Online Scientists Information System using AES

Suraj Kishor Desai
Computer Engineering
JSPM's, BSIOTR, Wagholi, Pune, India

Shahrukh Attar
Computer Engineering
JSPM's, BSIOTR, Wagholi, Pune, India

Sonali Haridas Mane
Computer Engineering
JSPM's, BSIOTR, Wagholi, Pune, India

Kalyan Bandu Dethe
Computer Engineering
JSPM's, BSIOTR, Wagholi, Pune, India

Archana Lomte, PhD
Computer Engineering
JSPM's, BSIOTR, Wagholi, Pune, India

ABSTRACT

Online Scientist Information Management System can be used by education institutes to maintain the records of scientists easily. Achieving this objective is difficult using a manual system as the information is scattered, can be redundant and collecting relevant information may be very time consuming. All these problems are solved using this project. We use the encryption algorithm for data security and OTP concept for email verification for valid user. The data protection is based on advance encryption algorithm for encryption and decryption files.

General Terms

AES Algorithm, SQL Queries

Keywords

Keywords: Online Scientist Information Management System(OSIMS), Web Technology, Record Maintains, Database, AES, OTP.

1. INTRODUCTION

In today's electronic age, the importance of digital cryptography in securing electronic data transactions is unquestionable. Every day, users electronically generate and communicate a large volume of information with others. This information includes medical, financial and legal files; automatic and Internet banking; phone conversations, pay-per-view television and other e-commerce transactions as well as military information and some top-secret government intel.[8] To meet these requirements, Advanced Encryption Standard (AES) for encryption of electronic data can be used. Governments prefer using AES for encryption of classified messages. Although no major attack on AES has been discovered yet, it is presumed that AES might have been broken without the attack being known to us. Thus, an added layer is used to make it safer.

The design and implementation of a comprehensive scientist information system and user interface is to replace the current paper records [1]. Staffs are able to directly access all aspects of scientists academic progress through a secure, online interface embedded in the website. The system utilizes user authentication, displaying only information necessary for an individual's duties. Additionally, each sub-system has authentication allowing authorized users to create or update information in that subsystem. All data is thoroughly reviewed and validated on the server before actual record alteration occurs. In addition to a staff user interface, the system plans for student user interface, allowing users to access information and submit requests online thus reducing processing time. All data is stored securely on MYSQL servers managed by the scientist's administrator and ensures highest possible level of security. The system features a complex logging system to track all users' access and ensure conformity to data access guidelines and is expected to increase the efficiency of the scientist record management thereby decreasing the work hours needed to access. This system provides a simple interface for the maintenance of scientist information. It can be used by educational institutes or colleges to maintain the records of students easily. Achieving this objective is difficult using a manual system as the information is scattered, can be redundant and collecting relevant information may be very time consuming. All these problems are solved using online scientist information management system. The paper focuses on presenting information in an easy and intelligible manner which provides facilities like online registration and profile creation of student's thus reducing paper work and automating the record generation process in an educational institution.

2. PROBLEM STATEMENT

Achieving the data protection and data retrieval any system, the objective is difficult using a manual system as the information is scattered, can be redundant and collecting relevant information may be very time consuming.

3. LITERATURE SURVEY

A. Paper name: Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach

Author name: Flevina Jonese D'souza, Dakshata Panchal

Description: This paper [1] AES is proved to be highly secure, faster and strong encryption algorithm. AES is used commonly because of its great competence and easiness. But in recent years cyber-attacks are continuously developing, therefore security specialists must stay busy in the lab inventing new schemes to keep attackers at bay. Possible attacks on symmetric algorithm can be Brute-force Attack, Differential Attack, Algebraic Attack and Linear Attack. So to provide strong security in message transmission, AES algorithm with hybrid approach of Dynamic Key Generation and Dynamic S-box Generation is proposed.

B. Paper name: Toward a Student Information System for Sebha University

Author name: Almahdi Alshareef, Ahmed Alkilany

Description: This paper [2] basically focuses on providing a simple interface for the easy collation and maintenance of all manner of student information. The creation and management of accurate, up-to- date information regarding students' academic careers is critical students and for the faculties and administration of Sebha University in Libya and for any other educational institution. A student information system deals with all kinds of data from enrollment to graduation, including program of study, attendance record, payment of fees and examination results to name but a few. All these data need to be made available through an onlineinterface.

C. Paper name: A Study of Student Information Management Software

Author name: Prabhu T Kannan, Srividya K Bansal

Description: This paper [3] focuses on providing information to support the operation, management and decision-making functions of enterprises or organizations. In the face of huge amount of information, it is required to possess the student information management system to improve the efficiency of student management. Through this system, the standardized management, scientific statistics and fast query of student information can be realized, and thus the workload of management can be reduced. In this paper, a typical student information management system will be established to realize the systematization, standardization and automation of student information relationship.

D. Paper name: Web Based Student Information System

Author name: S.R.Bharamagoudar, Geeta R.B, S.G.Totad

Description: This paper [4] focuses on simple interface for maintenance of student information. The creation and management of accurate, up-to- date information regarding a student's academic career is critically important in the university as well as colleges. Student information system deals with all kind of student details, academic related reports, college details, course details, curriculum, batch details, placement details and other resource related details too. It tracks all the details of a student which can be used for all reporting purpose, tracking of attendance, progress in the course, completed semesters, years. Different reports and Queries can be generated based on vast options related to students, batch, course, faculty, exams, semesters, certification and even for the entire college.

4. PROPOSED SYSTEM

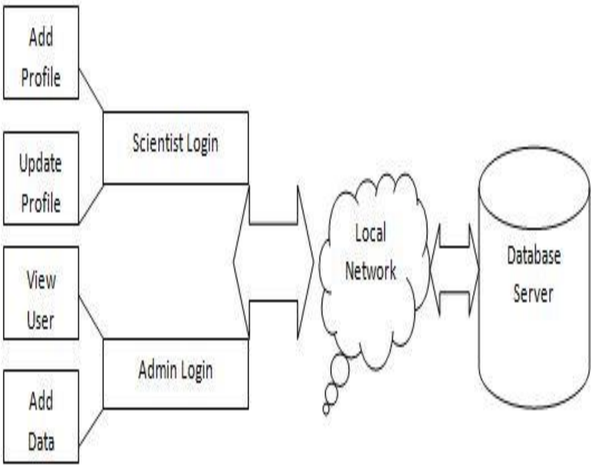

Fig 1. System architecture

Scientist:

The scientist is of center focus ,because in every research development team plays the very important role. Scientist can access the information of the all.

Admin:

Each Admin has one file that enables them to keep their scientist records securely and access information all in one place.

That single database file allows administrators to have up-to-date information about the scientist and their profile at any time.

Server:

Here we use the local server to communicate and stored the important records of the scientist.

Security:

SQL injection is a code injection technique, used to attack data-driven applications, in which nefarious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database.

Data Security:

Here we add the new model for security for all files for avoids data leakage. Here we use the AES algorithm for encryption process on all important files.

OTP:

Here OTP is used for validated user or not at initial stage on registration email. If email is valid then application can process next step.

5. ALGORITHM PROCESS

Encryption Process:

KeyGenCE(M) → K is the key generation algorithm that maps a data copy M to a convergent key K;

EncCE(K,M) → C is the encryption algorithm that takes both the convergent key K and the data copy M as inputs and then outputs cipher text C;

DecCE(K,C) → M is the decryption algorithm that takes both the cipher text C and the convergent key K as inputs and then outputs the original data copy M;

Steps:

1. Initially the user selects the file from the disk for the encryption process.
2. On selecting the files, the user must enter 16 bytes SecretKey as a password.
3. After entering the 16 bytes SecretKey, the user must re-enter to confirm password and Click on encrypt.
4. The encrypted file is created with FilenameEncryption.txt in a disk. The encrypted files are set as read only. 5.
5. To decrypt the encrypted text files, go to the decrypt screen. Select the encrypted files and enter the same SecretKey which is used for encryption process.

6. RESULT AND DISCUSION

Table 1: Algorithm comparison table

DES	AES
DES stands for Data Encryption Standard	AES stands for Advanced Encryption Standard
Key length is 56 bits in DES.	Key length can be of 128-bits, 192-bits and 256-bits.
DES can be broken easily as it has known vulnerabilities.	AES is more secure than the DES cipher and is the de facto world standard.
DES can encrypt 64 bits of plaintext.	AES can encrypt 128 bits of plaintext.
DES cipher is derived from Lucifer cipher.	AES cipher is derived from square cipher.

Table 2: Processing time

Parameter	File size	Image size
Encryption	100kb	100kb
Decryption	100kb	100kb
Processing Time	5sec	8sec

7. CONCLUSION

This system assists in automating the existing manual system. This is a paperless work. It can be monitored and controlled remotely. It reduces the man power required. It provides accurate information always. Malpractice can be reduced. All years together gathered information can be saved and can be accessed at any time. The data which is stored in the repository helps in taking intelligent decisions by the management. So it is better to have a Web Based Online Scientist Information Management system.

8. REFERENCES

[1] Flevina Jonese D’souza, Dakshata Panchal “Advanced Encryption Standard (AES) Security Enhancement using Hybrid Approach”, International Conference on Computing, Communication and Automation (ICCCA2017).

[2] Almahdi Alshareef, Ahmed Alkilany "Toward a Student Information System for Sebha University, Libya",Fifth international conference on Innovative Computing Technology (INTECH 2015)-p 34-39.

[3] Prabhu T Kannan, Srividya K Bansal,"Unimate: A Student Information System",2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI)-p-1251-1256.

[4] S.R.Bharamagoudar, Geeta R.B, S.G.Totad, “Web service api for student information and course management systems”International Journal of Advanced Research in Computer and Communication Engineering Vol. June 2013.

[5] Hanan A. Al-Souly, Abeer S. Al-Sheddi, Heba A. Kurdi “Enhanced TSFS Algorithm for Secure Database Encryption” Science and Information Conference 2013. -p328-335.

[6] D.Manivannan, R.Sujarani “Light Weight and Secure Database Encryption using TSFS Algorithm”.

[7] Li Qian, Jun Hu, Shuying Liu “SQL Injection Attack and Prevention Technology” International Conference on Estimation, Detection and Information Fusion(ICEDIF 2015) -p-303-307.

[8] System and method for communicating student information among student, parents guardians and educators.(US 20060127870 A1) [8] Web service api for student information and course management systems(US20080085502A1).

[9] Extended AES Algorithm with Custom Encryption for Government-level Classified Messages Sreyam Dasgupta, Pritish Das International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-8, June, 2019

[10] Archana C. Lomte” Biometric fingerprint authentication for security using minutiae matching, “international journal of computer application, 2015.