WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Design and Analysis of Cloud Data's Multi-Layer Security Protection

Ramesh Byali [b], Jyothi [c], Megha Chidambar Shekadar [d]

[b]*cse dept PDIT Hospet India ramesh.byali@gmail.com*
[c]*cse dept PDIT Hospet India*
dcse dept PDIT Hospet India

DOI: https://doi.org/10.55248/gengpi.2022.3.8.5

A B S T R A C T

To store and access sensitive information from distant locations utilizing an internet connection, cloud servers are now often employed. By adopting cloud servers as their primary source of data storage, almost all businesses and organizations made the transition from local to distant data storage. It has become a struggle for each and every person to give additional security for the cloud data because, in general, cloud servers do not have total protection for the data that is stored on them. Data is a useful resource that can take many different forms, including payment information, personal information, bank account information, and many others. Due to the absence of data security in all of these forms, we try to useSome cutting-edge encryption methods for protecting the data that is kept in remote locations. Two parties make sure that a third party cannot access their communication when they communicate through a medium. It is better to use encryption methods to encrypt data in a cipher, send it over the internet, and then decrypt it to reveal the original data. By transforming plaintext into cipher text, the science of cryptography encrypts and decrypts data to keep messages private. In this project, we primarily develop 3 techniques, including: The three strategies are columnar transposition, rail fence transposition, and caesar substitution. Data can be protected and returned to its original state using all three processes together.

Keywords:Rescue bag, Rescue techniques, Borewell rescue, Child safety

1. Introduction

The study of concepts like encryption and decryption, which are used to provide secure communication and are one of the methods for covertly keeping data, is known as cryptography. The word "crypt" denotes "hidden," while the suffix "graphy" denotes "writing." Data is transformed into a secret code through the process of encryption, which hides the information's true meaning. The process of restoring encrypted data to its original condition is called decryption. It basically follows a reverse encryption process. Authentication, Integrity, and Confidentiality are the fundamental principles of cryptography for data protection. [1]-[9].

Authentication: Authentication is the process of determining a user's identity.It involves tying a set of distinguishing credentials to an incoming request. The credentials entered are compared to those in a database of the information belonging to the authorized user on the local operating system or in an authentication server.Integrity: This is the consistency, accuracy, and dependability of data across the course of its life. It must not be changed while in transit, and security measures must be taken to prevent unauthorized parties from changing the data.Security measures are in place to guard against unauthorized access to sensitive information. Data is usually categorized based on the severity and type of harm it could bring about if it got into the wrong hands. Then, based on the classifications, stricter or less rigorous limitations may be put into effect.There are two types of cryptography:There are two divisions in cryptography[10].Both symmetric and asymmetric key cryptography are used. A symmetric cryptography uses a pair of keys—a public key for encryption and a private key for decryption—to carry out encryption and decryption operations.Symmetric cryptography: The sender and recipient share a shared key to encrypt and decrypt messages. Two different categories of symmetric cryptography exist. The two methods are substitution and transposition. Technique for substitution: Every plain text alphabet has aThe entire document uses a single encryption alphabet. Examples include the

* *Corresponding author.*
E-mail address: *shahida@pdit.ac.in*

Caesar, Play Fair, and Hill ciphers. Transposition technique: It involves doing some kind of permutation on plain text letters. Examples include rail fences, columnar transposition, and more. This project develops a layered strategy.

2. LITERATURE SURVEY

This section will mostly focus on the background research that has been done to demonstrate the effectiveness of our suggested Method. The most crucial stage of the software development process is the literature review. This step is extremely important for the creation of any program or application since it affects a number of variables, including time, cost, effort, the number of lines of code, and the strength of the firm. Once each of these many requirements has been met, we must choose the operating system and programming language that will be utilized to create the application. When the programmers begin creating the application, they will first look at the pre-defined innovations that have been made using the same concept before attempting to design the work in an innovative way[12].MOTIVATION
Binita Thakkar and Blessy Thankachan, among other well-known authors, proposed the paper "importance of cryptographic approaches."
The Play Fair, Homophonic, and Polygram ciphers, as well as transposition techniques like the Railfence and Vernam ciphers, were explored in that work by the authors, who also proposed a rail fence approach in Java.

In their paper, "Improving Efficiency of Cryptography Techniques Using Caesar Cipher Algorithm," well-known authors Dian Rachmawati, Mohammad Andri Budiman, Indira Aulia, and others introduced cryptography concepts, developed the Caesar cipher algorithm and the XOR algorithm using mathematical elements, and implemented the XOR and caesar algorithms in Python.

3. ARCHITECTURE

There was no suitable procedure in the current system to provide security for the data kept on storage servers. All prehistoric storage servers employed general authentication methods like login and password validation and others to provide security. However, no simple techniques offer data security in terms of encryption and decryption. Therefore, the main drawbacks of the current system are as follows.

1. Less security exists in the current systems.
2. Every technique now in use makes use of standard security measures like login and password authentication.
3. The current system lacks any concept like encryption or decryption that can provide total security for the data.
4. There is a common element that all primitive cryptography methods share:

4. METHODOLOGY

Cryptography is the science of encrypting and decrypting data using mathematics to keep messages private by turning plaintext into cipher text. It is used in the suggested system. In today's computer systems, cryptography provides a solid, economical foundation for data security. A layered approach is created in this project by combining three methodologies. The three methods are columnar transposition, railfence transposition, and caesar substitution. Data can be protected and returned to its original state using all three processes together.

5.CONCLUSION

Caesar substitution, Rail Fence transposition, and columnar transposition are the three techniques that we primarily construct in this application. Data can be protected and returned to its original state using all three processes together. Before uploading or downloading a file from the cloud server, we are attempting to link the three techniques to the cloud server in this instance..

REFERENCES

[1] Dr. C.N. Sakhale, D.M. Mate, SubhasisSaha, Tomar Dharmpal, Pranjit Kar, ArindamSarkar, RupamChoudhury, ShahilKumar , “An Approach to Design of Child Saver Machine for Child Trapped in Borehole “, International Journal of Research in Mechanical Engineering, October-December, 2013, pp. 26-38.

[2] K. Saran, S. Vignesh, Marlon Jones Louis have discussedaboutthe project is to design and construct a “Bore-well rescue robot” (i.e. torescue a trapped baby frombore well), International Journal of Research in AeronauticalandMechanical Engineering, Boar well rescuerobot , pp. 20-30 April 2014

[3] G. Nithin, G. Gowtham, G. Venkatachalamand S. Narayanan, School of Mechanical Building Sciences, VIT University, India, Design andSimulation of Bore well rescue robot– Advanced, ARPN Journal of Engineering andApplied Sciences, pp. MAY 2014.

[4] Camera - Direct web search on google.com

[5] J. Burke andR.R.Murphy, "Human-robot interaction in USAR technical search: Twoheads are betterthanone,"inProc.IEEE Int. Workshop ROMAN, Kurashiki, Japan, 2004, pp. 307-312.

[6] J. Casper and R. R. Murphy, "Human-robot interactionsduringthe robot assistedurban search andrescue response at theworldtrade center," IEEE Trans. Syst., Man, Cybern. B, Cybern., Vol. 33, no. 3, pp. 367–385, Jun. 2013.

[7] R. R. Murphy, "Activities of therescue robots at the World Trade Center from 11–21 September 2001," in Proc. IEEE Robot. Autom. Mag., 2004, pp. 50–61.

[8] Rodriguez, K. M., Reddy, R. S., Barreiros, A. Q., &Zehtab, M. (2012, June). Optimizing Program Operations: Creating a Web-Based Application toAssignand Monitor PatientOutcomes, Educator Productivity and Service Reimbursement. In DIABETES (Vol. 61, pp. A631-A631). 1701 N BEAUREGARD ST, ALEXANDRIA, VA 22311-1717 USA: AMER DIABETES ASSOC.

[9] Kwon, D., Reddy, R., & Reis, I. M. (2021). ABCMETAapp: R shinyapplicationforsimulation-basedestimation of meanand standard deviationfor meta-analysis via approximateBayesiancomputation. Research synthesismethods, 12(6), 842–848. https://doi.org/10.1002/jrsm.1505

[10] Reddy, H. B. S., Reddy, R. R. S., Jonnalagadda, R., Singh, P., &Gogineni, A. (2022). Usability Evaluation of anUnpopular Restaurant Recommender Web Application Zomato. Asian Journal of Research in Computer Science, 13(4), 12-33.

[11] Reddy, H. B. S., Reddy, R. R. S., Jonnalagadda, R., Singh, P., &Gogineni, A. (2022). Analysis of theUnexplored Security Issues Common toAll Types of NoSQL Databases. Asian Journal of Research in Computer Science, 14(1), 1-12.

[12] Singh, P., Williams, K., Jonnalagadda, R., Gogineni, A., &; Reddy, R. R. (2022). International students: What's missing andwhatmatters. Open Journal of Social Sciences, 10(02),

[13] Jonnalagadda, R., Singh, P., Gogineni, A., Reddy, R. R., & Reddy, H. B. (2022). Developing, implementingandevaluating training for online graduate teaching assistantsbased on Addie Model. Asian Journal of EducationandSocial Studies, 1-10.

[14] Sarmiento, J. M., Gogineni, A., Bernstein, J. N., Lee, C., Lineen, E. B., Pust, G. D., &Byers, P. M. (2020).Alcohol/illicitsubstanceuse in fatalmotorcycle crashes. Journal of surgical research, 256, 243-250.

[15] Brown, M. E., Rizzuto, T., &Singh, P. (2019). Strategic compatibility, collaborationandcollective impact for community change. Leadership&Organization Development Journal.

[16]Sprague-Jones, J., Singh, P., Rousseau, M., Counts, J., &Firman, C. (2020). The Protective Factors Survey: Establishingvalidityandreliability of a self-report measure of protective factors againstchild maltreatment. ChildrenandYouth Services Review, 111, 104868.

[17] Reddy Sadashiva Reddy, R., Reis, I. M., & Kwon, D. (2020). ABCMETAapp: R Shiny Application for Simulation-based Estimation of Mean and Standard Deviation for Meta-analysis via Approximate Bayesian Computation (ABC). *arXiv e-prints*, arXiv-2004.