IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE FILE STORAGE IN CLOUD USING CRYPTOGRAPHY FOR COLLEGE VOTING SYSTEM

Pavithra. R [1]
Computer Science
Sri krishna arts and science college
Coimbatore, India

Aswin. G [2]
Computer Science
Sri krishna arts and science college
Dindigul, India

Jeevarathinam. A [3]
Computer Science
Sri krishna arts and science college
Coimbatore, India

***Abstract*---A SECURE FILE STORAGE IN CLOUD USING CRYPTOGRAPHY is a venture oversees documents holding the votes of understudies in a college political decision, in an encoded configuration and de-crypted for got admittance. This project involves the Principal, Departments, Users, where the Users vote for their desired Candidate. The Departments encrypt the votes in a file and transfers them to the College Principal. Principal collects, download, and decrypt the files from various departments of the College. The result of the Election is released in the R Tool by Graphical display. The point is to safely store data into the cloud by parting information into a few lumps and putting away pieces of it on the cloud in a way that jam information secretly, honesty and guarantees accessibility.**

Keywords--- cryptography,encryption, decryption, college voting, R tool, election.

I. INTRODUCTION

The data over the web is turning into a basic issue because of safety issues. We have proposed a system for securing important data from a file. Cryptography algorithms provide an effective way of protecting sensitive information. It is a technique for putting away and sending information in a structure that is just intelligible by proposed clients. When the file is being added to the server, the file gets converted into byte array. With the increasing computing power, it was considered vulnerable against exhaustive key search attacks[13].

II. LITERATURE SURVEY

The Data Encryption Standard (DES) is a symmetric-key block cipher. DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size of DES is 64-bit. Though key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm. RC2 (Rivest Cipher) is a symmetric-key block cipher.

Cryptography is utilized to get and secure information during correspondence. Encryption is a process that transforms the original information into an unrecognizable form. Decryption is a process of converting encoded/encrypted data in a form that is readable and understood by a human or a computer. The encryption method helps you to protect your confidential data such as passwords and login id. Public, Private, Pre-shared, and Symmetric are significant keys utilized in cryptography. A worker is sending fundamental reports to his/her director is an illustration of an encryption technique. The chief is accepting the fundamental encoded records from his/her worker and unscrambling it is an illustration of a decoding strategy.

Kurihara & Fukushima, 2017 explained, it is not digital cash, which has prevailed all over the world. Unlike central bank- and government-issued currency, Bitcoin can be inflated at will, the supply of Bitcoin is limited to a certain volume, which cannot be changed. Wonglimpiyarat, 2016 highlights that there are obstacles of lawless tender where Bitcoin wants the government's legislation to boost the permissibility of this new currency. Bitcoin currency may transform the future of banking in developing countries but it is hard to substitute a cash-based society.

RC4 Encryption-A Literature Survey This paper presents a survey showing how the RC4 stream cipher algorithm is crypt analysis. The author has summarized numerous RC4 algorithm vulnerabilities followed by the latest proposed improvements available in the literature. Imaginative exploration endeavors are needed to create steady and secure RC4 algorithm that can eliminate the RC4 shortcomings [6].

Evaluation of the RC4 algorithm for Data Encryption Mousa et al [9]. study the RC4 parameters and showed that the speed of encoding and decoding time is directly related to an enciphered key length and size of the data file, if the data is large enough. Data type is also important as image data needs a longer processing time than text or sound data due mainly to the larger file size. This relationship has been translated into equations to model these relationships and can therefore be used to predict the RC4's output under various conditions.

III. SYSTEM STUDY

A. *Existing System*

Appointive extortion alluded to as political decision misrepresentation, political race control, citizen extortion, or vote fixing, includes unlawful obstruction with the interaction of a political decision, either by expanding the vote portion of a supported up-and-comer, discouraging the vote portion of adversary applicants, or both.

Drawback of existing system:

- ✓ Expensive elections
- ✓ Misuse of official machinery
- ✓ Rigging of election and booth capturing
- ✓ Delay in the disposal of election petitions

B. *Proposed System*

The proposed system is an electronic voting system, where the votes are secured by an encryption feature preserved under the Principal surveillance. Nobody except the principal can access the documents, using cryptography techniques.

Ascendancy of proposed system:

- ✓ Increasing the level of participation
- ✓ Security
- ✓ Accessibility
- ✓ Efficiency
- ✓ Precision

IV. SOFTWARE DESCRIPTION

A. *Python Language Introduction*

Python is a widely-used general-purpose, high-level programming language.It was at first designed by Guido van Rossum in 1991 and created by Python Software Foundation. It was principally developed for emphasis on code lucidness, and its syntax permits developers to communicate ideas in less lines of code. Python is a programming language that allows you to work rapidly and coordinate frameworks all the more effectively.

There are two significant Python versions- Python 2 and Python 3. Both are quite different.

B. *Flask Framework*

In case you're building up a web application in Python, odds are you're utilizing a structure. A system "is a code library that makes a designer's life simpler when building reliable, versatile, and viable web applications" by giving reusable code or augmentations to normal activities.

There are several frameworks for Python, including Flask, Tornado, Pyramid, and Django.

Flask is generally new framework that has taken the Python web development community by storm: in a brief time frame, it got quite possibly the most well known structures around. It offers a ton of adaptability and clean code with a great deal of extensibility. You won't feel dragged down by a huge framework that tells you what to do; instead, you'll feel free, productive, and creative!

C. *MySQL*

A data set is a different application that stores an assortment of information. Each database has one or more distinct APIs for creating, accessing, managing, searching, and replicating the data it holds.

Other kinds of data stores can be used, such as files on the file system or large hash tables in memory but data fetching and writing would not be so quick and simple with those kinds of frameworks. So nowadays, we use relational database management systems (RDBMS) to store and manage a huge volume of data. This is called a relational database because all the data is stored in different tables and relations are established using primary keys or other keys known as foreign keys.

A Relational Data Base Management System (RDBMS) is a software that:

- ✓ Enables you to implement a database with tables, columns, and indexes.
- ✓ Ensures the Referential Integrity between rows of various tables.
- ✓ Updates the records consequently.
- ✓ Interprets an SQL query and joins information from different tables

V. MODULE DESCRIPTION

A. *Authentication Process*

In this system, the Principal directly logs in to the website while the Departments and Students registers and logs in to the website for the first time, if already had registered then can log indirectly. While registering, the Department has to feed in some details like Name of Head of the Department, Name of the Department, E-mail id, phone number, Year of Joining. On the other hand, the user (Students) has to register with details like Name, Register Number, Date of Birth, E-mail id[8].

B. *Encrypt Module*

In the department module, the Head of the Department logs in with the credentials, adds the students for voting, stores the votes in a document, encrypts the document, and finally sends it to the Principal[10].

The beneficiary gets the information and converts it. The lone single algorithm is used for encryption and decryption with a couple of keys where each use for encryption and decryption.

C. *Decrypt Module:*

In Principal Module, The Principal logs in, add candidates who are standing in the election, view candidates, manages the added votes, views the Documents received from various departments, decrypt the documents and presents the resultant report.

The individual who is sending the information to the objective. The similar algorithm with the similar key is utilized for the encryption-decryption process[12].

D. *User Module:*

In the user module, the user (students), logs in with their register number. Views the Candidates and drops their votes.

E. Chart Module:

In this module, the result of the election will be displayed in chart format in R studio tool with analysis format as department wise and end overall report who as win the position.

VI. ENCRYPTING AND DECRYPTING

Encryption is the way toward changing over ordinary message (plain text) into pointless message (Cipher text). While Decryption is the way toward changing over pointless message (Cipher text) into its unique structure (Plain text).

Table.1. Distinguish between Encryption and Decryption.

ENCRYPTION	DECRYPTION
Encryption is the way toward changing over ordinary message into insignificant message	Decryption is the way toward changing over futile message into its unique form
Its significant undertaking is to change over the plain content into cipher text	While its fundamental undertaking is to change over the code text into plain content
Encryption is the interaction which occur at sender's end	While decoding is the interaction which happen at beneficiary's end
Furthermore, message can be encoded with either secret key or public key	whereas the encoded message can be decoded with either secret key or private key
In encryption measure, sender sends the information to recipient after encrypted it	Whereas in decryption process, receiver receives the information and convert into plain text

The significant differentiation between secret writing and associated secret writing is that secret writing is the transformation of a message into an indiscernible kind that is undecipherable except if decoded. Though secret writing is that the recuperation of the main message from the encrypted data.

A. *Information from end to end*

Encryption is main form which in paper votes as been convert into notepad as plain text then encrypted the message and send to principal[8].

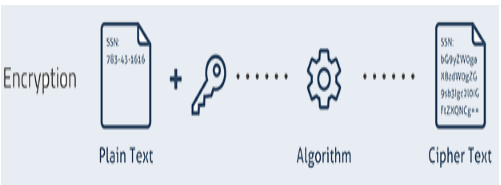

Fig.1. Plain text to Cipher text

After receiving all the department encrypted file the principal will decrypt the file with the help of keys and upload the votes to respective candidate then automatically result will be announce in the group[11].

Fig.2. Cipher text to Plain text

By this we can secure share the vote in the election process this paper deal with main about electron security purpose with the help of cryptography.

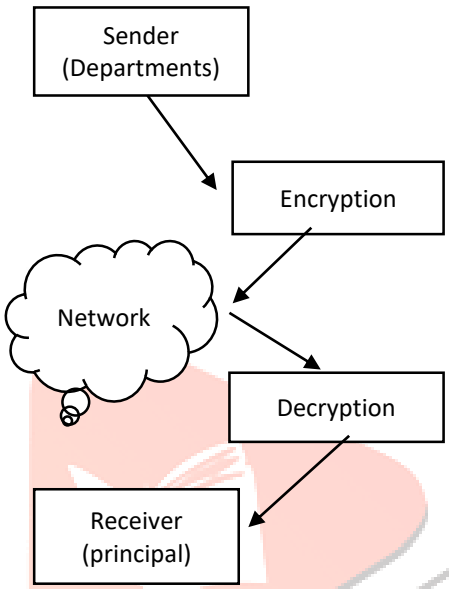

Fig.3. Role of cryptography in Networking

VII. CONCLUSION

This paper proved good for me as it provided practical knowledge of not only programming in PHP, HTML, CSS, and MySQL web-based application and no some extent Windows Application and Apache Server, but also about all handling procedure related to "secure file storage in the cloud using cryptography". 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 the future. This will give better opportunities and direction later on in creating projects autonomously.

VIII. FUTURE ENHANCEMENT

Future Enhancement of this system "secure file storage in the cloud using cryptography" is to implement in cloud computing and the data in Microsoft's one drive and implement this system in the mobile application.

IX. REFERENCES

[1] Luke Welling, Laura Thomson, "PHP and MySQL Web Development", 4th Edition,
[2] Publisher: Pearson Education Inc , Year :2009
[3] Rasmus Lerdorf, Kevin Tatroe , "Programming PHP" 2nd Edition, Publisher : O'Reilly Media Inc,2006
[4] W.Jason Gilmore , "Beginning PHP and MySQL" 3rd Edition, Publisher: Apress,2008
[5] Brad Bugler, Jay Greenspan ,David Wall, "MySQL and PHP Applications", 2nd Edition
[6] Publisher : Wiley 2003

[7] Michael kofler, "The Definitive Guide to MySQL 5 " 3rd Edition Publisher: Apress 2005

[8] https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography

[9] .Xiao Nie, Xiong Zhong "Security In the Internet of Things Based on RFID: Issues and Current Countermeasures" Proceedings of the Published by Atlantis Press, Paris, France.

[10] Yi-Pin Liao , Chih-Ming Hsiao "A secure ECCbased RFID authentication scheme integrated with ID-verifier transfer protocol " Department of computer science and information engineering , St.John's university,Taipei,ROC (2013), published by ELSEVIER, http://dx.doi.org/10.1016/j.adhoc.2013.02.004

[11] C.P. Schnorr," Efficient identification and signatures for smart cards", in: Gilles Brassard (Ed.), Advances in Cryptology – CRYPTO'89, Lecture Notes in Computer Science, 435, Springer-Verlag, 1989, pp. 239–252.

[12] T. Okamoto, "Provably secure and practical identification schemes and corresponding signature schemes", in: E.F. Brickell (Ed.), Advances in Cryptology – CRYPTO'92, Lecture Notes in Computer Science, 740, Springer-Verlag, 1992, pp. 31–53.

[13] [Y.K. Lee, L. Batina, I. Verbauwhede, "EC-RAC (ECDLP Based Randomized Access Control): Provably Secure RFID Authentication Protocol", IEEE International Conference on RFID, 2008, pp. 97–104.