ORIGINAL RESEARCH PAPER

Engineering

IMPROVE DATA SECURITY IN CLOUD USING ENHANCED BLOWFISH ALGORITHM WITH DIFFERENT KEY SIZES

KEY WORDS:

Athira S Assistant Professor, Department of Information and Technology, Hindusthan College of Engineering and Technology.

M. Ravikumar Assistant Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology.

ABSTRACT

Cloud Computing is a distributed and centralized network of inter connected and inter related systems with one or more IT resources provisioned based on pay-on-demand usage. Despite the fact that cloud consumers and users have more flexibility with cloud resources, a number of problems exist that limit the utilisation of cloud resources. The most important one among them is security. Data security and privacy concerns are a roadblock to the cloud computing industry's rapid expansion. All firm must reduce the cost of data processing and storage, and analysis of data and information is always the most crucial activity for decision-making in all enterprises. As a result, no organisations will move their data or information to the cloud unless consumers and cloud service providers have established a level of confidence. Researchers have put out a number of approaches for data protection and to achieve the maximum level of data security in the cloud. However, there are still many gaps to be filled by making these techniques more effective. More work is required in the area of cloud computing to make it acceptable by the cloud service consumers. This paper implementing the Enhanced Blowfish Algorithm techniques for data security, focusing on the data storage and use in the cloud, for data protection in the cloud computing environments to build trust between cloud service providers and consumers.

INTRODUCTION

Cloud computing serves as an architectural framework for numerous IT resources, including operating systems, processing power, storage, applications, platforms, etc. This innovative technology offers infrastructure, software, and platform services. Customers of the cloud can use any of the four different types of clouds: public, private, hybrid, and community to access these services. Users of the public cloud may have superior access to and control over the infrastructure. This new technology offers numerous benefits, including reduced costs, higher storage capacity, backup and recovery, ongoing resource availability, and geographical independence. The security of the sensitive data of the customer is a big problem in the cloud because users' data is shared among servers. This emphasises how crucial it is to save data securely. Cryptography serves as the standard security mechanism in a typical network. That significantly contributes to the security concern. Encryption is a key technology in cryptography. Data integrity and confidentiality are maintained by this technology. Only those with permission can access data, which is a quality of confidentiality. Integrity prevents unauthorised parties from changing the data that the user has stored. Many users increase their security by keeping their data very private. The similar approach to the security issue is also permitted by cloud. According to the cloud environment, the two parties that can encrypt the customers' data are Cloud Service Providers and Third Party Auditor (TPA) (CSP). The reliability of data kept in the cloud is compromised whenever users depend on these third parties. So, users these days take on the responsibility of encrypting their own sensitive data before transmitting it to the cloud for storage.

Data Integrity

Data integrity is defined as the absence of data corruption that can be guaranteed with consistency and accuracy throughout time. To put it more precisely, it means that the data must be entered as Original and that it must be sent as Original when being retrieved. In any information system, data integrity is one of the most important components. Data integrity generally refers to guarding against unlawful erasure, tampering, or creation of data. It is protected against misuse, appropriation, and theft by limiting the managing entity's access to and rights over particular enterprise resources. It is the characteristic of not having been altered by an unauthorized party. Integrity is also extended to hold how data is stored, processed and retrieved. In a cloud system, maintaining data integrity involves protecting information integrity. Unauthorized users shouldn't lose the data or alter it. The foundation for offering cloud computing services like SaaS, PaaS, and IaaS is data integrity. In addition to large-scale data storage, cloud computing environments typically offer data processing services. Techniques like digital signatures and RAID-type schemes can be used to ensure data integrity.

Data Confidentiality

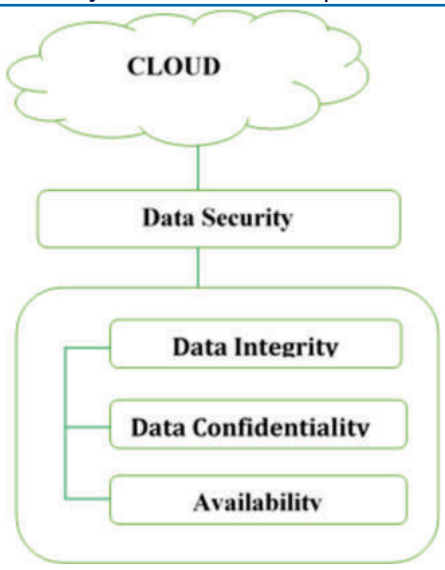
Data confidentiality is the process of preventing unauthorised users, an outsourced server, and illegal access to and disclosure of data. Data is encrypted in order to prevent unauthorised users from decrypting it. Users that save sensitive or private data in the cloud must ensure data confidentiality. Data confidentiality is ensured via authentication and access control techniques. By boosting the cloud's dependability and credibility, the problems with data privacy, authentication, and access control in cloud computing could be resolved. It is the quality of something only being accessible to those who have been given permission. Unauthorized access to data is prevented by security measures.

Availability

The percentage of time that an infrastructure, system, or solution is available to be used for its intended purpose while operating normally is referred to as availability. With cloud infrastructure solutions, availability refers to the fraction of the service's paid duration during which the data centre is reachable or provides the intended IT service.

The mathematical formula for Availability is :
Percentage of availability = (total elapsed time – sum of downtime)/total elapsed time

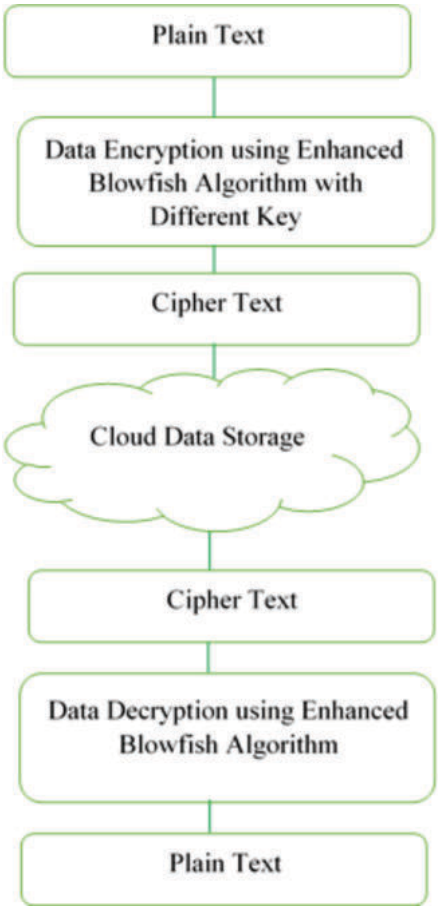
The client reputation of a business depends on the availability of data. For instance, clients are likely to grow dissatisfied and lose faith if they are unable to access their online data (such as a portal for paying invoices or purchasing history). They can choose a rival who can provide better experiences or services. In competitive industries, this may result in diminished market share and earnings.



Organisation Of Cloud Computing Data Security

Encryption Using Blowfish Algorithm

The algorithm's main goal is to protect cloud data privacy. In this way, information is protected before uploaded to the server. A multilevel encryption method is presented by the proposed algorithm. Data must first be encrypted using blowfish before being uploaded to the cloud server. BL employs a 64 bit block size and offers configurable key lengths ranging from 32 bits to 448 bits, as detailed in chapter 2. The user's variable key is expanded to subkey arrays of 4168 up to 8336 bytes for key expansion or key initialization. In addition, 18 sub-keys with a size of 32 bits each are employed in the P array along with four 32-bit S boxes.



Block Diagram For The Proposed Algorithm

Proposed Work

In comparison to the Standard Blowfish method, the suggested Enhanced Blowfish algorithm uses two extra prime integers. This concept was inspired by the High Speed and Security Blowfish technique, which employed two random numbers to generate keys. This algorithm generates two keys, Public Key E and Private Key D. The Blowfish algorithm typically uses two prime numbers. The Proposed Algorithm as Improved Blowfish Algorithm includes two additional prime integers, P1 and P2. The procedure then computes two "N" values, such as N1 and N2, in the subsequent phase.

N1 is calculated by multiplying four prime numbers. It uses two prime numbers to calculate N2. It will make the encryption phase more complex. In the process of Encryption converting plain text to cipher text. This process uses the Public key E and N1 values, where N1 is a product of four prime numbers. Thus the cipher text C is generated. In the process of decryption the original plain text is retrieved by using the values of cipher text, decryption key D and N2. N2 is computed using only two prime numbers. The calculated N1 value is used for encryption process as public key pair (E,N1). For the decryption process the private key pair composed of D and N2 is used. The usage of prime numbers instead of random numbers showed the strength of encryption process. Because it is difficult to identify a prime number rather than a random number it gives a way to improve the strength of the key. The time spent for encryption and decryption processes are mostly lesser than with random numbers

CONCLUSION AND FUTUREWORK

The suggested technique accelerates encryption and decryption by using Different Key Mechanism. The proposed algorithm Enhanced Blowfish Algorithm still speeds things up by breaking the file up into different pieces. The Enhanced Blowfish algorithm's implementation not only boosts calculation speed but also makes it sophisticated and strengthens security. In proposed scheme, 128 bit Blowfish is implemented. The notion of addition chaining can still be used in the future to reduce the time required for encryption and decryption. Statistical techniques can be used to test the algorithm's level of security and determine its strength.

REFERENCES

1. M. A. Muin, M. A. Muin, A. Setyanto, Sudarmawan and K. I. Santoso, "Performance Comparison Between AES256- Blowfish and Blowfish-AES256 Combinations," 2018 5th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), Semarang, 2018, pp. 137-141, doi: 10.1109/ICITACEE.2018.8576929.
2. H. Setiawan and K. Rey Citra, "Design of Secure Electronic Disposition Applications by Applying Blowfish, SHA-512, and RSA Digital Signature Algorithms to Government Institution," 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), Yogyakarta, Indonesia, 2018, pp. 168-173, doi: 10.1109/ISRITI.2018.8864280.
3. V. K. R. Gangireddy, S. Kannan, and K. Subburathinam, "Implementation of enhanced blowfish algorithm in cloud environment," Journal of Ambient Intelligence and Humanized Computing, pp. 1-7, 2020.
4. S. B. Nalawade and D. H. Gawali, "Design and implementation of blowfish algorithm using reconfigurable platform," 2017 International Conference on Recent Innovations in Signal processing and Embedded Systems (RISE), Bhopal, 2017, pp. 479-484, doi: 10.1109/RISE.2017.8378204.
5. I. A. Landge and B. K. Mishra, "VHDL based BLOWFISH implementation for secured Embedded System design," 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB), Chennai, 2017, pp. 497-501, doi: 10.1109/AEEICB.2017.7972363.
6. T. K. Hazra, A. Mahato, A. Mandal and A. K. Chakraborty, "A hybrid cryptosystem of image and text files using blowfish and Diffie-Hellman techniques," 2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON), Bangkok, 2017, pp. 137-141, doi: 10.1109/IEMECON.2017.8079577.
7. A. Chauhan and J. Gupta, "A novel technique of cloud security based on hybrid encryption by Blowfish and MD5," 2017 4th International Conference on Signal Processing, Computing and Control (ISPCC), Solan, 2017, pp. 349-355, doi: 10.1109/ISPCC.2017.8269702.
8. A. Gaur, A. Jain and A. Verma, "Analyzing storage and time delay by hybrid Blowfish-Md5 technique," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017, pp. 2985-2990, doi: 10.1109/ICECDS.2017.8390003.
9. RandaMohamed Abdel Haleem and Eltyeb Elsamani Abd Elgabar "Enhancing the Integrity of Cloud Computing by Comparison between Blowfish and RSA Cryptography Algorithms" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 11 Issue 01,

January-2022
10. R. S. Abdeldaym, H. M. Abd Elkader, and R. Hussein, "Modified rsa algorithm using two public key and chinese remainder theorem," IJ Electron. Inf. Eng., vol. 10, no. 1, pp. 51–64, 2019.