Enhancing Encryption Mechanisms using SHA-512 for user Authentication through Password & Face Recognition

Publisher: IEEE

Cite This PDF

Anurag Vankadara ; Varun Myneni ; Harish Pendyala ; Divya Vadlamudi All Authors

73
Full
Text Views

Abstract

Document Sections

I. Introduction

II. Levels of Authentication

III. Authentication Mechanisms

IV. Proposed Solution

V. Authentication Framework

Show Full Outline

Authors

Figures

References

Keywords

Metrics

Abstract:
Authentication is a process that is used to verify the identities of users, before allowing them access to the system. Authentication technology controls access to systems by comparing a user's credentials to those stored in a database of authorized users or on a data authentication server. Authentication ensures secure business processes, secure systems, and secure corporate data. There are a lot of authentication mechanisms employed by many technological entities and enterprises to validate their customers or employees. Every entrepreneurial, educational businesses like multi-national companies, institutions etc., uses web applications or websites for their business, marketing and growth of their enterprise and user authentication has become a must and should component in all their web applications, for their ERPs, with at least the basic level of authentication like passwords. But, the vastly growing technology also has its own negative side of people, who are a threat to the information of the companies, which made them to employ safer security measures. Inspite of increas ing their s ecuri ty mechanis ms in websites, there is still a lot of data being stolen by the people, who are a threat-hackers or attackers and increased their ability to adopt the newer and advanced security measures. This study has conducted some research in these areas and found out that, when a user data or an employee's data is procured by the hackers that almost compromises the security of the system and we've thought of a solution that can be used to increas e the security at the us er end. To sustain any data breach upon the attacks on the database we planned to use SHA-512 encryption for their databas es in order to increas e the data security and a second level of authentication, face recognition using Machine Learning models. As per the user data encryption done using SHA-512 algorithm, better encryption standards are provided.

Published in: 2023 International Conference on Inventive Computation Technologies (ICICT)

Date of Conference: 26-28 April 2023

DOI: 10.1109/ICICT57646.2023.10134233

Date Added to IEEE *Xplore*: 01 June 2023

Publisher: IEEE

ISBN Information:

Conference Location: Lalitpur, Nepal

ISSN Information:

I. Introduction

Most of the web applications still employ the outdated user authentication system. The usemame and password will be saved directly into the database without any encryptions when using the old approach such that the attackers would gain access to all credentials in the event of a cyberattack. Later, databases like Oracle introduced simple to decipher default encryption techniques like AES & DES. The SSL encryption in HTTPS connections utilising TCP/IP was developed to stop decryptions by creating a secure encrypted channel with RSA encryption. notwithstanding the possibility of code the data that was sniffed. After conducting extensiv d a way to stop all potential threats. Such that implementing direct SHA-512 encryption in application itself such that encrypted data will pass through the SSL channel and stored in database. Even if the data is sniffed, no one can decrypt it. At the least case possible, if any attacker decrypts the data from the database, he can't pas s through the facial recognition authentication. By this we are

Sign in to Continue Reading

Need Full-Text access to IEEE *Xplore* for your organization?

CONTACT IEEE TO SUBSCRIBE >

More Like This

Feature Selection Based on Machine Learning Algorithms: A weighted Score Feature Importance Approach for Facial Authentication
2022 3rd International Informatics and Software Engineering Conference (IISEC)
Published: 2022

A Novel Authentication Method for Password Encryption
2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)
Published: 2020

Show More

10 YEARS

IEEE *Access* is celebrating its 10 Year Publishing Anniversary!

View the top 10 articles published over the last decade based on downloads, citations, and overall impact in IEEE fields of interest.

View Articles

Authors

Figures

References

Keywords

Metrics

© Copyright 2024 IEEE - All rights reserved, including rights for text and data mining and training of artificial intelligence and similar technologies.

Feedback