Military Data Security System Using Encryption Technique

Vaishnavi Jirole[1], Shweta Patil[2], Prof. I. Y. Inamdar[3], Prof.S.D.Pandhare[4]
[1, 2, 3, 4] Dept of Computer Science and Engineering
[1, 2, 3, 4] Sahakar Maharshi Shankarrao Mohite Patil Institute of Technology and Research Shankarnagar, Akluj, Solapur, Maharashtra, (India)

Abstract- *In the current time of globalization, security is one of the main viewpoints in the advancement of site, particularly while sending secret records. Advanced Encryption Standard (AES) is one technique that can be utilized to get information by encrypting and decrypting data. AES is additionally a calculation that has a quick encryption process and has been broadly executed in different fields. To give information security that is move to the organization, AES is viewed as a quick and best calculation. AES is an open source cryptography with symmetric keys utilized for encryption and decoding of documents. The explanation is cryptography is right now just in view of consequences of a similar encryption. In decreasing cryptanalysis assaults, this paper talks about information security utilizing encryption technique.*

Keywords- Encryption, Decryption, Information Security, Advanced Encapsulation Standard (AES), Secure Hash Algorithm (SHA).

I. INTRODUCTION

Increased technologies and communication operation arises the need for stronger protection of information/ data transmitted and entered. Data Security is the most elevated need for any military system. Systems across the world have multiple protocols for limited access. These security systems are sophisticated so that the information is n't blurted to any person. We surveyed multiple security systems in use by US Air force and US Navy. These fabrics are military grade and have colorful encryption to stop any hacking or obscure access. Companies similar as Air Target, Dell manufacture systems which are fully usable in extreme conditions these politic outfit's are lately used for quicker operation and availability these companies help multiple armies to dissect adversary positions the quantum of people in particular terrain and quick transmission of classified data. Companies similar as Central Security Services have multiple products specific for military requirements and has complete and effective services which give you complete guidance on their operation. In this Scripts Military needs to be fully apprehensive of its complication of the systems which are being used. The system to be developed for this design is better than any other systems the system uses multiple encryption algorithm to cover the classified information.

II. PROPOSED SYSTEM

In the proposed system we are going to build web application. Which will help to secure military documents and their plans of mission so that no one can steal their plans. This system has two admin levels sub-admin and main-admin. main-admin has authority to control sub-admin and user. sub-admin has authority to approve/ disapprove user on the basis of contact ,address and other details. This framework is military evaluated and have different encryptions to stop any hacking or obscure access. Once user is approved by main-admin and sub admins, main-admin sends email key to user with his/her password and secret key. Then user can login to the system. user is able to download file only if he/she have private key. admin sends private key on email so that user can download the file. User can handle files can upload, download and delete the file. This will be a strong web application to secure military data because of strong use of algorithms.

III. LITERATURE REVIEW

Sandhya Anne Thomas, Saylee Gharge they arranged framework utilizing visual cryptography (VC) for upgraded security for military lattice reference framework. In Encryption VC works just on double pictures, consequently it is fundamental that it is made to works on assorted types on pictures. Halftoning helps in changing over a grayscale or shading picture into a parallel picture that is expected for VC. Different halftone strategies, for example, mistake dissemination and DBS is executed during encryption. In Error dispersion half conditioning which is a local interaction the blunder is diffused to the neighbors. They involved Decryption for the decoding stay same for all VC plans. The qualified members on stacking/superimposing will recuperate the first mystery picture. The stacking/superimposing is executed utilizing the Boolean capacity [1].

Mochamad M. Bachtiar, Sigit Wasista This paper tends to various information security and security assurance issues in a distributed computing climate and proposes a procedure for giving different security organizations like approval, endorsement and mystery close by checking in delay. 128 digit Advanced Encryption Standard (AES) is utilized for increment information security and classification. In this proposed approach, information is encoded utilizing AES and afterward transferred on a cloud. In this paper clarifies that, giving solid security in message transmission, the AES calculation with a mixture approach of Dynamic Key Generation and Dynamic SBox Generation is proposed [2].

Vishwanath S Mahalle, Aniket K Shahade In this “Enhancing the Data Security in Cloud by Implementing Hybrid (RSA&AES) Encryption Algorithm” paper they used hybrid encryption algorithm using RSA and AES algorithms for providing data security to the user in the Cloud. And they used public key for encryption, and private key and secret key for decryption. The data after uploading is stored in an encrypted form and can be only decrypted by the private key and the secret key of the user. The main advantage of that is that data is very secure on the cloud. This paper mainly focuses on the some key tasks. First Secure Upload of data on cloud such that even the administrator is unaware of the contents. Second Secure Download of data in such a way that the integrity of data is maintained. And third Proper usage and sharing of the public, private and secret keys involved for encryption and decryption [3].

Urvi Patel, Pradish Dadhania prepared a system Multilevel Data Encryption Using AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) For Image and Textual information Data. In this system They have used Key Generation concept, Keys are generation for the encryption of P. T by using Fiestel conviction anatomy and more identical technique are used could be a framework that's mindful for giving keys to the clients in a arrange that offers touchy or private information. And also they used a hash function multiplication functions that convert a predicated number value for input. Also use MD5 Hash, Fiestel concept, PRNG Pseudorandom generators (PRG) are used to create random sequences of numbers in pre-decided devices. AES (acronym of Advanced Encryption Standard) is a Symmetric encrypt algorithm, RSA the Rivest-Shamir-Adleman (RSA) algorithm, Information Encryption Standard (DES) may be asymmetric-key and this are algorithm they use.[4].

IV. DETAILED DESCRIPTION OF PROJECT

This system has two admin situations main-admin and subadmin. Main-admin has authority to control sub-admin and stoner. Sub-admin has authority to control stoner on the base of Address, Contact details and other information. This system is military canted and have multiple encryption to stop unknown access. Once stoner is approved by all the admin’s he gets stoner ID, word with private key. Private Key is used when stoner wants upload or download the train. Without private crucial train don’t get open.

a) Confidentiality Protection : Data confidentiality is about sequestration of information, including authorizations to view, partake, and use it.

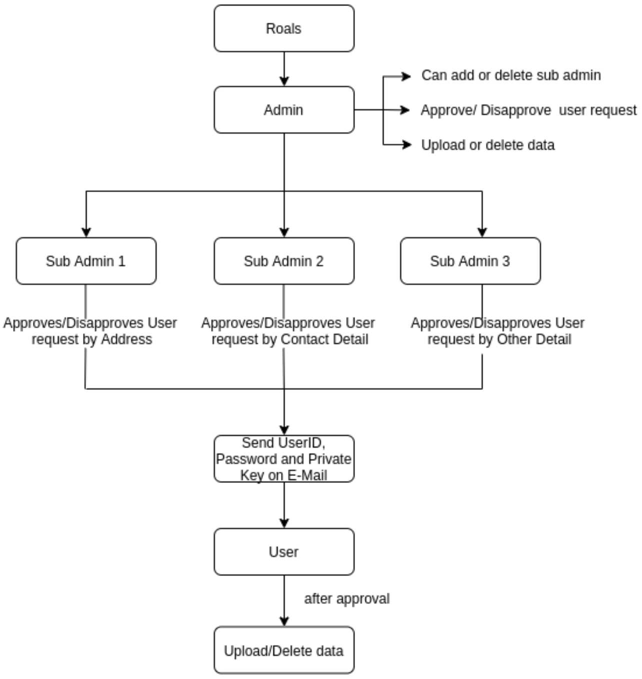
Roals
Admin
Can add or delete sub admin
Approve/ Disapprove user request
Upload or delete data
Sub Admin 1
Sub Admin 2
Sub Admin 3
Approves/Disapproves User request by Address
Approves/Disapproves User request by Contact Detail
Approves/Disapproves User request by Other Detail
Send UserID, Password and Private Key on E-Mail
User
after approval
Upload/Delete data

fig. Architecture

b) Integrity Protection : Integrity Protection means only authorized person can change the data

c) AES (Advanced Encryption Standard) : AES (acronym of Advanced Encryption Standard) is a Symmetric encrypt algorithm. AES bits for encrypt/ decrypt the data and fortifies lengths are and 256 bits.

1) Byte Supersede (Sub Bytes) The 16bit of word information is fine- turned layouts and affect in network shapes lines and section.
2) Indirect byte Shift rows Every four lines of matrix network are moved to left positions for each round other.
3) Mix Columns The yield of another frame is store of 16 incipient bytes and in last round this progression in not rehashed.
4) Add round crucial The 16 bytes of input matrix and round key and affair will stored in cipher textbook

128 bits and 16 bytes homogenous round of interpreted the data.

5) Decryption : The tasks of decode of an AES cipher textbook exertion in the inconsistency request. All round comprises of the four stage directed in the logical inconsistency request.

d) SHA (Secure Hash Algorithm) : SHA-1 produces a single affair 160- bit communication condensation (the affair hash value) from an input communication. The word communication is made out of different places. The word block, of 512 pieces, is parted into 80 32- bit words, meant as, one 32- number word for each computational round of the SHA-1 computation, Each round contains increases and coherent conditioning, for illustration, bitwise sensible tasks () and bitwise turns to one side (). The computation of depends on the round being executed, as well as the value of the constant. The SHA-1 80 rounds are separated into four gatherings of 20 adjusts, each with colorful rates for and the applied intelligent capacities (). The original values of the two variables in the morning of each data block computation correspond to the value of the current 160- bit hash value, too. After the 80 rounds have been reckoned, the two 32- bit values are added to the current Digest Dispatches (DM). The Initialization Vector (IV) or the DM for the first block is a predefined constant value. The affairFig. 3. SHA-2 round computation. Regard is the final DM, after every one of the information blocks have been figured. In a many more significant position operations, for illustration, the reconciled-4 Hash Communication Authentication Law (HMAC) (19), or when a communication is fractured, the original hash value (IV) may differ from the constant.

V. CONCLUSION

From this application we solve the problem of security using multiple algorithms such as advance encryption standard AES, Secure Hash Algorithm (SHA). To provide effective solution to secure any important classified documents creating this project will be a good help for the military. This project will definitely help bring changes to the existing processes and will bring the required change.

REFERENCES

[1] Sandhya Anne Thomas, Saylee Gharge “enhanced security for military grid reference system using visual cryptography” 9th icccnt 2018 july 10-12, 2018, iisc, Bengaluru Bengaluru, IndiaIEEE – 43488.

[2] Mochamad Mobed Bachtiar, Sigit Wasista, “Security Enhancement of AES Based Encryption Using Dynamic Salt Algorithm” 978-1-5386-8066-7/18/$31.00 ©2018 IEEE.

[3] Vishwanath S Mahalle Aniket K Shahade “Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa & Aes) Encryption Algorithm” 978-1-4799-7169-5/14/$31.00 ©2014 IEEE.

[4] Urvi Patel, PG Scholar Computer Eng. Department, Sardar Vallabhbhai Patel Institute of Technology, Vasad, Gujarat, India “Multilevel Data Encryption Using AES and RSA For Image and Textual information Data”2019 IEEE.

[5] F. J. D’souza and D. Panchal , "Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach," in International Conference on Computing, Communication and Automation (ICCCA2017) , Greater Noida, 2017.

[6] Mark R. Heckman, Member, IEEE, Roger R. Schell, Member, IEEE, and Edwards E. Reed, Member, IEEE “A Multi-Level Secure File Sharing Server and its Application to a Multi-Level Secure Cloud” 2015 IEEE.

[7] Jian-feng ZHAO Institute of Information Engineering Chinese Academy of Science Beijing, China “A Survey on the studies of Security guard technology for Memory”2016 IEEE.