Enhancing Security in Cloud Storage using ECC

Group members :	Student ID :
1. Rizwan Khan	15204050
2. Tejas waragade	15204018

Contents :

- Abstract
- Introduction
- Problem Statement
- Project Scope
- Literature Review
- Use-case Diagram
- Hardware and Software Requirements
- Summary
- Future Scope
- Project Planning
- References

Abstract :

- Security in cloud computing is an evolving area in today's world. It is subject of concern for Cloud Technology Services.
- One of the measures which customers can take care of is to encrypt their data before it is stored on the cloud.
- This work is intended towards providing security service such as confidentiality in the cloud services can use Elliptic Curve Cryptography (ECC) algorithm.

Introduction :

- Cloud computing security has become a hot topic in industry and academic research. This will explore data security of cloud in cloud computing by encryption and decryption with elliptic curve cryptography.

- Elliptic curve cryptography has the advantages over the familiar and generalized RSA in terms of smaller key sizes, lower CPU time and less memory usage.

Problem Statement :

- A cloud typically contains a virtualized significant pool of computing resources. The entire process of requesting and receiving resources is typically automated and is completed in minutes.

- The cloud in cloud computing is the set of hardware, software, networks, storage, services and interfaces that combines to deliver aspects of computing as a service.

Continue :

- However there still exist many problems in cloud computing today, a recent survey shows that data security and privacy risks have become the primary concern for the users.

Project Scope :

- **Sender Login**:- In this module, sender can login into the system using username and password authentication and gains the access to the application.

- **Encryption Module**:- In this module, sender enters the message which is to be sent to the receiver and encrypts the message using ***Elliptic Curve Cryptography.***

Continue :

- **Receiver Login**:- In this module, receiver can login into the system using username and password authentication and gains access to the application.

- **Decryption Module**:-Receiver decrypt the message using his private key.

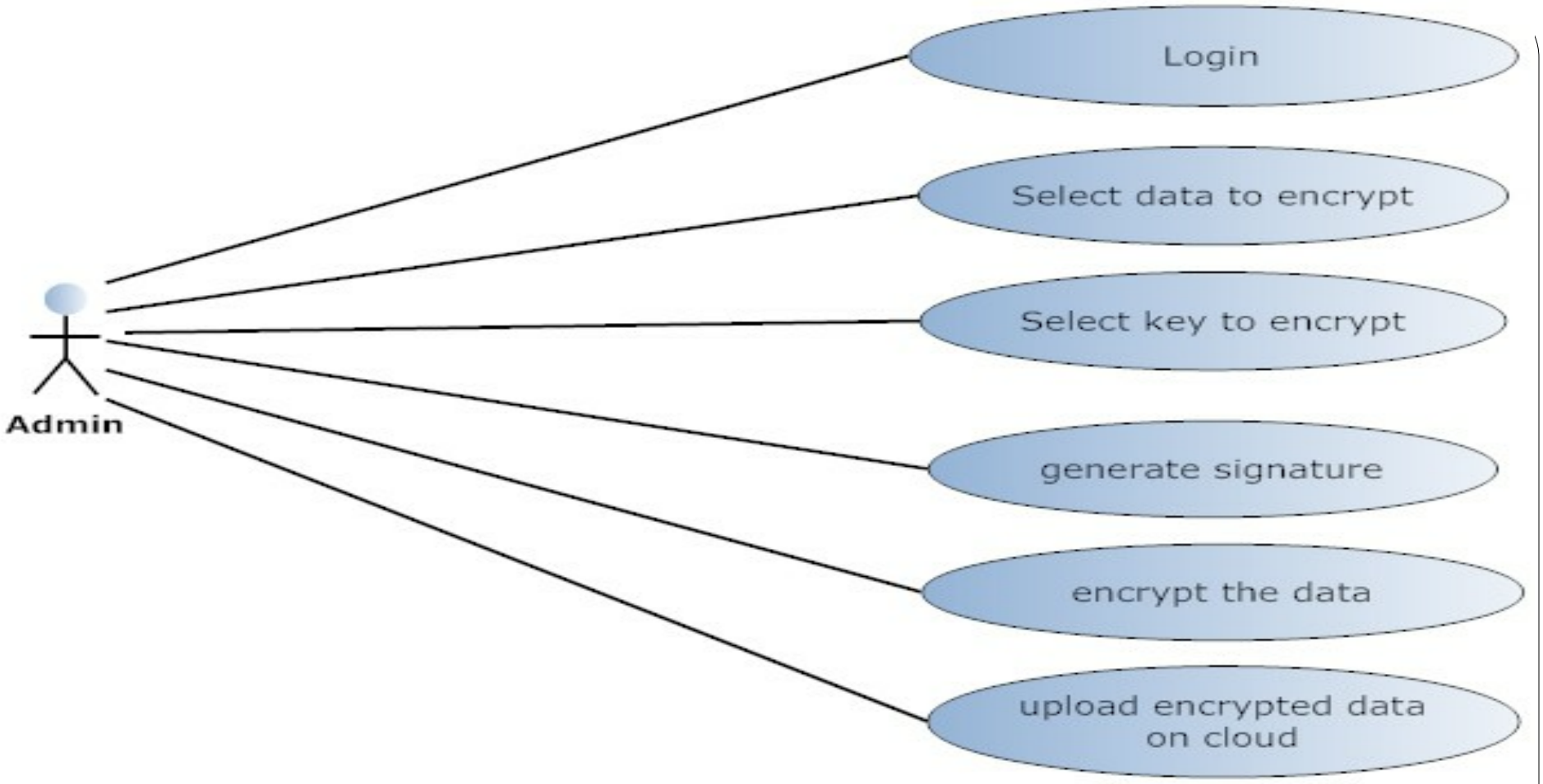
Literature Review :

Maryam Savari

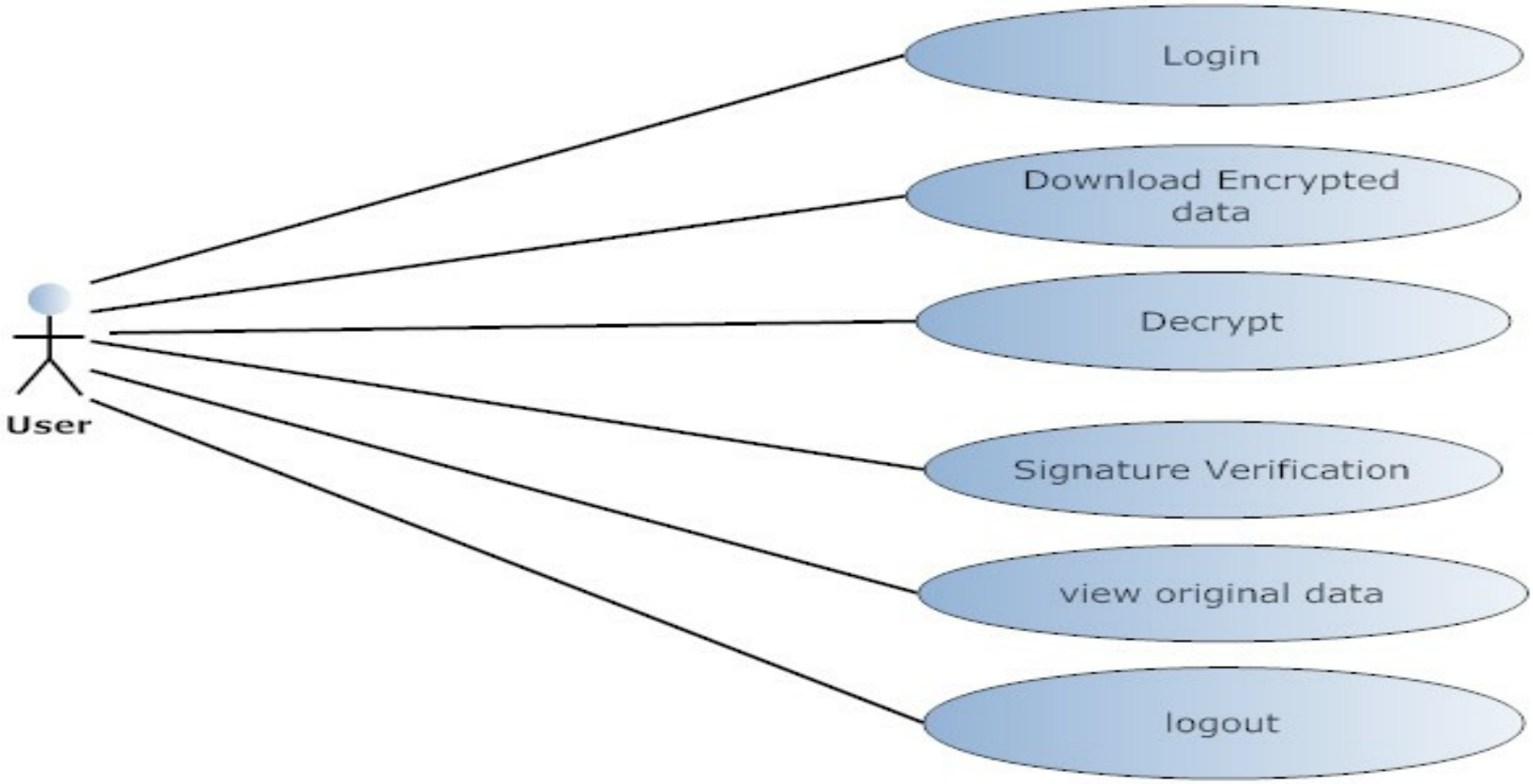
- For "Comparison of ECC and RSA Algorithm in Multipurpose Smart Card Application" compare the security of RSA 1024-bit key versus ECC 160-bit key sizes.

Xiao Zhang

- Talked about the physical security of data in data centers "Ensure Data Security in Cloud Storage"



Admin Use-case diagram



User Use-case diagram

Hardware Software Requirements :

HARDWARE REQUIREMENTS:

- 1 GB RAM.
- 200 GB HDD.
- Intel 1.66 GHz Processor Pentium 4

SOFTWARE REQUIREMENTS:

- Windows XP, Windows 7,8
- Visual Studio 2010
- MS SQL Server 2008
- Windows Operating System

Technology Stack :

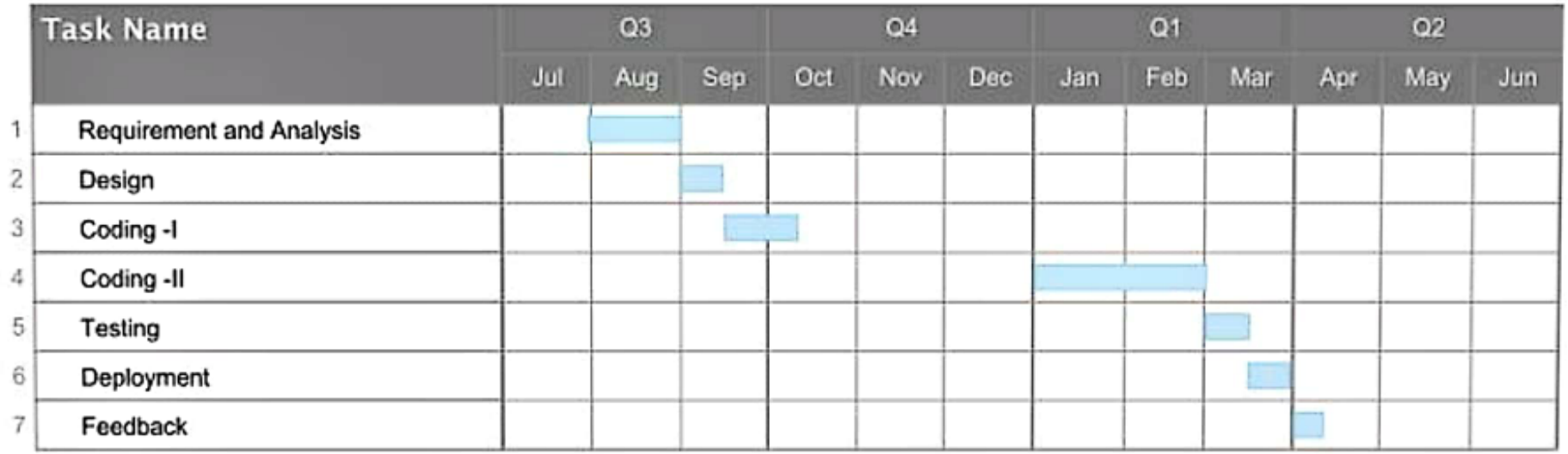
- HTML and CSS
- JavaScript
- MS SQL server
- ASP.Net and C Sharp

Summary :

- Elliptic Curve Cryptography provides greater security and more efficient performance than the first generation public key techniques like RSA, AES, DES, etc.

- As vendors look to upgrade their systems they should seriously consider the elliptic curve alternative for the computational and bandwidth advantages they offer at comparable security.

- After comparing the RSA and ECC ciphers, the ECC has proved to involve much less overheads compared to RSA. The ECC has many advantages due to its ability to provide the same level of security as RSA yet using shorter keys.



Project Planning

Future Scope :

- This work can be extended to compare ECC with other algorithms used for digital signatures, key exchanges, data integrity.
- The future of ECC looks brighter than RSA as today's application (smart cards, mobile phones, etc) cannot afford the overheads introduced by RSA.
- ECC makes it an ideal choice for portable, mobile and low power applications and their integration with cloud devices.
- Although ECC's security has not been completely evaluated, it is expected to come into widespread use in various fields in the future

References :

1] Elliptic curve cryptography,

https://en.wikipedia.org/wiki/Elliptic_curve_cryptography

[2] RSA (algorithm),

http://en.wikipedia.org/wiki/RSA_(algorithm)

[3] JavaTM Cryptography Extension (JCE), Reference guide

http://docs.oracle.com/javase/1.5.0/docs/guide/security/jce/JCERefGuide.html

Thank You ...!