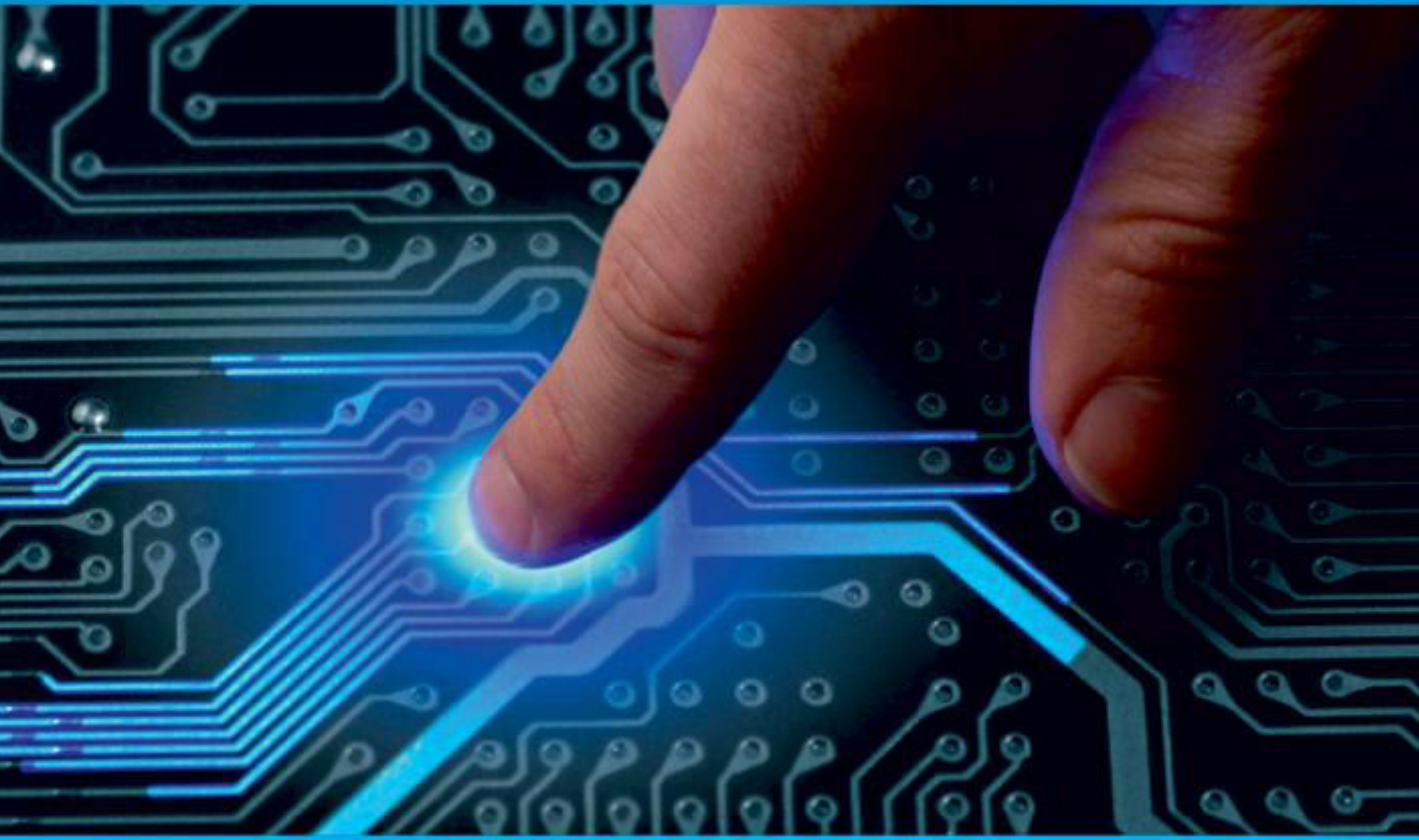
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

| DOI: 10.15680/IJIRCCE.2021.0907059 |

Implementing the Method of Blowfish for Storing and Sharing the Textual File Securely in a Database Using AES Algorithm

M. Sravya, M.Amulya, M.Vasantha lakshmi, K. Bhavya sree, Dr.P.L.Kishan Kumar Reddy(Ph.D)

Student, Dept. of Information Technology, Vasireddy Venkatadri Institute of Technology, Guntur, India

Student, Dept. of Information Technology, Vasireddy Venkatadri Institute of Technology, Guntur, India

Student, Dept. of Information Technology, Vasireddy Venkatadri Institute of Technology, Guntur, India

Student, Dept. of Information Technology, Vasireddy Venkatadri Institute of Technology, Guntur, India

Professor, Dept. of Information Technology, Vasireddy Venkatadri Institute of Technology, Guntur, India

ABSTRACT: File Transfer Web Application is used to upload various type of files like pdf into a database table and can download any type of files from the database. This web application is developed using the Java web framework. The web application is developed using 3 tier architecture that involves user interface, controller and database. The user interface is a web page that is hosted on a server. Both static and dynamic contents will be present in the website. The data required for the application will be stored in database tables. Controller accesses the data from the database and provides it to the user through the user interface (web page).

KEYWORDS: NodeJS, AES, Blowfish, firebase, QR

I. INTRODUCTION

The file sharing System is a web based project. The Main purpose of this application will be to manage a file sharing site. The user can create pdf files in the database, each one with his assigned folder. Within this folder, the user can upload its files or download the one already in the folder already uploaded by the sender itself. When the sender/receiver uploads a file in a user folder, the user will receive an email alerting him of the new file and with a link to download in the File Sharing System. The user can also log into the system any time and look for previously uploaded files. Here we use AES algorithm to encrypt the textual file and Blowfish algorithm is used to encrypt the key that was sent by the sender to receiver.

Choosing AES algorithms :

Fifteen competing symmetric algorithm designs were subjected to preliminary analysis by the world cryptographic community, including the National Security Agency (NSA). In August 1999, NIST
selected 5 algorithms for more extensive analysis:

1 MARS, submitted by a large team from IBM Research;
2 RC6, submitted by RSA Security;
3 Rijndael, submitted by two Belgian cryptographers, Joan Daemen and Vincent Rijmen;
4 Serpent, submitted by Ross Anderson, Eli Biham and Lars Knudsen; and
5 Two fish, submitted by a large team of researchers from Counterpane Internet Security, including noted cryptographer Bruce Schneier.

Executions of the entirety of the above were tried broadly in American National Standards Institute (ANSI), C and Java dialects for speed and unwavering quality in the encryption and unscrambling cycles, key and calculation arrangement time, and protection from different assaults - both in equipment and programming driven frameworks. Nitti gritty investigations were directed by individuals from the worldwide cryptographic local area, including a few groups that attempted to break their own entries.

After much criticism, discussion and examination, the Rijndael figure was chosen as the proposed calculation for AES in October 2000. It was distributed by NIST as U.S. Government Information Processing Standards (FIPS) PUB 197, which was acknowledged by the secretary of business in December 2001.

AES got compelling as a government standard in 2002. It is additionally remembered for the International Organization for Standardization (ISO)/International Electro technical Commission (IEC) 18033-3 norm, which determines block figures with the end goal of information classification.

In June 2003, the U.S. government declared that AES could be utilized to secure grouped data. It before long turned into the default encryption calculation for securing ordered data, just as the main freely open and open code endorsed by the NSA for Top Secret data. The NSA picked AES as one of the cryptographic calculations to be utilized by its Information Assurance Directorate to ensure public safety frameworks.

The fruitful utilization of AES by the U.S. government prompted the calculation's far and wide use in the private area. AES has become the most famous calculation utilized in symmetric key cryptography. The straightforward determination measure set up by NIST made an undeniable degree of trust in AES among security and cryptography specialists.

II. RELATED WORK

Online File Sharing is the act of dividing documents between various clients across the Internet. Normal types of record sharing are FTP (File Transfer Protocol) model and P2P (Peer-to- Peer) document sharing organization. Another normal type of sharing documents over the Internet is for a client to transfer records to a site and permit different clients to download them from the site. There are a great deal of issues to think about when growing such a site.

Clients of an online document sharing site who use highlights like transfer, download, share, search and so on would need a site that is intelligent and quick and not irritating with a great deal of post backs and glimmering screens. Another issue is the perception of their record framework where generally clients have a cutoff to transfer documents. The ordinary electronic record organizer view would be acceptable, however on the off chance that there are different sorts of perceptions it would be incredible. Another significant issue to consider is the area where the site stores the transferred records. Two spots where one can store the transferred documents are Database and Server.

III. PROBLEM STATEMENT

These days Device storage is a major issue for user because we get limited storage which are either covered by multimedia or other apps which lacks space for important stuffs. Security is also a major concern for storing any important files or documents. The Data which is stored in the Mobile is not safe as it’s not that hard to hack a phone or a virus to destroy it or damage or theft any situation the user looses the files. This project introduces AES algorithm to encrypt the file which is not that much easy to decrypt the file because AES is an advanced algorithm. Blowfish algorithm is used to encrypt the key.

IV. PROPOSED WORK

Here the first user should register with all personal details they need to fill while registering time. After storing the details of each of them are sent to the sender then if the sender accepts then only that individual receiver can log in. After sending the details, the sender can log in and can upload the file. While uploading that file the QR code and private key will be generated for that file. Like that, if any receiver comes to registration after login that user can view that file in user inbox if the user needs that file they need to send an invitation to admin. Then if the second-hand needs the file, they send a letter of invitation to admin, In sender box sender can view what are the files available they will view and people who send request they will be viewed in the sender page. The receiver need to scan and enter the key so that the receiver can access the file.

V. PROCESS

Here 1st sender and receiver should have an account, They have to log in or sign up into the account to access the file. After logging in, the account centre has to upload the files. Next centre will get a QR Code and generate the password that both Should be sent to the receiver. Now receiver has to log into this account to access the file. Now the Receiver has to get the QR Code and the code or password to access the file. After getting QR Code and password the receiver has to scan the QR Code and enter the code or password then the receiver can access the file as the result.

AES -256 Algorithm :

The Advanced Encryption Standard (AES) is the first and only publicly accessible cipher approved by the US National Security Agency (NSA) for protecting top secret information. AES was first called Rijndael after its two developers, Belgian cryptographers Vincent Rijmen and Joan Daemen.[13] AES includes three block ciphers: AES-128, AES-192 and AES-256. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each round consists of various processing steps which includes substitution, transposition and mixing of the input plaintext to transform it into the resultant cipher text. First step of the cipher is to put the data into an array -- after which, the cipher transformations are repeated over multiple encryption rounds.

Firstly, transformation in the AES encryption cipher is substitution of data using a substitution table;
Secondly, transformation shifts data rows, and the third mixes columns. At long last, change is performed on each fragment using a substitute piece of the encryption key. Longer keys need more rounds to complete.

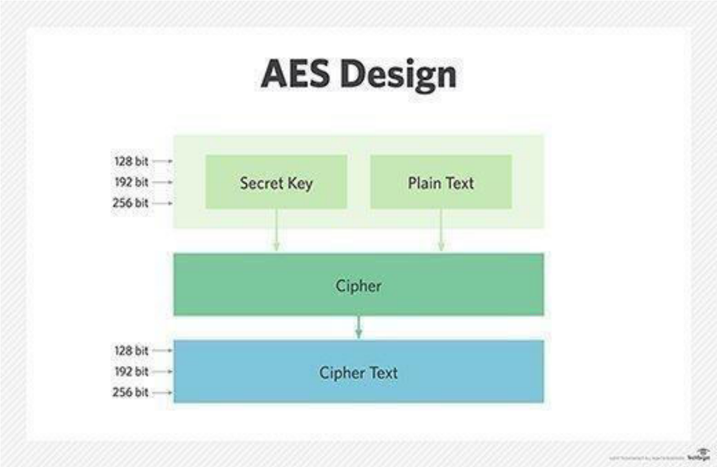


Fig 1. AES Design

Blowfish Algorithm:

An encryption strategy named Blowfish was planned in 1993 by Bruce Schneier as an option in contrast to DES Encryption Technique. It is more quicker than DES and gives a decent encryption rate with no viable cryptanalysis method found to date. It is one of the first, secure block ciphers which has not yet gained any patents and therefore it is freely available for anyone to use.

Block Size: 64-bits

Key Size: 32-bits to 448-bits variable size Number of sub keys: 18 [P-array] Number of rounds: 16
Number of S-boxes: 4 [each having 512 entries of 32-bits each]

Blowfish Encryption Algorithm:-
There are mainly three steps in Blowfish for encryption Step1: Generation of sub keys
Step2: initialize Substitution Boxes Step3: Encryption:
The encryption function consists of two parts:
Rounds: The encryption comprises of 16 rounds with each round(Ri) taking information sources the plaintext(P.T.) from past round and relating sub key(Pi).

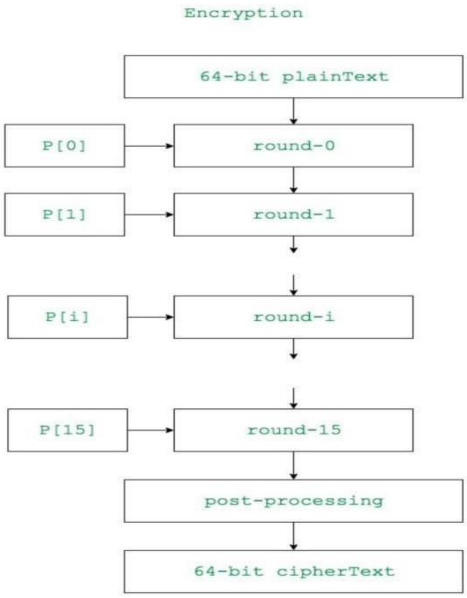


Fig 2 .Encryption for Blowfish

VI. CONCLUSION AND FUTURE ENHANCEMENT

It's anything but an extraordinary delight for us to deal with this astonishing and testing project It also provides knowledge about the latest technology used in developing web enabled applications and client server technology that will be in great demand in future. This will give good opportunities and guidance in the coming years for developing projects independently.

It can be implemented to upload files with a huge amount of size with the support of various file formats. This System being web-based and an undertaking of Cyber Security Division, needs to be
tested thoroughly to fill security gaps. A console for the data center may be made available to allow the personnel to monitor on the sites which were cleared for hosting during a particular period.
Furthermore, it is just a beginning; further the system may be utilized in different types of auditing operation viz. Network auditing or similar process/workflow based applications.

REFERENCES

[1]. Yima, The survey of the technologies of peer-to-peer.
[2]. Modern peer-to-peer file-sharing over the Internet:
http://www.limewire.com/index.jsp/p2p
[3]. http://www.openp2p.com/pub/a/p2p/2001/07/02/morpheus.html
[4]. Yang, B. & Garcia-Molina. Comparing Hybrid Peer-to-Peer Systems.
[5]. http://www.napster.com/help/win/faq/#x- 2 8 [6]. What is Gnutella?
http://www.gnutellanews.com/information/what_is_gnutella.shtml.
[7]. Sander, S. Investigating one incidence of anomalous network traffic. [8]. Super node specification:
http://groups.yahoo.com/group/the_gdf/files/Supernodes.html 11. Clarke, L.; Sandberg, O.; Wiley, B.; Hong,
T.W. (Edited by: Federrath, H.) Free net: a distributed anonymous information storage and retrieval system. Designing Privacy Enhancing Technologies. International Workshop on Design Issues in Anonymity and Unobservability. Proceedings (Lecture Notes in Computer Science Vol.2009), (Designing Privacy Enhancing Technologies. International Workshop on Design Issues in Anonymity and Unobservability. Proceedings (Lecture Notes in Computer Science Vol.2009), Designing Privacy Enhancing Technologies. International Workshop on Design Issues in Anonymity and Unobservability, Berkeley, CA, USA, 25-26 July 2000.) Berlin, Germany:
Springer-Verlag, 2001. p.46-66
[9]. Clarke, I. A distributed decentralized information storage and retrieval system. unpublished dissertation, University of Edinburgh, 1999.
[10]. Secure your data with AES-256 encryption, Data security Technologies, https://www.atpinc.com/blog/what-is-aes-256-encryption

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details