Employee Work Log Management

Last updated on: 05.02.2018

Vivek Vellaiyappan Surulimuthu
Engineer

Abstraction

This document explains about the development of a web application that is used to safely secure Employee Working Hours information that includes but not limited to sensitive information such as employee login credentials, private notes, working hours being logged and so on. This securement of the information is done by using AES (Advanced Encryption Standard) to encrypt-cum-decrypt it. Hashing algorithms are also used to provide extra security.

Keywords:

128-bit AES, SHA3-256

Introduction

Security plays an important role ever since the digital technology came into existence. Many mathematicians and computer scientists have come up with lots of ideas to improve security features.

In this project, we aim to secure the vital information of the employees in any organization by using the security algorithms. The AES and SHA-3 algorithms are used to safely secure the information.

Related Work

In the past, while creating this project, to secure the login credentials, only the simple recovery answer or email being used. Also, the data were not secured.

Methodology

To achieve the aim of this project successfully, Django web framework being used with python's cryptographic libraries to secure the information. The actions involved are discussed below.

Methodology - Security Layers Implementation

I. Additional Layer of Encryption

II. Login Information

- Organization ID: User registers using the organization ID.
- Email Recovery: User have the options of recovering after verifying received random credentials - email authentication
- 2-Step Authentication: User can login using the real-time 2-step authentication feature - password and random password received via mail
- Using SHA-3 256, storing the hashed data as encrypted information in the database and matching the input hashed information accordingly to provide the raw data back to the user if it matches with the one in the db along with username.

III. Working Log Information

- Using AES 256 encryption, storing the encrypted information in the database and decrypting accordingly to provide the raw data back to the user.

Experiments

Experimented with the data by using the caesar cipher over the information.

Discussion/Analysis

- Everything worked as planned.
- Planning to implement AES and SHA-3 combined to provide additional security

Conclusion

Encryption algorithms are awesome and this project helps me to understand the stuffs happening around such algorithms to safely secure the data in real time. Additional features will be added to this project to provide extra secureness to the information.

References

- A. Stanoyevitch, Introduction to Cryptography with Mathematical Foundations and Computer Implementations, 1st Ed. 2010. (IC).
- N. Ferguson, et.al., Cryptography engineering: design principles and practical applications, John Wiley & Sons, 2011. (CE).
- https://en.wikipedia.org/wiki/Secure_Hash_Algorithms
- https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf
- https://en.wikipedia.org/wiki/SHA-3