Assignment 3 Report: On-the-go verification of Driver's License

Contributors:
Paras Dhiman (2021482)
Aekansh Kathunia (2021127)

April 21, 2024

Abstract

The "On-the-go Verification of Driver's License" project addresses the challenge of verifying the authenticity of driver's licenses in real-time, considering the prevalent issue of counterfeit or tampered physical documents. The project leverages technology to enable police officers to verify driver's licenses securely, even when presented digitally using smartphones. This report outlines the system's components, implementation details, security measures, and addresses specific questions related to information exchange, central server requirement, digital signatures, data confidentiality, and the importance of date and time in communication.

1 Introduction

This report elaborates on the functionality and implementation of an On-the-go Driver's License Verification System. The system facilitates the verification of driver's licenses by police officers in real-time.

It employs digital signatures and encryption techniques to ensure the authenticity and confidentiality of the communication between the Transport Authority Server, Police Officers, and Drivers.

2 System Components:

The system comprises four main components:

- **Driver Class**: Represents a driver with attributes such as name, date of birth, mobile number, and a digital driver's license. Each driver possesses a private and public RSA key pair for secure communication with the Transport Authority Server.
- **License Class**: Defines the structure of a driver's license including name, license number, and expiry date.
- **TransportAuthorityServer Class**: Manages the database of driver licenses, generates RSA key pairs, initiates license verification processes, and handles communication with drivers and police officers.
- **PoliceOfficer Class**: Represents a police officer who interacts with the Transport Authority Server to request and verify driver's licenses.

3 Implementation Overview:

3.1 Key Generation

Both drivers and police officers generate RSA key pairs for secure communication.

3.2 Driver Registration

When a new driver is initialized, they generate a digital driver's license and sign it with their private key. The license is then stored in the Transport Authority Server's database.

3.3 License Verification Process

3.3.1 Initiation

Police officers initiate the license verification process by providing the license number. The Transport Authority Server generates an OTP and encrypts it with the driver's public key before sending it to the driver's mobile.

3.3.2 Continuation

The driver enters the OTP, which is then signed by the police officer and sent back to the server for verification. If the verification is successful, a success message is returned.

3.3.3 Verification

The Transport Authority Server verifies the received OTP signature and the driver's license signature. If both verifications pass and the license is not expired, the verification is considered successful.

4 Security Measures

- **Digital Signatures**: Used to verify the authenticity of messages and documents exchanged between the server, drivers, and police officers.
- **Encryption**: Employed to secure the transmission of sensitive information such as OTPs between the server and drivers.
- **RSA Key Pair Generation**: Ensures the confidentiality and integrity of communication channels.

5 Input and Output Analysis

5.1 Input

The user interacts with the On-the-go verification of Driver's License system by providing the following input:

- **License Number**: The user enters the license number displayed on their driver's license card.

5.2 Output

Upon providing the input, the system processes the information and generates the following output:

- **Text Message to Mobile**: After entering the license number, the system sends a text message to the mobile number associated with the provided license. The message contains the following details:
  - A greeting addressing the driver by name.
  - Notification of being stopped for license verification.
  - Display of License Number and Expiry Date.
  - Provision of a One-Time Password (OTP) for verification.
  - Instruction to contact emergency services if the verification is unauthorized.
- **Verification Result**:
  - The system prompts the user to enter the OTP received on their mobile.
  - Upon successful verification, a message confirming the successful verification of the license is displayed.
  - Details of the verified license, including the driver's name, date of birth, mobile number, license information, and public key, are printed.

6 Example Output

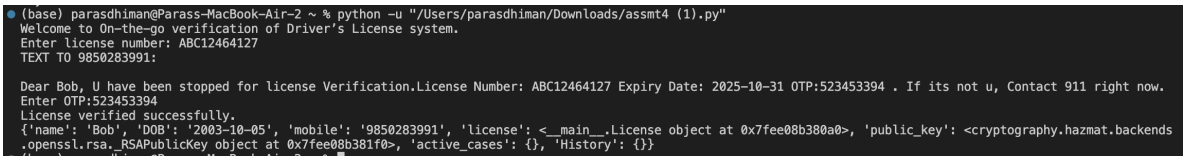

Figure 1: Example Output

Output Text

```
Welcome to On-the-go verification of Driver's License system.
Enter license number: ABC12464127
TEXT TO 9850283991:

Dear Bob, U have been stopped for license Verification.
License Number: ABC12464127
Expiry Date: 2025-10-31
OTP: 523453394
If its not u, Contact 911 right now.
Enter OTP: 523453394
License verified successfully.
{'name': 'Bob', 'DOB': '2003-10-05', 'mobile': '9850283991',
'license': <__main__.License object at 0x7fee08b380a0>, 'public_key':
<cryptography.hazmat.backends.openssl.rsa._RSAPublicKey object at
0x7fee08b381f0>, 'active_cases': {}, 'History': {}}
```

Security Measures

- **Digital Signatures**: Used to verify the authenticity of messages and documents exchanged between the server, drivers, and police officers.
- **Encryption**: Employed to secure the transmission of sensitive information such as OTPs between the server and drivers.
- **RSA Key Pair Generation**: Ensures the confidentiality and integrity of communication channels.

Performance Analysis

The On-the-go Driver's License Verification System exhibits efficient performance characteristics in terms of key generation, cryptographic operations, and network interactions.

Key Generation

The system utilizes RSA key pairs for secure communication between drivers, police officers, and the transport authority server. Key generation involves generating two large prime numbers and performing modular exponentiation operations. Despite the computational complexity of key generation, it is a one-time process during system initialization and does not significantly impact runtime performance.

Cryptographic Operations

Digital signatures and encryption are employed to ensure the authenticity, integrity, and confidentiality of transmitted data. The computational overhead of cryptographic operations, such as signing and verifying messages, largely depends on the key size and algorithm used. However, modern cryptographic libraries, such as `cryptography`, optimize these operations for performance without compromising security.

Network Interactions

The system interacts with external services, such as fetching current time from a well-known server and sending OTPs via SMS. Network latency and reliability can influence the overall performance of the system, especially during real-time verification processes. Implementing efficient error handling and retry mechanisms can mitigate the impact of network disruptions on system performance.

Overall, the On-the-go Driver's License Verification System demonstrates efficient performance, balancing computational complexity with security requirements to ensure reliable and responsive operation.

Conclusion

The On-the-go Driver's License Verification System employs a combination of robust security measures to ensure the integrity, confidentiality, and authenticity of the verification process. By leveraging digital signatures, the system verifies the authenticity of messages and documents exchanged between the server, drivers, and police officers, thereby preventing unauthorized access or tampering. Additionally, encryption techniques are utilized to secure the transmission of sensitive information, such as OTPs, over the communication channels, protecting them from interception or eavesdropping. The generation of RSA key pairs further enhances security by ensuring the confidentiality and integrity of communication channels, safeguarding against unauthorized access or data manipulation. Overall, the system provides a secure and efficient mechanism for verifying driver's licenses in real-time, thereby enhancing road safety and law enforcement efficiency.