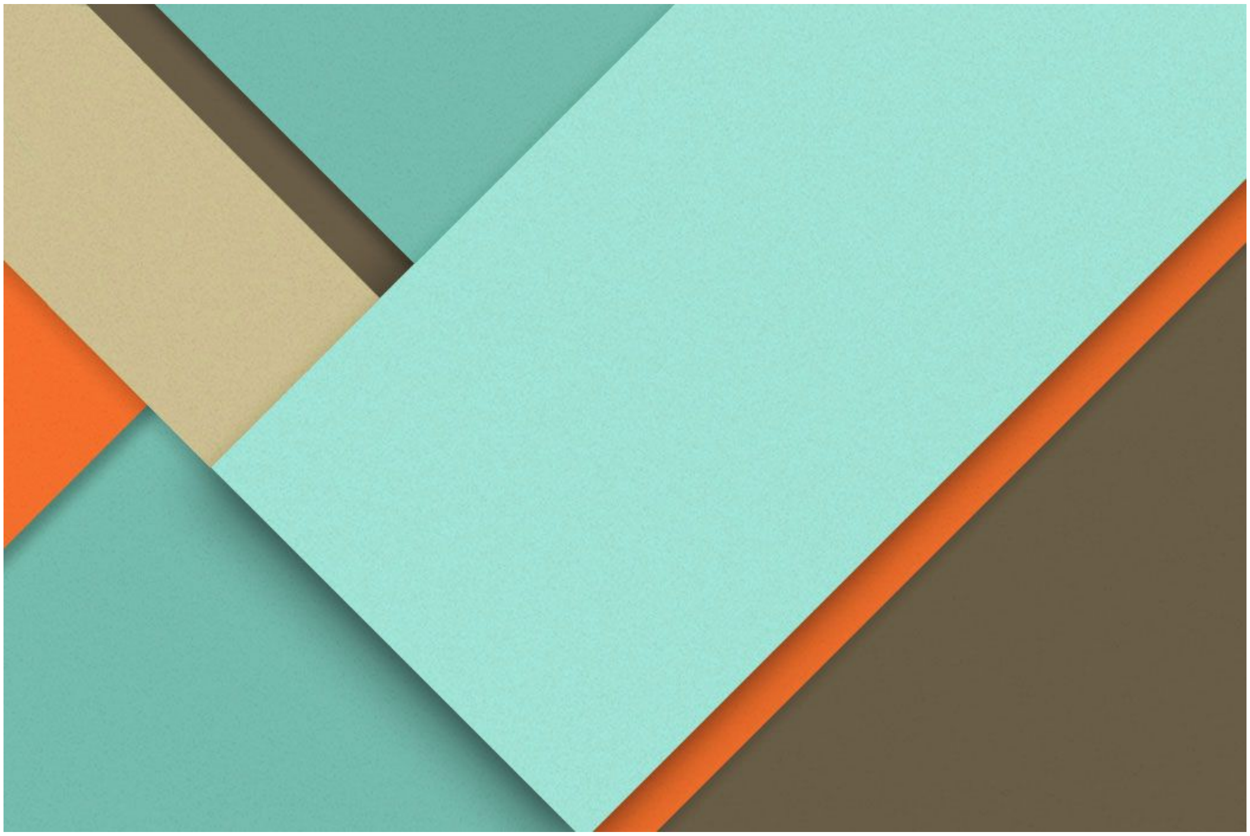


Presentation Evaluation Tool

Last updated on: 05.07.2018

Vivek Vellaiyappan Surulimuthu

MSCS 630 - Security Algorithms and Protocols

Project Final Write-up

Computer Science Engineer

Abstraction

This document explains about the development of a web application that is used to safely secure Peer review of presentation skills evaluation of presenters' that includes but not limited to sensitive information such as being presentation skills evaluation over others, reviewing the received evaluation 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:

AES, SHA2-256, Django, Pyaes, Sqlite3, HTML, CSS, Bootstrap

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 evaluation reviews by using the security algorithms. The AES and SHA-2 algorithms are used to safely secure the information.

Related Work

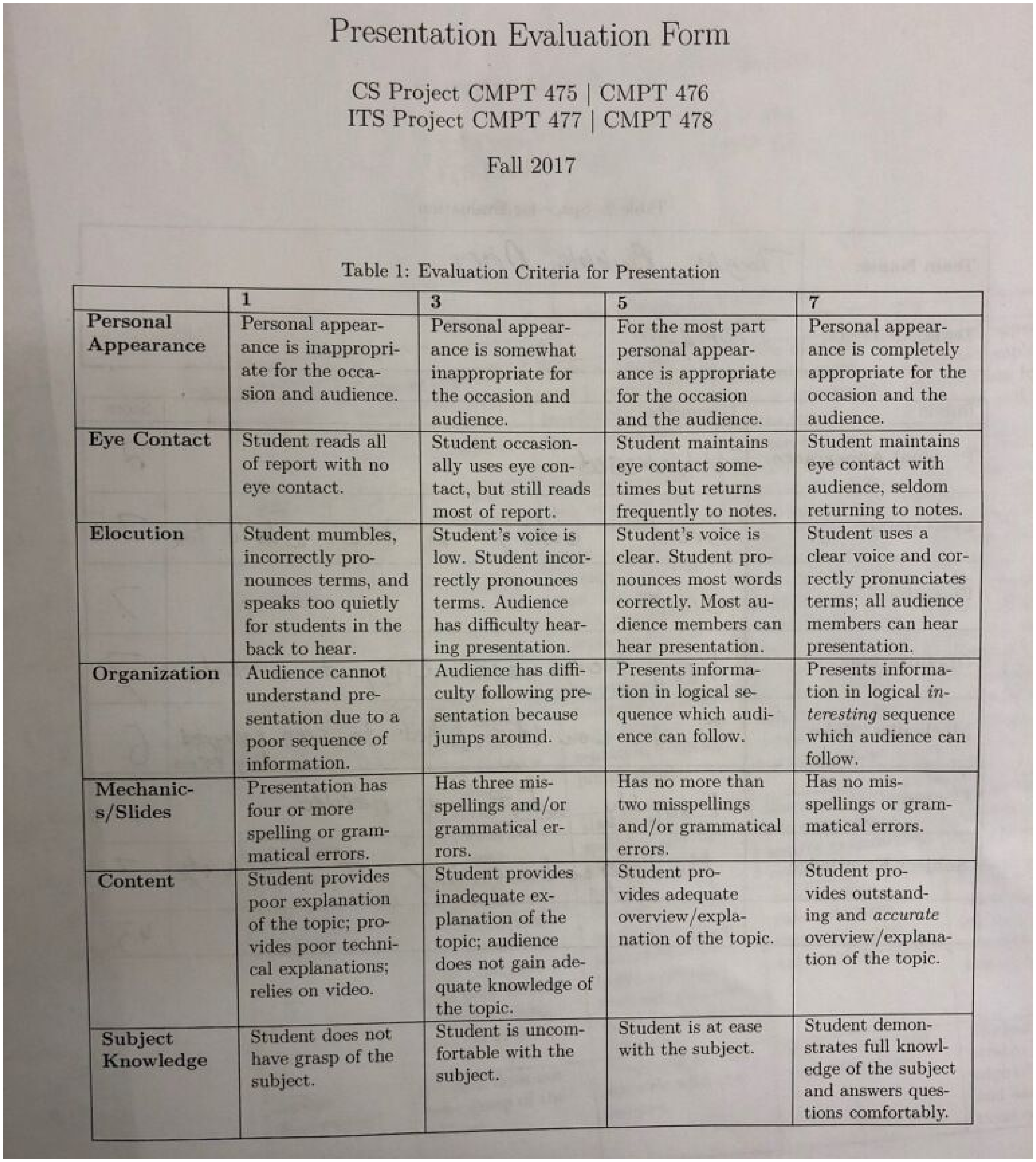
In the past, while creating this project, to secure the login credentials, only the simple recovery answer or email being used. Also, the data were not secured.

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.

The Problem to resolve

The Evaluation Paper being used: (The spec sheet form - design content)



Presentation Evaluation Form

CS Project CMPT 475 | CMPT 476
ITS Project CMPT 477 | CMPT 478

Fall 2017

Table 1: Evaluation Criteria for Presentation

	1	3	5	7
Personal Appearance	Personal appearance is inappropriate for the occasion and audience.	Personal appearance is somewhat inappropriate for the occasion and audience.	For the most part personal appearance is appropriate for the occasion and the audience.	Personal appearance is completely appropriate for the occasion and the audience.
Eye Contact	Student reads all of report with no eye contact.	Student occasionally uses eye contact, but still reads most of report.	Student maintains eye contact sometimes but returns frequently to notes.	Student maintains eye contact with audience, seldom returning to notes.
Elocution	Student mumbles, incorrectly pronounces terms, and speaks too quietly for students in the back to hear.	Student's voice is low. Student incorrectly pronounces terms. Audience has difficulty hearing presentation.	Student's voice is clear. Student pronounces most words correctly. Most audience members can hear presentation.	Student uses a clear voice and correctly pronunciates terms; all audience members can hear presentation.
Organization	Audience cannot understand presentation due to a poor sequence of information.	Audience has difficulty following presentation because jumps around.	Presents information in logical sequence which audience can follow.	Presents information in logical *interesting* sequence which audience can follow.
Mechanics/Slides	Presentation has four or more spelling or grammatical errors.	Has three misspellings and/or grammatical errors.	Has no more than two misspellings and/or grammatical errors.	Has no misspellings or grammatical errors.
Content	Student provides poor explanation of the topic; provides poor technical explanations; relies on video.	Student provides inadequate explanation of the topic; audience does not gain adequate knowledge of the topic.	Student provides adequate overview/explanation of the topic.	Student provides outstanding and *accurate* overview/explanation of the topic.
Subject Knowledge	Student does not have grasp of the subject.	Student is uncomfortable with the subject.	Student is at ease with the subject.	Student demonstrates full knowledge of the subject and answers questions comfortably.

Problems because of using Paper for presentation skills evaluation

- Time
    - Reducing the efforts of professors time
    - Print out
    - Distribution of evaluation papers to students
- Resource
    - Paper
    - Printer (electricity, printing ink)
    - Money (to buy paper, printer, writing pen/pencil)
- Data remains data
    - Presenter unable to keep track of received data
    - Unable to compare all students' marks in real time efficiently.
    - Peer-to-peer review is hard (if applicable)
    - Data analysis over different students' presentation skills
- Labor
    - Manually input the presenter's final evaluated scores into iLearn
    - Have to collect the returned papers and calculate the marks

Solution Description:

- Using a Secure Progressive Web Application to record and keep track of the evaluation points over the presenters' presentation.

Why it's better than existing Paper Usage

- Security
    - All data are securely stored using AES algorithm and SHA. Professor's password will be used as key to unlock the encrypted data
- Time
    - All the evaluators can fill out the evaluation online in real time at ease
- Resource
    - Avoiding the use of paper and thus saving natural resources, printer and thus saving money being spent
- Data remains data
    - Professor can now have a better insights of the presenters' marks
    - Presenters' can review their marks and comments anytime in future at ease

  - Data analysis over presenter’s attributes can be done.
- Labor
  - All the evaluated data is recorded in real time and thus removing professor’s painful manual entry

What’s the Planning and Requirement

- **Objective:**
  - To reduce the efforts taken by the professors for presenters’ presentation evaluation
  - To get better data insights over the received marks of the presenter
  - To keep track or review the received marks by Presenter
- **Requirements / Specsheet:**
  - A way to avoid aforementioned problems in real time at ease - This can be done in Web or Mobile app using the ‘Presentation Evaluation Tool’ project concept.
  - End User: Professor, Presenter and Rosters
  - Have to choose either web or mobile or both platform
  - Security features implementation
  - Language Selection
  - Frontend Backend Libraries Hosting website

Software Requirements

Platform: Web Application **Language Specification:** Frontend languages Django-2.0.4 Python-3.6.5 Sqlite3	**Security Implementation:** SHA2 AES Pyaes-1.6.1 - python library **IDE:** Pycharm

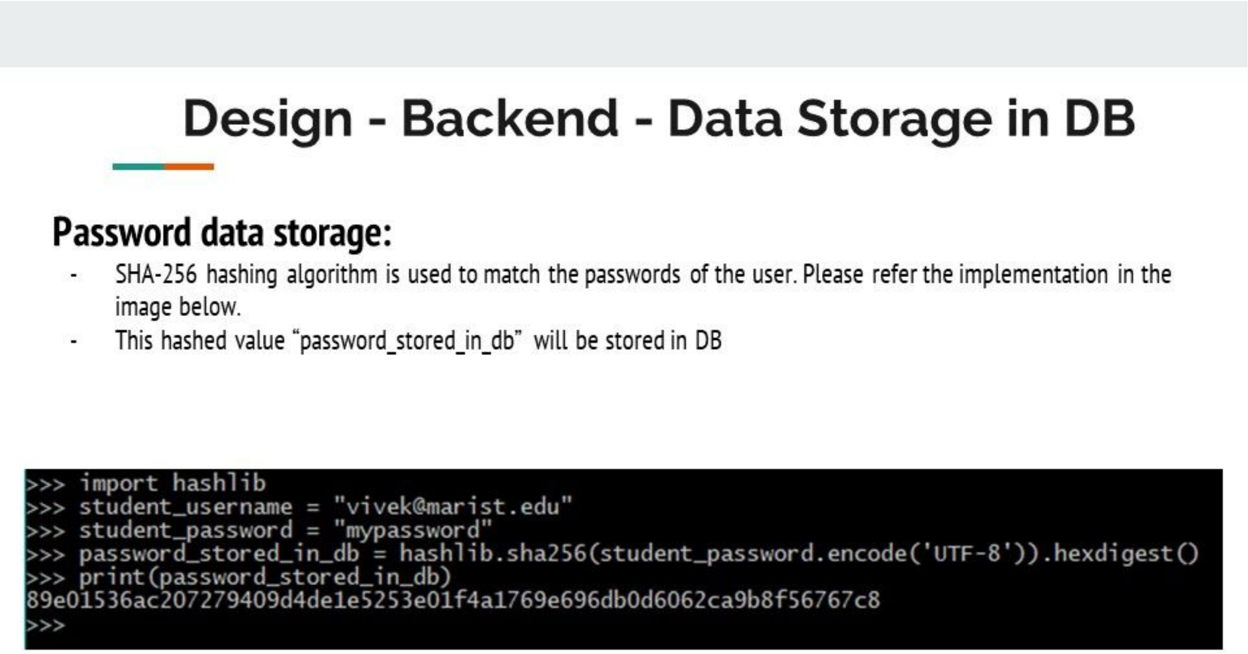
Methodology - Security Layers Implementation

I. Additional Layer of Encryption

- The password is first AES encrypted, hashed and then stored in the database

II. Login Information

- Student ID: student's email ID being used.
- 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-2 256, 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.



Design - Backend - Data Storage in DB

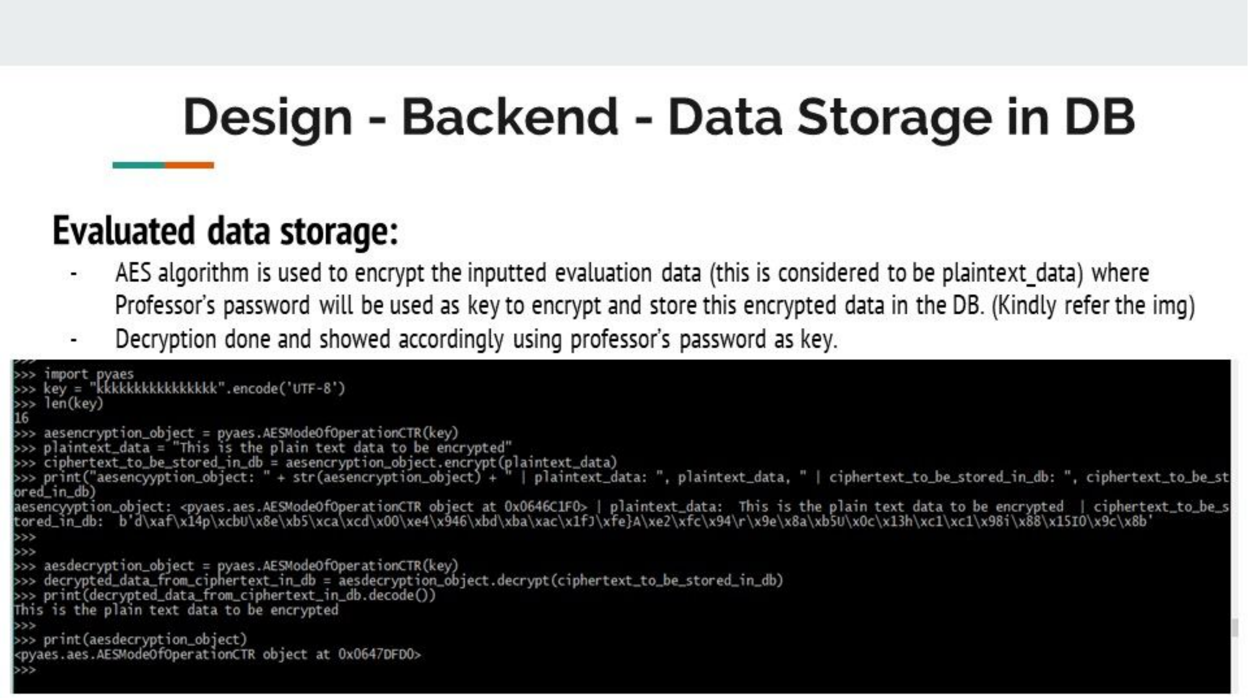
Password data storage:

- SHA-256 hashing algorithm is used to match the passwords of the user. Please refer the implementation in the image below.
- This hashed value "password_stored_in_db" will be stored in DB

```
>>> import hashlib
>>> student_username = "vivek@marist.edu"
>>> student_password = "mypassword"
>>> password_stored_in_db = hashlib.sha256(student_password.encode('UTF-8')).hexdigest()
>>> print(password_stored_in_db)
89e01536ac207279409d4de1e5253e01f4a1769e696db0d6062ca9b8f56767c8
>>>
```

III. Evaluated Information

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



Design - Backend - Data Storage in DB

Evaluated data storage:

- AES algorithm is used to encrypt the inputted evaluation data (this is considered to be plaintext_data) where Professor's password will be used as key to encrypt and store this encrypted data in the DB. (Kindly refer the img)
- Decryption done and showed accordingly using professor's password as key.

```
>>> import pyaes
>>> key = "kkkkkkkkkkkkkkkk".encode('UTF-8')
>>> len(key)
16
>>> aesencryption_object = pyaes.AESModeOfOperationCTR(key)
>>> plaintext_data = "This is the plain text data to be encrypted"
>>> ciphertext_to_be_stored_in_db = aesencryption_object.encrypt(plaintext_data)
>>> print("aesencyyption_object: " + str(aesencryption_object) + " | plaintext_data: ", plaintext_data, " | ciphertext_to_be_stored_in_db: ", ciphertext_to_be_st
ored_in_db)
aesencyyption_object: <pyaes.aes.AESModeOfOperationCTR object at 0x0646C1F0> | plaintext_data:  This is the plain text data to be encrypted  | ciphertext_to_be_s
tored_in_db:  b'd\xaf\x14p\xcbU\x8e\xb5\xca\xcd\x00\xe4\x946\xbd\xba\xac\x1fJ\xfe}A\xe2\xfc\x94\r\x9e\x8a\xb5U\x0c\x13h\xc1\xc1\x98i\x88\x15I0\x9c\x8b'
>>>
>>>
>>> aesdecryption_object = pyaes.AESModeOfOperationCTR(key)
>>> decrypted_data_from_ciphertext_in_db = aesdecryption_object.decrypt(ciphertext_to_be_stored_in_db)
>>> print(decrypted_data_from_ciphertext_in_db.decode())
This is the plain text data to be encrypted
>>>
>>> print(aesdecryption_object)
<pyaes.aes.AESModeOfOperationCTR object at 0x0647DFD0>
>>>
```

Design - Backend - DB designing

- My Aim: to reduce database data redundancy and to have a consistent data integrity
- Used Bridge or Junction Methodology and Normalization concepts to achieve my aim

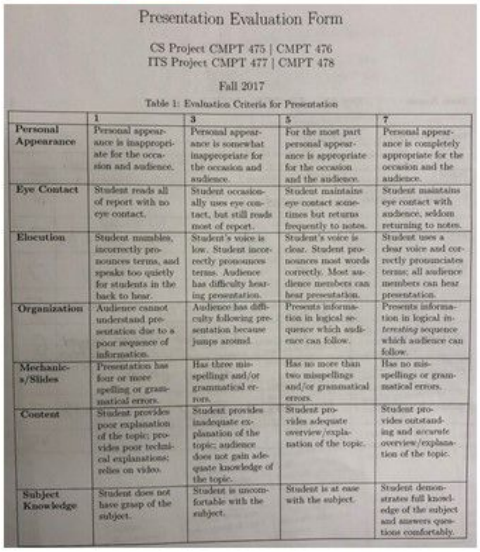
Design - Backend - Data Storage in DB - Password data storage:

- SHA-256 hashing algorithm is used to match the passwords of the user. Please refer the implementation in the image below.
- This hashed value "password_stored_in_db" will be stored in DB

Design - Backend - Data Storage in DB - Evaluated data storage:

- AES algorithm is used to encrypt the inputted evaluation data (this is considered to be plaintext_data) where Professor's password will be used as key to encrypt and store this encrypted data in the DB. (Kindly refer the img)
- Decryption done and showed accordingly using professor's password as key.

Wireframes - specSheet Content



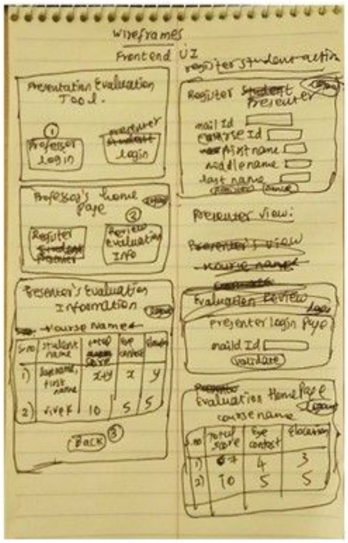
Presentation Evaluation Form

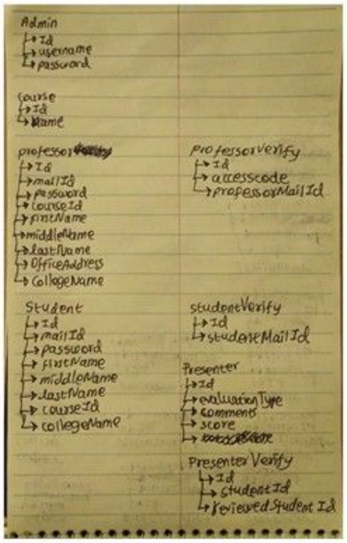
CS Project CMPT 475 | CMPT 476
ITS Project CMPT 477 | CMPT 478

Fall 2017

Table 1: Evaluation Criteria for Presentation

	1	3	5	7
Personal Appearance	Personal appearance is inappropriate for the occasion and audience.	Personal appearance is somewhat inappropriate for the occasion and audience.	For the most part personal appearance is appropriate for the occasion and the audience.	Personal appearance is completely appropriate for the occasion and the audience.
Eye Contact	Student reads all of report with no eye contact.	Student occasionally uses eye contact, but still reads most of report.	Student maintains eye contact sometimes but returns frequently to notes.	Student maintains eye contact with audience, seldom returning to notes.
Elocution	Student mumbles, incorrectly pronounces terms, and speaks too quietly for students in the back to hear.	Student's voice is low. Student incorrectly pronounces terms. Audience has difficulty hearing presentation.	Student's voice is clear. Student pronounces most words correctly. Most audience members can hear presentation.	Student uses a clear voice and correctly pronunciates terms; all audience members can hear presentation.
Organization	Audience cannot understand presentation due to a poor sequence of information.	Audience has difficulty following presentation because jumps around.	Presents information in logical sequence which audience can follow.	Presents information in logical *interesting* sequence which audience can follow.
Mechanics/Slides	Presentation has four or more spelling or grammatical errors.	Has three misspellings and/or grammatical errors.	Has no more than two misspellings and/or grammatical errors.	Has no misspellings or grammatical errors.
Content	Student provides poor explanation of the topic; provides poor technical explanations; relies on video.	Student provides inadequate explanation of the topic; audience does not gain adequate knowledge of the topic.	Student provides adequate overview/explanation of the topic.	Student provides outstanding and accurate overview/explanation of the topic.
Subject Knowledge	Student does not have grasp of the subject.	Student is uncomfortable with the subject.	Student is at ease with the subject.	Student demonstrates full knowledge of the subject and answers questions comfortably.





Admin
- Id
- username
- password

course
- Id
- Name

professor
- Id
- mailId
- password
- courseId
- firstName
- middleName
- lastName
- OfficeAddress
- CollegeName

Student
- Id
- mailId
- password
- firstName
- middleName
- lastName
- courseId
- collegeName

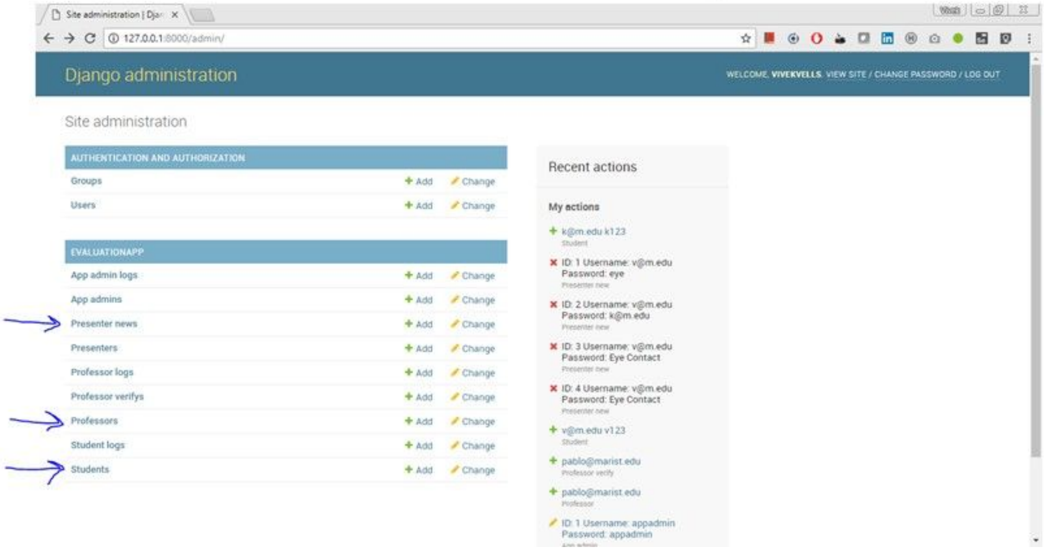
ProfessorVerify
- Id
- accesscode
- professorMailId

studentVerify
- Id
- studentMailId

Presenter
- Id
- evaluationType
- comments
- score

PresenterVerify
- Id
- studentId
- ReviewedStudent Id

Backend - Django Models


Site administration | Dja
127.0.0.1:8000/admin/
Django administration
WELCOME, VIVEKVELLS. VIEW SITE / CHANGE PASSWORD / LOG OUT

Site administration

AUTHENTICATION AND AUTHORIZATION		
Groups	+ Add	Change
Users	+ Add	Change

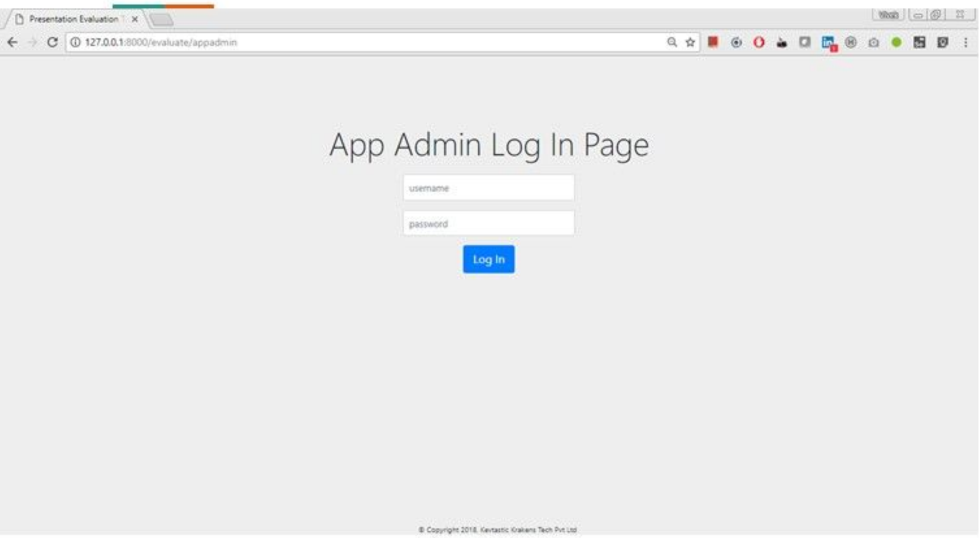
EVALUATIONAPP		
App admin logs	+ Add	Change
App admins	+ Add	Change
Presenter news	+ Add	Change
Presenters	+ Add	Change
Professor logs	+ Add	Change
Professor verifys	+ Add	Change
Professors	+ Add	Change
Student logs	+ Add	Change
Students	+ Add	Change

Recent actions

My actions

- + k@m.edu k123
  Student
- ✗ ID: 1 Username: v@m.edu
  Password: eye
  Presenter new
- ✗ ID: 2 Username: v@m.edu
  Password: k@m.edu
  Presenter new
- ✗ ID: 3 Username: v@m.edu
  Password: Eye Contact
  Presenter new
- ✗ ID: 4 Username: v@m.edu
  Password: Eye Contact
  Presenter new
- + v@m.edu v123
  Student
- + pablo@marist.edu
  Professor verify
- + pablo@marist.edu
  Professor
- ID: 1 Username: appadmin
  Password: appadmin
  App admin

Website UI - App Admin

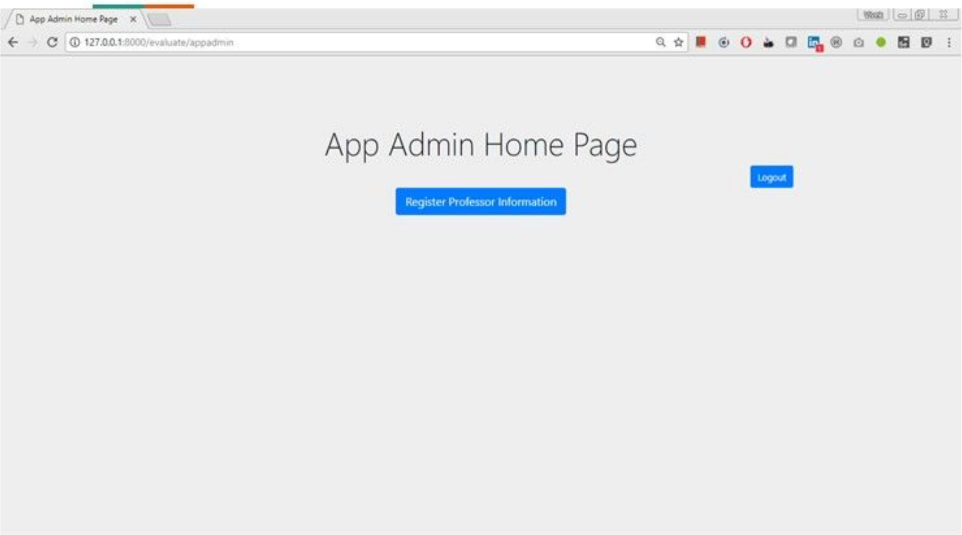


© Copyright 2018, Kevtastic Krakens Tech Pvt Ltd

App Admin

- To register and maintain the professor's login information

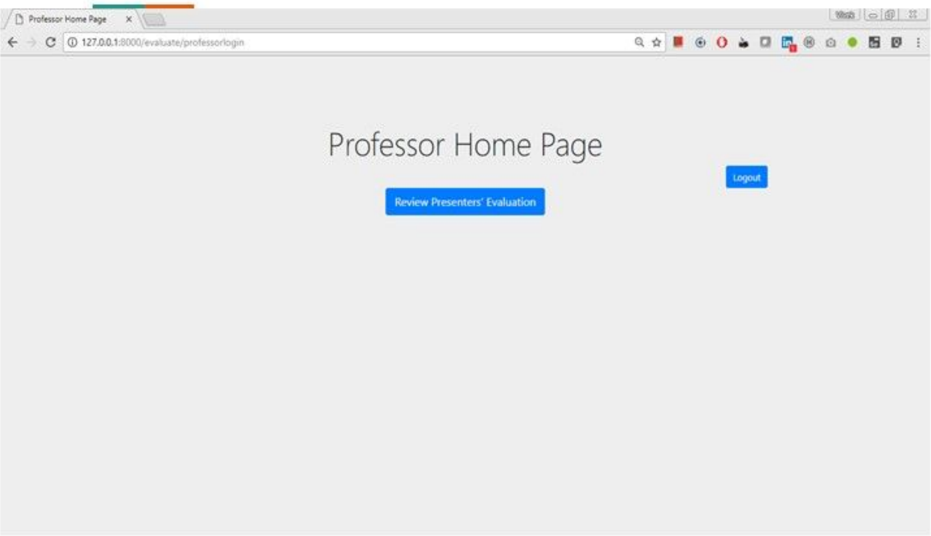
Website UI - App Admin


App Admin Home Page
127.0.0.1:8000/evaluate/appadmin
App Admin Home Page
Logout
Register Professor Information

App Admin

- To register and maintain the professor's login information

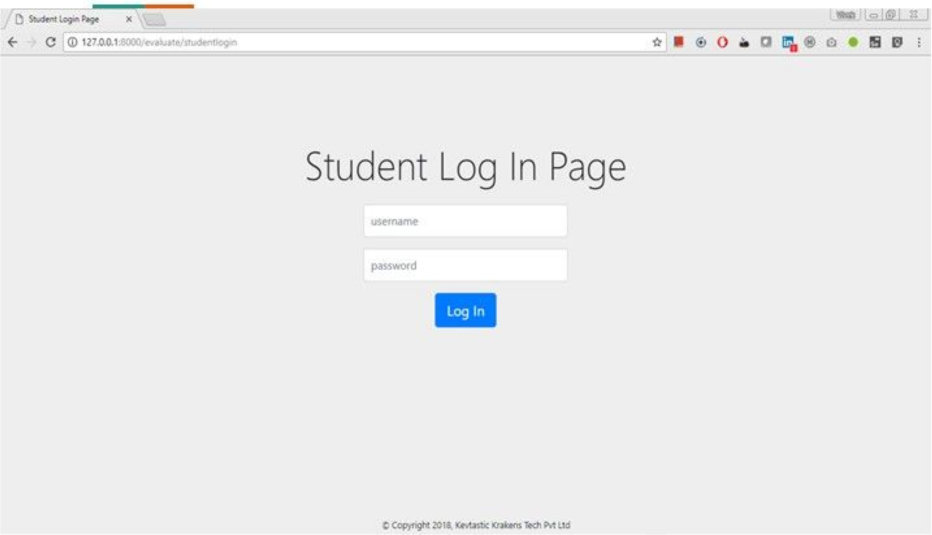
Website UI - Professor Home Page


Professor Home Page
127.0.0.1:8000/evaluate/professorlogin
Professor Home Page
Logout
Review Presenters' Evaluation

Professor Page

- To review presenter's evaluation remarks
- To keep track of the presenter's score

Website UI - Student Login Page

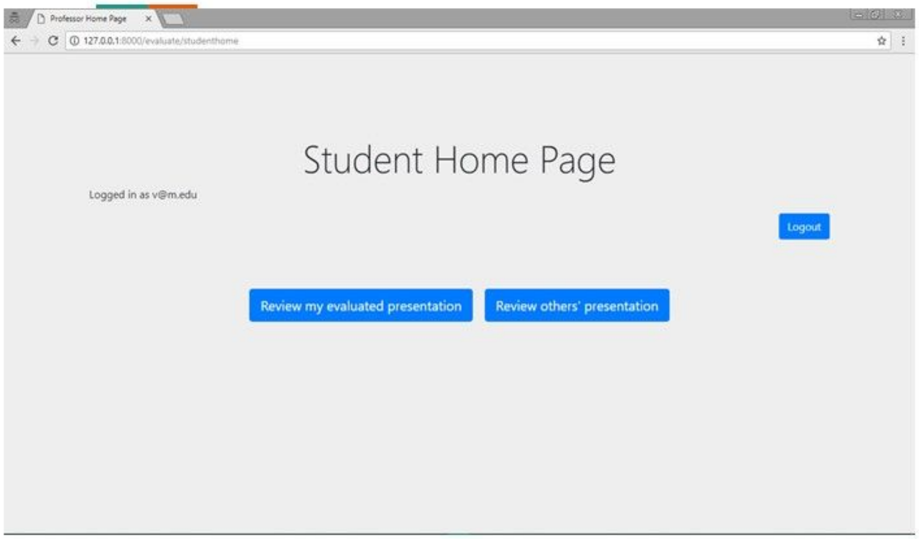


© Copyright 2018, Kevtastic Krakens Tech Pvt Ltd

Student Page

- To login using student's credentials
- To evaluate other's presentation skills or to review the received evaluation remarks from his/her peers/professor

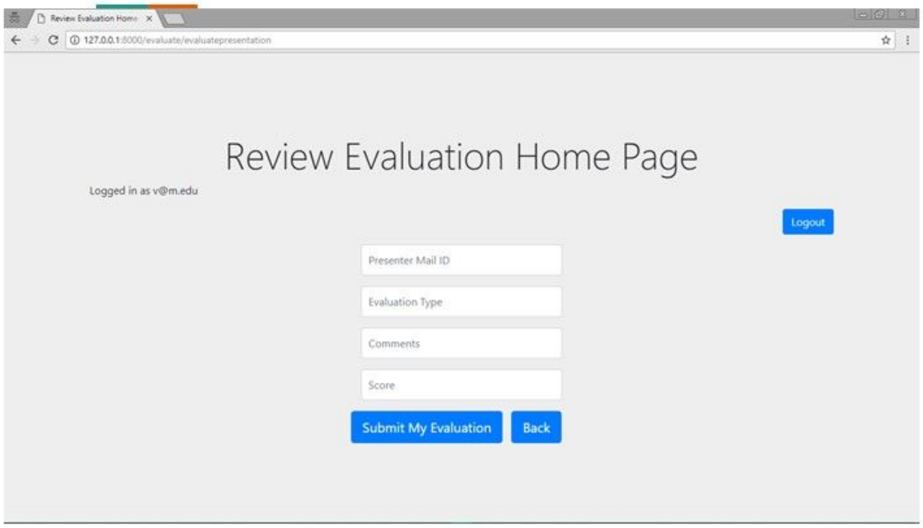
Website UI - Student Home Page


Professor Home Page
127.0.0.1:8000/evaluate/studenthome
Student Home Page
Logged in as v@m.edu
Logout
Review my evaluated presentation
Review others' presentation

Student Page

- To evaluate other's presentation skills or to review the received evaluation remarks from his/her peers/professor
- '**Review my evaluated presentation**' - to review received evaluation score/remarks
- '**Review other's presentation**' - to review other's presentation.

Website UI - Student Evaluating Peer Page



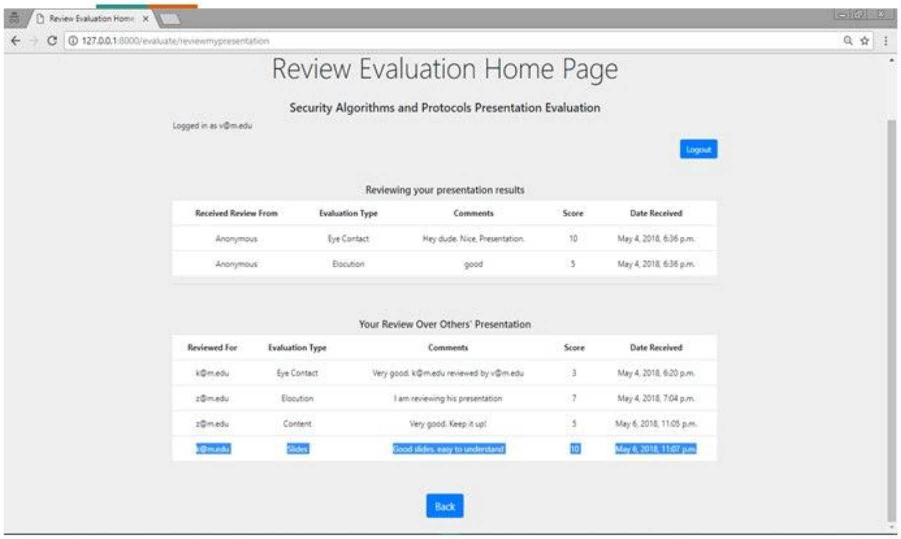
Review Evaluation Home Page

Logged in as v@m.edu

Student Review Evaluation Over Peer Page

- After login, Student can review other's using this page.
- Student can comment on evaluation type, score or comments
- **v@m.edu evaluating k@m.edu**

Website UI - Student Reviewing Received Evaluation from Others



Review Evaluation Home Page

Security Algorithms and Protocols Presentation Evaluation

Logged in as v@m.edu

Reviewing your presentation results

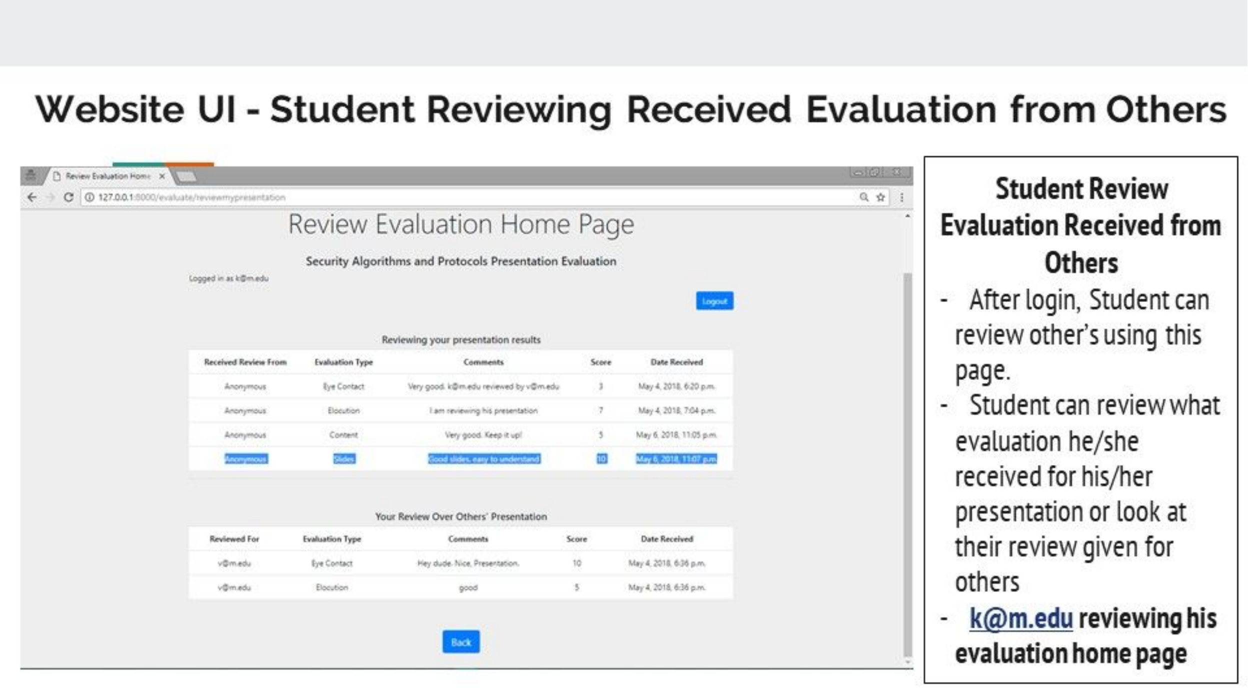
Received Review From	Evaluation Type	Comments	Score	Date Received
Anonymous	Eye Contact	Hey dude. Nice. Presentation.	10	May 4, 2018, 6:36 p.m.
Anonymous	Elocution	good	5	May 4, 2018, 6:36 p.m.

Your Review Over Others' Presentation

Reviewed For	Evaluation Type	Comments	Score	Date Received
k@m.edu	Eye Contact	Very good. k@m.edu reviewed by v@m.edu	3	May 4, 2018, 6:20 p.m.
z@m.edu	Elocution	I am reviewing his presentation	7	May 4, 2018, 7:04 p.m.
z@m.edu	Content	Very good. Keep it up!	5	May 6, 2018, 11:05 p.m.
k@m.edu	Slides	Good slides, easy to understand	10	May 6, 2018, 11:07 p.m.

Student Review Evaluation Received from Others

- After login, Student can review other's using this page.
- Student can review what evaluation he/she received for his/her presentation or look at their review given for others
- **v@m.edu evaluated k@m.edu**



Website UI - Student Reviewing Received Evaluation from Others

Review Evaluation Home Page

Security Algorithms and Protocols Presentation Evaluation

Logged in as k@m.edu

Reviewing your presentation results

Received Review From	Evaluation Type	Comments	Score	Date Received
Anonymous	Eye Contact	Very good. k@m.edu reviewed by v@m.edu	3	May 4, 2018, 6:20 p.m.
Anonymous	Elocution	I am reviewing his presentation	7	May 4, 2018, 7:04 p.m.
Anonymous	Content	Very good. Keep it up!	5	May 6, 2018, 11:05 p.m.
Anonymous	Slides	Good slides, easy to understand	10	May 6, 2018, 11:07 p.m.

Your Review Over Others' Presentation

Reviewed For	Evaluation Type	Comments	Score	Date Received
v@m.edu	Eye Contact	Hey dude. Nice. Presentation.	10	May 4, 2018, 6:36 p.m.
v@m.edu	Elocution	good	5	May 4, 2018, 6:36 p.m.

Student Review Evaluation Received from Others

- After login, Student can review other's using this page.
- Student can review what evaluation he/she received for his/her presentation or look at their review given for others
- **k@m.edu reviewing his evaluation home page**

Demo - Video - url:
https://drive.google.com/open?id=13AzwiiyqGelA-GXrr3fCDm-0DwkWvvty

Demo - Working - Gif:
https://github.com/vivekVells/Presentation-Evaluation-Tool/blob/master/demo/Presentation%20Evaluation%20App%20Demo%20-%20Version%201.gif

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

Future Enhancements Planned

- Enhancement tweaks
- Make data visualization features such as Charts and graphs
- Data analysis over the evaluated scores of the students
- To download the scores in files such as image, pdfs

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