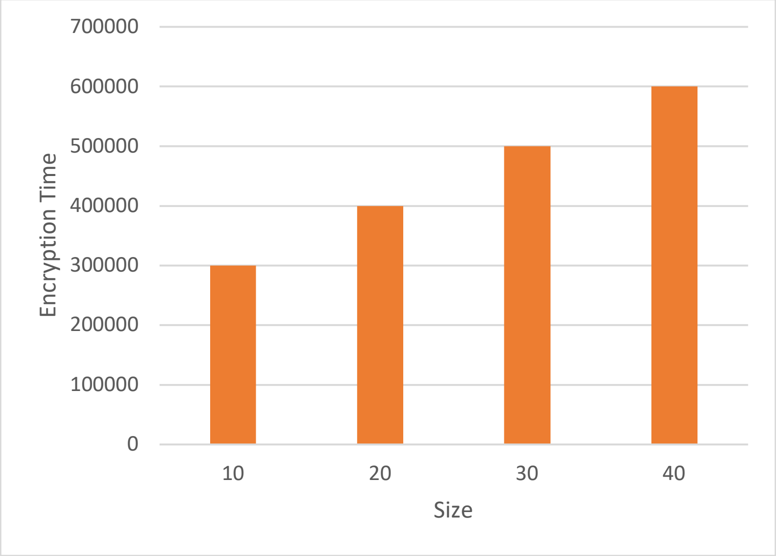


Figure 6: Performance based on encryption time

Similar to Fig. 6, the performance of the recommended methodology is assessed in terms of decryption time in Fig. 7, and the performance of the proposed methodology is assessed in terms of encryption time in Fig. 6. Here as well, the time required for encryption and decryption was reduced to a minimum.

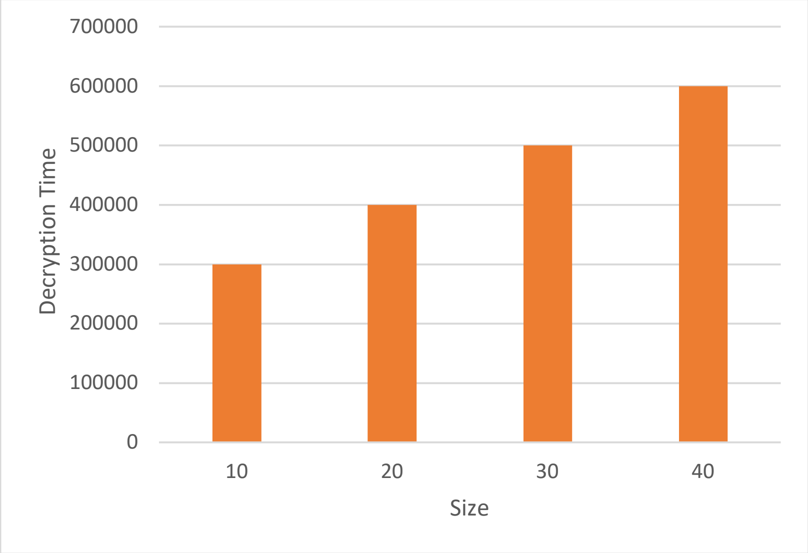


Figure 7: Performance based on Decryption time

The memory performance of the recommended technique is examined in Figure 8. In this case, memory utilisation increases steadily as the file size increases.

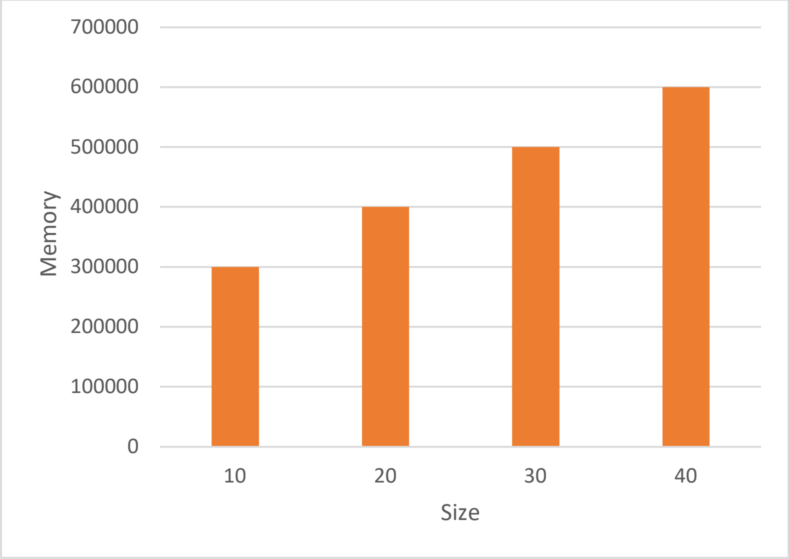


Figure 8: Performance based on Memory

When looking at Fig. 8, it is necessary to send 40 kb of data utilising 15,359,766 bits of RAM. There isn't much of it.

Conclusion

This article describes how to transfer security-sensitive data to the cloud. Here, client verification as described earlier is an important task. The information here is encoded using the OBA procedure. BA was created with the BCSO algorithm. The mathematical expression for these two operations is clarified. Used this technique, we can prevent unofficial users from accessing the system. Presentation of the plan is analysed based on variables such as encoding time, decryption time, data entry time, and memory. From the test results, it can be seen that our proposed method takes less time for encoding and decoding than the current method. So, our plan will be better than the current system. Users cannot save data without authentication, so this is very secure. These efficient algorithms can be used in the future to speed up the entire process.

Future Work

We want to resolve this issue in the future by changing the algorithm and upgrading the optimisation model. Additionally, our system recognises that some factors, like the processing time and the rate of transmission between the mobile phone and the base station, are set and known in advance. To do this, we must use measuring tools or profiling techniques in order to assess the importance of these factors. Though, in the real situation, the processing time and program may be somewhat different due to the indecision of the environment, and there is no latency problem. To spread the pertinence of our algorithm in the attendance of these changes, we must contain an optimization technique for the change-sensitive problem.

REFERENCES

1. T. Taleb, K. Samdanis, B. Mada, H. Flinck, S.Dutta, D. Sabella, On Multiple Access Edge Computing: A Study on Edge Cloud Architecture and Orchestration for Emerging 5G Networks, IEEE Communications. Live. teacher. 19 (3) (2017) 1657-1681.
2. Tao Z., Xia, Z. Hao, C. Li, L.Ma, S. Yi, Q. Li, Virtual Machine Management Research in Edge Computing, Proc. IEEE 107(8) (2019) 1482–1499.
3. Y. Mao, J. Zhang, K.B. Letaief, Joint task offloading scheduling and transmit power allocation for mobile-edge computing systems, in: IEEE Wireless Communications and Networking Conference, 2017.
4. Kang, ZJ Li, Gao, L. Zhao, A.Liu, Partial programming and power distribution for mobile edge computing systems, IEEE Internet Issues J. 6 (4) (2019) 6774–6785.
5. Y. Zhang, D. Niyato, P.Wang, Offloading in mobile cloud systems with intermittent connectivity, IEEE Trans. pain. computer. 14 (12) (2015) 2516–2529.
6. M.Jia, J. Cao, W. Liang, Optimal Cloud Deployment and User-to-Cloud Assignment in Wireless Metropolitan Area Networks, IEEE Trans. huab xam. 5 (4) (2017) 725–737.
7. B. Huang, Z. Li, P. Tang, S. Wang, J. Zhao, H. Hu, W. Li, V. Chang, Security modelling and efficient computation offloading for service workflow in mobile edge computing, Future Gener. Comput. Syst. 97 (2019) 755–774.
8. M.K. Marichelvam, T. Prabaharan, S.Y. Xin, A discrete firefly algorithm for the multi-objective hybrid flowshop scheduling problems, IEEE Trans. Evol. Comput. 18 (2) (2014) 301–305.
9. X. Zuo, G. Zhang, W. Tan, Self-adaptive learning PSO-based deadline constrained task scheduling for hybrid IaaS cloud, IEEE Trans. Autom. Sci. Eng. 11 (2) (2014) 564–573.
10. M.F. Tasgetiren, Y.C. Liang, M. Sevkli, G. Gencyilmaz, A particle swarm optimization algorithm for makespan and total flowtime minimization in the permutation flowshop sequencing problem, European J. Oper. Res. 177 (3) (2007) 1930–1947.
11. M. Qin, L. Chen, N. Zhao, Y. Chen, F.R. Yu, G. Wei, Power-constrained edge computing with maximum processing capacity for IoT networks, IEEE Internet Things J. 6 (3) (2019) 4330–4343.
12. Y. Sahni, J. Cao, L. Yang, Data-aware task allocation for achieving low latency in collaborative edge computing, IEEE Internet Things J. 6 (2) (2019) 3512–3524.
13. H. Xing, L. Liu, J. Xu, A. Nallanathan, Joint task assignment and resource allocation for D2D-enabled mobile-edge computing, IEEE Trans. Commun. 67 (6) (2019) 4193–4207.
14. W. Zhang, Z. Zhang, S. Zeadally, H. Chao, Efficient task scheduling with stochastic delay cost in mobile edge computing, IEEE Commun. Lett. 23 (1) (2019) 4–7.
15. Y. Xie, Y. Zhu, Y. Wang, Y. Cheng, R. Xu, A.S. Sani, D. Yuan, Y. Yang, A novel directional and non-local-convergent particle swarm optimization-based workflow scheduling in cloud-edge environment, Future Gener. Comput. Syst. 97 (2019) 361–378.
16. F. Jiang, K. Wang, L. Dong, C. Pan, W. Xu, K. Yang, Deep learning based joint resource scheduling algorithms for hybrid MEC networks, IEEE Internet Things J. (2019) http://dx.doi.org/10.1109/JIOT.2019.2954503.

17. V. Yadav, B.V. Natesha, R. Guddeti, GA-PSO: Using Hybrid Bionic Algorithms for Distributed Services in Fog Computing Environments In: TENCON 2019 - 2019 IEEE Region 10 Conference, TENCON, 2019, p. 1280-1285.
18. [18] A. Mseddi, W.Jaafar, H. Elbiaze, W. Ajib, Common container layout and task configuration in dynamic fog computing, IEEE Internet Things J. 6 (6) (2019) 10028–10040.
19. W. Na, S. Jang, Y. Lee, Park, N.S.Dao, S. Cho, Frequency resource allocation and interference management in mobile edge computing for IoT systems, IEEE Internet Things J. 6 (3) (2019) 4910–4920.
20. C. Yi, J.Cai, Z. Su, Multi-User Mobile Computing Offload and Transmission Programming Mechanism for Delay Sensitive Applications, IEEE Trans. mob please computer 19 (1) (2020) 29–43.