International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

AWS Cloud Based Encryption Decryption System

Ankush Pachpor[1], Sanskar Mali[2], Sarvesh Thakur[3] ,Prof. Madhuri Patil [4]

[1],[2],[3]B.E. Student, Department of Information Technology, MGMCET, Kamothe
[4]Professor, Mahatma Gandhi Mission's College of Engineering and Technology Kamothe, Maharashtra, India

---

Abstract - This project presents an encryption and decryption system for the safety and awareness between the people to keep their data secure. We used a web app that can be easily used by people. In all devices the web app is featured. Whenever somebody wants to keep their private data in a very secret manner they visit the web app and encrypt their data very securely and keep that data where they want.

Nowadays the security of data is becoming a very serious issue and the common people need this type of encryption to keep their data secure. To decrease the incidents of Stole of data the big companies are also using this type of systems. But when it comes to the common man they don't have this type of security. Because of these issues, we decided to make this software.

Keywords: Security, encryption, decryption, SHA-512, XOR Cipher, AWS.

1. INTRODUCTION:

This web app is designed to provide security to common people confidential data . The main purpose of this webapp is to provide awareness to common people for their private data from hackers or other malicious people. Generally People can't take much care about their data. Because of this webapp they can convert their data in very secure encryption format and after that they can store this file in their Mobile phone or any other device that no one can doubt about this file because this file can't be opened by any other software. In day-to -day life millions of people use the internet. There are many people on the internet who can steal the data and many people don't know that their data may be stolen. This type of data is used in cyber crime. In several years cyber crime has increased rapidly. A data breach is an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner. A small company or large organization may suffer a data breach. Stolen data may involve sensitive, proprietary, or confidential information such as credit card numbers, customer data, trade secrets, or matters of national security Most data breaches are attributed to hacking or malware attacks. . To avoid this type of data breach we had decided to make such a project that if anyone can steal the data of the user but the data will not be opened by the attacker. This is more reliable and no cost software This is very High-grade encryption for sensitive data.

1.2 Motivation

The main motivation of this project is to learn the concepts of Cryptography. We wanted to develop a web app that is useful to its users in terms of safety and About bringing awareness among the people for their personal confidential data. We started this application with an intent to provide safety to society.

2. RELATED APPROACHES/WORK :

2.1 AppZaza : Free Online Text Encryption and Decryption Automatically encrypt or decrypt any text document using many different algorithms with this text encrypter app. Paste any text document into the text box, choose your passwords and encryption algorithm, then click encrypt to receive the encrypted text. Make sure to save the passwords, algorithm used and encrypted text, you will need all of it to decrypt the results later and view the original message. Use this app to encrypt any text document, such as an email, pdf, secret memo, confidential or classified information, love letter, etc, and save that message or securely send it to someone. For the most success, you should send the two password values and algorithm separately from the message and through an alternate secure means (preferably in person).

2.2 A new image encryption and decryption using quasigroup (Durgesh Kumar):

This paper provides authenticity, confidentiality, secrecy, and integrity to the data one of them is Cryptography. In these papers they survey each encryption and decryption system, their strengths and weaknesses. In this paper they focus on the selecting the best cryptography and quantum cryptography used for image encryption and decryption. Quantum cryptography is a science that applies quantum mechanics principles to data encryption and data transmission so that data cannot be accessed by hackers – even by those malicious actors that have quantum computing of their own. The broader application of quantum cryptography also includes the creation and execution of various cryptographic tasks using the unique capabilities and power of quantum computers. Theoretically, quantum computers can aid the development of new, stronger, more efficient encryption systems that are impossible using existing, traditional computing and communication architectures.

3. THE PROPOSED SYSTEM

This proposed system is much more productive than the existing system. This system fulfills all the drawbacks of the existing system. This system can encrypt all the types of file. There are no limitations to encrypt the file. For encrypting this use XOR cipher which is a very powerful encryption cipher . This uses the most advanced encryption algorithm for password protection. This is called SHA-512. This is a one way process. If anyone can proceed with the password for the encryption, this can generate the hash code and that hash code cannot be cracked by anyone. If someone encrypts the file using this software they want to decrypt the file using only this software. Not any other software is used to open the file. If anyone wants to tamper with the file. This file will not be op

Fig 1 Landing Page of Website

3.1 XOR Cipher :

XOR Encryption is an encryption method used to encrypt data and is hard to crack by brute-force method, i.e generating random encryption keys to match with the correct one. The concept of implementation is to first define XOR – encryption key and then to perform XOR operation of the characters in the String with this key which you want to encrypt. To decrypt the encrypted characters we have to perform. XOR operation again with the defined key. Here we are encrypting the entire String.The basic idea behind XOR – encryption is, if you don't know the XOR-encryption key before decrypting the encrypted data, it is impossible to decrypt the data. For example, if you XOR two unknown variables you cannot tell what the output of those variables is. Consider the operation A XOR B, and this returns true. Now if the value of one of the variables is known we can tell the value of another variable. If A is True then B should be False or if A is False then B should be true according to the properties of the boolean XOR operation. Without knowing one of the values we can not decrypt the data and this idea is used in XOR – encryption.

3.2.SHA -512 :

SHA-512 are the most commonly accepted and used hash functions computed with 32-bit and 64-bit words, respectively.SHA-512 is very close to SHA-256 except that it uses 1024 bits "blocks", and accepts as input a 2^128 bits maximum length string. SHA-512 also has other algorithmic modifications in comparison with SHA-256.the message is broken into 1024-bit .The initial hash values and round constants are extended to 64 bits. there are 80 rounds instead of 64 bit words instead of 64 – 32-bit words

3.3 Amazon Web Services (AWS) :

Amazon Web Services (AWS), a subsidiary of Amazon.com, has invested billions of dollars in IT resources distributed across the globe. These resources are shared among all the AWS account holders across the globe. These accounts themselves are entirely isolated from each other. AWS provides on-demand IT resources to its account holders on a pay-as-you-go pricing model with no upfront cost. Enterprises use AWS to reduce capital expenditure of building their own private IT infrastructure (which can be expensive depending upon the enterprise's size and nature). All the maintenance cost is also borne by the AWS that saves a fortune for the enterprises.

4. SYSTEM DESIGN:

4.1 Presentation tier:

This is the topmost level of the application. The presentation tier displays information and gives the option to encrypt / decrypt files.

4.2 System Architecture

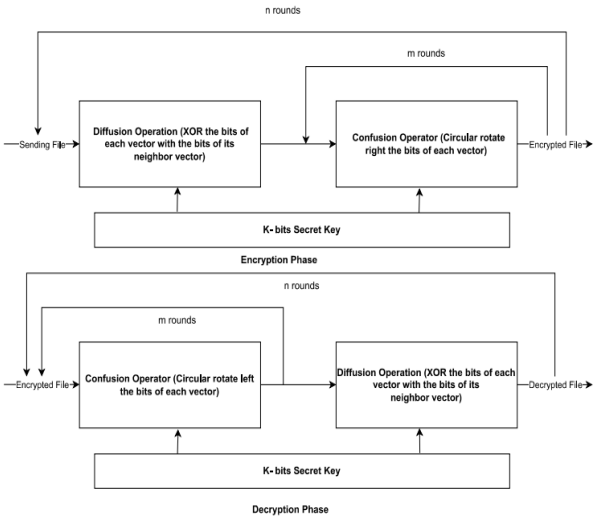

Fig 2 System Architecture

4.2 Class Diagram :

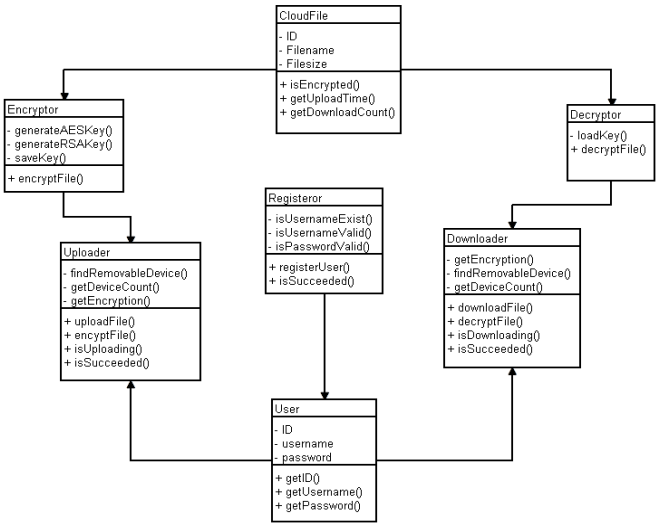

Fig 3 Class Diagram

Class diagram is a static diagram. It represents the static view of an application. Class diagram is not only used for visualizing, describing, and documenting different aspects of a system but also for constructing executable code of the software application.

Class diagram describes the attributes and operations of a class and also the constraints imposed on the system. The class diagrams are widely used in the modeling of object oriented systems because they are the only UML diagrams, which can be mapped directly with object-oriented languages

4.3 Flow Chart :

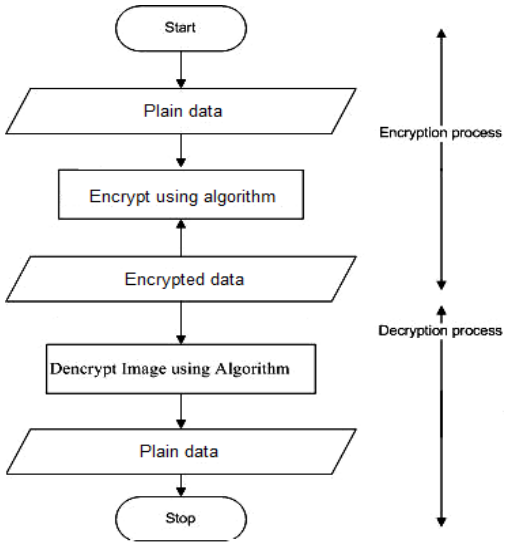

FIg 4 Flowchart

5. Conclusion:

Aws Cloud Based Encryption Decryption System encrypts and decrypts every type of file, it can be image, video, html page, anything. It encrypts the file with a strong password, which can be decrypt through this software only.

Data security is the biggest concern in today's life because of the future wars, and everything depends on data. The application title and its intention is not that the people can't take their data safe or they don't know about the data breach but the hackers are so smart that normal people can't know when the hackers hack the data and people don't know in such situations. But the safety of data should be our first priority. Basically everybody should take care of themselves and be alert.

6. REFERENCES:

[1] Classical and Quantum Cryptography for Image Encryption & Decryption IEEE

[2]Image-Encryption-and-Decryption-using-Enigma-Abir-Rahman

[3] Image encryption and decryption in public key cryptography based on MR(IEEE)

[4] Kazumaro Aoki; Jian Guo; Krystian Matusiewicz;Yu Sasaki; Lei Wang "Preimages for Step-ReducedSHA-2", Asiacrypt 2009

[5] William Stallings,The Whirlpool Secure HashFunction, Taylor and Francis Group, 2006

[6] An Overview of Cryptographic Hash Functions and Their Use s, John Edward Silva, 2003,GIACSecurity Essentials Practical Version

[7] A new image encryption and decryption using quasigroup (Durgesh Kumar)

[8]A New Approach for Encryption and Decryption(A. Manimaran[1,*], V. M. Chandrasekaran[2], Arnav Bhutani[3], Vansh Badkul[4]) researchgate

[9]Encryption using XOR based Extended Key for Information Security – A Novel Approach by E. Anupriya* and Amit Agnihotri researchgate

[10] Encryption of images using XOR Cipher IEEE by S Arul Thileeban Department of Computer Science and Engineering, SSN College of Engineering, Kancheepuram