DATA SECURITY IN CLOUD COMPUTING USING AES UNDER HEROKU CLOUD

Abstract

- Cloud security is an evolving sub-domain of computer and network security.
- Cloud platform utilizes third-party data centers model. An example of cloud platform as a service (PaaS) is Heroku.
- In this paper, we implement Heroku as a cloud platform, then we implement AES for data security in Heroku.

Contd..

- The performance evaluation shows that AES cryptography can be used for data security.
- Moreover, delay calculation of data encryption shows that larger size of data increases the data delay time for encrypting data.

INTRODUCTION

- Cloud computing is a computing paradigm, where a large pool of systems are connected in private or public networks, to provide dynamically scalable infrastructure for application, data and file storage.
- With the advent of this technology, the cost of computation, application hosting, content storage and delivery is reduced significantly.

Contd..

- 1. **Reduced Cost:** There are a number of reasons to attribute Cloud technology with lower costs. The billing model is pay as per usage;
- 2. **Increased Storage:** With the massive Infrastructure that is offered by Cloud providers today, storage & maintenance of large volumes of data is a reality.
- 3. **Flexibility:** With enterprises having to adapt, even more rapidly, to changing business conditions, speed to deliver is critical.

LITERATURE SURVEY

- **A NOVEL EFFICIENT REMOTE DATA POSSESSION CHECKING PROTOCOL IN CLOUD STORAGE**
- **PRIVACY PRESERVING AND BATCH AUDITING IN SECURE CLOUD DATA STORAGE**
- **TOWARD SECURE AND DEPENDABLE STORAGE SERVICES IN CLOUD COMPUTING**

A NOVEL EFFICIENT REMOTE DATA POSSESSION CHECKING PROTOCOL IN CLOUD STORAGE

- As an important application in cloud computing, cloud storage offers user scalable, flexible and high quality data storage and computation services.
- Because cloud storage servers are not fully trustworthy, data owners need dependable means to check the possession for their files outsourced to remote cloud servers.
- To address this crucial problem, some remote data possession checking (RDPC) protocols have been presented. But many existing schemes have vulnerabilities in efficiency or data dynamics.

PRIVACY PRESERVING AND BATCH AUDITING IN SECURE CLOUD DATA STORAGE

- Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance.
- However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources.

TOWARD SECURE AND DEPENDABLE STORAGE SERVICES IN CLOUD COMPUTING

- Cloud storage enables users to remotely store their data and enjoy the on-demand high quality cloud applications without the burden of local hardware and software management.
- In order to address this new problem and further achieve a secure and dependable cloud storage service,
- we propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed erasure-coded data

SYSTEM ANALYSIS

- **EXISTING WORK**
- **PROPOSED WORK**

EXISTING WORK

- There are several security concerns associated with cloud computing.
- The issues are divided into two categories. Firstly, a security issued by cloud providers.
- Secondly, security issues faced by their customers. They put data in the cloud and entrust the provider.

Contd..

- That is why data security on cloud computing is needed.
- Data security becomes a major challenge in cloud computing to reduce the risk.
- These risks are generally associated with open, shared upload, and distributed environments

PROPOSED WORK

- Data store can be encrypted by the customer's applications to fulfill the security requirements.
- Accordingly, Heroku needs some applications to secure the data before storing it to the database.
- One of the most popular and the most secure encryption algorithm is Advanced Encryption Standard (AES).

Contd..

- AES is a symmetric block chipper with block size variation of 64 to 256 bits.
- In this paper, we discuss data security in cloud computing using AES under Heroku cloud.
- We implement Heroku cloud as cloud computing platform, then we implement AES in the website to secure data.

SYSTEM SPECIFICATION

- **HARDWARE REQUIREMENTS**
- **SOFTWARE REQUIREMENTS**

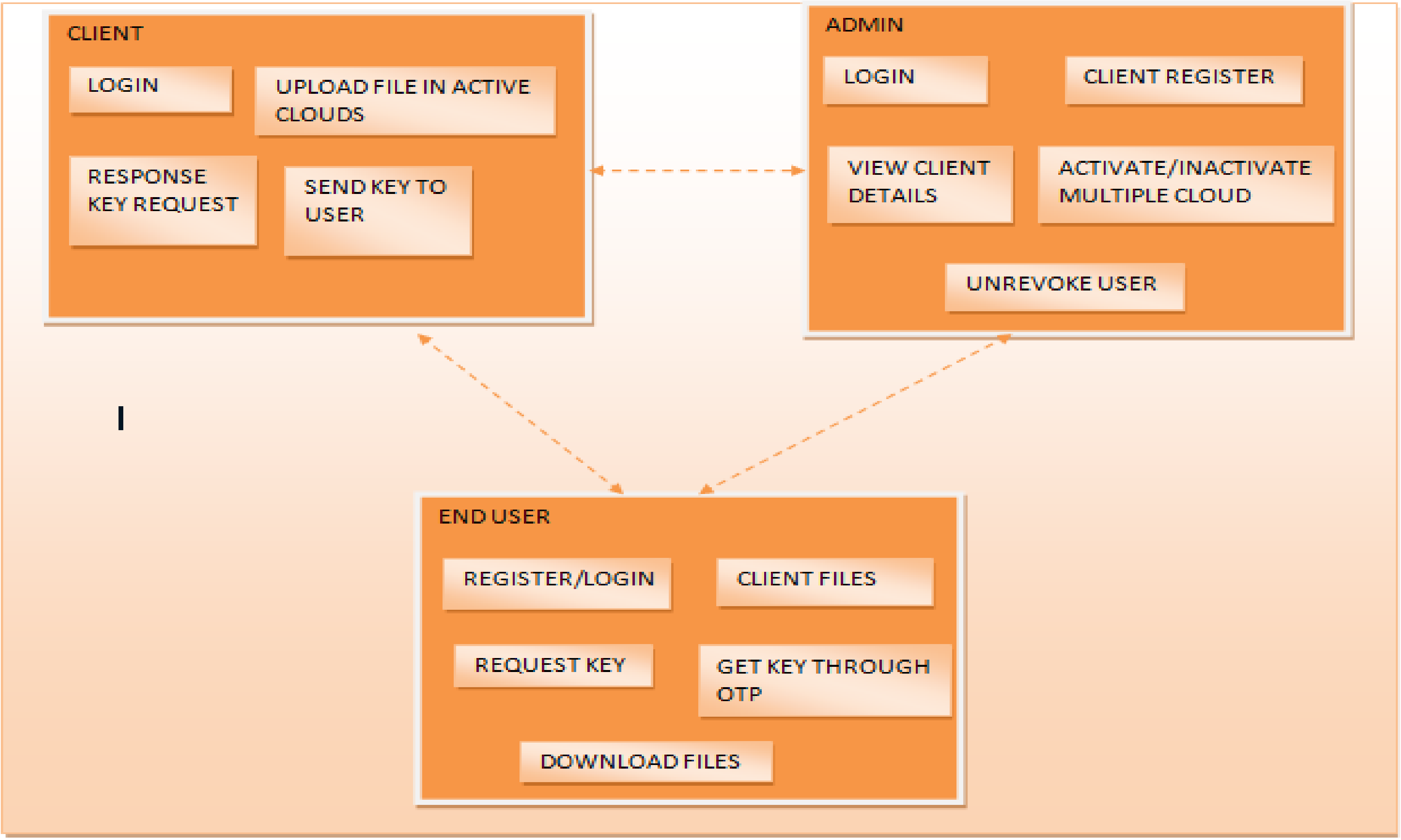
HARDWARE REQUIREMENTS

Processor	-	Pentium –III
Speed	-	1.1 Ghz
RAM	-	256 MB(min)
Hard Disk	-	20 GB
Floppy Drive	-	1.44 MB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

SOFTWARE REQUIREMENTS

Operating System	-	Windows 7/8
Application Server	-	Tomcat 5.0
Front End	-	Java
IDE	-	NetBeans 7.1
Back-End	-	MySQL

SYSTEM ARCHITECURE



CLIENT

LOGIN

UPLOAD FILE IN ACTIVE CLOUDS

RESPONSE KEY REQUEST

SEND KEY TO USER

ADMIN

LOGIN

CLIENT REGISTER

VIEW CLIENT DETAILS

ACTIVATE/INACTIVATE MULTIPLE CLOUD

UNREVOKE USER

END USER

REGISTER/LOGIN

CLIENT FILES

REQUEST KEY

GET KEY THROUGH OTP

DOWNLOAD FILES

IMPLEMENTATION

- MODULES
  - CLIENT
  - ADMIN
  - USER

CLIENT

- The CLIENT (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data.
- Then, David encrypts the data under the identities Alice and Bob, and uploads the ciphertext of the shared data to the cloud server.

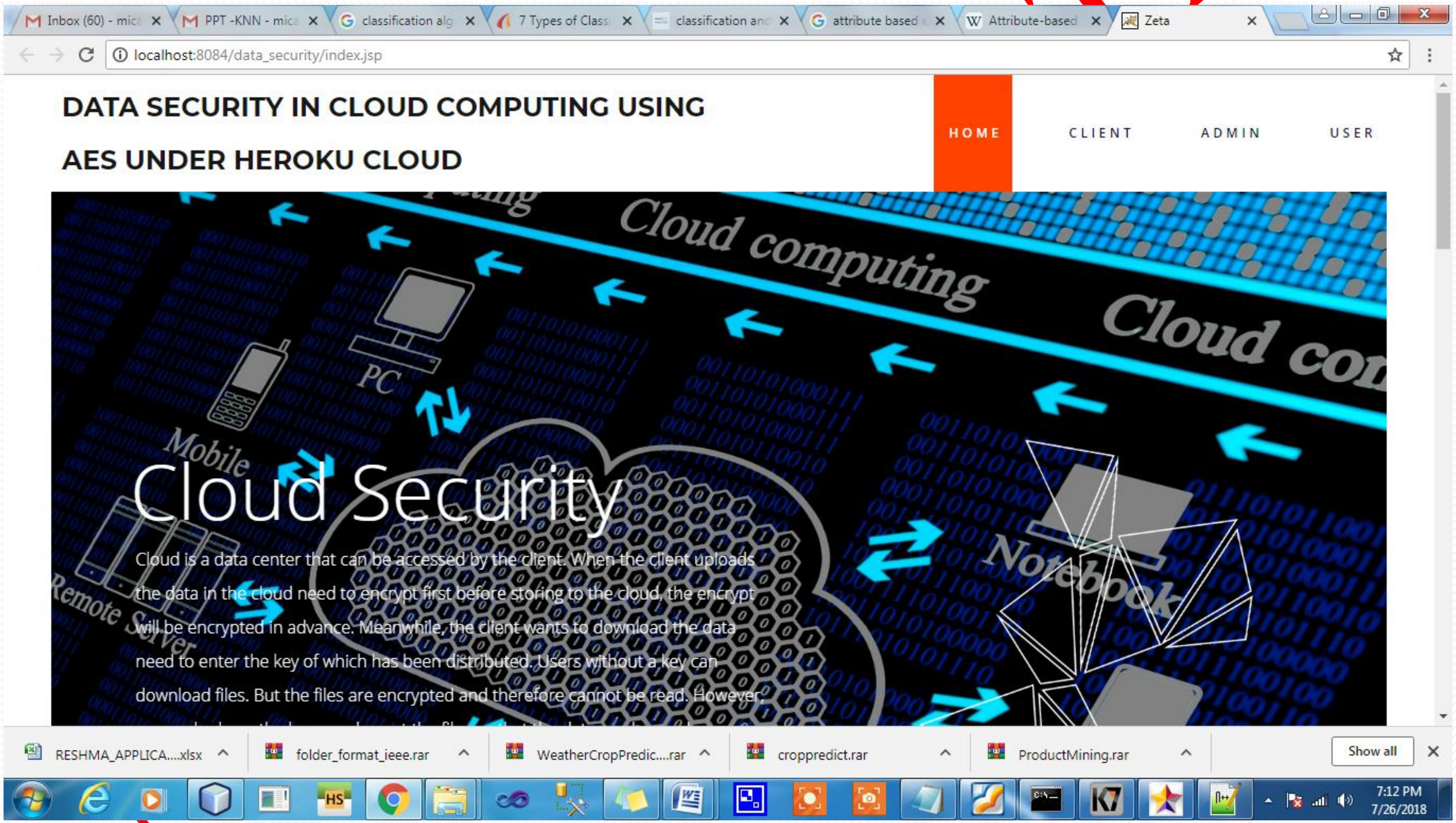
ADMIN

- A cloud service provider has huge storage space, computation resource and shared service to provide the clients.
- It is responsible for controlling the data storage in outside users' access, and provides the corresponding contents.

USER

- In this module, either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding ciphertext.
- However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.

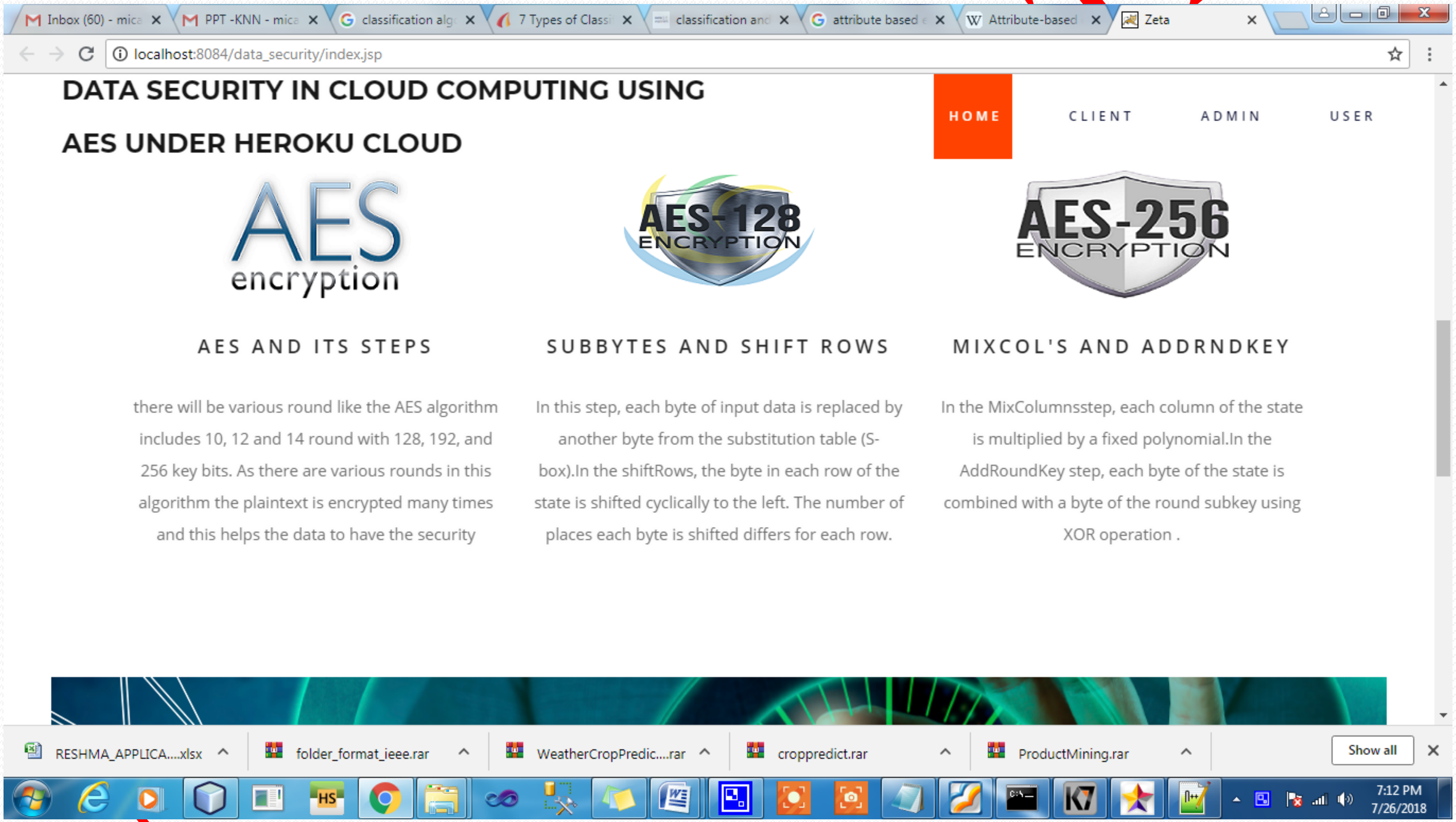
SCREEN SHOTS



DATA SECURITY IN CLOUD COMPUTING USING AES UNDER HEROKU CLOUD

Cloud Security

Cloud is a data center that can be accessed by the client. When the client uploads the data in the cloud need to encrypt first before storing to the cloud, the encrypt will be encrypted in advance. Meanwhile, the client wants to download the data need to enter the key of which has been distributed. Users without a key can download files. But the files are encrypted and therefore cannot be read. However,



DATA SECURITY IN CLOUD COMPUTING USING

AES UNDER HEROKU CLOUD

HOME CLIENT ADMIN USER

AES AND ITS STEPS

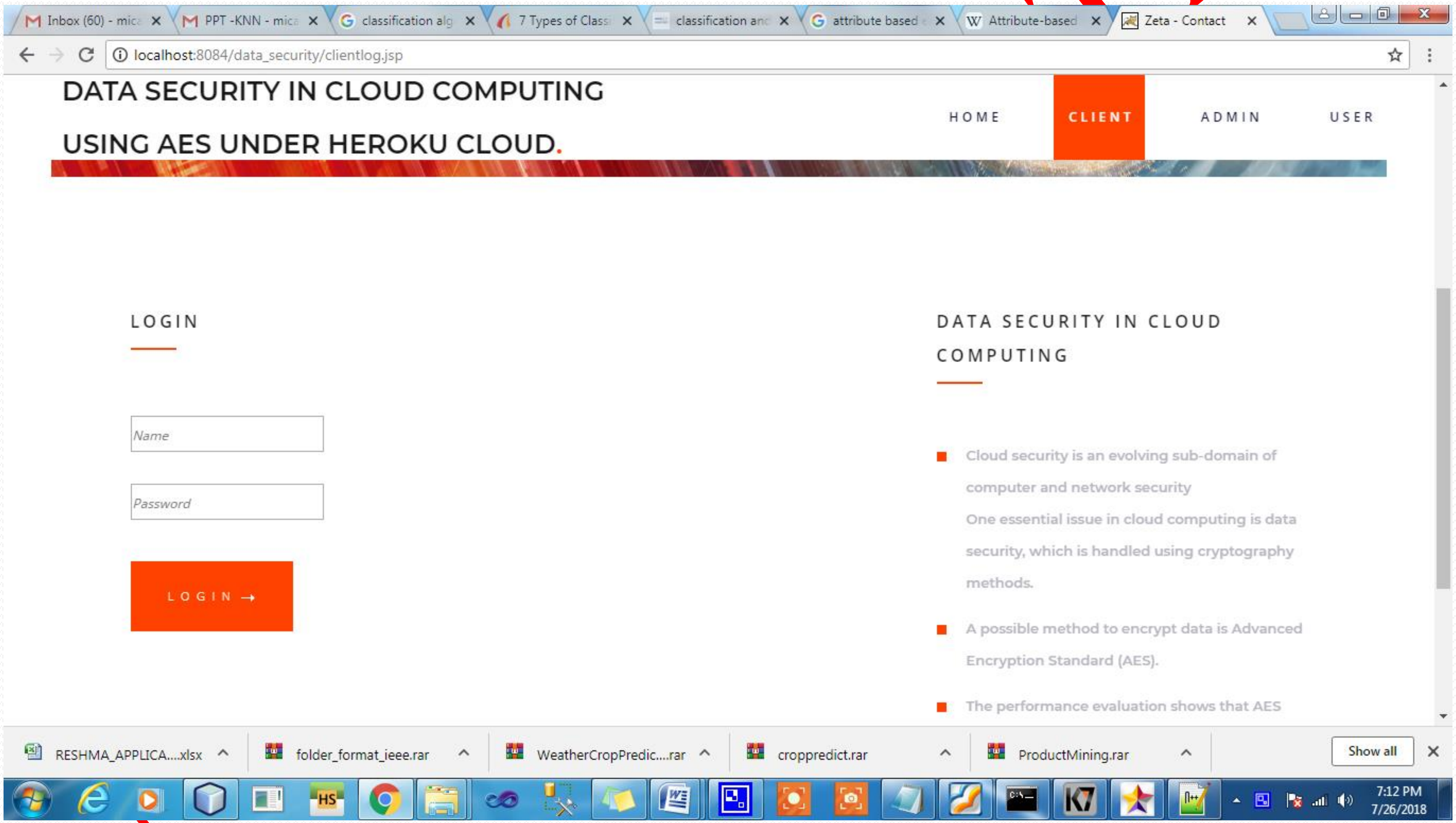
there will be various round like the AES algorithm includes 10, 12 and 14 round with 128, 192, and 256 key bits. As there are various rounds in this algorithm the plaintext is encrypted many times and this helps the data to have the security

SUBBYTES AND SHIFT ROWS

In this step, each byte of input data is replaced by another byte from the substitution table (S-box).In the shiftRows, the byte in each row of the state is shifted cyclically to the left. The number of places each byte is shifted differs for each row.

MIXCOL'S AND ADDRNDKEY

In the MixColumnsstep, each column of the state is multiplied by a fixed polynomial.In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using XOR operation .



DATA SECURITY IN CLOUD COMPUTING

USING AES UNDER HEROKU CLOUD.

LOGIN

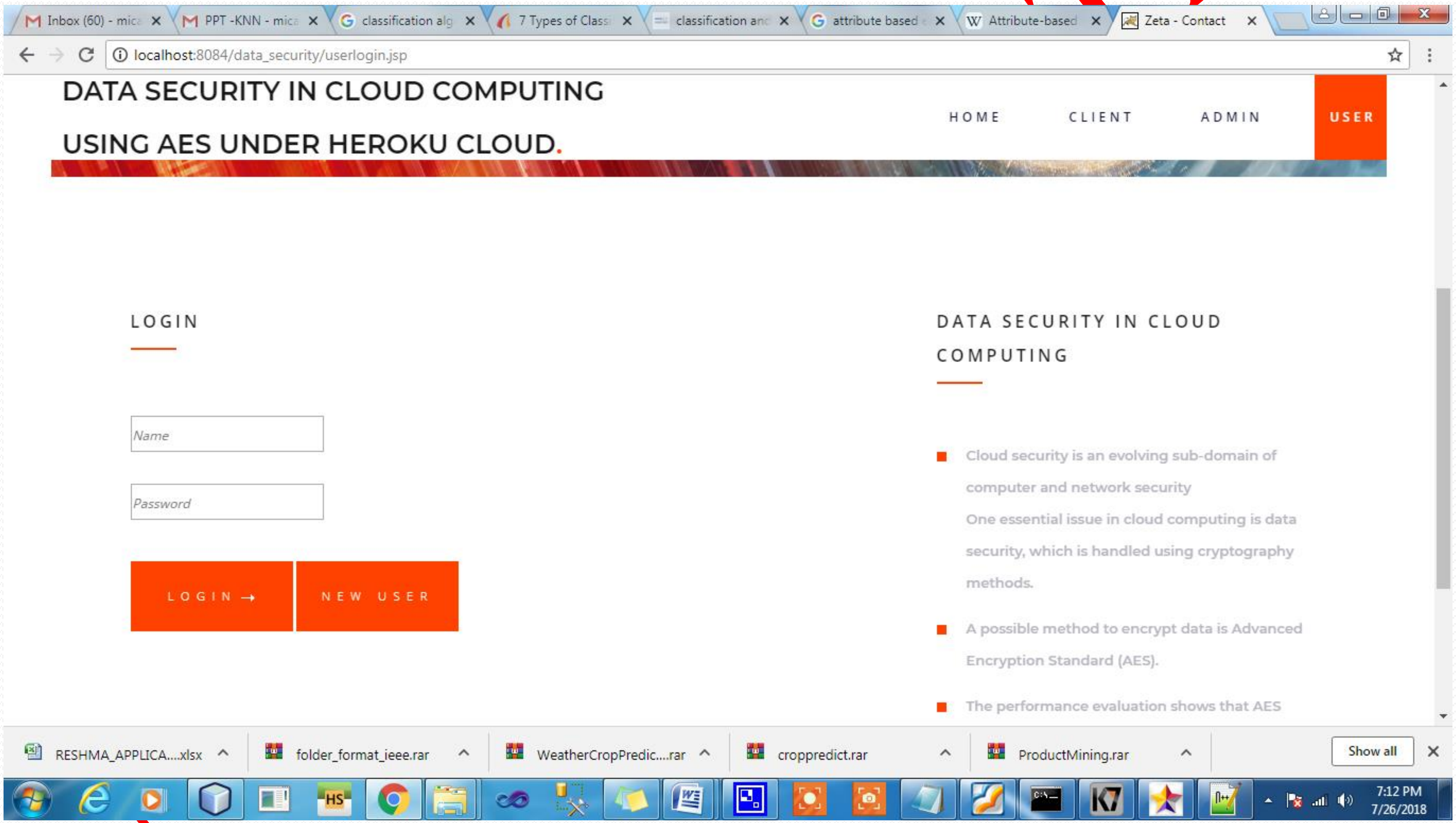
Name

Password

LOGIN →

DATA SECURITY IN CLOUD COMPUTING

- Cloud security is an evolving sub-domain of computer and network security
  One essential issue in cloud computing is data security, which is handled using cryptography methods.
- A possible method to encrypt data is Advanced Encryption Standard (AES).
- The performance evaluation shows that AES

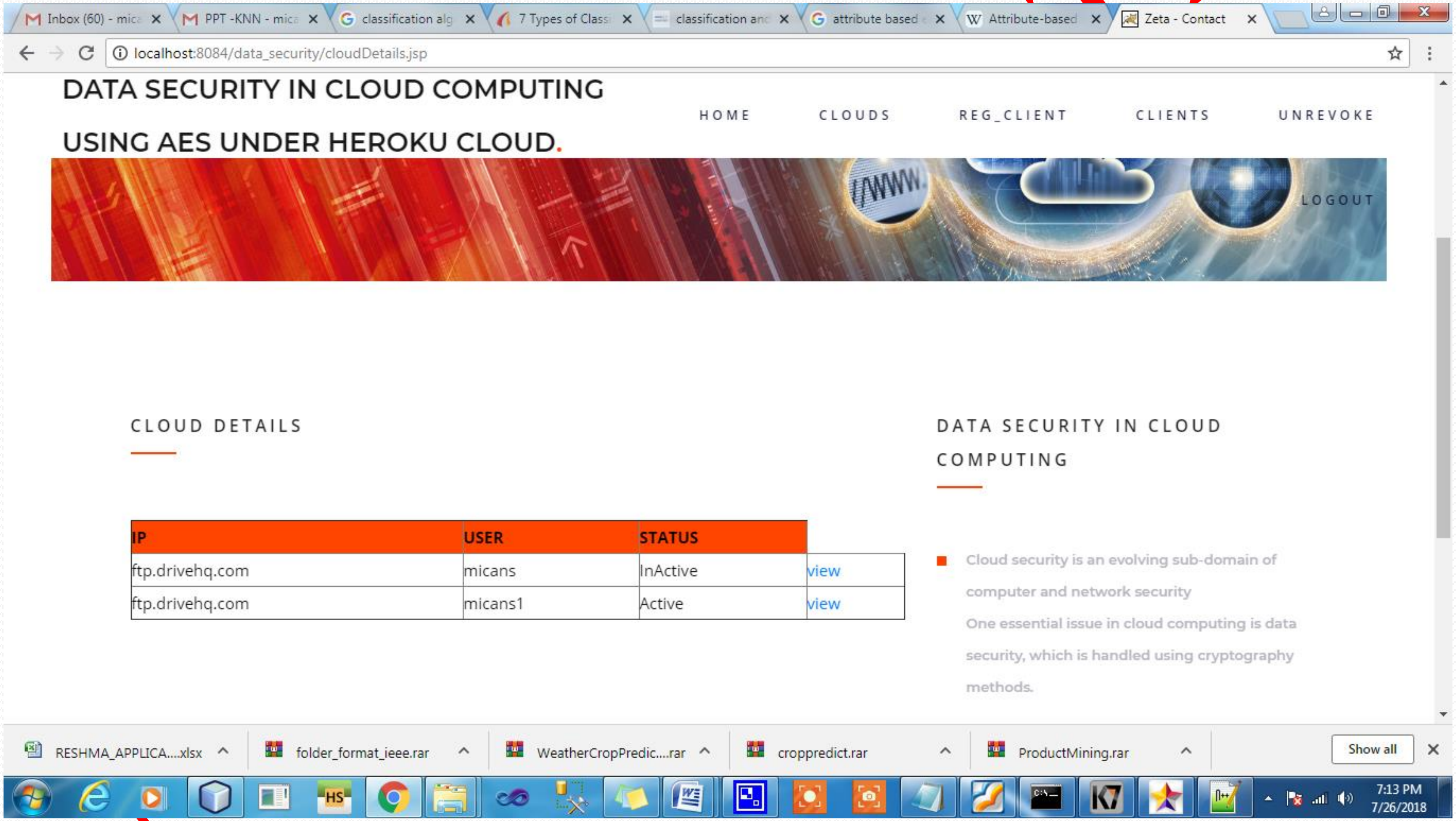


DATA SECURITY IN CLOUD COMPUTING USING AES UNDER HEROKU CLOUD.

LOGIN

DATA SECURITY IN CLOUD COMPUTING

- Cloud security is an evolving sub-domain of computer and network security One essential issue in cloud computing is data security, which is handled using cryptography methods.
- A possible method to encrypt data is Advanced Encryption Standard (AES).
- The performance evaluation shows that AES



DATA SECURITY IN CLOUD COMPUTING

USING AES UNDER HEROKU CLOUD.

HOME CLOUDS REG_CLIENT CLIENTS UNREVOKE

LOGOUT

CLOUD DETAILS

IP	USER	STATUS	
ftp.drivehq.com	micans	InActive	view
ftp.drivehq.com	micans1	Active	view

DATA SECURITY IN CLOUD COMPUTING

- Cloud security is an evolving sub-domain of computer and network security One essential issue in cloud computing is data security, which is handled using cryptography methods.

Conclusion

- In this paper, we proposed data security in cloud computing using AES under Heroku cloud.
- The implementation for deploying Heroku as a cloud platform consists of several steps.
- Then, we implement a website as an application to data security.
- Moreover, delay calculation of data encryption shows that larger size of data increases the data delay time for encrypting data.