CTS CAFÉ PROGRAM

PROJECT NAME:

LOGGING FRAMEWORK USING ENCRYPTION

BY,

MENTOR: Ms. R. NIVEDHA

STUDENTS:

SUJITH.K. R (TEAM LEADER)

SANTHOSH.I

SARAVANA.S

SHAIK SUHAIL

SUDHEENDRA.S. S.

SRIKAR.P

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING

SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade “A” by NAAC

JEPPIAAR NAGAR, RAJIV GANDHISALAI,

CHENNAI – 600119 MARCH– 2023

Table of Contents

1.0 Introduction:

Logging is an important concept in software development and systems administration. It refers to the practice of recording events, actions, and messages that occur during the operation of a program or system. These events can include user actions, error messages, system warnings, and other information that can help developers and administrators understand what is happening within the program or system. Logging with encryption refers to the practice of encrypting the log data that is generated by a program or system. This is done to ensure that sensitive information that may be included in log messages is protected from unauthorized access. Encryption is the process of transforming data into a format that can only be read by someone with the correct decryption key

2.0 Technology/Framework used for Development:

2.1 Tools Used

- **Django framework:**
  - Django is open-source Python-based web framework which is used to develop the backend of the file upload. Django comes with included batteries which provides with variety of tools and libraries to develop a web app.
- **Flask framework:**
  - Flask is a lightweight and flexible web framework for Python. It is designed to make it easy to build web applications with Python, with a minimalistic approach to web development that emphasizes simplicity, flexibility, and extensibility.
  - Flask provides a simple yet powerful API that allows developers to quickly build web applications with features such as routing, request handling, template rendering, and database integration. Flask is known for its simplicity and ease of use, making it a popular choice for small to medium-sized web applications and prototypes.

- **MySQL:**
    - MySQL is relational database management which stores data in form of tables. MySQL uses structured query language. Here MySQL use as DB.
    - It may be anything from a simple shopping list to a picture gallery or the vast amounts of information in a corporate network. To add, access, and process data stored in a computer database, you need a database management system such as MySQL Server.
    - MySQL provides supports for native JSON data type from **version 5.7.8** that stores JSON document in an internal format, which enables quick and efficient read access to document objects. This data type can store JSON documents more accurately than the JSON text format we had used in the past MySQL versions.
- **Python:**
    - Python is popular programming language used to wide variety of applications across the computer science branch ranging from GUI apps to being used extensively in Artificial Intelligence and machine learning.
    - Python is dynamically typed and garbage-collected. It supports multiple programming paradigms, including structured (particularly procedural), object-oriented and functional programming. It is often described as a "batteries included" language due to its comprehensive standard library.
- **React JS:**
    - React is JavaScript-based Front-end library developed by Facebook to develop beautiful UIs based on components.
    - React makes it painless to create interactive UIs. Design simple views for each state in your application, and React will efficiently update and render just the right components when your data changes.
    - Declarative views make your code more predictable and easier to debug.

3.0 Business Scenario:

3.1 Problem in Business

- Logging without encryption can pose several problems for businesses, particularly when sensitive information is included in the log messages. Some of the potential problems of logging without encryption include:

- **Security risks:** Log files often contain sensitive information, such as user credentials, credit card numbers, and other confidential data. Without encryption, this information is vulnerable to unauthorized access by attackers who may gain access to the log files.

- **Compliance issues:** Many industries and jurisdictions have regulations and standards that require businesses to protect sensitive data. Failure to encrypt log files that contain sensitive information can result in non-compliance and potential legal liabilities.

- **Reputation damage:** If sensitive information is exposed as a result of logging without encryption, it can damage a business's reputation and erode customer trust. This can have long-term impacts on the business's bottom line.

- **Difficulty in detecting and responding to breaches**: Without encryption, it may be difficult for businesses to detect and respond to breaches that involve log data. Encrypted log files can limit the scope of a breach and help businesses identify the source of the breach more quickly.

3.2 Overcome by using Encryption

- There are several advantages to using encryption in logging, including:

- **Enhanced security**: Encryption helps protect sensitive information in log files from unauthorized access. By encrypting log data, businesses can ensure that only authorized users can access this information, minimizing the risk of data breaches and cyber attacks.

- **Compliance with regulations**: Many industries and jurisdictions have regulations and standards that require businesses to protect sensitive data. By encrypting log files, businesses can ensure compliance with these regulations and avoid potential legal liabilities. Improved reputation: If sensitive information is exposed as a result of logging without encryption, it can damage a business's reputation and erode customer trust. By implementing encryption, businesses can demonstrate a commitment to protecting sensitive data, improving their reputation and building customer trust.

- **More effective incident response**: Encrypted log files can make it easier for businesses to detect and respond to breaches. By limiting the scope of a breach and identifying the source of the breach more quickly, businesses can respond more effectively and minimize the potential impacts of a breach.

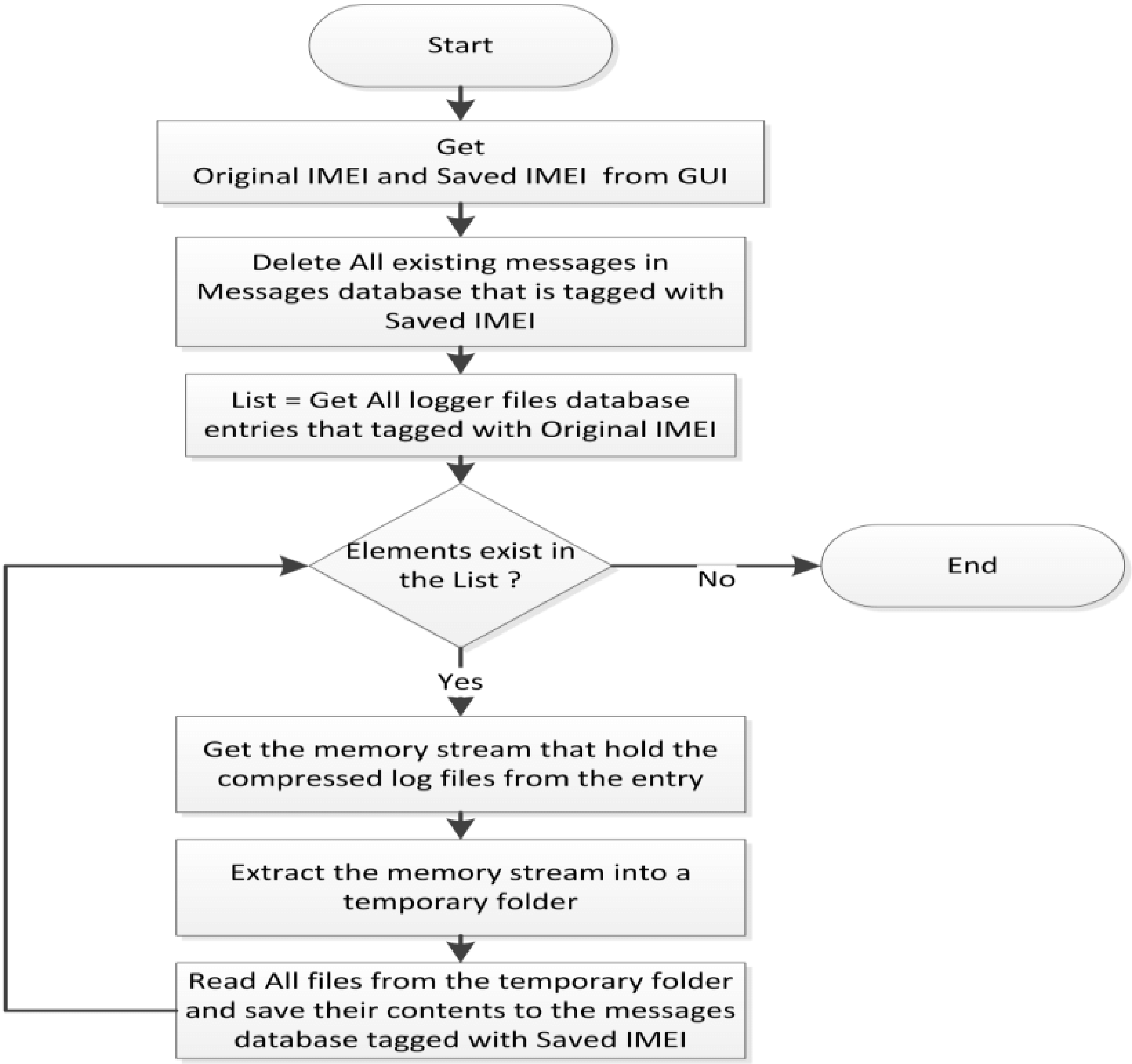
- Overall, using encryption in logging can help businesses protect sensitive information, comply with regulations, improve their reputation, and respond more effectively to security incidents and other issues.

4.0 Workflow:

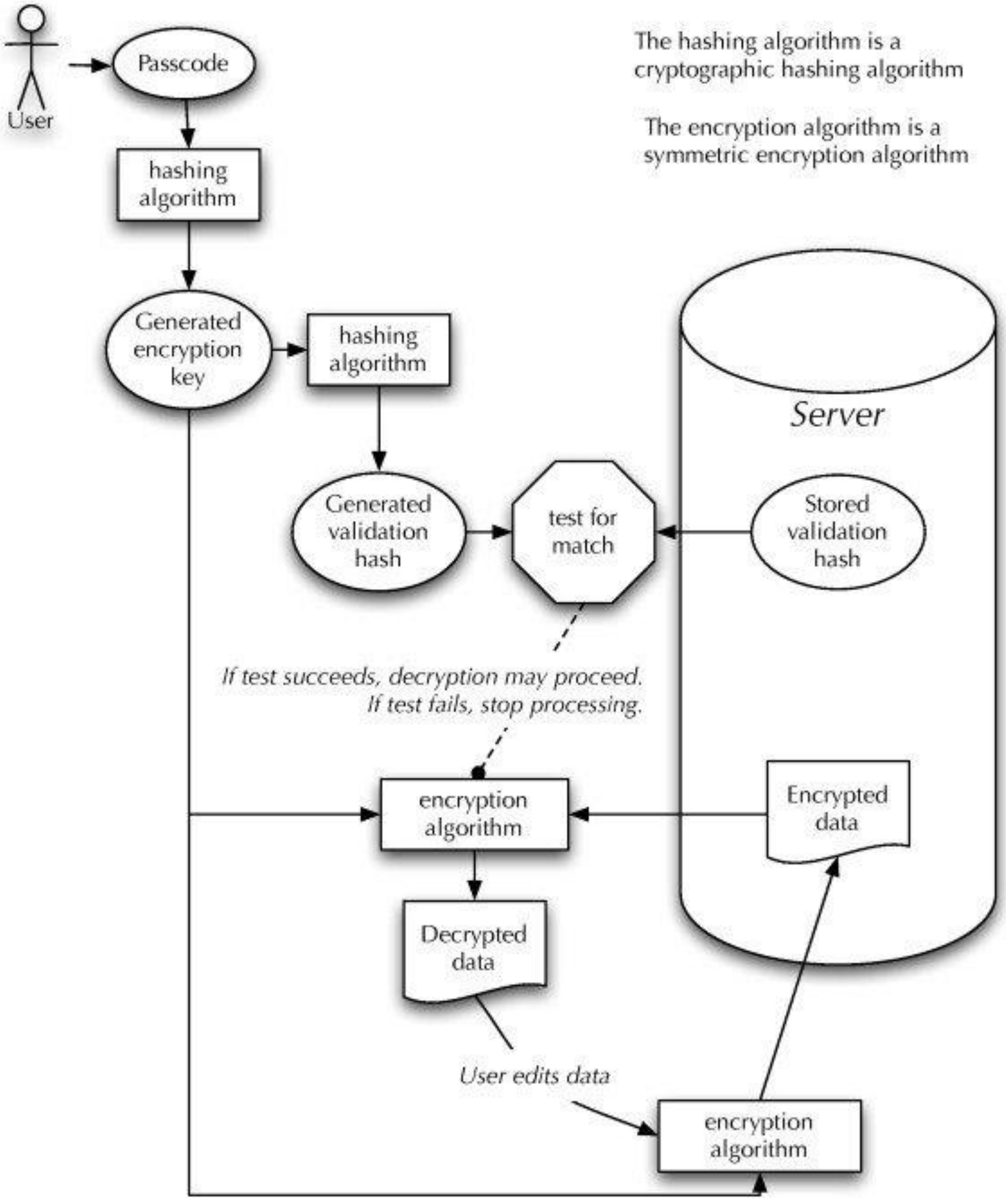
- Determine which data needs to be encrypted: Before implementing encryption for logging, businesses should determine which data needs to be encrypted to protect sensitive information. This might include data such as user credentials, credit card numbers, and other confidential data.
- Choosing an encryption algorithm: Businesses should choose an encryption algorithm that is appropriate for the type of data being encrypted and meets their security requirements. Common encryption algorithms include AES and RSA.
- Generating encryption keys: Encryption keys are used to encrypt and decrypt log data. Businesses should generate strong encryption keys and ensure that they are properly protected and securely stored.
- Implementing encryption in the logging system: Businesses should implement encryption in the logging system to ensure that log data is encrypted before it is written to disk. This might involve modifying existing logging frameworks or implementing custom logging code.
- Managing encrypted log data: Encrypted log data must be properly managed to ensure that it can be decrypted when needed. This might involve securely storing encryption keys, implementing key management policies, and setting up secure access controls.
- Monitoring and maintaining the logging system: Once encryption is implemented, businesses should regularly monitor the logging system to ensure that it is working as expected and that log data is properly encrypted. Any issues or anomalies should be promptly investigated and addressed.
-

5.0 Flowchart:

5.1 Frontend Flowchart


Start
Get Original IMEI and Saved IMEI from GUI
Delete All existing messages in Messages database that is tagged with Saved IMEI
List = Get All logger files database entries that tagged with Original IMEI
Elements exist in the List ?
No
End
Yes
Get the memory stream that hold the compressed log files from the entry
Extract the memory stream into a temporary folder
Read All files from the temporary folder and save their contents to the messages database tagged with Saved IMEI

5.2 Backend Flowchart


User
Passcode
hashing algorithm
Generated encryption key
hashing algorithm
Generated validation hash
test for match
Stored validation hash
Server
The hashing algorithm is a cryptographic hashing algorithm
The encryption algorithm is a symmetric encryption algorithm
If test succeeds, decryption may proceed.
If test fails, stop processing.
encryption algorithm
Encrypted data
Decrypted data
User edits data
encryption algorithm

6.0 Exception Handling:

- **Key management errors**: If encryption keys are not properly managed or stored, this can result in errors or exceptions when attempting to encrypt or decrypt log data.
- **Encryption algorithm errors :**If the encryption algorithm used to encrypt log data is not properly configured or implemented, this can result in errors or exceptions.
- **Input validation errors:** If input data is not properly validated before it is encrypted, this can result in errors or exceptions.
- **Communication errors:** If there are communication errors between different components of the logging system, this can result in errors or exceptions.

7.0 Conclusion

By implementing encryption in logging, businesses can protect sensitive data, comply with regulations, improve their reputation, and respond more effectively to security incidents and other issues. The workflow for logging with encryption involves determining which data needs to be encrypted, choosing an appropriate encryption algorithm, generating encryption keys, implementing encryption in the logging system, managing encrypted log data, and monitoring and maintaining the logging system. Effective exception handling mechanisms are also important for detecting and responding to errors and exceptions that may occur during the encryption process. By following these best practices for logging with encryption, businesses can ensure that their log data is properly secured and protected from unauthorized access.