Republic of Iraq
Ministry of Higher Education and Scientific Research
University of Babylon
College of Engineering
Department of Electrical Engineering

Design and Implementation of Secure Smart Ports Gates System

A Dissertation

Submitted to the College of Engineering / University of Babylon in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Electrical Engineering / Electronic and Communications

By

Hayder Ali Hassoon

(B.Sc. 1998)

(M.Sc. 2015)

Supervised by

Prof. Dr. Hassan Jassim Motlak

2023 A.D ***1445 A.H***

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿ نَرْفَعُ دَرَجَاتٍ مَنْ نشَاءُ وَفَوْقَ كُلِّ ذِي عِلْمٍ عَلِيمٌ ﴾

صَدَقَ اللَّهُ الْعَلِيّ الْعَظِيم

الآية ٧٦ من سورة يوسف

Abstract

The global surge in international sea trade has driven the competitive nature of seaport management, with a focus on efficiency, performance, and cost reduction. This study specifically targets the challenges and opportunities within Iraq's ports, highlighting the decline due to war, economic sanctions, and the rise of corruption and inefficiency. A perfect solution is proposed by adopting innovative port technologies to align Iraqi ports with global competitors.

The centerpiece of the research is the proposal of a smart gate for the Umm Qasr port, positioning it as the first step in transitioning Iraqi ports to more innovative functionality. The proposed smart gate is built based on RFID, fingerprint sensors, and an automatic license plate recognition system for authentication, with computer clouds employed for data storage and processing. Information is exchanged between the smart portal and the cloud through a hybrid security system to ensure confidentiality and information integrity.

The devised smart port gate mechanism has been simulated using MATLAB, with individual steps modeled on specific datasets, such as utilizing the FVC2002 dataset for fingerprint accuracy. The matching precision for fingerprints has been observed to attain up to 96.6% across the various datasets. Additionally, the vehicle license recognition was assessed on European and Iraqi numbers using a template recognition method, and the algorithm was successful in both instances. A comprehensive simulation, including all three gates, was subsequently conducted, and verified.

Hybrid security systems were simulated, consisting of commonly used algorithms, namely AES, DES, and RSA, and hybridizing them with the SHA256 hashing algorithm. Simulation results showed that the encryption

and decryption time for RSA is about 1000 times slower than the encryption time for AES. Therefore, the throughput will be about 1000 times lower than the throughput of AES. As for entropy, it was constant for all algorithms, about 5.9.

The proposed system was implemented practically using the C# programming language, along with using the SQL-Server language to program the cloud database. Practical implementation of smart gate port automation has been proven to improve the time taken for a vehicle to pass through the smart gate by approximately 10%, which depends on the type of vehicle. The empirical findings are congruent with the simulated outcomes, demonstrating that the suggested system is robust, secure, and highly effective in recognition. This innovative approach helps alleviate traditional port challenges by facilitating processing, thereby enhancing efficiency and performance.

The study concludes that the gradual implementation of smart port technologies in Iraq is a feasible solution to combat existing challenges and a promising pathway to enhance the ports' global competitiveness significantly. The initiation of the smart gate not only increases reliability and security but also aids in preventing corruption and smuggling, making it an essential step towards a modernized and efficient port system in Iraq.

Dedication

To my Family

To my supervisors, my teachers, and friends

Acknowledgments

In the name of **ALLAH**, the Most Gracious and the Most Merciful for giving me the determination and will to complete this research work.

I appreciate the inspirations and guidelines that I have received from my supervisor Prof. Dr. ***Hassan Jassim Motlak***, for his advice, guidance, and encouragement. Without his continuous support and interest, this work would not have been the same as presented here.

I would like to extend my indebtedness to the teaching staff members of the Department of Electrical Engineering, University of Babylon, for their continuing support and fruitful discussion throughout all steps of the research work presented in this dissertation.

I would also like to thank Mr. ***Suhail***, shipping manager at Umm Qasr port, for his assistance in collecting information about the port.

Table of Contents

List of Abbreviations

Abbreviation	Definition
3G	Third Generation
4G	Fourth Generation
4IR	Industrial Revolution 4.0
AES	Advanced Encryption Standard
AFRS	Automated Fingerprint Recognition Systems
AGVs	Automated Guided Vehicles
ALPRS	Automatic License Plate Recognition System
DC	Direct Current
DES	Data Encryption Standard
DGPS	Differential GPS
DSA	Digital Signature Algorithm
DSP	Digital Signal Processor
ECC	Elliptical Curve Cryptography
GHE	Green House Gas
GPS	Global Positioning System
GSM	Global System for Mobile
GUI	Graphical User Interface
HAR	Hybrid AES Rail Fence
IAVs	Intelligent Autonomous Vehicles
ICT	Information and Communication Technology
IOT	Internet of Things

IP	Internet Protocol
ITS	Intelligent Transportation Systems
LED	Light-Emitting Diode
LS	Land Side
M2M	Machine to Machine
MD5	Message Digest algorithm
MITM	Man-In-The-Middle
NIST	National Institute of Standards and Technology
OCR	Optical Character Recognition
OTP	One Time Password
PC	Personal Computer
PLC	Programmable Logic Controllers
QCs	Quay Cranes
RF	Radio Frequency
RFID	Radio Frequency Identification
RMG	Rail-Mounted Gantry
RSA	Rivest-Shamir-Adleman
RTG	Rubber-Tire Gantry
SHA	Security Hash Algorithm
SMS	Short Message Service
SQL	Structured Query Language
STS	Ship-To-Shore
TCP	Transmission Control Protocol
UHF	Ultra-High Frequency

WS	Water Side
WSN	Wireless Sensor Network

List of Symbols

Symbol	Definition
$H^{(0)}$	Initial Hash Value
$+$	OR Gate
$\oplus$	Exclusive OR
$\wedge$	AND Gate
$\varphi(n)$	The Golden Ratio of n
C	Cipher Text
GCD	Greatest Common Divisor
M	Message Text
$ROTR$	Rotate To the Right
SHR	Shift To the Right
d	Private Key
e	Public Key
k	Encryption Key
p, q	Two Random Large Prime Numbers

List of Figures

List of Tables

List of Publications

The following papers were published while this dissertation was being prepared.

1. Hayder Ali Al-Fatlawi and Hassan Jassim Motlak, " Smart ports: towards a high performance, increased productivity, and a better environment," International Journal of Electrical and Computer Engineering (IJECE), vol. 13, no. 2, pp1472-1482, 2023.
2. IEEE Accepted paper,Hayder Ali Al-Fatlawi and Hassan Jassim Motlak, "Design and Implementation of Smart Port Gate System Based on Internet of Things ," in the 5th International Conference on Information Technology, Applied Mathematics and Statistics (ICITAMS), 2023.

Chapter One

Introduction

1.1Introduction

Maritime ports face unique challenges as they operate within a complex network of interconnected transportation, industrial, and civic infrastructure, and function as a regional multimodal hub for global supply chains. Finding efficient, cost-effective, eco-friendly international shipping means is no simple task [1].The global economy of today is characterized by market liberalization and fast expansion, which has increased port competition and raised awareness of environmental issues. These difficulties have gotten worse, necessitating a greater emphasis on modernity and transition at ports [2].

The COVID-19 pandemic has profoundly impacted the maritime industry. This industry plays a crucial role in the immediate pandemic response by supporting jobs, international trade, and the global economy. The influence of COVID-19 on international transport and the maritime sector is both direct and indirect, affecting operations, cash flow, production, delivery, and even the shipping crew. Labor shortages have particularly hit challenging industries such as retailing, warehousing, manufacturing, and logistics[3]. Consequently, the technologies central to the current phase of the Industrial Revolution, often referred to as "Industry 4.0" or 4IR, have become increasingly significant. The 4IR involves the creation of cyber-physical production systems that allow real-time transactions and decision-making by ensuring compatibility among systems, people, and the environment [4]. Many competitive shipping and port logistics sectors are embracing initiatives to gain an edge through the 4th IR which opening up new business avenues. As a result, the 4IR

is triggering significant changes in the future of seaports, which act as the nation's primary gateways to the world and are vital for the success of its export industry [5].

The length of the quay, the quantity and effectiveness of cranes, and other factors were historically the primary considerations for port operations. However, more recently, Industry 4.0 technologies have been making headway in the ports and maritime industry, which had previously been seen to be trailing behind other industries in digitization. Ports are anticipated to have a comparable adoption of new technology and new business models, building on the effects of Industry 4.0 on other industries [6].

Strategic plans have been laid out to foster the expansion of seaports and their transformation into global logistics hubs. Over the past few decades, interest in creating smart transportation systems has surged. These systems aim to develop transportation networks that are safer, more environmentally friendly, efficient, and innovative. Smart transport systems employ various technologies to observe traffic conditions, interface with vehicles and control centers, and skillfully manage and maintain traffic operations [7].

The smart port concept solves these current and future challenges. For this reason, many port authorities around the world are investing in smart ports.A smart port is a port that utilizes advanced technology and data analytics to improve efficiency, reduce costs, and enhance the overall operations of the port. A smart port aims to optimize resource use, improve stakeholder communication and collaboration, and enhance customer experience [8].

On the other hand, Smart port automation refers to using technology, such as automation and digitalization to improve port operations' efficiency, safety, and sustainability. This can include the use of autonomous vehicles, sensors, and data analytics to optimize the movement of cargo and vessels and use renewable energy

sources to power port operations. It can also involve using digital systems for communication and coordination between stakeholders, such as shipping companies, customs authorities, and logistics providers [9].

A smart port can use the installation of sensors to aid in the detection of any disruption or damage to the port's operations and infrastructure. The data collected from the sensors enables quicker problem resolution and aids in averting any possible issues before they worsen. By offering on-demand computing resources that including data, software, platforms, and infrastructure through internet hosted services, cloud computing services increase processing capacity while reducing costs. In other words, cloud computing services offer scalable, customizable, cost-effective IT infrastructure that is available on demand and that can be easily and widely accessible through distant "cloud" computing resources. The goal of the Internet of Things is to link a network of ships, port workers, and physical things to the pervasive Internet. The Internet of Things enables device-to-device communication, collecting and exchanging data. IoT may thereby increase the flow of real-time streaming data in a port environment, and improving the smart port operations by enhancing the ability to instantly adapt to changing port surroundings and then take speedy remedial action, if necessary [10].

A smart port can bring many benefits, such as increased efficiency, cost savings, and improved customer experience. However, building a smart port requires significant investments in technology and infrastructure and close collaboration among all stakeholders.

Iraqi ports face stiff competition from neighboring countries such as the UAE, Qatar, and Kuwait. While these ports have made significant progress over the last two decades, the performance and efficiency of Iraqi ports have declined for various reasons. Some reasons include Iraq's involvement in numerous wars and the presence

of corruption, including the falsification of the number, types, and weight of goods arriving at ports in general and bribing relevant personnel and falsifying official documents, such as invoices, certificates of origin, standardization, and quality control certificates, to reduce or evade taxes. Other reasons include administrative and bureaucratic procedures that necessitate the acquisition of numerous licenses and the lengthy wait to release goods, which incurs additional costs for exporters (see Appendix A). Port yields and efficiency suffer as a result [11].

These reasons must be eliminated by turning to smart ports to increase the efficiency and performance of Iraqi ports. This work can be divided into two parts. The first part deals with the essential requirements to transition to a smart port and knowledge of modern technologies used in smart ports. It helps port owners and decision-makers to make the right decision and also facilitates other researchers to choose what suits them in their field of research.

In the second part of this research project, a smart port gateway is implemented and controlled by the Internet of Things (IoT). This portal relies on modern technologies such as Radio Frequency Identification (RFID), Fingerprint Identification System, and Automatic License Plate Recognition System (ALPRS). These technologies work with a pre-existing cloud database to open and close the gate. A secure system was used to transmit information online to ensure the portal works reliably and safely. This work contributes to eliminate many of the problems that Iraqi ports suffer from, the most important of which are document forgery, tax evasion, and human errors. It also contributes to regulate traffic, preventing congestion, achieving more revenues, and facilitating the management of information on goods leaving the port. Since it reduces traffic congestion, it helps reduce environmental pollution.

1.2 Literature Survey

D. Xisong et al.,2013, [12] In this article, the stages of development of the leading international ports are summarized, and the main requirements for the next generation of smart ports are presented. Later, they presented the techniques used on the Internet of Things, such as Sensors, RFID, Wireless Sensor Networks (WSN), Network Communication Technology, Machine to Machine (M2M), and proposed to build smart ports.

N. Bahnes et al., 2016,[13] Intelligent Autonomous Vehicles (IAVs) are integral to Intelligent Transportation Systems (ITS), operating in both restricted private areas and open public spaces. Within seaports or container terminals, which can be considered virtually confined spaces, IAVs are commonly utilized. This study introduces an inter-vehicle communication system, allowing IAVs to interact and collaborate. This cooperative approach aims to prevent collisions within the yard's predefined intersection zones, decreasing the unloading time at the seaport.

J. Odiete et al., 2017,[14] Presented the development of an automated fingerprint-based door control system. The fingerprint of the person trying to open the door is taken using the fingerprint sensor. Then it is matched with the fingerprints previously stored in the database. If the fingerprint matches, the door will open; otherwise, it will not open. The system records the registration time and date of any person who opened the door, which helps monitor the actual time and date of the individual's registration in the event of any emergency.

Y. Yang et al.,2018, [15] This paper planned the principal requirements and challenges distinctive to various ports, emphasizing the examination of distributed sensor systems integral to vital port equipment. This includes quayside cranes, automated guided vehicles for container handling, and yard cranes. The manuscript details smart outlets' architecture, operations, and sensor systems within the port

environment. Additionally, the paper discusses the communication standards pertinent to smart outlets, shedding light on their function and implementation within the modernized port setting.

H. Ohal et al.,2018,[16] This article introduces a sophisticated gate management system that integrates sensor technology with the Internet of Things (IoT). The system facilitates gate control via a Smartphone interface, enabling manual and fully automated operation. The primary functional components include Radio-Frequency Identification (RFID) tags and a corresponding receiver that identifies and verifies authorized users. Upon successful authentication, control is transferred to a motor, coordinated through an Arduino microcontroller. A unique feature tailored to two-wheeled vehicles allows the gates to open only 30%, conserving resources.

D. P. Holkar Vaijayanti, Tile Neha, 2020,[17] Introduced an automatic gate system based on an image processing method for vehicle license plate detection. The Raspberry Pi was used as a microprocessor for processing the vehicle's license plate image. From a security point of view, this system can be hacked using fake or stolen license plates.

A. Molavi et al., 2020,[18] This scholarly paper introduces an innovative concept of smart ports, employing cutting-edge digital technologies that incorporate monitoring, control, automation, and intelligent equipment. These technologies aim to enhance port operations and rejuvenate the existing infrastructure to create a more resilient port system. The paper delineates specific evaluation indicators within four primary domains – operations, environment, energy, safety, and security – to provide a comprehensive framework for the future development and improvement of port systems.

N. Prabhakaran et al.,2020,[19] Used Radio Frequency Identification (RFID) technology to create an autonomous gateway security system. They used a

PIC16F877A microcontroller to open and close the gate and a GSM system to send short messages to the organization if an unauthorized person tried to open it. This system can be tampered with using an RFID card by another person.

S. S. N. Dileep kumar, 2020,[20] Introduced an automatic door-opening system using facial recognition technology. It created a database containing photos of authorized persons. When a person tries to enter, the camera takes a picture of his face. This image is sent to the database for matching with the stored images. If this image matches one of the images, the door will be opened, and an acknowledgment will be saved in the database system. If not, a message will be sent through the system to the administrator's device, warning that an unauthorized person is trying to open the door. Facial recognition technology depends on lighting, image angle, facial changes such as hair growth, etc.

S. Jalapur and A. Maniyar , 2020,[21]Created an IoT-based Door Lock System that uses cryptographic techniques such as AES-128 and Security Hash Algorithm SHA-512 for hashing and encryption to safeguard data transmitted over the network. The IoT-based system accomplishes secrecy, security, and remote data access applications. Data shared via a network may not always be secure. As a result, many researchers are interested in constructing such a safe system. So, because data is as precious as the treasures behind the door, the cryptographic techniques utilized in this lock system for doors will safeguard it from hackers.

P. Elechi et al., 2021,[22] Used a Global System for Mobile GSM to open the door automatically. Use the Atmega328 Microcontroller as the system's brain that receives, sends, and shares information with the GSM modem and the stepper engine. The gate is opened by a password sent by Short Message Service SMS from the GSM system. This method can be used in gates, allowing an authorized person to pass without identifying the vehicle.

A. Y. Cil et al., 2022,[23] In this scholarly investigation, a container port system empowered by the Internet of Things (IoT) is meticulously crafted by developing specialized software, an interface, and corresponding equipment. This system can remotely monitor crucial environmental parameters within the container environment, including temperature and humidity. Should the instantaneous values of a refrigerated container approach the pre-established upper or lower thresholds, the innovative IoT-based system activates visual and auditory alarms and dispatches notifications via e-mail and Short Message Service (SMS).

M. A. Ben Farah et al., 2022,[24] Innovative services within ports and autonomous vessels need to implement new cybersecurity measures and increase protection methods. If vital information systems are not sufficiently safeguarded, every port and ships are at danger of cyberattacks. The problem is worsened by the widespread adoption of new technologies, which has increased the number and severity of vulnerabilities affecting the essential infrastructures to business operations. As a result, there is a greater vulnerability to the danger of new cyberattacks and unauthorized access.

References refer to one or more areas of the smart port. This dissertation is discussed the main parts of the port that must be converted into a smart port to transform the traditional port into a smart port, starting with the ship and ending with the goods leaving the port gate.

This dissertation proposed a smart gateway system to address some of the problems facing Iraqi ports. Biometric technology is considered one of the most effective technologies for secure human identification systems due to its uniqueness and durability. Combining several technologies to create an Auto Gateway will make for a more reliable and secure system. Fingerprint, license plate number detection and RFID are used to control the gate opening.

To combine high security and information integrity of data exchanged with the cloud using cyber algorithms and hashing algorithms to obtain a hybrid algorithm. We discussed the use of asymmetric (Rivest, Shamir, and Adelman (RSA)) and symmetric (Advanced Encryption Standard (AES) and Data Encryption Standard (DES)) algorithms and combining them with a hashing algorithm (SHA256). We chose to use a hybrid system of RSA and SHA256 for the reasons mentioned below.

Table (1.1) represents a comparison of the proposed designed smart gate system with other systems reported in previous works. The comparison included the type of technology that was used, as well as the security algorithm, programming language, and the use of cloud computing to store data to ensure that it is not tampered with.

Table 1.1 Comparison of the proposed designed Smart Gate system with other systems reported in previous works.

Reference No.	**[14]**	**[17]**	**[19]**	**[20]**	**[22]**	**Proposed Systems**
Type of technology	Fingerprint Identification System	ALPRS	Radio Frequency Identification RFID	Face Recognition	SMS by GSM	Radio Frequency Identification RFID, ALPRS, Fingerprint Identification System
programming language	C#	Python	C	Python	C++	C# + SQL server
Security algorithms	Not use	Not use	Not use	Not use	Not use	RSA-SHA256 hybrid
Cloud Computing	Not use	Not use	Not use	Not use	Not use	Used cloud computing

1.2 Problem Statement

According to the review of the background and literature, traditional outlets, including Iraqi ports, face some challenges that can be resolved through the implementation of a smart port gate, which include:

1. The custom police make the verification process manually, so more time is required.
2. Errors in the declared data (on purpose or mistakes).
3. Bribing relevant personnel and falsifying official documents, such as invoices, certificates of origin, standardization, and quality control certificates, to reduce or evade taxes.
4. High labor cost
5. Usually, Port Traffic is directly related to Port Profits (high traffic leads to low profits).
6. Low security, low reliability, and slow response.

1.4 Thesis Objectives

The main objectives of designing and implementing a smart port gate based on the Internet of Things (IoT) technology are:

1. Design and simulate a smart port gate based on IoT technology to investigate the following aims: Real-time monitoring and tracking, Increased efficiency, Improved collaboration, Reduced environmental impact, Improved security, Predictive maintenance, Smart logistics, and Smart Energy Management.
2. This dissertation proposes two hybrid security algorithms to secure the port's data: Rivest–Shamir–Adleman (RSA) and Security Hash Algorithm (SHA256).
3. Implemented the hybrid security dependent to examine it under different cases and finally integrate it with the smart port gate, which consists of the RFID,

sensors, Automatic License Plate Recognition System (ALPRS), and fingerprint.

4. Examination of the proposed smart port gate in light of real-time data obtained from the Umm Qasr Port Administration (see Appendix B) to verify the automation of the proposed smart port gate.

1.5 Thesis Contributions

The main contribution of this thesis can be summarized as follows:

1. Designing a hybrid of two security algorithms, Rivest–Shamir–Adleman (RSA) and Security Hash Algorithm (SHA256) are used to secure the data during the transition by cloud to the server and return to the stored data in the port. This thesis uses this hybrid for the first time in a smart port gate. The main advantage of this algorithm is simplicity and high security in encryption and data decryption.
2. Designing a smart port gate and applying it on the Umm Qasr port based on IoT technology, including RFID, fingerprint, and hybrid security algorithm.
3. Implemented and simulated the proposed smart port gate and security algorithm; the simulation and practical results match.

For more focus on using RFID and IoT in smart ports, the main contribution of using RFID (Radio-Frequency Identification) based on the Internet of Things (IoT) in smart port automation is the ability to track and manage the movement of cargo and vehicles in real-time.

1.6 Thesis Layout

This thesis consists of five chapters, including chapter one, as follows:

Chapter One: Introduces the general background of the smart port and the advantages and disadvantages compared with the traditional port. In addition, the

literature review and problem states are presented in this chapter. Finally, the thesis objectives and the main contributions are addressed.

Chapter Two: Presents the theoretical background of smart ports and the smart technology that will be used to transition from traditional ports to smart ports, taking into account the main challenges and the security aspects.in addition, this chapter focuses on the IoT employed in the smart port gate in chapter three.

Chapter Three: Introduces the proposed smart port gate automation based on IoT technology. In addition, the proposed hybrid security is used as a portion of the smart port. Also, the hardware and simulation design is presented in this chapter.

Chapter Four: The simulation results for fingerprint, hybrid security techniques, and the whole smart port are discussed in this chapter. In order to validate the proposed system for automation of the smart port of Iraq port in Basrah, the hardware results are discussed and compared with previous work in this chapter.

Chapter Five: the main contribution and the proposed smart port gate findings with the essential recommendations for future work are listed in this chapter.

Chapter Two

Theoretical Background and Automation for the Smart Ports

2.1 Introduction

This chapter reviews the concept of smart ports and the most important work carried out by ports to reach smart applications that can be used as a basis for building a smart port, such as building innovative ships, smart gantry cranes, container cranes, smart port operations, smart containers, and modern technologies in the field of energy to raise port efficiency. This section also deals with the concept of the smart gate and the technologies that can be used to control the work of the smart gate. The third and fourth sections deal with modern communication systems in port operations and port connectivity and management via the Internet of Things (IoT). Finally, the last section deals with the database in cloud computing and information security algorithms while sending it to cloud computing.

2.2 Smart Port Logistics

Maritime logistics services increase international trade, as most goods are transported through seaports [25]. To accommodate this quantity of goods, it has become necessary to develop these ports to be more efficient and productive. Smart ports can be used to achieve this objective. Smart ports rely upon utilizing from modern information technologies to arrive at the best degree of planning and management inside and among ports, accordingly facilitating managerial systems and improving the administration of cargo traffic [26]. The idea of a smart port method is automating all tasks performed by the port and conveying all port operations through the auto-transmission of mobile data in real time. As a result, the ability of ports to complete and integrate port operations doubles [27].

The smart Port reduces human resources, which saves money and time on documentation. It also makes tracking and traffic management easier, which aids reduce congestion, increase productivity, and keep workers safe [27]. Any smart port should combines sensors, actuators, wireless equipment, and database processing centers. This makes the services provided by port authorities more efficient and resilient in a more sustainable way. Among the most prominent sensors used in the smart Port to collect appropriate data are eddy current, ultrasonic, imaging, inertial, radio frequency identification (RFID), and radar [15]. To work on transforming traditional ports into smart ports, it is necessary to be aware of the most important operations in ports. As shown in Figure 2.1(a) and (b), the port areas can be divided as:

i) The terminal consists of several quays. Each quay deals with specific goods, such as containers, oil and gas tankers, and cruises.

ii) The quay is the ship's anchorage to unload its cargo. Dock container cranes unload containers from ships to horizontal transport systems, eventually transferring them to the container yard.

iii) A yard is where containers are unloaded from horizontal conveyor systems into a container yard for temporary storage until customer distribution. The yard has gantry cranes that stack containers.

iv) Trucks enter through the port gates to transport containers from the container yard. The gantry cranes load the containers onto trucks, which exit through the port gates and transfer the containers to the customers.

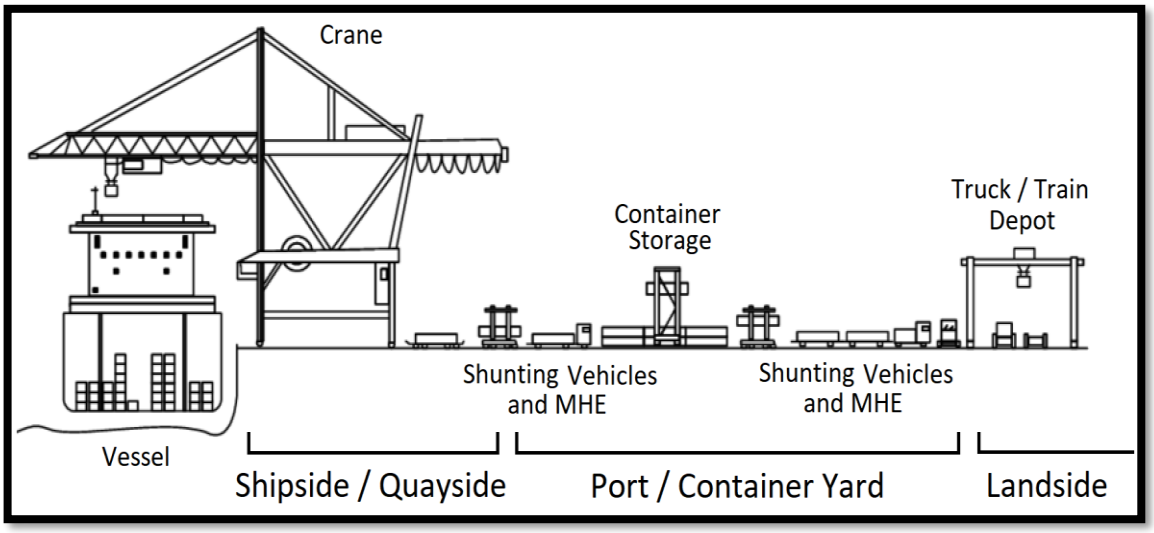


Figure 2.1. Port operations[28].

As shown in Figure 2.2, five main applications of smart outlets can be identified, which are as:

i) Smart ships.

ii) Smart gantry and quayside container cranes.

iii) Automation of transportation.

iv) Smart container.

v) Smart energy management.

vi) Smart gate

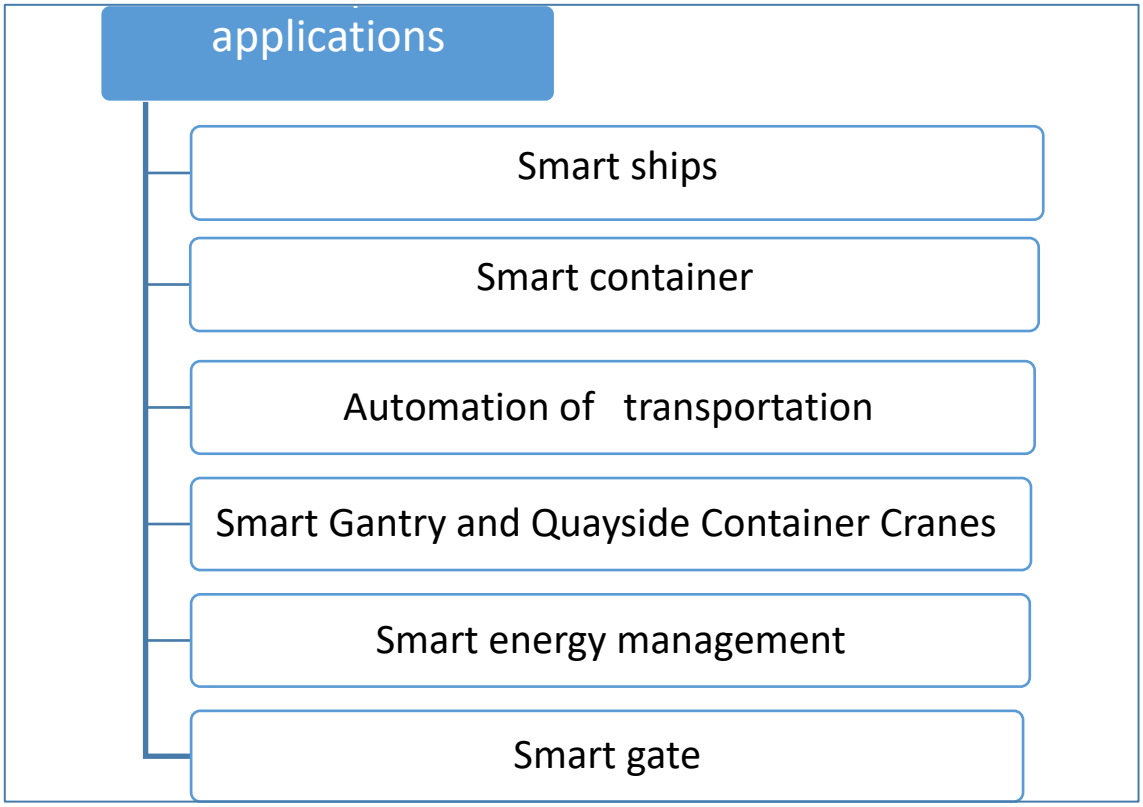


Figure 2.2. Main smart port applications.

2.2.1 Smart Ship

During the past two decades, the movement of ships increased, which led to congestion in the sea lanes due to the remarkable development of global maritime trade. This caused the number of ships, and eventually, the amount of greenhouse gas emissions and environmental pollution, to increase [29]. In order to avoid marine accidents and other undesirable problems, such as delays in the departure and arrival of ships, there was a need for effective navigation systems that enable communication among ships and ports.

Due to congestion, about 48% of ships arrive at least 12 hours later than the scheduled time. This increases fuel consumption, cost, and pollution [30]. For exemple, reducing one hour of ship waiting time could save up to $80,000[31].

The smart management of ships helps minimize the waiting time and the mooring of ships and helps them commit to their arrival schedule by selecting the paths and ports based on their location and the traffic rate .

For ships, the global positioning system (GPS) is an essential tool for navigation in and out of the port area. The importance of real-time data increases during port operations to identify the location and condition of objects for planning and coordinating activities with high efficiency [32], [33]. The retrieved positioning data can be used for prediction (e.g., route prediction, arrival times) and combined with other data sources to achieve contextual data about individual objects and points of interest [34]. Figure 2.3 represents the process of ships collecting information and exchanging it with other sources through satellites or 3G/4G communication technologies. The ships can communicate with the Port and its departments to know the traffic of ships and the docking times. This also enables the Port to track goods and identify their status and location [35].

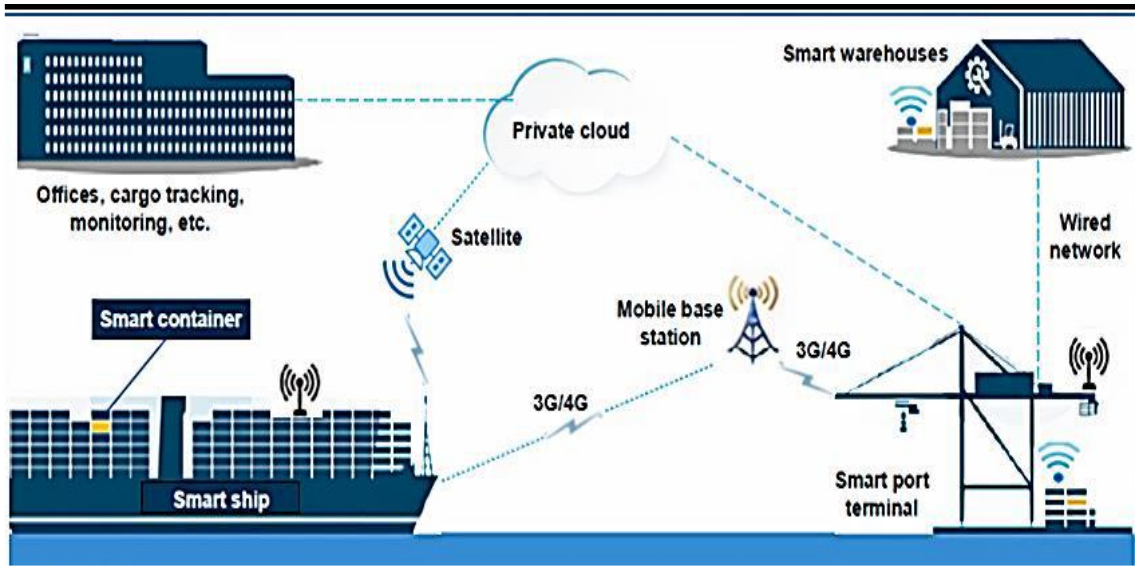


Figure2.3 Communication systems types in the smart ship at sea [35].

Table 2.1 compares smart and traditional ships, noting that they have advantages that help them outperform their counterparts. Obtaining more accurate

information about the paths of ships and possible congestion in marine traffic is possible. Through this, it is possible to estimate the time of arrival and delivery for ships, eventually reducing waiting time for ships, as well as the emission of Green House Gas emissions (GHG) and the carbon footprint resulting from the continuous operation of ships during the waiting period. It can be stated that it mitigates the adverse effects on the climate and the environment and improves the clarity of the air. From the points mentioned earlier, it can be noted that using smart ships allows for more efficient and productive planning of port operations [35, 36].

Table 2.1 Comparison between Smart ships and Conventional ships

Smart ships	**Conventional ships**
Less fuel consumption	More fuel consumption
More accurate information on ship movements	Less accurate information on ship movements
Improved ship scheduling and time of arrival of ships	Congestion in sea traffic and more delay time of arrival of ships
Increase in ports' efficiency	Less efficient ports
Reduction in greenhouse gas emissions (GHG)	Increase in greenhouse gas emissions (GHG)

2.2.2 Smart Gantry and Quayside Container Cranes

The increasing demands of customers for low-cost and fast shipping have led to competition in the global economy. To enter that competition, the automatization of the loading/unloading of equipment has the potential to dramatically improve the performance of port operation as it becomes efficient and high-tech. The most critical aspect is Ship-To-Shore container cranes (STS),

which comprise the bulk of the investment (70% of total port costs). It is used in the cargo loading and unloading system. It is a factor affecting the efficiency of port operations [37].

The control systems in traditional STS cranes depend on placing the load in the required place quickly and safely, which is determined by the personal skill of the workers and can be rather time-consuming. To increase the lifting speed and reduce the time, the cranes need to be fully automated to achieve high productivity. The higher the operating speeds of the crane, the more complex the control task [37].

In the traditional crane, the crane operator from the top of the cabin looks down to transport containers from one place to another. Over a long period through which the work is repeated periodically, it may cause fatigue and exhaustion for the operator. This could eventually lead to accidents and delays in completing work [38]. Rail-Mounted Gantry Cranes (RMGC) and Rubber-Tire-Gantry Cranes (RTGC) are two cranes frequently used in ports. Figures 2.4 and 2.5 shows the two types of cranes. Three operators must work alternately to operate one crane for 24 hours a day, implying the need for hundreds of workers as crane operators [39].

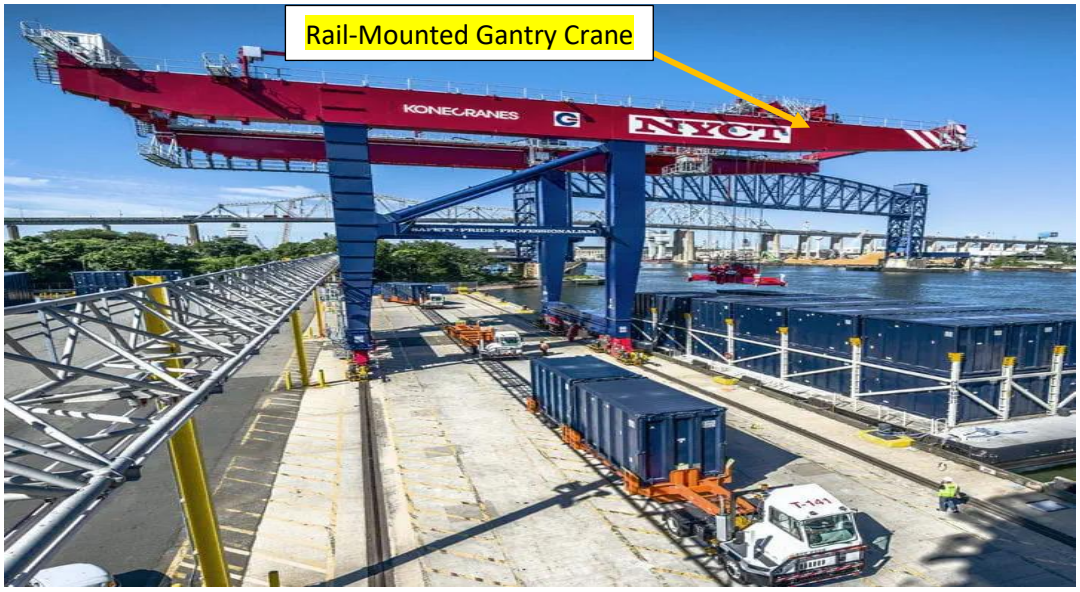


Figure 2.4. Rail-Mounted Gantry Crane (RMG)[28].

Figure 2.5 Rubber-Tire-Gantry Cranes (RTG)[40].

To switch from conventional cranes to robotic cranes, advanced sensors are installed on the crane chassis to detect the position of carriages and containers. These sensor systems include encoders for reading container data, laser rangefinders, cameras, and Programmable Logic Controllers (PLCs) [41, 42].

Automation of cranes significantly reduces labor costs, as one operator can operate three to six cranes remotely from the console room via video surveillance in Figure 2.6. It also helps to ensure operational safety [41].

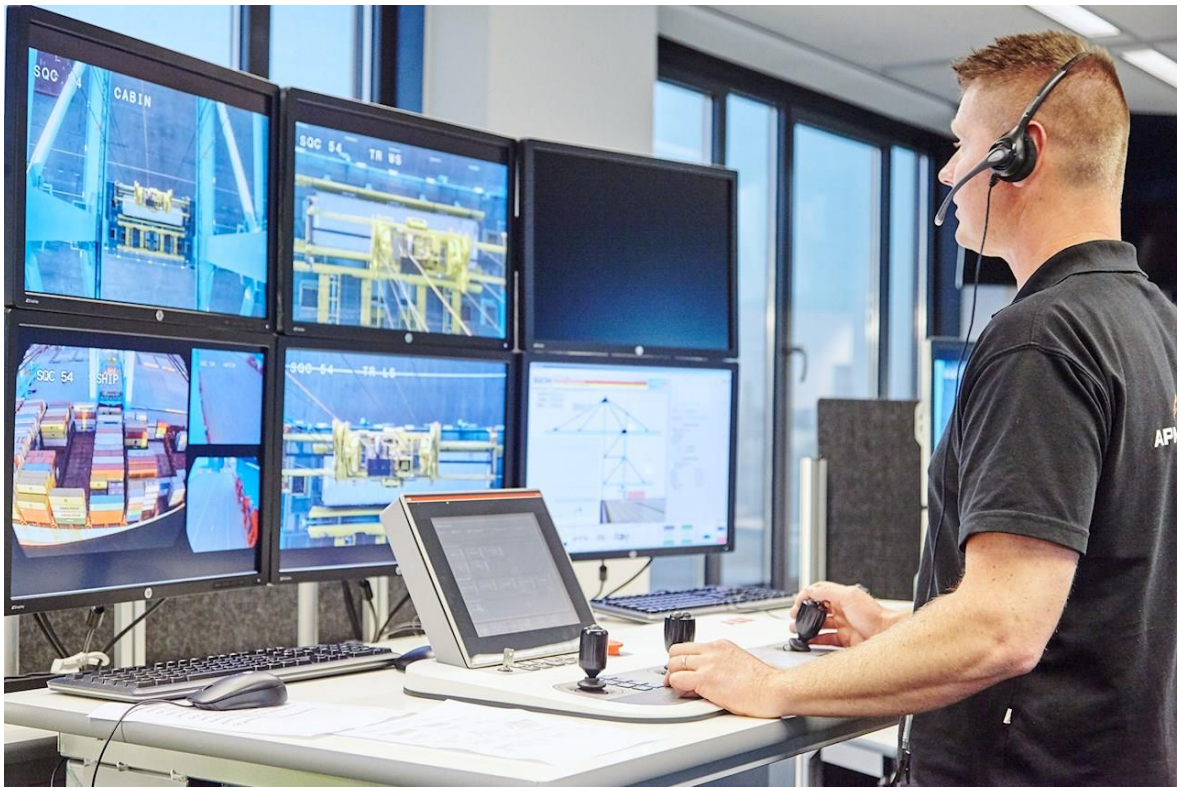


Figure 2.6 Supervision of the operation of more cranes is performed from a remote office [43].

Table 2.2 presents the comparison between smart cranes and traditional cranes. It is noted that the use of smart cranes significantly increases the productivity and efficiency of the Port, as a result of reducing the cost of labor and speed in carrying out the work, as well as preventing human errors as a result of accuracy in loading and unloading [15, 36].

Table 2.2 Comparison between Smart Cranes and Traditional Cranes

Smart cranes	**Traditional cranes**
No need for much labor	Requires much labor
No human errors	Human errors occur
Accuracy in loading and unloading	Less accuracy in loading and unloading
Speed in handling loads	Delays in the handling of loads
More efficient and productive	Less efficient and productive

2.2.3. The Automation of Transportation

At the Port, the horizontal transportation of containers consists of two separate logistic operations, as outlined below [42]: i) Land Side transport (LS): it is the process of transporting containers from the port gate to the yard and vice versa; ii) Water Side transportation (WS): the process of moving containers from ships after unloading by Quay Cranes (QCs) to the yard and vice versa. The road transport process is performed by trucks through the Port's main gate to the yard. Since those trucks are non-automated and the truck drivers are off-street laborers entering the station driven by outside labor and unfamiliar with unmanned cranes, special attention must be paid to ensure safety at those stations [42].

Transport on the waterside can be done either by conventional means of transport, such as tractors and trailers, or by automated platform-type vehicles, Automated Guided Vehicles (AGVs) as seen in Figure 2.7. Horizontal transportation on the waterside of the harbor with traditional gantry cranes was done by tractors and trailers. However, the use of conventional transportation appeared to be waning with the use of unmanned cranes due to safety issues while the driver was in the cabin of those vehicles [42].

Figure 2.7 Automated Guided Vehicles (AGVs)[44].

With the automation of the processes in the smart Port, such as storage and cranes inside the Port, traditional trucks also ought to be automated and replaced with electronically guided transport platforms. Smart ports prefer the use of AGV to reduce operating costs. However, several problems are associated with the use of AGV like positioning, route planning, obstacle avoidance, and route tracking [45].

Given its robustness and accuracy, the positioning problem can be solved using the Differential GPS (DGPS) system as a navigation system for uncrewed vehicles and systems, especially for AGVs [46]. The path tracking of AGV dumps is done using several technologies, including a camera sensor, laser navigation system, inductive guidance using underground electric wire, wall tracking algorithm, and semi-guided navigation method using magnetic tapes [47, 48] [49-51]. From the aspects stated, it is concluded that transportation automation has

many benefits, including reducing labor costs and safety and collision accidents and improving the environment by reducing gas emissions.

2.2.4 Smart Containers

To transform traditional containers into smart ones, they must be equipped with several sensors that track containers by collecting data on their geographical location and remote monitoring of events and conditions (such as temperature) for containers throughout their journey. Examples of events that can be noted include whether or not containers have been opened, changes in temperature, emergencies such as vibrations and falling of fragile goods, and floods and fires that occur during container transport. This technology alerts investors immediately to take the necessary measures [36]. Throughout its voyage, the intelligent container continuously updates its location in real-time, making it easier to arrange maintenance or report damage [52]. The smart container technology decreases the ship's berthing time in the port, which results in a 10% operating cost reduction [7], [53].

At container terminals, DGPS technology has been used. This system extends GPS through fixed reference stations that detect the difference between a known exact location and GPS positioning data. Thus, the exact location of the containers can be determined along with the tracking of container movements within the terminal [54]. Used RFID seals track commercial containers from the point of origin until they reach their destination, thus helping protect goods from damage, theft, and terrorist threats [55]. Figure 2.8 shows a container with a security seal that reveals any unauthorized attempt to open or tamper with the contents of the container.

Figure 2.8 A container with an RFID seal[56].

Table 2.3 Comparison between smart containers and traditional containers

Smart container	**Traditional container**
Locate the actual places and keep track of them.	Employees must look for containers.
Alerts can be set up to shed light on essential information	Not possible
Allow employees, suppliers, and customers to view specific information or get email notifications.	Not possible
The data is produced electronically and encrypted from end to end. Thus it is safe and reliable.	The data can be tampered with because it is generated manually.

Table 2.3 shows the comparison between smart containers and traditional containers. Through smart containers, physical locations can be identified and tracked. Alerts can be created, and important information can be sent to the information center. Employees, suppliers, and consumers can also view information or get email notifications. Because smart container data is electronically created and end-to-end secured, it is safe and reliable [27], [36].

2.2.5 Energy Efficiency of Smart Port

Due to the increasing rise in energy prices and to preserve the climate from environmental changes, many ports seek to enhance energy efficiency by adhering to environmental regulations issued by the authorities for reducing pollutants and greenhouse gas emissions from energy stations [57]. Equipment electrification, alternative fuels, renewable energy sources, and operational efficiency dramatically cut hazardous emissions and constitute the Port's future generation [58]. Automating smart port devices and equipment reduces energy consumption and improves energy efficiency [59]. There are a variety of technical solutions that may be used at the Port to improve energy efficiency and enhance the environment. Electricity can be used as a source of energy for numerous equipment, electric vehicles, renewable energy, energy storage systems, reefer cooling systems, lighting technologies, and alternative fuels are just a few of these options [57].

While docked, most ships turn off their main engines and turn on auxiliary engines to supply power for lighting and cooling activities. These engines burn fuel and emit greenhouse gases. Cold ironing, or the so-called beach card, uses electricity supplied through the grid or renewable sources to provide the energy required for such activities in ships [60-62]. The use of cold ironing in ports has

contributed to reducing toxic emissions. On average, 29.3% of carbon dioxide is reduced in port areas [63].

Because direct current may minimize peak demand and average power usage, using Direct Current (DC) instead of alternating current for more energy efficient [64]. Energy can also be stored in supercapacitors for later use [65]. Adopting new technologies in improving port lighting instead of traditional lighting (which represents about 3-5% of total energy) improves energy efficiency. Light-Emitting Diode (LED) bulbs instead of high-pressure sodium lamps to light the outlet storage facilities and administration building is an example of this technology [66]. The use of lighting leveling techniques can also save electricity [67].

Renewable energy resources include solar panels, windmills, tidal movement, waves, and underground heat [68]. The Jurong Port in Singapore has generated an annual electrical power of 12 million kWh using solar panels to cover the warehouse's rooftop [69], as shown in Figure 2. 9 . Hamburg's Port also covered the roofs of warehouses with solar panels and generated electric power of 500 megawatts per hour annually [70]. As for the latter, it generated 25.4 megawatts using wind energy by installing more than 20 turbines [57]. In the ports of Valencia and Hamburg, lighting energy consumption has been reduced by up to 80% through motion-sensitive lights that illuminate when vehicles pass [71]. As seen above, the smart Port substantially contributes to reducing gas emissions and global warming by continuously improving its energy efficiency and incorporating renewable energy into its operations. Furthermore, the efficiency of automated port systems and equipment provides for cost savings in energy, and the usage of automated guided vehicles has a substantial environmental impact.

Figure 2.9 PVs covered on the warehouse roof space [72].

2.2.6 Smart Gate

Gate scheduling systems are frequently established at port locations to enhance the timing of cargo exchanges. They function as a negotiating platform for transport appointments, aiming to regulate truck arrivals to prevent over-concentration during peak hours at terminal gates. This helps mitigate congestion at the gate and within the port region, facilitating smoother cargo flows, reducing drayage truck wait times, and diminishing vehicular emissions [73].

Creating an intelligent gate system has become an essential strategy for preventing congestion and optimizing the delivery scheduling of goods. The smart gate represents a critical technological innovation in the context of smart ports.

The Automated Gated System signifies a transition from conventional mechanisms to digital and automated solutions. Automation is a concept that has

substantially alleviated human efforts and minimized human-induced errors. It has fostered a connection between society and technology, leading to more advanced and progressive communities. In the traditional context, gates serve as security barriers, a role that can be compromised when controlled by humans. Therefore, technological solutions in this sphere can offer heightened security compared to human operators [16].

The limitation of access control in both private and commercial settings is essential for monitoring entry and exit points. By supplanting conventional gates with automated ones, unauthorized access can be effectively prevented. Robotic and automation technologies have been employed in gate design, utilizing different methodologies for controlling automatic gates, including biometrics, voice, and facial authentication techniques [74].

Utilizing various technologies to create fully automated gates provides a range of security and convenience features. Among them, biometric recognition systems offer superior security compared to traditional identification methods [75]. However, many technologies may be integrated into automated gate control systems.

Sensors are pivotal components within these systems, functioning as the fundamental mechanism for their proper operation. The availability of these sensors in the market enables the system to be developed cost-effectively. Furthermore, the ongoing operational costs are significantly lower than those associated with human security personnel which rendering the system wholly reliable, functional, and secure[16].

Biometrics technology is a highly effective solution for secure human identification due to its unique and permanent attributes. In this project, we explored the amalgamation of various technologies to create an Auto Gateway,

aiming for a more robust and secure system. Techniques such as fingerprint recognition, vehicle plate number detection, and RFID were deployed for gate control. An in-depth review of how these techniques function will be presented, followed by a discussion of the design and operation in the subsequent chapter.

2.2.6.1 Radio Frequency Identification RFID

RFID (Radio Frequency Identification) is a remote identification method for returning or saving data from RFID Tags [76]. RFID Tags, RFID Readers, Middleware, and a Backend database are significant parts of RFID technology [77]. Each RFID tag has a unique identification number saved in the tag's microchip [78]. Most RFID tags contain at least two parts see Figure 2.10. One is an integrated circuit for data storage and processing, RF signal modulation and demodulation, and other specific tasks. The second is an antenna for signal reception and transmission [16].

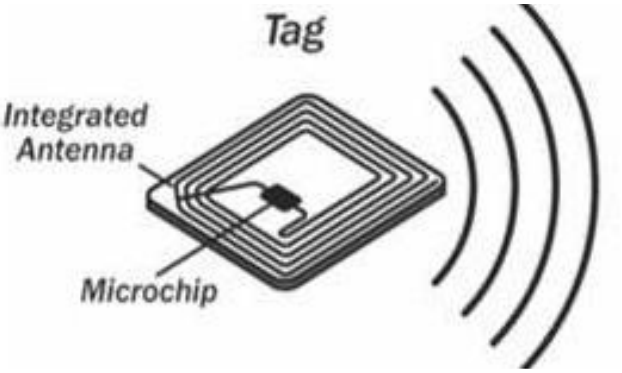


Figure 2.10 RFID Tag components [16].

There are two ways to activate the tag passively via the RFID reader or by sending an RF signal from the tag to the reader [79]. Passive tags are used in this work due to their features. The most crucial advantage of passive tags based on the proposed system is that they do not require routine maintenance. When the RFID reader is in its vicinity, it retrieves the information saved on these tags by

using its antenna [80]. The RFID reader is the second essential part of an RFID system, also known as an interrogator or scanner. This device communicates with the RFID tag via antennas, transmitting and receiving RF data. Some readers include numerous antennas that can transmit and receive radio waves to alert the data processing system to the existence of an object that has been tagged.

Structurally, a reader contains of three principal sections: the control unit, high-frequency interface section, and antenna section. Various factors, such as antenna gain, frequency utilization, and antenna orientation, influence the reader's read range [81]. The radio frequency at which RFID systems operate is used to identify them, and each frequency has unique read distance, power requirements, and performance characteristics. The frequency used depends on the purpose, and RFID technology typically uses four different types of frequencies [81]:

A. Low Frequency (120-140 KHz): Operating within the low-frequency range, these tags are commonly utilized for transactions involving deposits and withdrawals and tracking and managing assets.

B. High Frequency (13.56 MHz): These tags, working within the high-frequency range, are instrumental in asset-tracking applications, contactless credit cards, and identification badges.

C. Ultra-High Frequency (869 MHz-928 MHz): UHF tags, operating between 869 MHz and 928 MHz, are pivotal in supply chain management applications. They offer an extended reading range and are more cost-effective for mass production.

D. Microwave (2.4 GHz-2.5 GHz): Microwave systems provide a higher reading rate, though the associated tags are more expensive than UHF tags. They find their application mainly in electronic toll systems.

The reader's specific frequency dictates its effective range, spanning from 125 kHz to 2.4 GHz.[80]. The MR6111E UHF Long Range Integrated Reader was employed in this work, utilizing a UHF frequency range of approximately 900 MHz. This choice was congruent with the system's requirements.

Middleware encompasses all components that convey pertinent data from the RFID reader to the backend management system. This can include hardware elements like cables and link ports and software components such as filters for overseeing the system's performance. Each tag's unique identifier is cataloged in the backend database to delineate the roles of individual tags [78, 80]. The RFID system's functionality is contingent on the cohesive operation of its core parts, maximizing efficiency and application performance. This technology's adaptability facilitates its deployment across various practical scenarios, ranging from confined storage locations to comprehensive supply chain management systems [82]. As a vital and widely applicable technology, RFID plays an instrumental role in transportation, aiding in tracking, identification, safety, and security during transit [83]. Additional applications include animal tracking, storage management systems, secure toll payments, and automated access control [80].

2.2.6.2 Automatic License Plate Recognition System (ALPRS)

The Automatic License Plate Recognition System (ALPRS) is a modern system based on image processing technologies. It is used to identify vehicles based on the image processing of their license plates. This technology maintains law enforcement in traffic on public roads and security installations [84]. It also plays a vital role in border control, parking lot management, stolen vehicle detection, physical intrusion, and protection in safety [85]. It is crucial in this

work because it can solve various issues, including manipulation and authorization.

One of the primary challenges in License Plate Recognition (LPR) is the extensive diversity of license plates. This diversity manifests in color, shape, size, and pattern variations across different plates. Additional hurdles that complicate the process include adverse weather conditions, suboptimal lighting, and low camera resolution, all of which can degrade the quality of the image when a camera captures a license plate in real-time. The movement of a vehicle can also influence the camera's shutter speed, leading to a potential blurring effect [86]. As shown in Figure 2.11, the operation of the system can be classified into four principal segments: capturing the image of the vehicle, localizing the plate, segmenting the characters, and recognizing the characters [87].

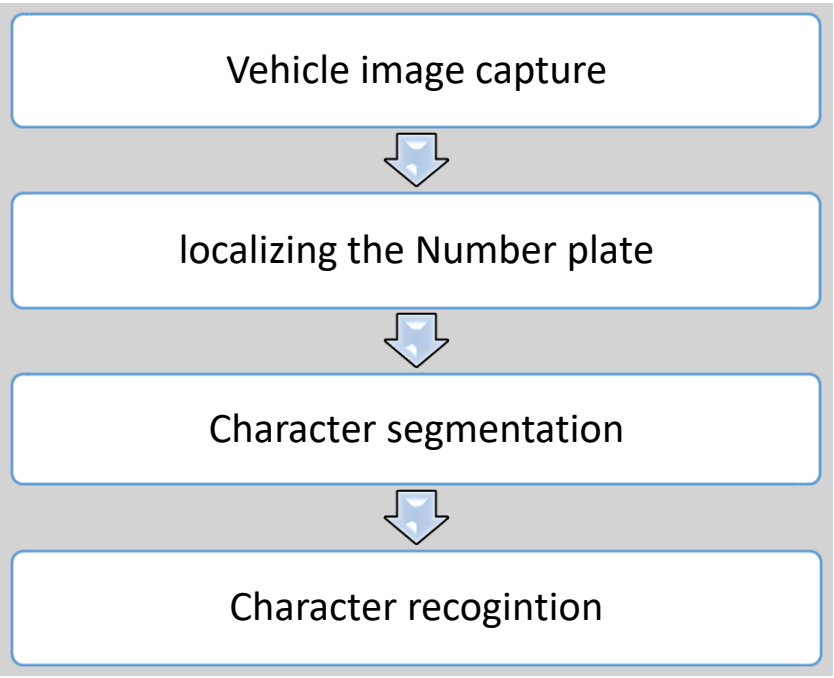


Figure 2.11 ALPR System [87].

The first step is to capture images of vehicles, remove noise and improve image quality to facilitate knowing vehicle plate numbers by transforming the

characters in the image that cannot be read into readable text [88]. The image obtained is preprocessed. This stage's primary goal is to enhance the low-quality image and eliminate undesirable noise [89]. The second stage is plate localization, also known as plate extraction. It is the process of locating the plate in a captured photograph. Many algorithms for detecting vehicle number plates can be classified into multiple categories based on their different techniques. The detection of a vehicle number plate must take into account several specific factors:

Plate Size: The plate size can vary within an image of a vehicle.

Plate Location: The plate's location may differ across vehicles, as it can be anywhere on the vehicle's body.

Plate Background: Plates can exhibit various background colors depending on the type of vehicle. For instance, a government vehicle's number plate may have a different background color than the number plates on public vehicles.

Screw Consideration: Screws on a plate may complicate detection, as they could be misconstrued as characters.

The extraction of a number plate can be achieved by applying image segmentation methods. Many image segmentation techniques are described in existing literature, and a common approach across many of these methods is the utilization of image binarization[87].

The third phase is character separation, an algorithm that locates the alphanumeric characters on a number plate [90]. The final phase is optical character recognition, identifying the extracted characters [91]. Arms such as template matching or neural network classifiers are used for character recognition.

2.2.6.3 Fingerprint Identification System

Fingerprint identification is one of the most dependable methods of confirming a person's identity. The fingerprint is one of the biological traits characterized by uniqueness and permanence. "uniqueness" refers to the absence of feature similarity between two unlike biometrics datasets [92]. For example, even if they are twins, no two personals have the same fingerprint lines. When the characteristics of biometrics do not change over time or with age, this is referred to as permanence. These systems are currently the most widely used type of biometric identification. Fingerprint systems are widely used for their ability to adapt and develop in the future and are inexpensive [93].

Enrolment and recognition are the two modes of the fingerprint identification system. The person's fingerprint is taken from the sensor to be saved in a database with the person's information to identify it, and this process is called Enrolment mode. In the recognition mode, the fingerprint is re-requested from the sensor and matched with the saved data for user identification [94]. Upon verification, the system compares the input fingerprint with the registered fingerprint of a particular user in the database to see if they belong to the same finger. Through identification, the system matches the fingerprint of the entry fingerprint with the fingerprints of all saved users in the database to decide whether the person is registered [95, 96]. There are different types of sensors used to obtain fingerprints, the most common of which are optical sensors [97].

Fingerprint comparison is conducted by analyzing specific features present in the ridge patterns of the prints. These characteristics can be organized into three distinct levels. Level 1 features include highly discernible elements such as ridges, cores, and deltas, as illustrated in Figure 2.12-a. The next category, Level 2 features, pertains to the minutiae, which are fine details found on the ridges of

a fingerprint. These details often manifest as ridge endings or bifurcations, as depicted in Figure 2.12-b. Finally, Level 3 features encompass intricate intraridge details observable at a highly refined scale, including attributes like ridge contours, sweat pores, and dots, as shown in Figure 2.12-c [98].

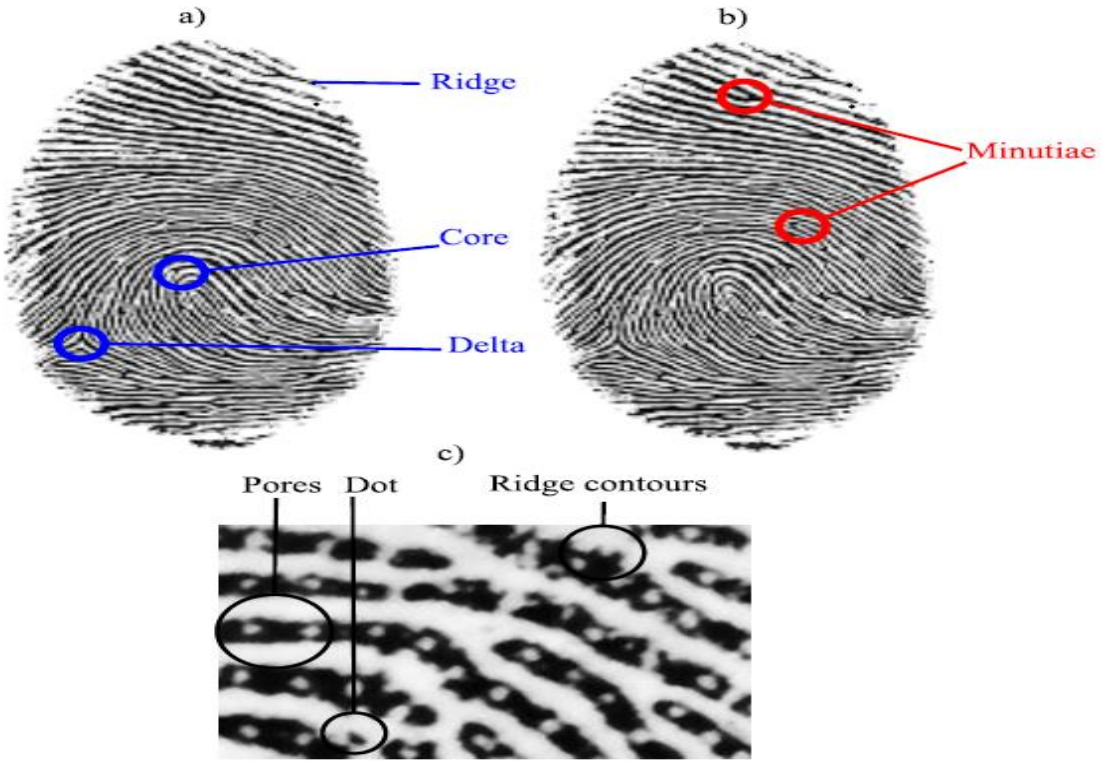


Figure 2.12: Levels of fingerprint features[98].

The steps of the Fingerprint recognition system are [99]:

- Capture Image: The initial step involves digital sensors capturing the fingerprint image. Often, the resultant image appears blurred and noisy due to suboptimal image quality.
- Preprocessing: This stage focuses on enhancing image quality by applying practical algorithms. These algorithms eliminate visible imperfections in the fingerprint, such as noise, missing minutiae, and blurriness,

transforming it into a high-quality image where the ridges and valleys are discernible.

- Feature Extraction: The third stage entails the identification of various fingerprint features. Feature extraction is conducted at three different levels:

Level 1: Global Level, where general patterns such as deltas, whorls, and loops are identified.

Level 2: Local Level, which involves the examination of irregular ridges, often manifested in minutiae form. This level focuses on bifurcations, ridge endings, lakes, and crossovers.

Level 3: Very Fine Level, where excellent details are considered, including detecting sweat pores and other minuscule features.

- Pattern Recognition (PR): The retrieved characteristics are now being compared to a template that already exists in the database. A training picture from the database—a template made at the time of enrollment—and the input test image—used when a user has to confirm their identity—are compared during the matching process.

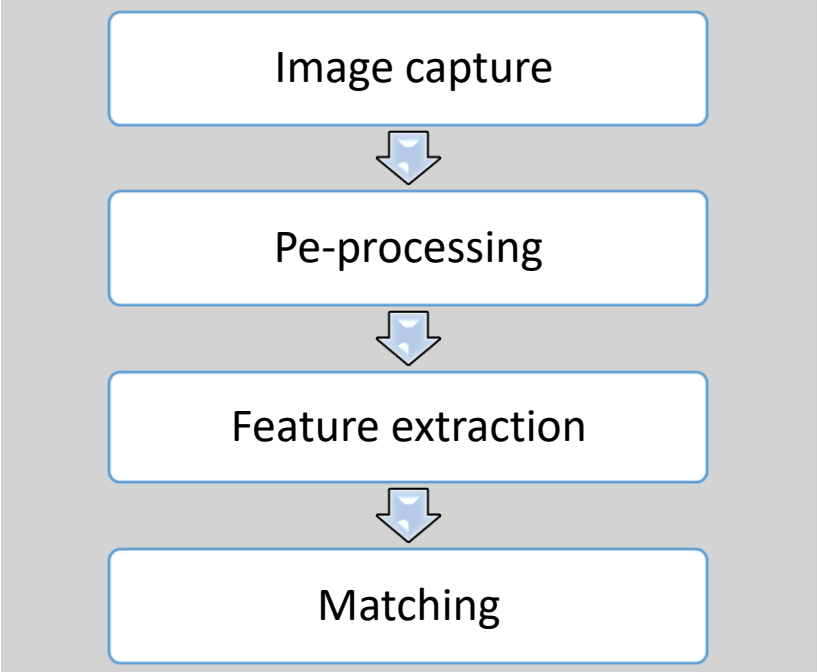


Figure 2.13: Fingerprints recognition system[99].

2.3. Communication Systems of Smart Port

Due to their unique advantages, wireless communication systems are urgently necessary for automated ports. However, there are some complex problems faced by these systems during implementation. The biggest challenge is that it is affected by the large metal parts that make up the containers and most of the port equipment. The second challenge is that it is affected by high-energy electrical equipment. Some of these problems can be solved by developing anti-jamming (antenna) techniques so that wireless communications become more widespread [15].

WSN is one of the most promising technologies due to its size, cost-effective nature, less energy consumption, ability to deploy in the target environment quickly, and entry into many sensitive applications. WSN is widely used for many applications such as military, medical care, environmental monitoring, smart agriculture, ground earthquake monitoring, control lighting,

smart cities, and monitoring electric grids [100, 101]. Many port areas employ a WSN, comprised of linked wireless sensors installed at a point of interest to monitor physical or environmental parameters, including location, temperature, and humidity [102]. These sensors can contact one another with a base station linked to a remote storage, processing, and analysis system.

The WSN is built with ZigBee. It is simple, utilizes lower data rates, low cost, is small in size, and uses little energy, allowing ZigBee-built devices to function for six to two years by used two batteries kind Mignon. Furthermore, ZigBee bases many nodes (May be up to 65,000) and may thus be utilized to construct a large-scale WSN[54, 103]. ZigBee is used for short-distance radio networks, telemetry systems, sensors, and surveillance devices [104]. A ZigBee sensor network allows for increased security of container shipments by detecting door openings, temperature and humidity, and photometry and by tracking the location of containers via GPS [105].

Wi-Fi can also be used in intelligent ports due to its wide range and broadband advantages. It uses specific frequencies, such as 2.4 or 5 GHz channels [104]. Wi-Fi is mainly utilized for video surveillance and AGV remote control [15]. For example, using video recognition technology, the camera installed in front of the yard crane will make it simple to determine the encoding information of containers. For standard Wi-Fi, the maximum range is 100 meters, but the standard range is 10-35 meters [104].

RF communication is a wireless point-to-point communication method. Long-distance communication up to 5 km and the possibility for users to connect directly through radio frequency stations without additional infrastructure support are two advantages of RF communication. The smart port uses RF technologies to facilitate communications between ships, ports, and distant personnel without

the need for additional infrastructure support [15]. Table 2.4 compares the popular wireless technologies and relevant smart port applications [15].

Table 2.4 Comparison of wireless communication systems.

Wireless Technologies	**ZigBee**	**RF**	**Wi-Fi**
Bit rate	250 kbps	9.6 kbps	300 Mbps
Range (outdoor)	100 m	20 km	100 m
Frequency	784 MHz	433 MHz	2.4 GHz/5GHz
Cost	$	$$	$$
Popularity	+	++	+++
Public Access	-	+	+

2.4. Internet of Things in Smart Port

The IEEE defines the Internet of Things (IoT) as a network of sensors and embedded devices that are connected to the Internet and used to gather and share data [106]. As seen in Figure 2.14, The Internet of Things has been employed in most aspects of life, including smart farming, smart cities, the field of healthcare, smart homes, smart river surveillance system, bright street lighting, and intelligent transport [107-113].

In the context of a smart port, the devices are interconnected through what is referred to as the IoT Smart Port. This integrated network comprises intelligent sensors and actuators, wireless technology, and data centers. It collectively forming the core infrastructure of the smart Port. Such an arrangement enables

port authorities to expedite essential services, enhancing efficiency and productivity.

The transformation from a conventional port to a "smart port" requires diverse sensors, including inertial sensors, ultrasonic sensors, eddy current sensors, radar, lidar, imaging sensors, and RFID readers and tags. These tools facilitate the collection of necessary data and contributing to the Port's intelligence.

Critical IoT applications implemented within smart ports encompass real-time route planning and tracking for intelligent ships [114], surveillance of containers [115], applications related to transportation [116], optimization of storage capacity [117], and electronic navigation (e-navigation) [118]. These applications aim to harness technological advancements to increase overall efficiency and effectiveness within the port environment.

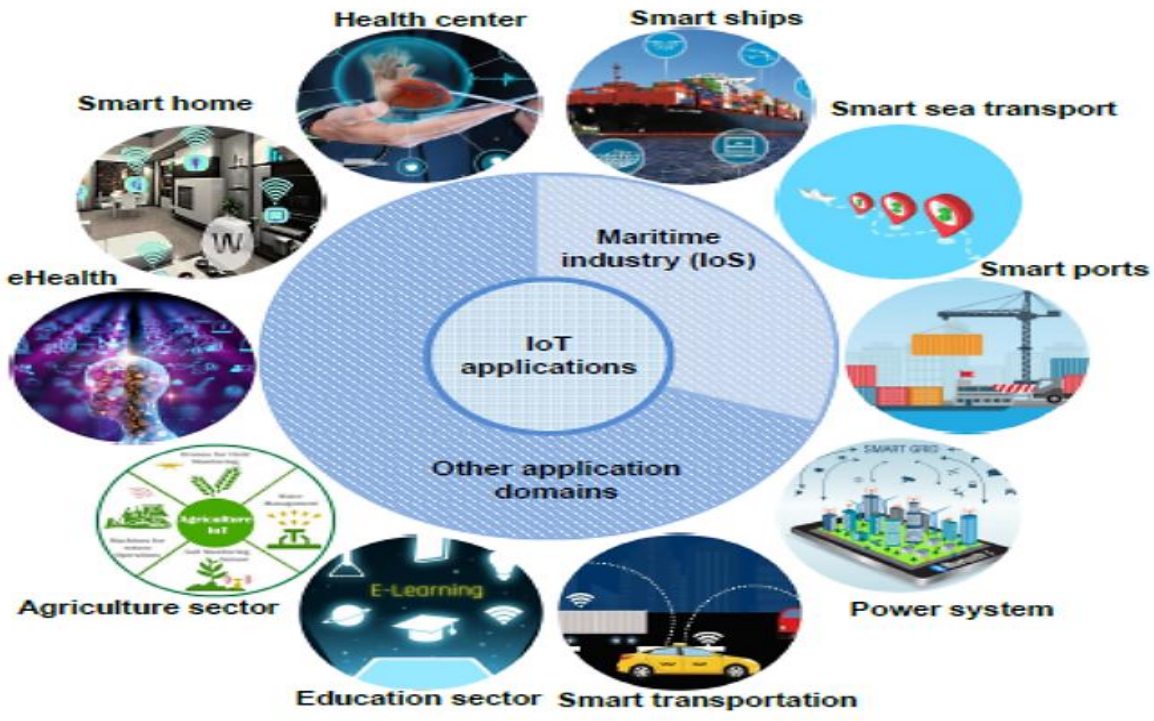


Figure 2.14 Main IoT application fields [35].

2.5 Cloud Computing Database

Cloud computing is a new technology that has been created to virtualize the use of information technology systems. It delivers on-demand computer system resources and is pay-as-you-go. This means there will be no cost to set up, operate, and maintain hardware or servers. Traditionally, building an IT environment requires purchasing servers, hardware, and licenses and installing software. This process is costly and time-consuming, with many infrastructure requirements [119].

The cloud database is created using cloud computing, which means it uses the software and hardware resources of the cloud computing service provider. Many companies have started moving towards using cloud computing and accessing their data from cloud databases. Many companies worldwide will use cloud databases to store massive data [120].

Database as a service provider includes Amazon Relational Database Service, Microsoft's Structured Query Language SQL AZURE, Google Datastore, Google Cloud SQL, and Database.com. Each service provider differs in terms of the quality and type of services offered [119, 120].

2.6 Cloud Security

Web technology, by harnessing the potential of the World Wide Web, offers clients seamless access to information from any location. The ubiquity of internet connectivity permits global users to engage with various resources, such as communications systems, computing devices, and diverse software applications. Cloud computing further facilitates this, wherein providers extend numerous shared resources like memory, networks, processing power, and other computational functionalities to users [121].

In the era following the COVID-19 pandemic, a noticeable trend toward the adoption of cloud services, software, and infrastructure has emerged. These resources, accessible at any time and from any place, have become increasingly attractive. Nevertheless, security concerns form a significant barrier to the broader adoption of cloud computing systems. Ensuring the security of the cloud, especially at the infrastructure level, it remains paramount. While extensive research has been conducted in cloud infrastructure security, specific gaps remain unaddressed, and new challenges continually emerge [122].

Concerning data-level security, protection measures must be implemented for data at rest and in transit to prevent loss, leakage, and the consequential impact on privacy. Furthermore, data confidentiality, integrity, and availability at rest could be threatened by various issues such as data leakage, hijacking, manipulation, and eradication [123]. Such challenges underscore the criticality of data security within cloud services.

Cryptography is a widely accepted approach to ensuring data safety, providing mechanisms that assure confidentiality, integrity control, access control, and message authentication [124].

Within the cloud network, cryptography safeguards stored or communicated data by employing encryption techniques to prevent unauthorized access. This enables cloud users to securely and easily access shared data and protects sensitive information during exchanges within the cloud. Numerous security algorithms have been devised using cryptographic techniques that affirming their importance for data security in the cloud environment [125]. The application of hybrid security in cloud computing and IoT systems offers confidentiality to each device, with the hybrid algorithm strengthening the confidentiality of data transmission across both domains [126].

2.6.1 Encryption Algorithms

There are two primary types of encryption techniques: Symmetric encryption (or private) and Asymmetric encryption (or public). In the case of Symmetric key encryption, also known as secret key encryption, a single key is utilized both to encrypt and decrypt the data, as depicted in Figure 2.15.

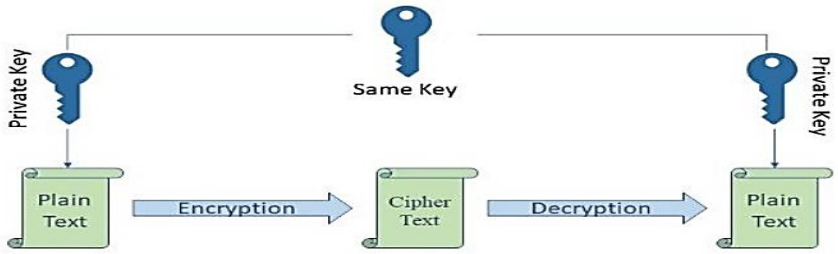


Figure 2.15 Symmetric Key Cryptography[127].

Asymmetric key encryption employs two keys: a public key for encryption and a private key for decryption, examples of which include RSA and Digital Signatures, as illustrated in Figure 2.16. This encryption technique relies on mathematical functions and is computationally demanding. Cryptography algorithms manifest solid and weak keys, such as DES and AES. For instance, DES utilizes a 64-bit key, while AES can use keys of 128, 192, or 256 bits. Asymmetric or public key encryption has been developed to address the critical distribution issue. Despite its utility, it is essential to note that asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, owing to the increased computational processing power they require [128, 129].

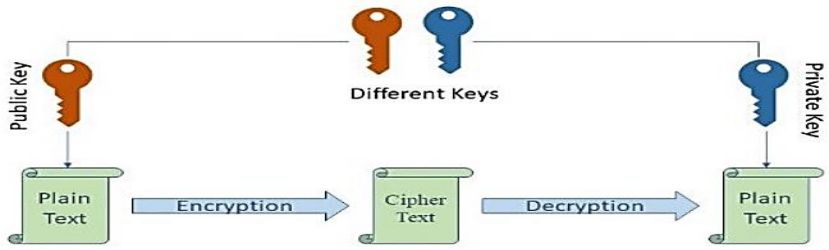


Figure 2.16 Asymmetric Key Cryptography[127].

A. Data Encryption Standard (DES)Algorithm

The Data Encryption Standard (DES) is a form of symmetric encryption that utilizes a 64-bit plain text block and a 56-bit key, with an additional eight bits designated for parity, to produce a corresponding 64-bit encrypted block. The bits of the plain text block are subjected to certain procedures throughout each round of encryption, as outlined in Figure 2.17. The specific steps of the algorithm are as follows [130]:

- Fundamental Division: The original key is segmented into two halves containing 28 bits.
- Critical Shifting: Both key segments are subjected to a bit shift, with the magnitude of the shift (one or two bits) determined by the particular round.
- Essential Recombination and Reduction: The two halves of the key are recombined and reduced from 56 bits to 48 bits, and this resultant key is employed to encrypt the plain text within the current round.
- Utilization of Subsequent Keys: The key derived from step 2 is utilized in subsequent rounds of the encryption process.
- Data Block Division: The 64-bit data block is segmented into two equal 32-bit sections.

- Expansion Permutation: One section of the 32-bit data block undergoes an expansion permutation, increasing its size to 48 bits.
- XOR Operation: The product of step 6 is combined with the 48-bit key derived from step 3 using an XOR (Exclusive OR) operation.
- S-Box Substitution: The output of step 7 is fed into an S-box, a specific function that substitutes key bits and compresses the 48-bit block back to 32 bits.
- P-Box Permutation: The result of step 8 undergoes a permutation using a P-box, which rearranges the bits according to a predefined pattern.

The process illustrates the complexity and intricate structure of the DES algorithm, relying on both bit-level permutations and substitutions to ensure the security of the encrypted data.

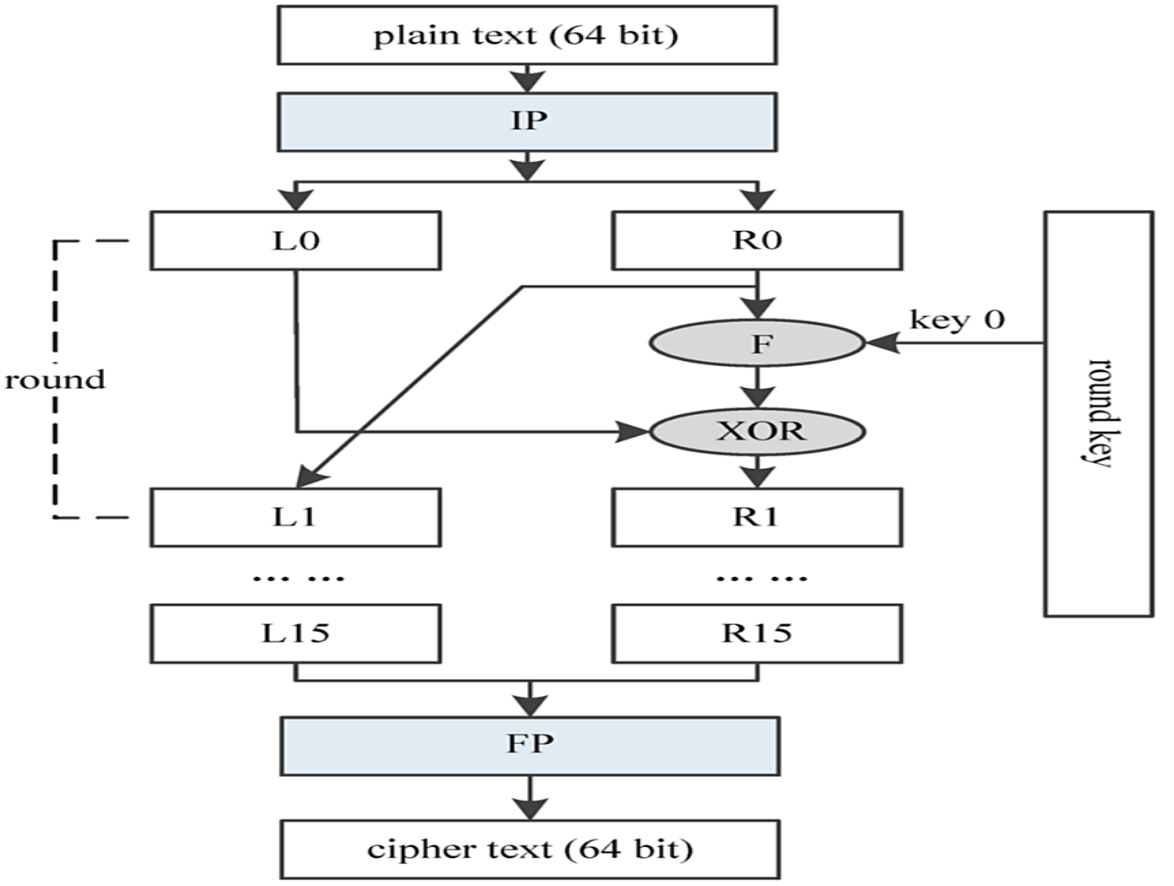


Figure 2.17 DES algorithm [130].

DES uses a 56-bit key size which is too small, so it is easy to break the algorithm [131].

B. Advanced Encryption Standard (AES) Algorithm

The Advanced Encryption Standard (AES) operates as a symmetric encryption algorithm, accepting a 128-bit plain text block and generating corresponding keys utilized within various rounds of the encryption process derived from the cipher key[130]. The algorithm's security is contingent upon its structural design and the length of the encryption key employed. AES offers three discrete key lengths, each furnishing different degrees of security. This algorithm is acknowledged for its proven security, wide application in data encryption, relatively low complexity, and high-security standards.

The core of the AES process is bifurcated into two distinct pathways [127]:

1. Data Encryption Path
2. Key Expansion Path

Moreover, the AES algorithm comprises four salient rounds, each serving a unique function:

1) Essential Expansion: The round keys are extracted from the cipher key through three sub-processes: Rotate, S-Box, and Rcon (as depicted in Figure 2.18).

2) Initial Round (Add Round Key): Individual bytes of the state are combined with corresponding segments of the round key using a bitwise XOR operation.

3) Rounds:

a. Sub Bytes: This is a non-linear substitution phase where each byte is mapped to another via a specified lookup table.

b. Shift Rows: A transposition step that cyclically shifts the final three rows of the state by specific step lengths.

c. Mix Columns: This mixing step operates on the state's columns that integrating the four bytes in each column and it is followed by the Add Round Key operation.

4) Final Round: This stage includes all the regular rounds operations except for the Mix Columns step.

AES is defined by its 128-bit block size and variable key lengths of 128, 192, and 256 bits:

A 128-bit key necessitates 10 encryption rounds.

A 192-bit key demands 12 encryption rounds.

A 256-bit key requires 14 encryption rounds.

Figure 2.19 illustrates a block diagram encompassing the 10 rounds of AES-128. The selection of the number of rounds is determined by assessing the maximum number of rounds for which shortcut attacks, which are more efficient than an exhaustive key search, have been identified and incorporating a substantial security buffer. For AES with a 128-bit block and key lengths whith no shortcut attacks have been uncovered for reduced versions with more than 6 rounds, and 4 additional rounds are appended as a security precaution. This methodology underscores a conservative approach to maintaining the integrity and robustness of the encryption process.

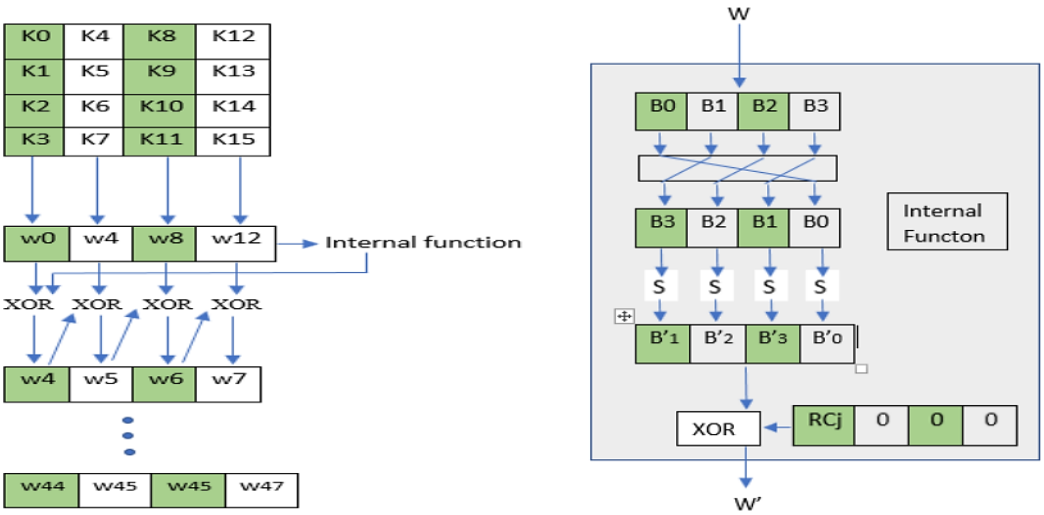


Figure 2.18 AES – Key Expansion [127].

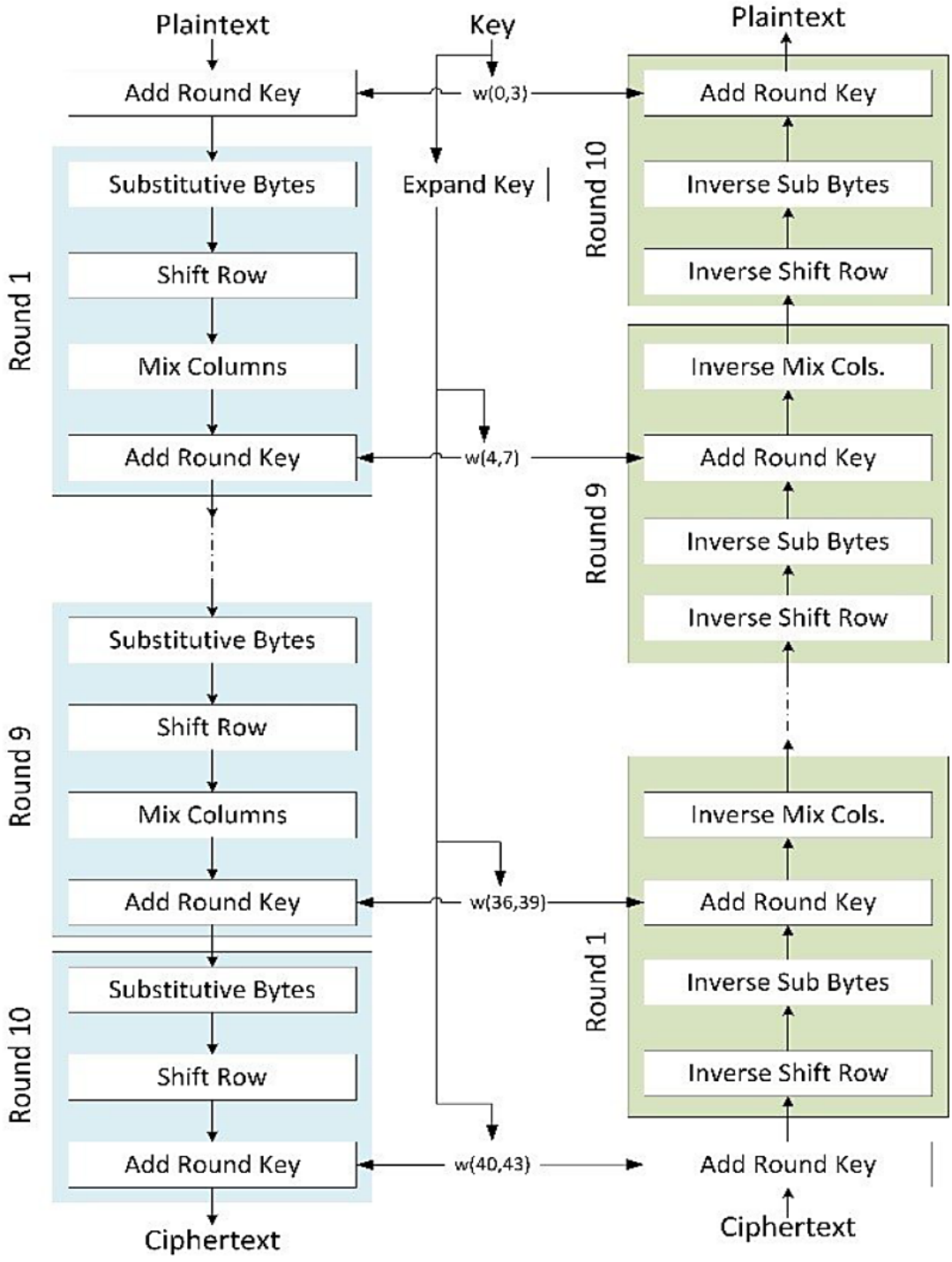


Figure 2.19: Block Diagram of 10 rounds of AES – 128 [127].

The Advanced Encryption Standard (AES) is known for its computational efficiency relative to other encryption algorithms, contributing to its robust

security attributes. This swiftness in processing renders unauthorized access or hacking attempts on the encrypted data particularly challenging. However, the deployment and execution of AES are not without complexities. The algorithm's architecture involves an extensive utilization of intricate algebraic structures. This complexity necessitates careful consideration and specialized expertise in software implementation, which may present challenges in specific contexts. The balance between speed and implementation difficulty underscores the nuanced design of AES and has implications for its applicability across various domains and security requirements [132].

C. Rivest, Shamir, and Adelman (RSA) Algorithm

The RSA algorithm, renowned as one of the most prevalent public essential cryptography methods that operates on the principle of two distinct keys [133]. In this scheme, the sender's public key encrypts the data, while a corresponding private key is used for decryption. This versatile algorithm relies on a prime factorization and leverages big prime integer numbers to enhance it's security. It finds extensive application across various domains, including email encryption and electronic document authentication [132].

In the RSA approach, the sender initiates the encryption process, which utilizes the recipient's public key and a specified encryption algorithm chosen by the recipient. The recipient, in turn, provides only the data encryption key and the corresponding public key. The public key can be used exclusively for encryption without the capability for decryption. Conversely, decryption is performed solely with the private key, which is retained confidentially by the recipient. The method for generating these paired keys in the RSA system adheres to a specific procedure [134]. Here two random large prime numbers, p and q, are assigned and calculate as follows[132]:

$n = p * q$ ---------- (2.1)

1- Compute the golden ratio of n:

$\varphi(n) = (p - 1)(q - 1)$ ---------- (2.2)

2- Select an integer e such that its greatest common factor of

$\varphi(n),e)=1$ ---------- (2.3)

And $1< e < \phi(n)$ ---------- (2.4)

3- Calculate d:

$d = e^{-1} \, mod \, (\varphi(n))$ ---------- (2.5)

4- The public key is determine from *(e, n)* and the private key is determine from *(d, n);*

The cipher text is created by using the public key on plaintext P on the transmitter side.

$C = M^e mod \, n$ ----------(2.6)

The plaintext is found by using the private key on the cipher text at the recipient side.

$M = C^d mod \, n$ ----------(2.7)

Figure 2.20 depicts an explanation block diagram of the RSA algorithm's with general component.

To make it impossible for hackers and crackers to access the information, RSA offers a safe, secure, and secured transfer of data. However, using huge data slows down the procedure and requires more time from RSA [132].

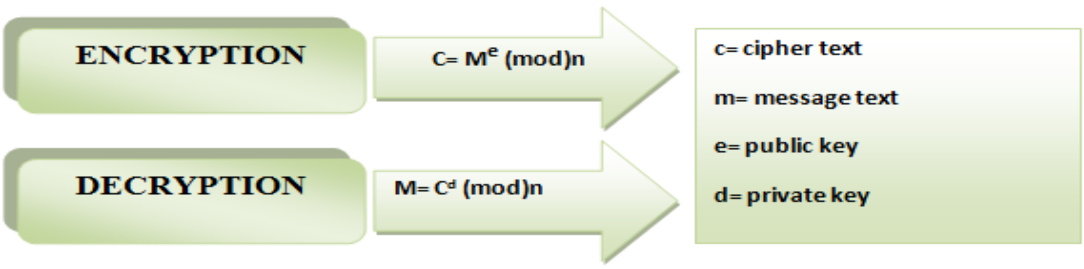


Figure. 2.20: RSA Block diagram [135].

D. Secure Hash Function 256 (SHA256) Algorithm

The term hash function refers to a function that compresses a string of arbitrary input to a fixed-length string. Cryptographic Hash functions are one of the most essential tools in cryptography. They are used to achieve several security goals like authenticity, digital signatures, pseudo number generation, steganography, and time stamping [136]. One example of a hash function is SHA256, developed by the National Institute of Standards and Technology (NIST). Digital certificates and data integrity employ the cryptographic hash function known as the SHA256 algorithm. It outputs a 256-bit message digest from an input of a message with a random length of less than 264 bits. Due to the enormous rise in data being processed daily globally and locally by data networks [137].

In the SHA256 algorithm, a message of any arbitrary length less than 264 bits is taken as an input and after hashing, produces an output of a 256-bit message digest [138].

To achieve this, stated the steps as follows [137]:

1. The message is first of all filled such that its length is congruent to 448 mod 512. This is known as padding. This involves adding a single 1 bit to the end of the message and the extra zeros so that the length equals 448 mod 512.

2. To make the message length precisely a multiple of 512 bits, the result is appended with a 64-bit representation of the message "s length.

3. The next step is to parse the padded message into N different 512-bit blocks of messages, namely $M^{(1)}$, $M^{(2)}$, $M^{(3)}$,…, $M^{(N)}$. This can be achieved by appending a 64-bit block.

4. An initial hash value, $H^{(0)}$ is set with eight 32-bit words. This must be in a hexadecimal form.

5. The message schedule is then prepared and labelled as $W_0, W_1, W_2,\ldots, W_{63}$. This involves a message schedule of sixty-four 32-bit words.

The steps of SHA256 algorithm are[137] :

$$W_t = f(x)$$

$$= \begin{cases} M_t^{(t)} & 0 \le t \le 15 \\ \sigma_1^{256}(W_{i-2}) + W_{i-7} + \sigma_0^{256}(W_{i-15}) + W_{i-16} & 16 \le t \le 63 \end{cases}$$

$$Where:$$

$$\sigma_1^{256}(W_{i-2}) = ((W_{i-2})ROTR17) \oplus ((W_{i-2})ROTR19) \oplus ((W_{i-2})SHR10)$$

$$\sigma_0^{256}(W_{i-15}) = ((W_{i-15})ROTR7) \oplus ((W_{i-15})ROTR18) \oplus ((W_{i-15})SHR3)$$

a. The eight working variables A, B, C, D, E, G, and H are initialized with the $(i-1)^{th}$ hash value.

$For\ t = 0\ to\ t = 63$:

$T_1 = H + \sum_1^{(256)}(E) + Ch(E,F,G) + k_1^{(256)} + W_1$

$T_2 = \sum_0^{(256)}(A) + Mag(A,B,C)$

$H = G$

$G = F$

$F = E$

$E = d + T_1$

$D = C$

$C = B$

$B = A$

$A = T_1 + T_2$

$Where$:

$$\sum_1^{(256)}(E) = (E\ ROTR\ 6) \oplus (E\ ROTR\ 11) \oplus (E\ ROTR\ 25)$$

$$\sum_{0}^{(256)}(A) = (A\ ROTR\ 2)\oplus(A\ ROTR\ 13)\oplus(A\ ROTR\ 22)$$

$$Ch(E,F,G) = (E \wedge F)\oplus(\sim E \wedge G)$$

$$Mag(A,B,C) = (A \wedge B)\oplus(A \wedge C)\oplus(B \wedge C)$$

b. The resulting hash function, after repeating all the steps a total of N times will yield:

$$H_0^N \| H_1^N \| H_2^N \| AH_3^N \| H_4^N \| H_5^N \| H_6^N \| H_7^N \|$$

Chapter Three

Proposed Smart Port Gate

3.1. Introduction

International maritime trade has expanded due to the low cost of maritime transport. In order to boost marine trade and attract foreign investment, most countries today are competing to turn their seaports into "smart" ports. The smart gate is a piece of essential equipment for modern "smart" ports. Faster product flow is the key to increase profits and reduced opportunities for human error.

This chapter presents the proposed system design and implementation of a "smart gate" that uses various authentication methods, including radio frequency identification, fingerprint sensors, and an automatic license plate recognition system. The use of computational clouds accomplishes data storage and processing. This is an example of an application of the Internet of Things (IoTs), in which the outcomes of these methods are compared to information saved in a cloud database. The reliability and security of the port and the city as a whole have been enhanced by this gate.

In this chapter there are two ways to represent the system. The first is to simulate the system by MATLAB. The simulations include the use of algorithms to process fingerprint images and license plate images to check if the results match the database to ensure more security. Hybrid security algorithm is also introduced in this chapter. The second method is to design a hardware system to test it in practice and match its work with the work of the simulation system. The critical stage in this message is the encoding and description of the information during the comparison stage with the database by sending it.

3.2. The Proposed System

The smart gate control system's design depends on using a set of devices and sensors included in the Internet of Things (IoT) system based on the services provided by the cloud computing model. The Internet of Things and cloud computing

allows users to control the gate via the Internet remotely. Figure (3.1) is a block diagram of the automated gate opening system where all components are connected to a personal computer, which will receive the data sent by the RFID reader, ultrasonic sensor, and camera and exchange the data with a cloud platform to give the respected result to open the gate or not. When the vehicle arrives near the port's exit gate, it will open when three conditions are satisfied: an identified container by RFID tag, an authorized driver by fingerprint, and a valid vehicle by plate number.

The RFID reader reads the data from the RFID tag/card installed next to the container and sends it to the PC using the Transmission Control Protocol TCP protocol. The ultrasonic sensor sends a signal when the vehicle arrives, and the fingerprint device starts receiving the driver's fingerprint. Fingerprints will be obtained using a microcontroller (ESP8266+UNO) and an optical fingerprint sensor. The camera takes a picture of the license plate after making the fingerprint (to ensure the vehicle is stopped for image quality). The PC sends the image to the ALPR cloud. This website analyses that image, knows the vehicle's license plate number, and then returns it to the PC. After the PC obtains the required information (the driver's fingerprint ID, the RFID ID and the vehicle numbers), it sends them to the cloud to make a decision about opening the gate after comparing it with the data stored in the database and recording this process in the database.

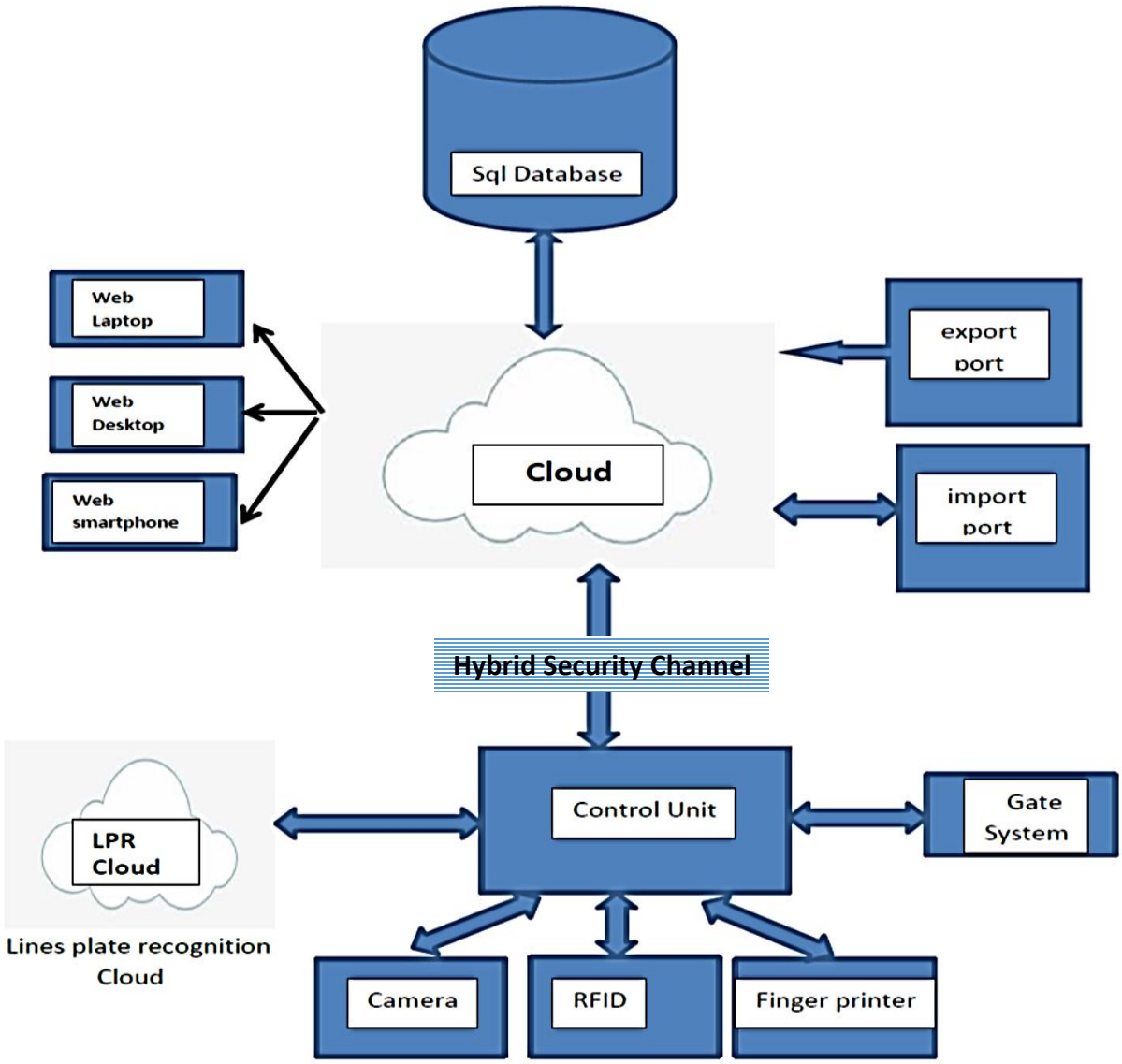


Figure 3.1: Block diagram of the proposed system of smart port gate.

The database was established in two stages; the first stage was done by the exporting port and included the ID of the RFID card and other information about the goods, such as the country of origin, the type of goods, the date of export, container line, ship agent, the degree of danger of the goods, weight, container number, and the name and address of the customer, etc. The second stage occurs at the importing port, where other information is added, such as the date of arrival, the number of

financial fees, the vehicle plate number, the driver's name, fingerprint, and other information.

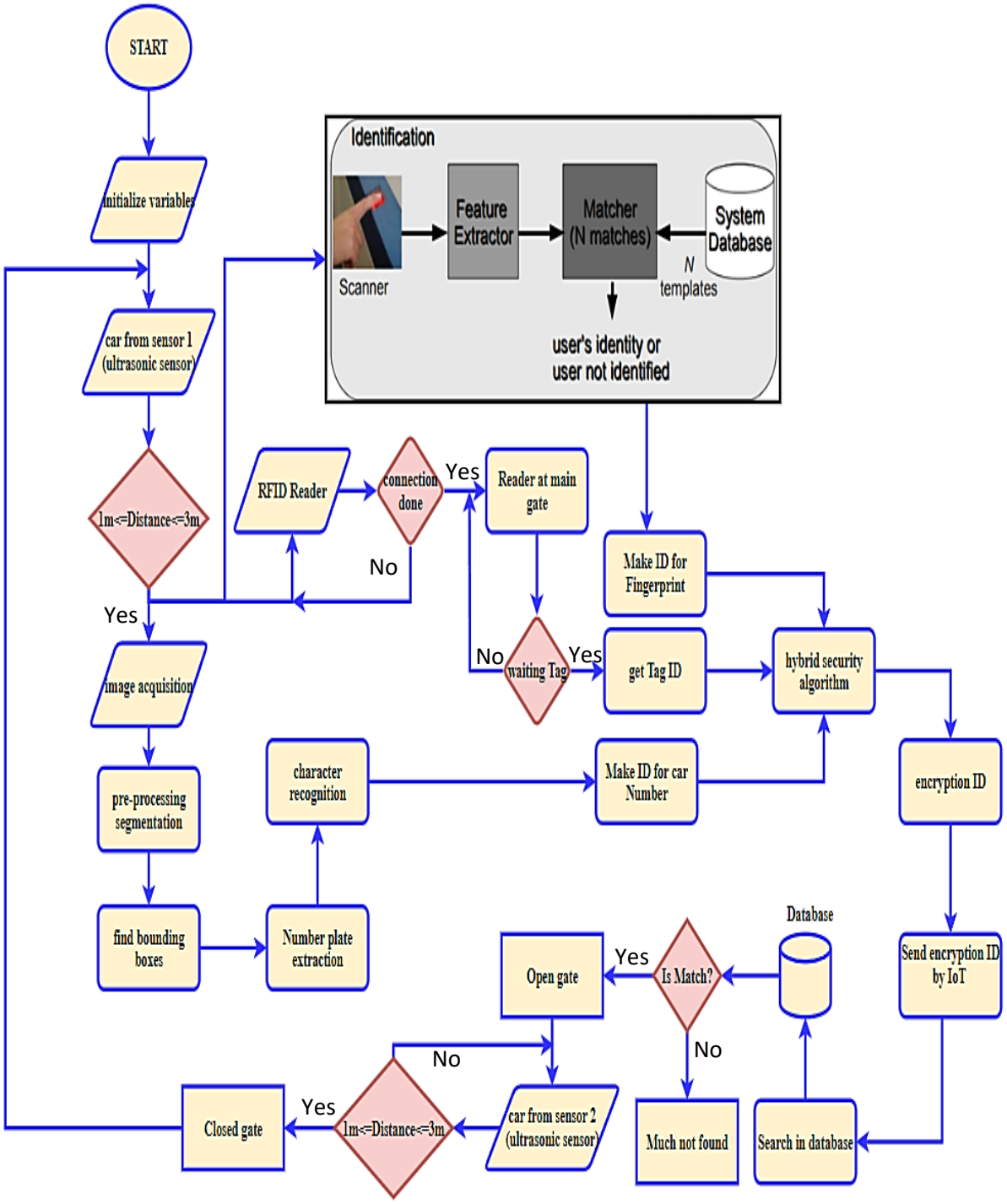


Figure 3.2: Flowchart of the proposed system of smart port gate.

The proposed system export full report includes all information in the database in addition to the departure time of the vehicle. The flowchart in Figure (3.2) shows a

big picture of all cases that lead to opening the gate, saving the reports, and dealing with the cloud. It is clear from the flowchart that there is an additional method to open the gate: using the master card. This scenario can be used in some situations, like with visitors.

3.3. RFID reader steps and algorithm

In this thesis, the three crucial stages are the ID of RFID that send with another two IDs for fingerprinting and the license car number to open the gate of the port. This processing involved when using RFID to match information by ID saved in a database for opening the gate of a port:

RFID Tagging: Each authorized vehicle or object that needs access to the port is equipped with an RFID tag. The RFID tag contains a unique identifier (ID) associated with the vehicle or object in the database.

RFID Reader Placement: RFID readers are installed at the entrance gate of the port. These readers are positioned in a way that allows them to detect the RFID tags of approaching vehicles or objects.

Vehicle/Object Detection: As an RFID-tagged vehicle or object approaches the entrance gate, the RFID reader within the gate's vicinity emits radio waves to power the RFID tag.

RFID Tag Response: The powered RFID tag responds to the reader by transmitting its unique ID back to the reader using radio frequency signals.

Data Capture: The RFID reader captures the transmitted ID from the RFID tag. The reader then sends this information to a computer or a central database system for processing.

Database Lookup: The computer or central database system receives the ID from the RFID reader and performs a lookup in the database. The database contains records of authorized vehicles or objects and their corresponding information, such as owner details, access permissions, or other relevant data.

Authentication and Access Decision: The system matches the received ID with the stored IDs in the database. The system determines whether the vehicle or object can access the port based on the database lookup results.

After gating feedback from the database during the cloud using IoT technology, all three ID are matching the system, sending a signal to the Arduino to open the gate of the port based on the following steps:

Step 1: RFID Identification

The RFID reader scans the RFID tag attached to a vehicle as it approaches the gate. The RFID reader captures the unique ID (RFID ID) embedded in the RFID tag.

Step 2: Fingerprinting

The system prompts the driver/passenger to place their finger(s) on a fingerprint scanner. The fingerprint scanner captures the fingerprint(s) and generates a unique fingerprint ID.

Step 3: License Plate Recognition

A camera installed near the gate captures an image of the vehicle's license plate. The license plate recognition (LPR) system extracts the license plate number from the image.

Step 4: Database Lookup

The system performs a database lookup using the captured RFID ID, fingerprint ID, and license plate number. The database contains stored information related to authorized vehicles, including their RFID ID, fingerprint ID, and license plate number.

Step 5: Information Matching

The system compares the captured RFID ID, fingerprint ID, and license plate number with the corresponding records in the database. If all three IDs match the database records, the system proceeds to the next step. If any IDs do not match or are not found in the database, the system denies access and alerts the appropriate personnel.

Step 6: Gate Control

If the ID is successfully matched and the vehicle or object is authorized, the system sends a signal to control the gate. The gate opens, allowing the authorized vehicle or object to enter the port.

Step 7: Logging and Recording

The system logs the access event, recording the date, time, and other relevant information such as the ID, vehicle/object details, and access status. This log serves as an audit trail for future reference.

3.4. Fingerprint matching algorithm

Algorithms for matching fingerprints may be divided into three categories: a)correlation-based, b)minutiae-based, and c)non-minutiae feature-based. Superimposing two fingerprint pictures to calculate pixel-wise correlation for various displacements and rotations is the basis of correlation-based matching, as shown in Figure (3.4).

To facilitate alignment and get matched minutiae sets from both fingerprints, matching by minutia-based usage extracted minutiae from two images. Compared to other features levels of fingerprint, minutiae point sets achieve a better level of uniqueness while remaining practically applicable, and this method is dependent in this thesis to verify and match the set fingerprint with the database.

Figure 3.4: The FVC2002 database has eight copies of the same fingerprint, each with its unique region overlap, offset, orientation, and image quality [139].

3.4.1. Proposed fingerprint matching algorithm

A. Minutiae extraction

Minutiae extraction is a fundamental step in fingerprint-matching algorithms. It involves the identification and extraction of a the unique characteristics or minutiae points from a fingerprint image, which are then used to compare and match fingerprints. The similarity score measures two fingerprints' similarity based on their extracted minutiae.

Here is an overview of the process of minutiae extraction and fingerprint matching:

Preprocessing: The fingerprint image is first preprocessed to enhance its quality and remove noise or artifacts. This may involve noise reduction, image enhancement, and ridge orientation estimation.

Ridge Segmentation: The ridges and valleys in the fingerprint image are segmented to separate the foreground (ridge) from the background. This step helps in isolating the fingerprint ridges for further analysis.

Minutiae Detection: In this step, the individual minutiae points are detected and extracted from the segmented fingerprint ridges. Minutiae are specific features that include ridge endings (where a ridge terminates) and ridge bifurcations (where a ridge splits into two branches). Other types of minutiae, such as ridge crossings and dots, may also be considered.

Minutiae Representation: The extracted minutiae points are represented in a standardized format to facilitate comparison and matching. Each minutia is typically described by its location coordinates (x, y) and orientation angle.

Similarity Score Calculation: A similarity score is calculated once the minutiae have been extracted and represented for both the query fingerprint (the fingerprint to be matched) and the reference fingerprint (the fingerprint in the database). Various algorithms and techniques can be used for comparing and measuring the similarity between the sets of minutiae.

One common approach is to compute a similarity score based on the number and spatial arrangement of matching minutiae points. The higher the similarity score, the more corresponding minutiae pairs are found between the query and reference fingerprints. The scoring algorithm may also consider other factors, such as the quality of minutiae (reliability of detection and representation) and the use of additional information (e.g., ridge flow, ridge shape).

Thresholding: The similarity score is then compared to a predefined threshold value. If the score exceeds the threshold, the fingerprints are considered a match. Otherwise, they are considered non-matching. The final processing of proposed is depicted in figure (3.5)

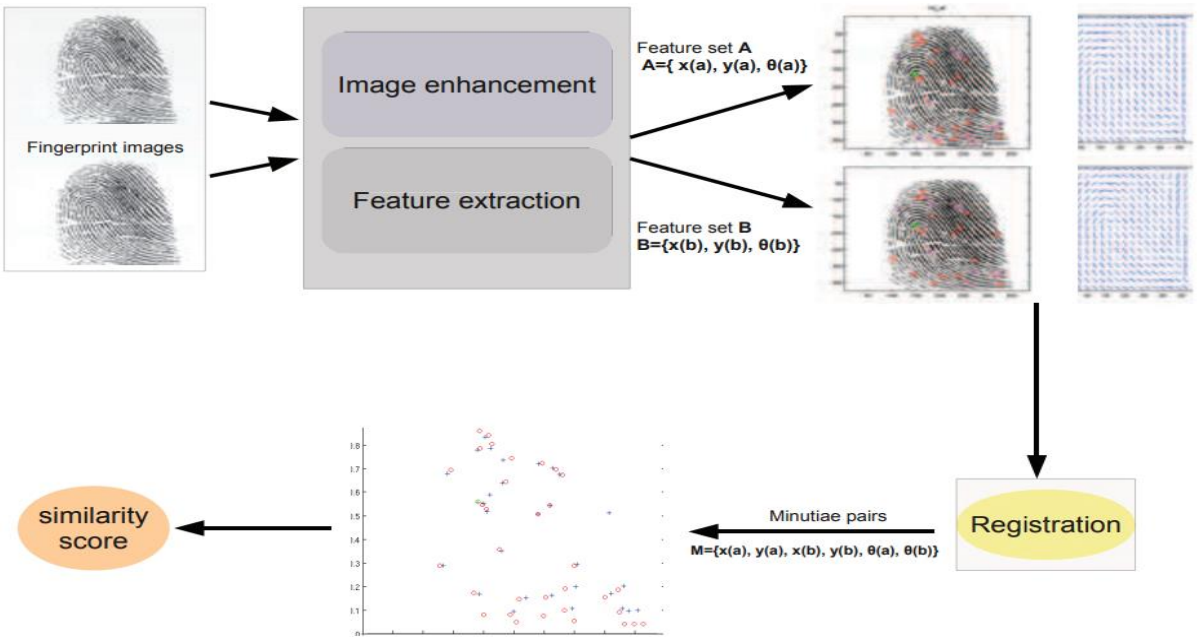


Figure 3.5. Proposed strategies for matching fingerprints based on minutiae processing.

It is important to note that minutiae-based fingerprint matching is just one approach among several fingerprint recognition techniques. Other methods, such as ridge-based and correlation-based matching, may be combined as alternatives to minutiae-based approaches. Deep learning and neural network advancements have also led to more sophisticated and accurate fingerprint-matching systems.

The proposed algorithm accepts a single fingerprint as input and checks it against all the others in the database. The fingerprint owner's ID will be shown if a match is found, as shown in Figure (3.6). We can also enroll a new fingerprint into the system. Two fingerprints are used to collect and preserve detailed information about the fingerprints' owners.

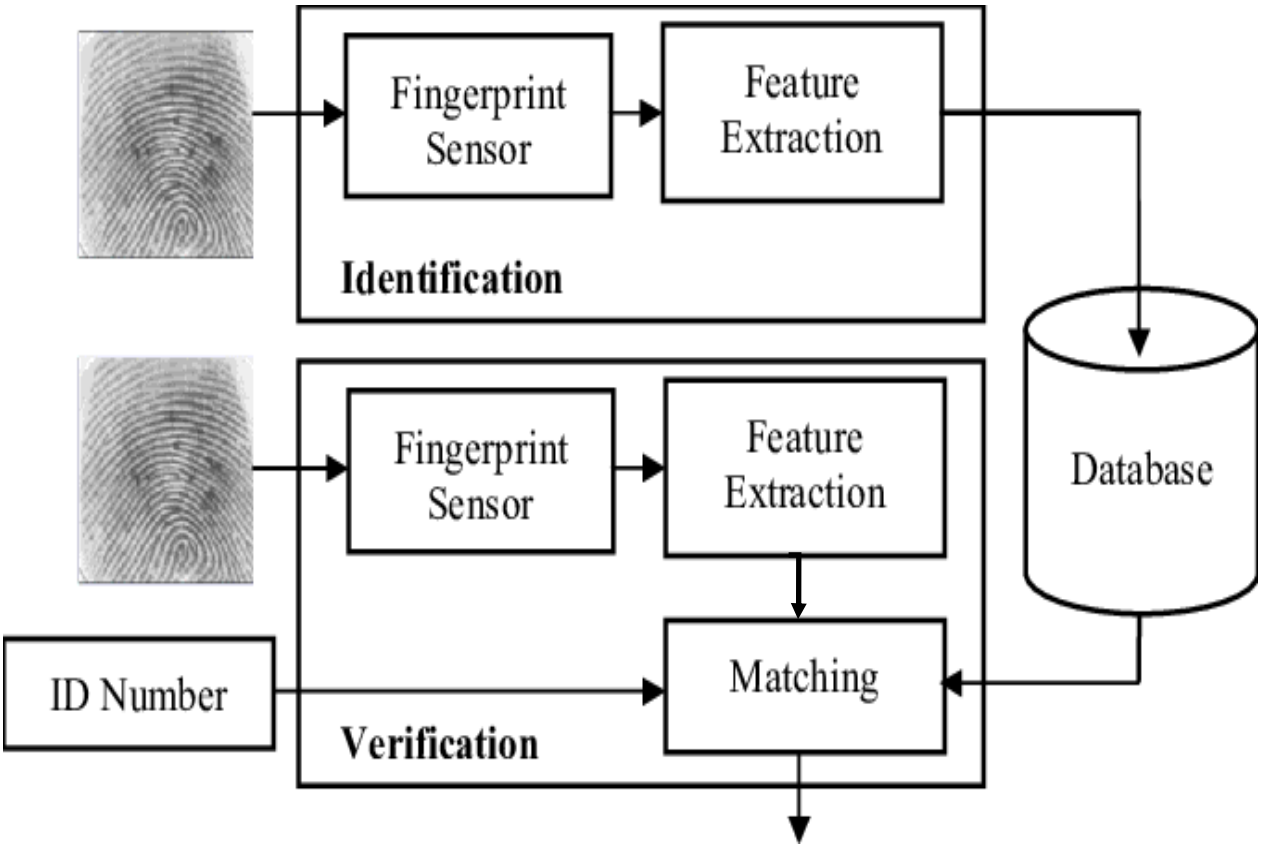


Figure 3.6: proposed diagram of verification of fingerprint.

3.5. Proposed Vehicle License Plate Detector

One of the most crucial parts of identifying the vehicle is reading its license plate. As the number of vehicles rises, verifying that they are correctly licensed is becoming increasingly important. This work presents an Automatic Number Plate Recognition algorithm based on Optical Character Recognition (OCR) with a template matching technique. The proposed technique has three primary components: license plate detection, image segmentation, and recognition. The

MATLAB implementation of the proposed system is evaluated using real-world photos of license plates to gauge its efficacy.

OCR technology allows computers to recognize and extract text from images or scanned documents. On the other hand, template matching is a technique where a template or pattern is compared to an image to find instances that closely match the template.

In the context of a car license plate detector using OCR and template matching, the process typically involves the following steps:

License Plate Localization: The first step is to locate the region of the image where the license plate is present. Various techniques for license plate localization can be used, such as edge detection, morphological operations, or machine learning-based methods.

Character Segmentation: Once the license plate region is identified, the characters on the license plate need to be segmented. This involves separating individual characters from each other to enable further processing.

Template Creation: For template matching, we must create a template representing each character or digit. These templates should be generated from training images containing different variations of license plate characters.

Template Matching: In this step, the generated templates are compared with the segmented characters to find the closest match. The comparison can be based on techniques such as cross-correlation, Euclidean distance, or correlation coefficient.

Character Recognition: After template matching, the recognized characters must be decoded to obtain the license plate number. This can be achieved using an algorithm that matches the recognized patterns with known characters and converts them into text.

The steps mentioned are shown in Figure (3.7), and they are used for detecting the license car number based on OCR with a template matching and making a unique ID

for this car and comparing with the database ID and decision is true or false to help open the gate port.

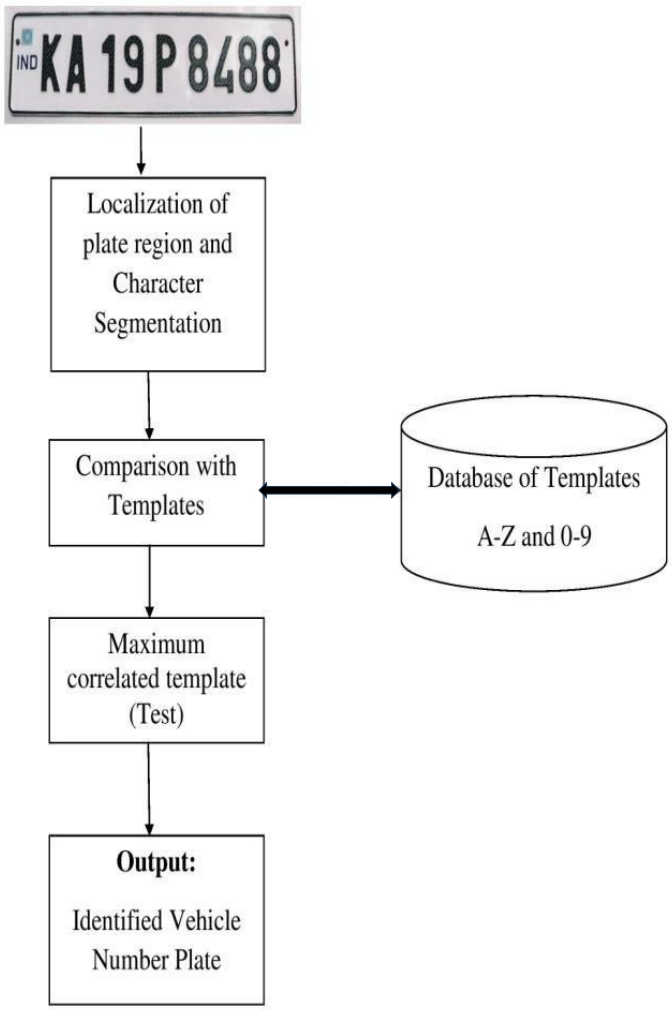


Figure 3.7: Block diagram of proposed license plate car detector.

3.6. Proposed Security Algorithm

The proposed system is based on the design of the intelligent gate control system depends on the use of a set of devices and sensors included in the Internet of Things (IoT) system based on the services provided by the cloud computing model. The Internet of Things and cloud computing allows users to control the gate via the Internet remotely.

All components are connected to a personal computer, which will receive the data sent by the RFID reader, ultrasonic sensor, and camera and exchange the data with a cloud platform to give the respected result to open the gate or not when the vehicle arrives near the port's exit gate, pc will send the gathered information (which is an identified container by RFID tag, an authorized driver by fingerprint, and a valid vehicle by the plate number) to the cloud in order to get the decision about opening the gate after comparing them with stored data in the database, as well as register this operation in the database. It will open when three conditions are satisfied. Otherwise, the gate stays closed.

To ensure the security of information exchange with the cloud database via the Internet, a hybrid security system of symmetrical algorithms AES-SHA256, DES-SHA256, and A Symmetric RSA-SHA256 was proposed. The cloud is decrypted, and the plaintext values are matched to the stored values.

3.6.1. Proposed AES Procedure

The Advanced Encryption Standard, or AES, is a symmetric block cipher. It is implemented in software and hardware to encrypt sensitive data. AES has three key sizes: 128, 192, or 256 bits. In this work, a 128-bit key is used to extract the ciphertext. The general steps for implementing AES to encrypt the proposed text are :

1- Encrypt the given text and give the byte array.
2- The byte array is converted to the corresponding encrypted text.
3- Adding password or encryption key generated by "salt" random generator.
   The salt is used as another input of the essential derivation function. It prevents brute force attacks using "rainbow tables," where keys are pre-computed for specific passwords. Because of the salt, the attacker cannot use pre-computed values, as he cannot generate one for each salt. The salt should typically be 16 bytes (128 bits) or longer. It also ensures that identical passwords do not have

the same derivation results. The AES key will be identical to the generated secret.

4- The result is returned as "The encrypted text."

While the general steps for implementing AES to decrypt the cipher text are:

1- Checks if a string (Keywords) is founded.

2- Decrypts the given text by the public class for decryption known below require two parameters. The first one is represented by (encryption text) or the output (cipher text), and the second by a key generator (same salt key)

3- Then convert the value of cipher text with specific procedures to convert it and returns it to the original text.

4- The result returns the decrypted text (plaintext). Figure (3.9) illustrates the AES block diagram implemented for the proposed system.

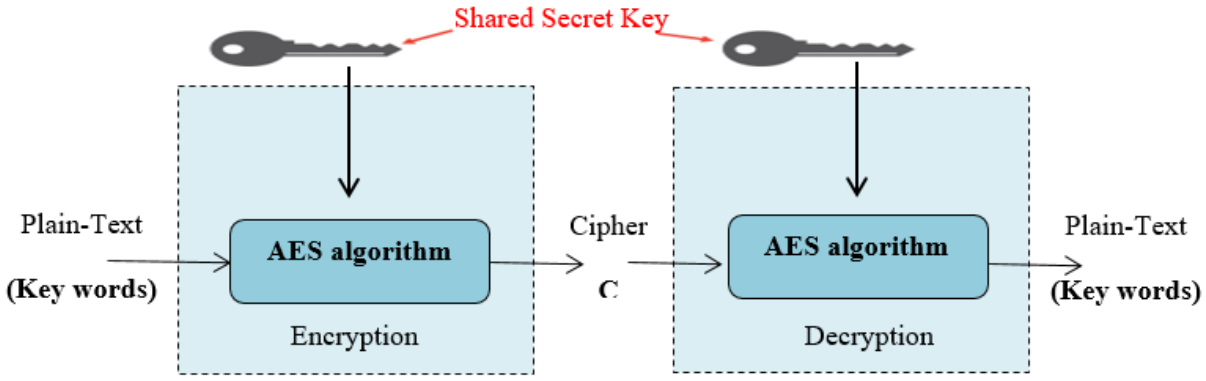


Figure 3.9: AES Block Diagram for the proposed system.

3.6.2. Proposed RSA Proceture

One of the most used and safe algorithms for asymmetric encryption is Rivest-Shamir-Adleman (RSA). The algorithm runs as follows for the encryption key (e,n):

- Large messages can be divided into several blocks. The message is represented in each block as an integer between 0 and (n-1) in size.
- To get an encrypted text message (C), raising it to the e^{th} power modulo N.

- To recover the original text of the message from the C ciphertext, raise it to another power d modulo n
  - Public Key (e, N) which is made public and used for encryption.
  - Private Key (d, N) for decryption is also known as a secret key. The user keeps the decryption key (d, N) private.

Figure (3.10) explains the block diagram with the general component of the RSA algorithm.

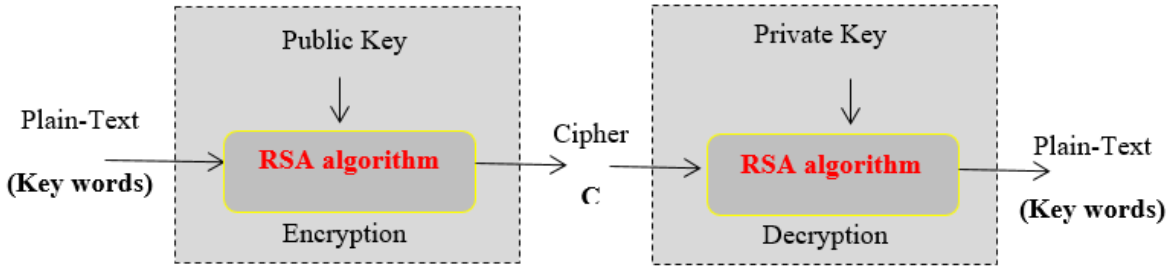


Figure 3.10: RSA Block Diagram for the proposed system.

The difficulty of factoring the huge composite number n into its prime components (p) and (q) is the foundation for RSA's security. If someone can factor n, they can compute the private key and decrypt the ciphertext, which is why the security of RSA relies on the hardness of this factorization problem.

3.6.3. Proposed DES Procedure

In DES 64 bits of plaintext are entered to create 64 bits of ciphertext. DES uses the same key in the encryption and decryption process. The two fundamental characteristics of cryptography are the foundation of DES: substitution (confusion) and transposition (diffusion). DES consists of 16 rounds. The steps of substitution and transposition are carried out in each round. Let's now talk about the DES fundamental steps.

- In the initial stage, the 64-bit plaintext block is rearranged by the initial permutation (IP) function.

- Then, the initial permutation (IP) generates Left Plain Text (LPT) and Right Plain Text (RPT) from the permuted block.
- Now, Each LPT and RPT pass through 16 rounds of the encryption process.
- LPT and RPT are eventually reunited, and the combined block is subjected to a Final Permutation (FP).
- This procedure yields 64-bit ciphertext as the end result.

Figure (3.11) explains the block diagram with the general component of the DES algorithm.

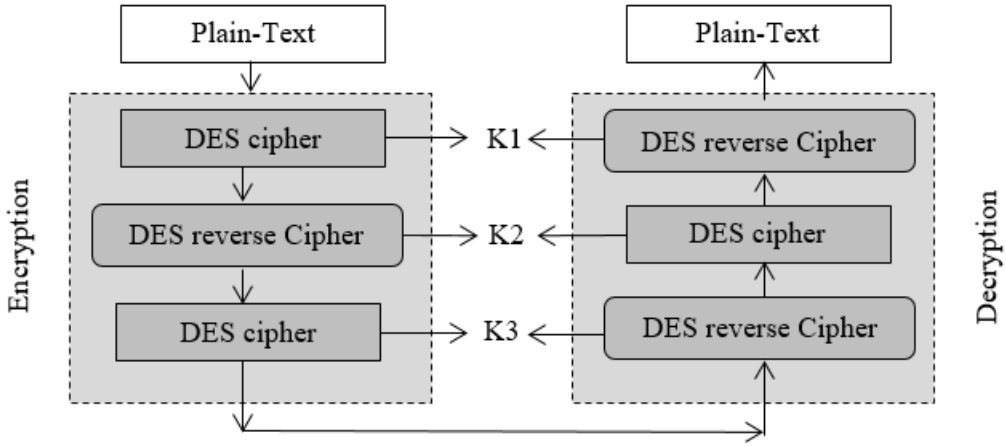


Figure 3.11: DES Block Diagram for the proposed system.

3.6.4. SHA256 algorithm

Among the numerous progressions in network security, encryption, and hashing have been the centre standards of extra security modules. The SHA 256 is a hashing algorithm commonly used in real-world applications. It is a safe hash with a size of 256 bits. Figure (3.12) shows the SHA256 algorithm block diagram within the proposed system.

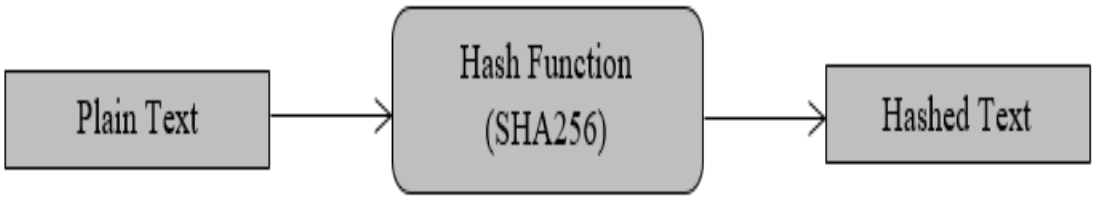


Figure 3.12: SHA256 Block Diagram for the proposed system.

3.7. Hybrid algorithms

The hybrid method of using AES, RSA, or DES, and SHA256 are depicted here to store the reads values of the smart gate . The strength of this security depends on the length and complexity of the secret phrase. If the user relies on the most widely used information as the secret phrase, the attacker can simply brute force it or use a rainbow table to crack it. To avoid this, the user must remember a long and robust secret phrase, which is challenging. The proposed system combines security algorithm (AES, RSA, or DES) modules with SHA256 to create a solid and secure password-storing strategy. Figure (3.13) shows the proposed hybrid approach.

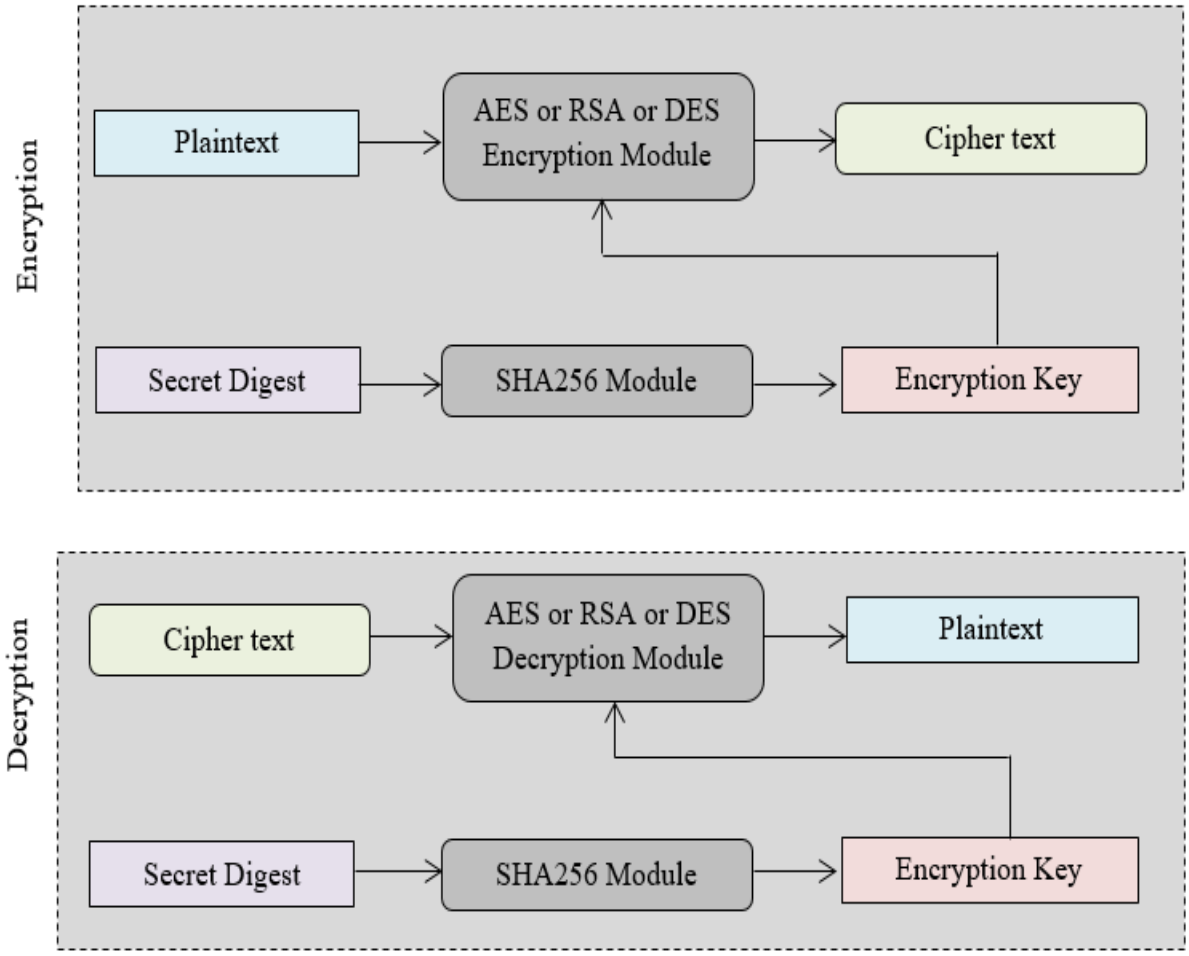


Figure 3.13: The proposed Hybrid security approach.

Besides, the proposed security hybrid system is based on the specifications of algorithms shown in Table 3.1.

Table 3.1: The used algorithm specifications

Algorithm type	DES	AES	RSA	SHA256
Key size (bits)	56	128	1024	256

3.7.1. The employment of a Hybrid security algorithm for the Smart gate system

RSA and SHA256 are both cryptographic algorithms commonly used for encryption and decryption. The hybrid encryption scheme is employed to secure the transmission and comparison of three IDs (car license plate, RFID card ID, and fingerprint ID) to open a smart port gate automation. Here is a high-level overview of how RSA and SHA256 could be used together in this scenario:

Key Generation: The system would generate an RSA key pair of public and private keys. The Public Key is encrypted, while the private Key is kept secret and used for decryption.

Encryption:

RFID Card ID,Car License Plate, and Fingerprint ID would be encrypted using RSA public key. The resulting ciphertext is then encrypted using the SHA256.

Transmission: The encrypted car license plate ID, RFID card ID, and securely transmitted fingerprint ID are sent to the cloud for processing.

Decryption:

Cloud Processing: The encrypted car license plate ID and RFID card ID are received in the cloud. First it decrypts with SHA256 and then decrypts with RSA private key. These decrypted IDs can then be compared with the database to decide to open the smart port gate automation.

3.8. Proposed Smart Gate Automation

The system can work as follows:

Barrier access control using motion sensors, license plates, RFID, and fingerprint authentication is a comprehensive approach to ensure secure and efficient access to a restricted area. Let's break down how this system would work:

Motion Sensors: Motion sensors can be installed near the barrier to detect the presence of a vehicle approaching. These sensors can trigger the access control process, initiating the authentication steps.

License Plate Recognition (LPR): As the vehicle comes closer to the barrier, a camera equipped with License Plate Recognition (LPR) technology captures the image of the license plate. LPR software processes the image to extract the license plate number.

RFID (Radio-Frequency Identification): Vehicles that are authorized to access the area are equipped with RFID tags. As the vehicle gets within the range of the RFID reader, the tag's unique identifier is read.

Fingerprint Authentication: The driver of the vehicle undergoes fingerprint authentication. A fingerprint reader, either integrated into the barrier system or through a separate device, scans the driver's fingerprint.

Matching with Stored Information: The collected data from the motion sensors, license plate recognition, RFID, and fingerprint reader are sent to a centralized access control system.

Access Control System: The access control system processes the incoming data and compares it with the stored information in the database. The stored information includes the authorized vehicles' license plate numbers, associated RFID tag IDs, and the fingerprints of authorized drivers.

Decision and Barrier Control: If all the collected information matches the stored data for an authorized vehicle and driver, the access control system sends a signal to open the barrier. Otherwise, the barrier remains closed, and appropriate actions (such as sending an alert) may be taken based on the security policies.

Logging and Monitoring: The access control system should log all access attempts and outcomes for security auditing and monitoring purposes. This helps in tracking any suspicious activities or attempts at unauthorized access.

Generate Reports: The access control system can generate detailed reports on access events and activities. The date and time of each access attempt, the license plate number, the RFID tag ID, the driver's fingerprint verification result, and whether access was granted or denied may be included in these reports. These reports can be helpful for security personnel and management to monitor access patterns and identify any unusual activities.

Container Tracking: The proposed system sends three emails to the customer to track the container as follows:

1. When leaving the container from the port of the country of origin.
2. When the container arrives at the port of destination.
3. When the container leaves the port towards the customer.

It's important to note that this system requires robust security measures to prevent tampering or hacking attempts. Encryption and secure communication protocols should be used to protect the data transmitted between different components of the system.

The above steps are simulated in Matlab with graphical user interface (GUI) tools for three gates.

The system has three gates, each with a set of stored IDs (car license ID, fingerprint ID, and RFID) for authorized users. When a user enters the correct combination of IDs for a specific gate, the gate opens and displays an opening animation. After a few seconds, the gate automatically closes. The system also generates a report for each successful gate opening containing relevant information about the user and their cargo.

The principle of this code is to simulate a smart gate system that can open and close gates based on the input of car license ID, fingerprint ID, and RFID ID. The code creates a graphical user interface (GUI) that allows users to interact with the gates by entering the required IDs. Each gate has an "Open" and "Close" button, and when the "Open" button is pressed, the code checks if the entered IDs match the stored IDs

for that gate. If the IDs are valid, the gate opens, and an opening animation is displayed. After a few seconds, the gate automatically closes, generating a report containing details about the gate opening. The "Close" button allows the user to close the gate if it is open manually.

The code provided is a MATLAB function named "smartGateSimulation" that simulates a smart gate system with multiple gates. The smart gate system has the following procedure:

1. It creates a Graphical User Interface (GUI) with a prominent figure window.
2. Each gate has an "Open" button and a "Close" button, allowing the user to manually open and close the gates.
3. Each gate requires the user to enter certain identification information (car license ID, fingerprint ID, and RFID) to open the gate.
4. The system has a database of stored information for each gate, including driver names, departure times, destinations, container details, and more.
5. The gate status (open or closed) is maintained using a container. Map.
6. When a gate is successfully opened, the system generates a report with relevant information and saves it to a text file.

The complete flowchart of the proposed system explained in this chapter is demonstrated in Figure (3.2).

3.9. Hardware design and installation

Implementing a smart gate port system that integrates ultrasonic sensors, an RFID reader, a car number extraction camera, and an electrical circuit with Arduino, as demonstrated in Figure (3.16) to manage gate barriers, requires careful planning and installation. The wiring connection of all sensors is depicted in Figure (3.17), and the aim of each component is demonstrated as follows:

Ultrasonic Sensors (2): For detecting the distance or presence of a vehicle before opening the gate and after accessing the gate as demonstrated in the flowchart (see Figure (3.2).

RFID Reader: To read the RFID tags.

Camera: To extract the car's license number.

Fingerprint Scanner: To authenticate the driver's fingerprint.

Arduino Board: To control the entire system, including opening and closing the barrier.

Gate Barrier: This could be a motorized mechanism controlled by the Arduino.

Relay Module: To control the barrier's motor with Various cables, resistors, and connectors for connections.

WiFi Module (ESP8266): This will enable the Arduino to connect to a WiFi network and server.

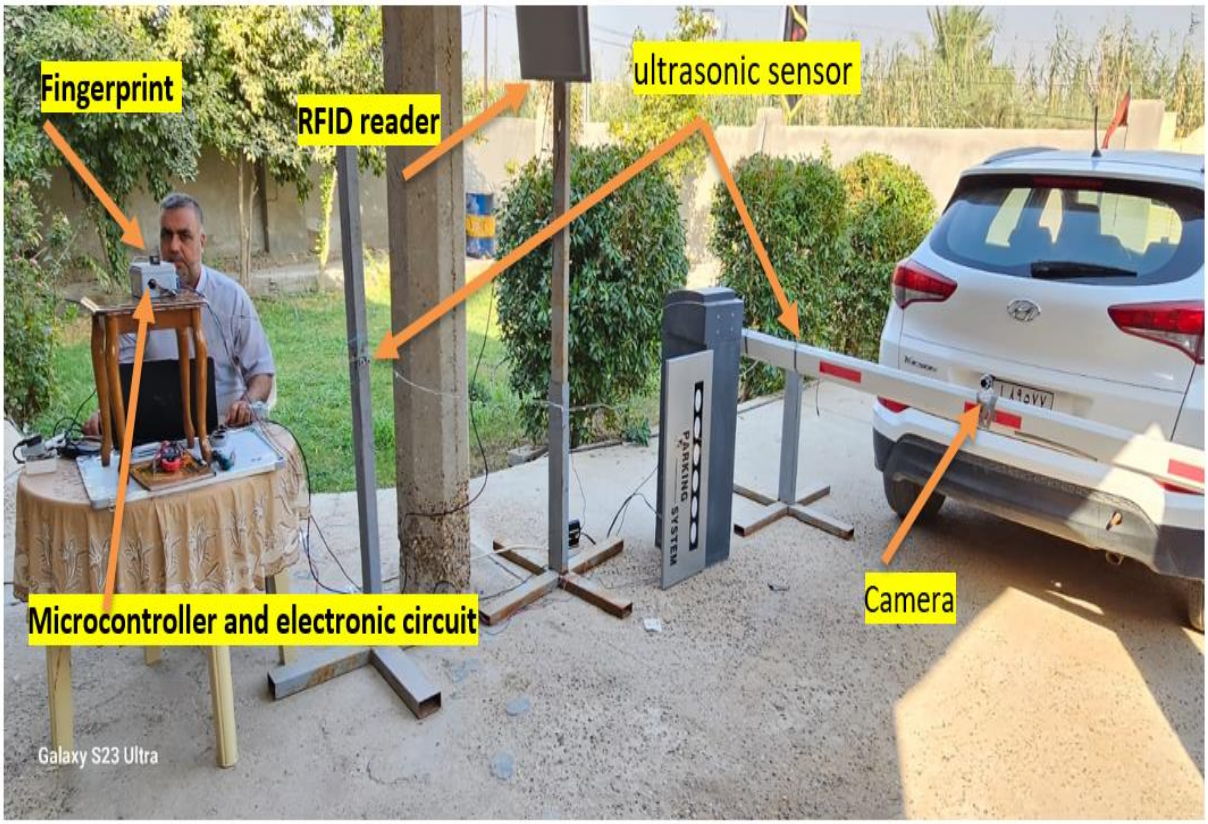


Figure 3.16: Proposed prototype system of smart gate.

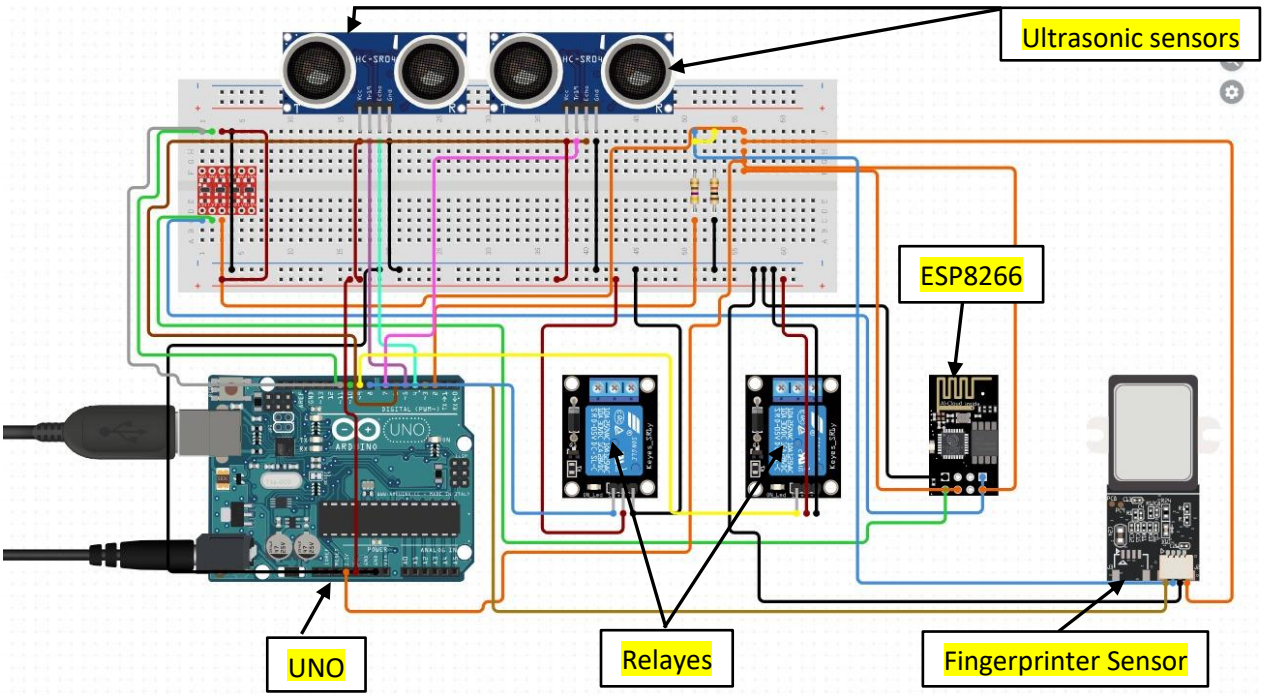


Figure 3.17: Wiring connected of sensor, microcontroller, and relay.

Set up a server that will handle the incoming data, which is used to match information, as shown in Figure (3.18. This could be on a cloud platform like AWS, Azure, or Google Cloud. The primary setting of the RFID reader with IPs is shown in Figure (3.19). In addition, the creation tag ID of RFID with the description as an example computer is shown in Figure (3.20). This Figure likely illustrates creating or assigning an identification number (Tag ID) to an RFID (Radio-Frequency Identification) tag. RFID tags are used to store data that an RFID reader can retrieve. In a smart gate system, this tag might be attached to a vehicle or carried by a driver to provide secure access to a location.

Figure (3.21) describes associating a driver's car with a fingerprint and an ID within the system. It might show a graphical user interface (GUI) where administrators can input a driver's details, their car's information, and a scanned fingerprint. This data could be used for authentication, allowing only authorized individuals to access a secured area. The Figure might detail how the system captures, enters, and stores this information.

The extracted tag ID by the RFID reader from the car that was put in the car is shown in Figure (3.22), and it can be observed is attached to the sore tag. This Figure may depict the process of an RFID reader scanning and extracting the Tag ID from an RFID tag associated with a car. In a smart gate system, this reading process would likely be part of an authentication procedure, where the RFID reader verifies that the car has the correct Tag ID before granting access.

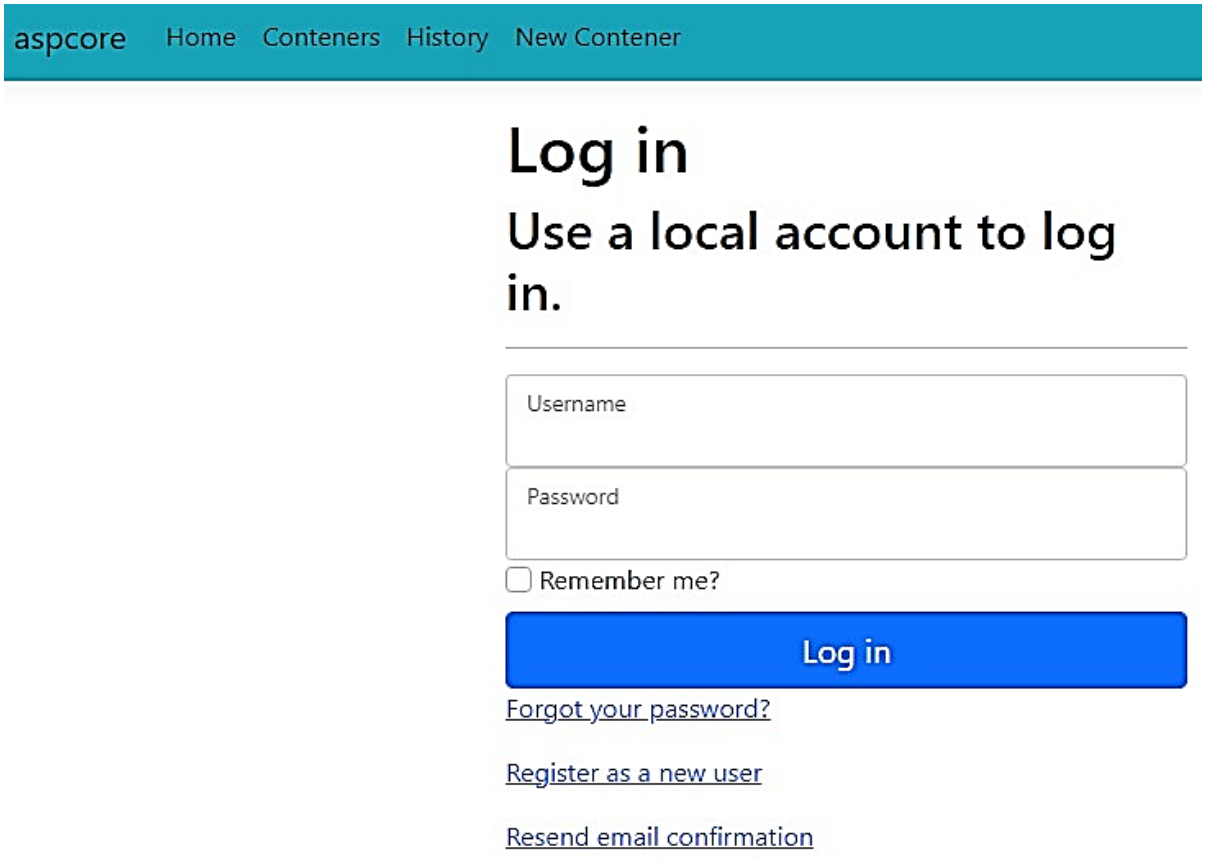


Figure 3.18: Log-in and general home icons of a server.

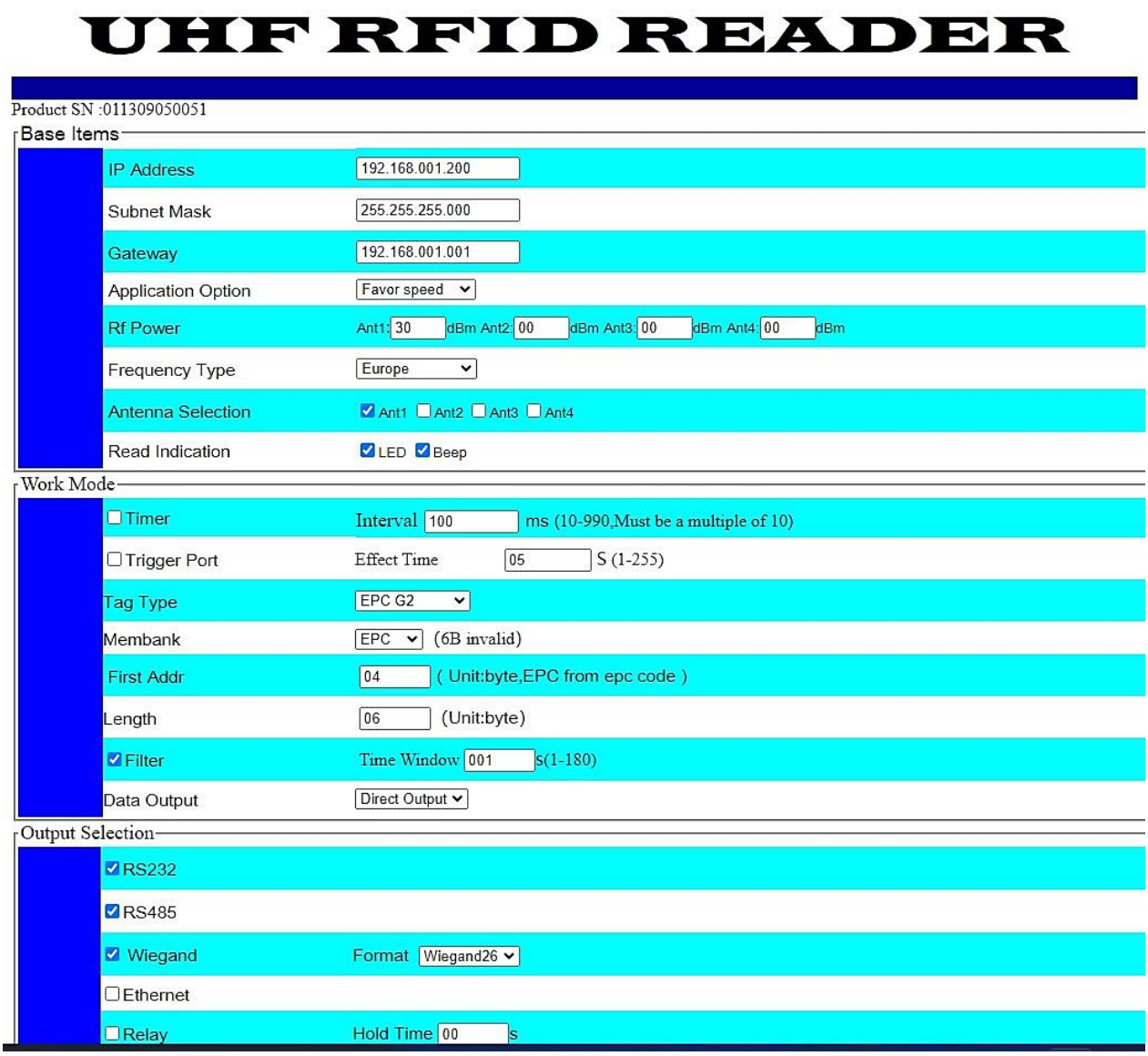


Figure 3.19: UHF RFID reader setting.

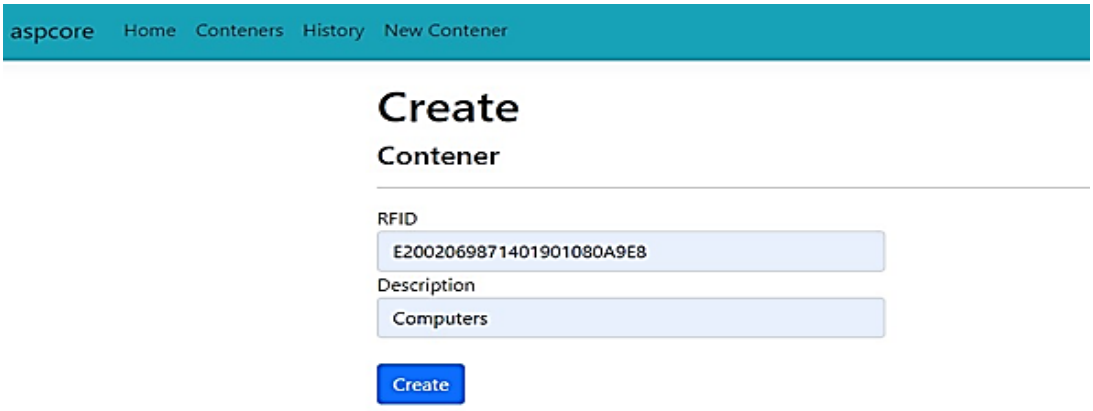


Figure 3.20: Create Tag ID of RFID.

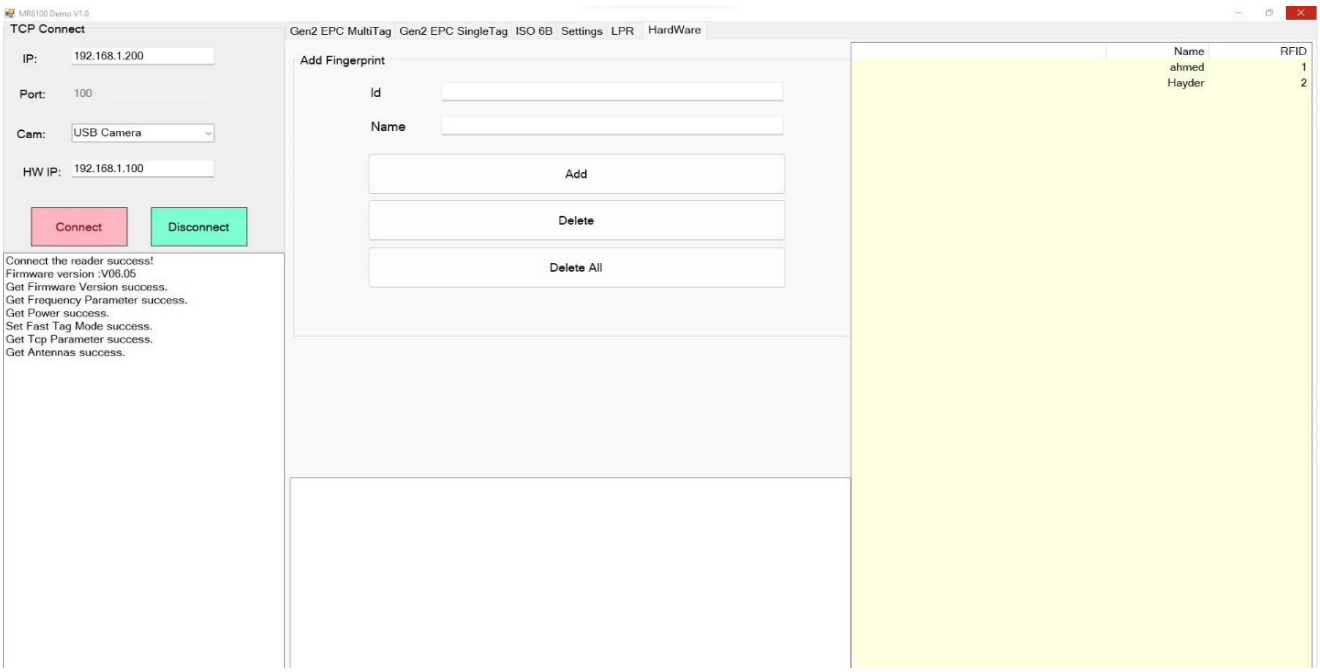


Figure 3.21: Adding the ID and name of the driver's car of the fingerprint.

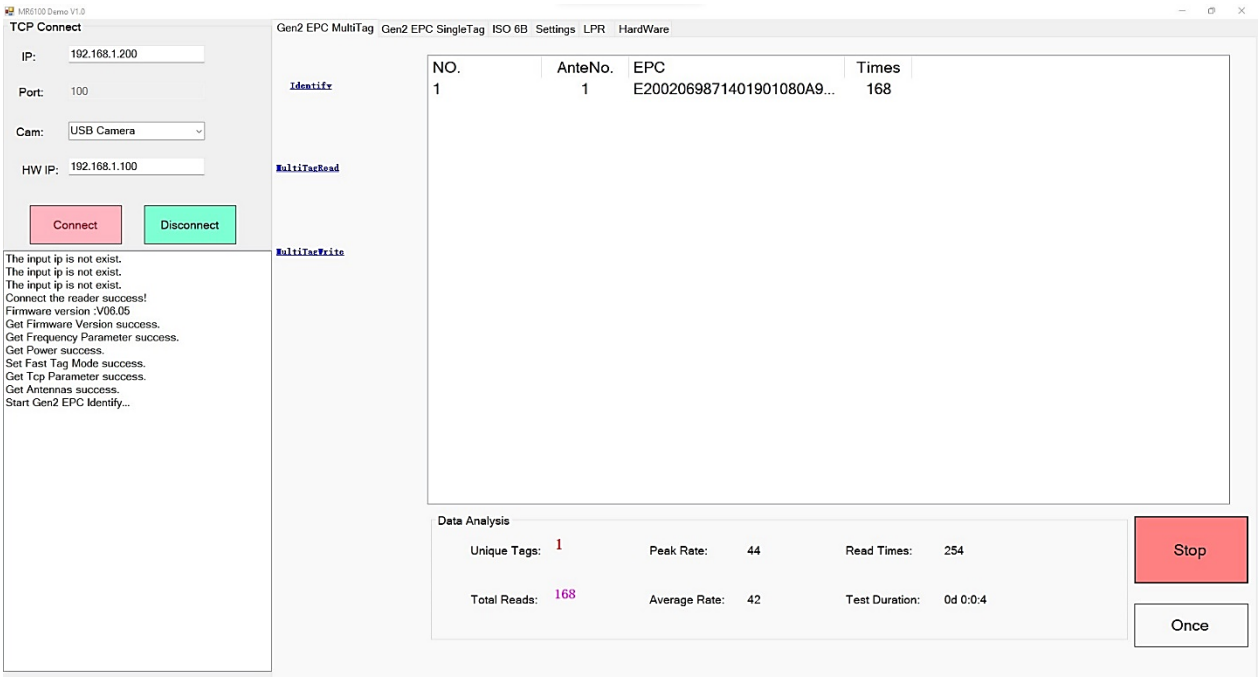


Figure 3.22: Extracting tag ID from a car by RFID reader.

3.10. Summary

The proposed smart gate system utilizes a hybrid security algorithm consisting of RSA and SHA256 encryption to secure the transmission and comparison of

identification information (car license plate, RFID card ID, and fingerprint ID) for accessing a smart port gate automation.

In the smart gate automation process, motion sensors detect approaching vehicles, the fingerprint device takes the vehicle's driver's fingerprint, and then the License Plate Recognition System (LPR) captures the license plate numbers. RFID tags are used for the container that is authorized to exit the port. All collected data is sent to a centralized access control system.

The access control system matches the data with stored information in the database, including authorized license plate numbers, RFID tag IDs, and authorized drivers' fingerprints. If the data matches, the barrier opens; otherwise, it remains closed.

The system allows the customer to track it by sending an e-mail, where a message is sent after the completion of each stage (leaving the port of export, arriving at the port of the importer, leaving the port towards the customer). The access control system integrates with the tracking system to record the real-time entry and exit events of the container.

A MATLAB-based simulation with a Graphical User Interface (GUI) is used to demonstrate the intelligent gate system's functionality for three gates. The GUI allows users to interact with the gates by entering the required IDs for access. The gates have "Open" and "Close" buttons, and when valid IDs are entered, the gate opens, displaying an opening animation before automatically closing. A report containing relevant information about the gate opening is generated and saved to a text file.

The system has been practically designed to match the simulation results.

Overall, the proposed smart gate system aims to provide secure and efficient access control, combining various authentication methods, encryption, and container tracking to ensure the controlled movement of authorized vehicles and cargo.

Chapter Four

Results and Discussion of Simulation and Experimental Results

4.1. Introduction

This chapter contains three types of results. The first results are security test results and hybrid algorithms, with emphasis on RSA, AES, DES, SHA256, and hybrid encryption and decryption. The chapter analyzes the performance of these algorithms for different plaintext sizes and discusses metrics such as encoding/decoding time, throughput, and entropy. The second results are the simulation results of the proposed system, which includes reading the RFID identifier, processing the driver's fingerprint, processing the vehicle number plate image, and matching it with the information stored in the cloud. The latest results include the implementation of the proposed system in practice, which matched the simulation results.

4.2. Results of Security Algorithms

In this section, the security and hybrid algorithms are tested under different plaintext and demonstrated in the next sections.

4.2.1. RSA Simulation Results

The provided results in Table (4.1) demonstrate the performance of RSA encryption and decryption for different plaintext sizes. Let's analyze each metric and discuss the findings:

RSA Encryption Time (msec.): This metric represents the time taken to encrypt the plaintext using RSA. As the plaintext size increases, the encryption time increases, indicating that larger plaintexts require more computational effort to encrypt.

Throughput of Encryption (Mbps): This metric measures the encryption speed in kilobits per second (Mbps). It indicates the rate at which the plaintext can be encrypted. Interestingly, the throughput of encryption remains relatively consistent

across different plaintext sizes, ranging from approximately 0.262 Mbps to 0.472 Mbps. This suggests that the plaintext size does not significantly affect the encryption speed.

RSA Decryption Time (msec.): This metric represents the time taken to decrypt the ciphertext using RSA. Like encryption, the decryption time increases as the plaintext size grows. This is expected since larger plaintexts require more computational effort to decrypt.

Throughput of Decryption (Mbps): This metric measures the decryption speed in kilobits per second (Mbps). Like the encryption throughput, the decryption throughput remains relatively consistent across different plaintext sizes, approximately 0.057 Mbps. This implies that the plaintext size does not significantly impact the decryption speed.

Table 4.1: RSA algorithm results under different plane text sizes.

Plane text size (kB)	**RSA Encryption time (msec)**	**Throughput of Encryption (Mbps)**	**RSA Decryption time (msec)**	**Throughput of Decryption (Mbps)**	**Entropy**
5kB	129	0.472	717	0.057	5.870
10kB	270	0.452	1437	0.057	5.871
15kB	428	0.424	2129	0.057	5.873
20kB	648	0.374	2842	0.057	5.873
25kB	951	0.319	3562	0.057	5.873
30kB	1386	0.262	4273	0.057	5.873

Entropy: Entropy measures the randomness or unpredictability of the plaintext. The provided entropy values remain constant at 5.870, 5.871, and 5.873 for different plaintext sizes. This indicates that the plaintext data does not exhibit significant variations in randomness across different sizes.

Overall, the results demonstrate that the encryption and decryption throughput is relatively consistent across different plaintext sizes, while the time taken for encryption and decryption increases with larger plaintexts. This behavior is expected since RSA encryption and decryption involve complex mathematical operations that scale with the plaintext size. The constant entropy values suggest that the randomness of the plaintext data remains unchanged regardless of the size.

4.2.2. DES Simulation Results

Table (4.2) displays the results of performing DES encryption and decryption operations on different sizes of plain text. Here is a summary and analysis of the results:

Plain Text Size: The Table shows the different sizes of plain text used in the encryption and decryption operations, ranging from 5kB to 30kB.

DES Encryption Time: This column represents the time to encrypt the plain text using the DES algorithm. The encryption time decreases as the plain text size increases, indicating that more significant plain texts can be encrypted more quickly.

Throughput of Encryption: This column represents the throughput of encryption, measured in kilobits per second (Mbps). It indicates the speed at which the encryption process is performed. The throughput of encryption increases as the plain text size increases, suggesting that more significant plain texts can be encrypted faster.

DES Decryption Time: This column represents the time to decrypt the cipher text using the DES algorithm. Like encryption, the decryption time decreases as the plain text size increases.

Throughput of Decryption: This column represents the throughput of decryption, measured in Mbps. It indicates the speed at which the decryption process is performed. The throughput of decryption also increases as the plain text size increases.

Entropy: Entropy is a measure of the randomness or unpredictability of data. The Table includes the entropy value for each plain text size. The entropy values range from 5.993 to 5.999, indicating high levels of randomness in the data.

Table 4.2: DES algorithm results under different plane text sizes.

Plane text size (kB)	**DES Encryption time (msec)**	**Throughput of Encryption (Mbps)**	**DES Decryption time (msec)**	**Throughput of Decryption (Mbps)**	**Entropy**
5kB	0.9844	56.269	0.691	59.276	5.993
10kB	1.4029	78.420	1.261	32.461	5.997
15kB	1.6955	97.085	1.525	53.714	5.997
20kB	2.0608	106.055	1.895	64.837	5.999
25kB	2.4159	113.355	2.199	74.506	5.999
30kB	2.7966	117.445	2.574	79.558	5.999

Overall, Table (4.2) shows that as the plain text size increases, the encryption and decryption times decrease, and the throughput of encryption and decryption increases. This suggests that DES encryption and decryption operations are more

efficient and faster when dealing with more significant plain texts. Additionally, the high entropy values indicate that the data used for encryption is highly random and provides good security properties.

4.2.3. AES Simulation Results

The provided data represents AES's encryption and decryption performance (Advanced Encryption Standard) for different plaintext sizes. Let us analyze the results and outcomes based on the given information:

AES Encryption Time and Throughput: As the plaintext size increases, the AES encryption time also increases. This is expected since encrypting more data requires more computational effort.

The throughput of encryption, measured in kilobits per second (kbps), shows how many kilobits can be encrypted in one second. The throughput decreases as the plaintext size increases, indicating that it takes longer to encrypt larger plaintexts.

AES Decryption Time and Throughput: Similar to encryption, the decryption time increases as the plaintext size increases. Decrypting larger ciphertexts requires more computational resources and thus takes more time.

The throughput of decryption also decreases as the plaintext size increases. This is because larger ciphertexts take longer to decrypt, resulting in lower throughput.

Entropy: Entropy is a measure of randomness or uncertainty in data. The given entropy values are constant for all plaintext sizes, indicating that the data has a consistent level of randomness regardless of size.

The results in Table (4.3) show that the encryption and decryption processes take more time for larger plaintexts, which is expected due to the increased computational

requirements. The throughput decreases for larger plaintexts, indicating a reduction in the speed of encryption and decryption.

It is important to note that the specific performance values provided in the data, such as the encryption and decryption times and throughput, may vary depending on the implementation, hardware, and software used. These results should be interpreted in the context of the specific system and environment in which they were measured.

Table 4.3: AES algorithm results under different plane text sizes.

Plane text size (kB)	**AES Encryption time (msec)**	**Throughput of Encryption (Mbps)**	**AES Decryption time (msec)**	**Throughput of Decryption (Mbps)**	**Entropy**
5kB	0.6936	78.985	0.4243	96.535	5.994
10kB	0.9044	120.973	0.7139	114.749	5.997
15kB	1.1252	145.780	1.0079	121.916	5.998
20kB	1.3242	165.098	1.2903	126.978	5.998
25kB	1.5276	178.874	1.5903	128.780	5.999
30kB	1.7408	188.731	1.8642	131.831	5.999

4.2.4. Comparison performance of RSA, DES, and AES

RSA, DES, and AES are all encryption algorithms that secure data. Let us compare them based on their encryption time, throughput, decryption time, and entropy.

Figures (4.1,4.2, 4.3, and 4.4) compare all results mentioned in tables (4.1, 4.2, and 4.3) regarding encryption time, throughput, decryption time, and entropy.

In summary, the comparison between RSA, DES, and AES can be summarized as follows:

RSA offers good security but slower encryption and decryption times and lower throughput than DES and AES. It is commonly used for key exchange and digital signatures rather than bulk data encryption.

DES has high-speed encryption and decryption times with very high throughput. However, it is considered relatively less secure than RSA and AES due to its shorter key length.

AES provides a good balance between security and performance. It has fast encryption and decryption times with high throughput. AES is widely used for secure communication and data encryption.

The following sections discuss the hybrid outcomes of RSA, DES, and AES with the SHA 256 algorithm to choose the most suitable hybrid algorithm for integrating it with the smart gate port system to investigate this thesis's objective.

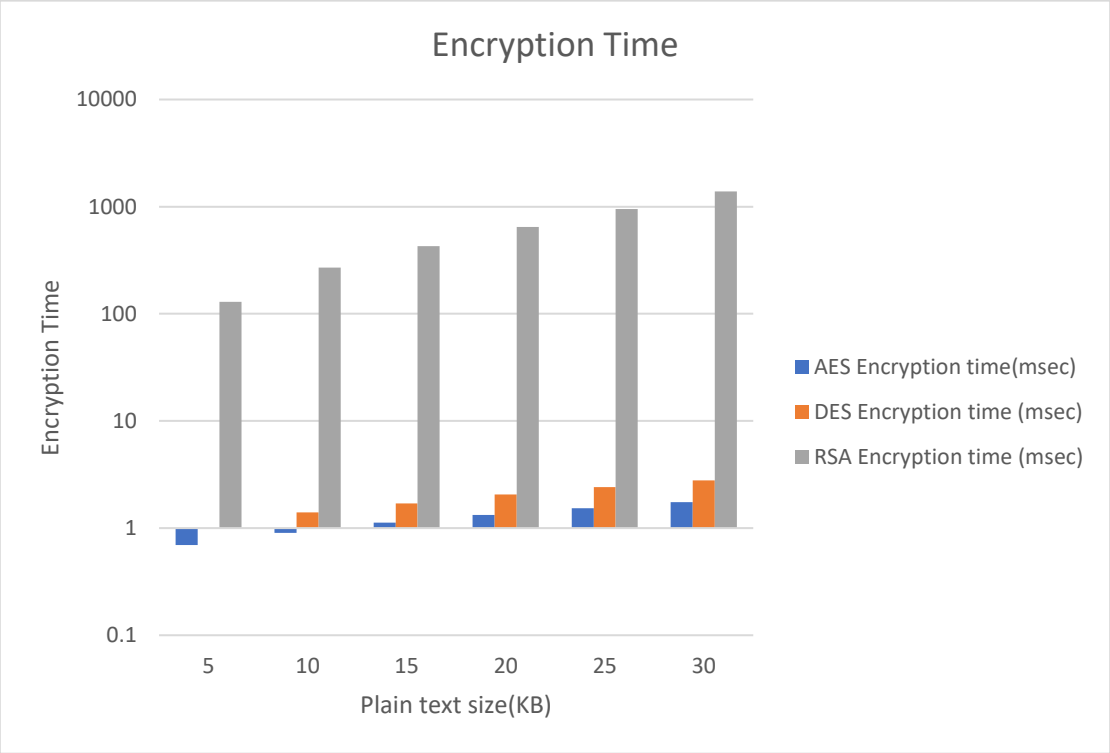


Figure 4.1. Comparative performance of encryption time among RSA, DES, and AES.

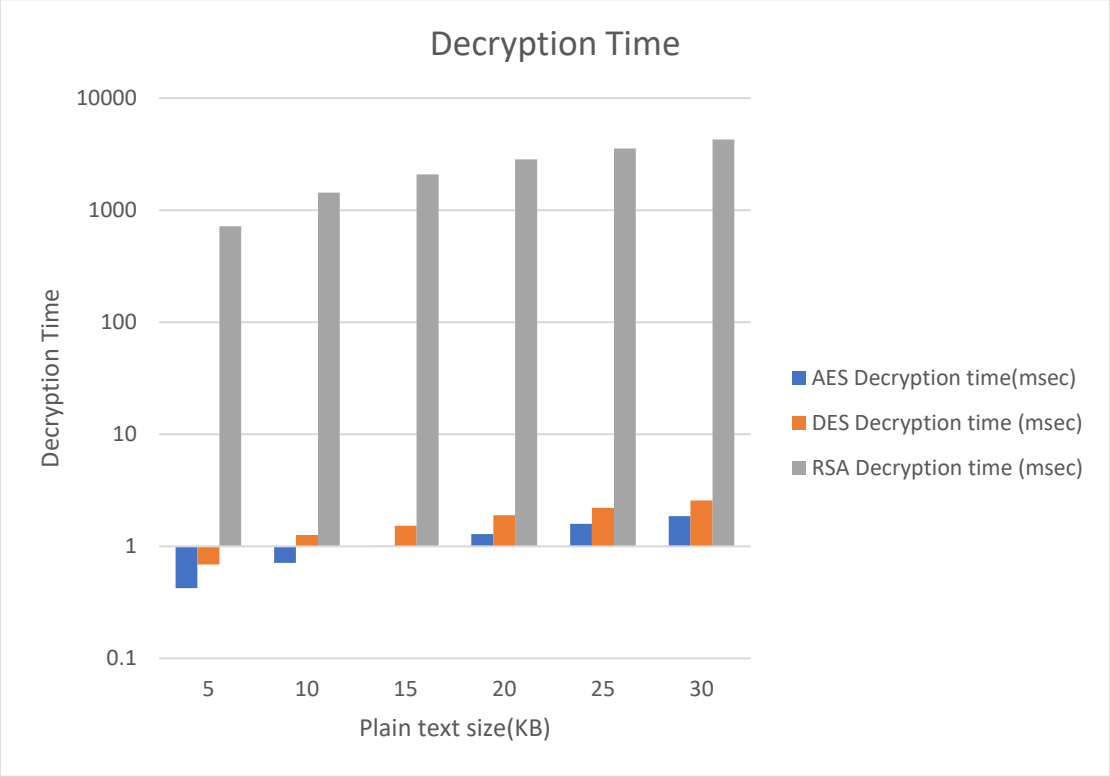


Figure 4.2. Comparative performance of decryption time among RSA, DES, and AES.

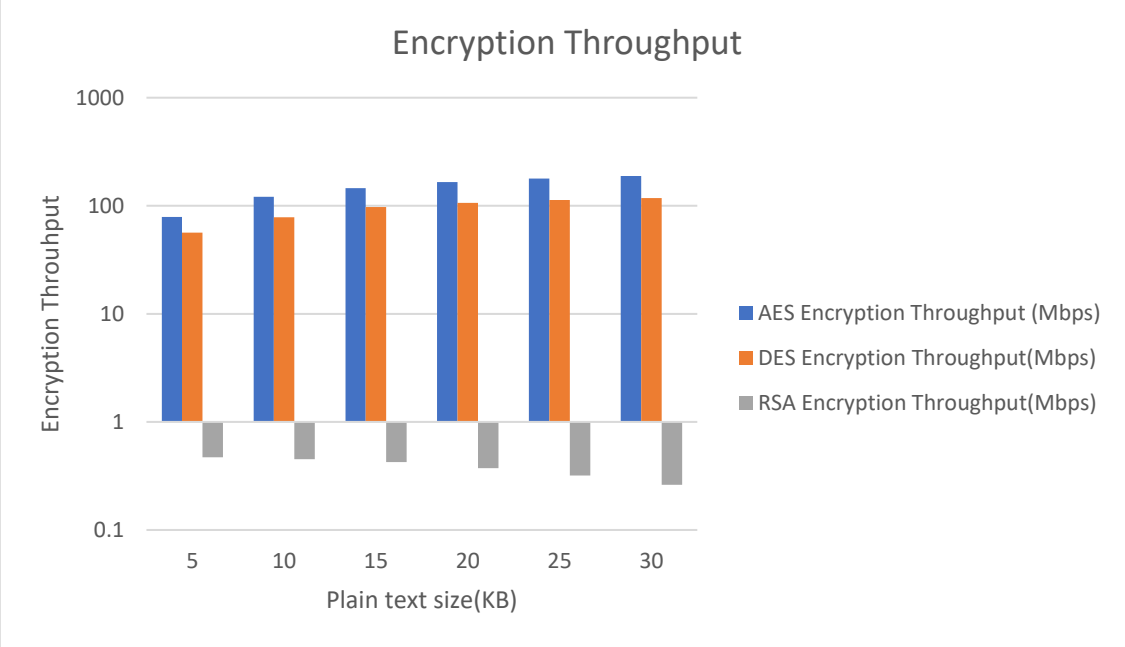


Figure 4.3. Comparative performance of encryption throughput among RSA, DES, and AES.

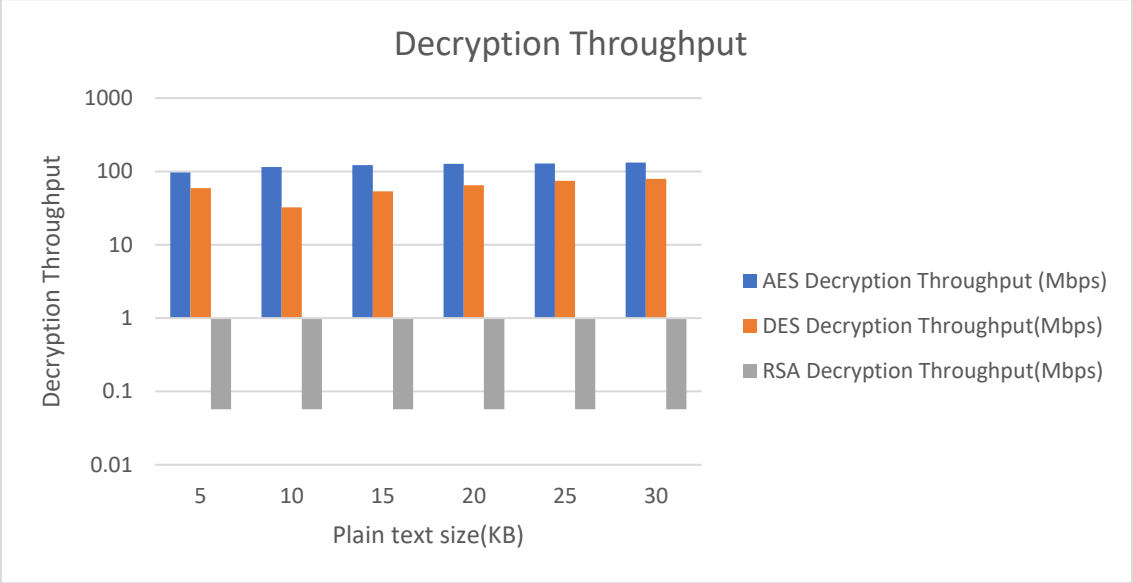


Figure 4.4. Comparative performance of decryption throughput among RSA, DES, and AES.

4.3. Results of Proposed Hybrid Security Algorithms

Based on the provided tables (4.4, 4.5, and 4.6), we have encryption and decryption performance metrics for three different algorithms: RSA-SHA256, DES-AHA256, and AES-SHA256. To determine the best algorithm, we compare the results:

4.3.1. RSA-SHA256 Simulation Results

Encryption Time (msec.): Ranges from 76 to 1419 Throughput of Encryption (Mbps.): Ranges from 0.256 to 0.819

Decryption Time (msec.): Ranges from 733 to 4314

Throughput of Decryption (Mbps.): Ranges from 0.055 to 0.056

Entropy: Constant at 5.8698-5.8736

4.3.2. DES-AHA256 Simulation Results

Encryption Time (msec.): Constantly low (ranging from 1.1451 to 3.6227)

Throughput of Encryption (Mbps.): High (ranging from 48.373 to 90.663)

Decryption Time (msec.): Constantly low (ranging from 0.8693 to 3.5539)

Throughput of Decryption (Mbps.): High (ranging from 47.118 to 69.152)

Entropy: Constant at 5.995-5.998

4.3.3. AES-SHA256 Simulation Results

Encryption Time (msec.): Constantly low (ranging from 0.8053 to 2.5757)

Throughput of Encryption (Mbps.): High (ranging from 68.903 to 127.555)

Decryption Time (msec.): Constantly low (ranging from 0.6236 to 2.8725)

Throughput of Decryption (Mbps.): High (ranging from 65.683 to 85.556)

Entropy: Constant at 5.997-5.999

4.3.4. Comparison performance of RSA-SHA256, DES-SHA256, and AES - SHA256:

RSA-SHA256 has the highest encryption and decryption times, indicating slower performance than the other two algorithms, as shown in Figures (4.5 and 4.6).

DES-AHA256 and AES-SHA256 have consistently low encryption and decryption times, suggesting faster performance.

DES-AHA256 and AES-SHA256 exhibit high throughput for encryption and decryption, indicating efficient data processing as indicated in figures (4.7 and 4.8).

The entropy values are relatively similar for all algorithms and do not significantly impact decision-making.

Based on these observations, it appears that both DES-AHA256 and AES-SHA256 offer superior performance compared to RSA-SHA256. However, if we focus on encryption and decryption speeds, DES-AHA256 and AES-SHA256 demonstrate consistently faster performance and higher throughput.

Therefore, based on the provided results, DES-AHA256 and AES-SHA256 have outstanding over RSA-AHA256 regarding fast encryption and decryption times with high throughput. However, RSA-AHA256 offers more security as compared with DES-AHA256 and AES-SHA256. For this reason, the most suitable algorithm for the smart port gate is RSA-AHA256 in our applications, the priority for security over encryption and decryption times, and in smart gate port, the plaintext is short, so RSA-SHA256 is considered the best algorithm for encryption and decryption. In addition, the processing of opening and closing the smart port gate for the following

vehicle and container needs more time; therefore, the fast time for encryption and decryption is not essential compared to security robust.

Table 4.4: RSA-SHA256 hybrid algorithm results under different plane text sizes.

Plane text size (kB)	RSA-SHA256 Encryption time (msec)	Throughput of Encryption (Mbps)	RSA-SHA256 Decryption time (msec)	Throughput of Decryption (Mbps)	Entropy
5kB	133	0.819	733	0.055	5.8698
10kB	274	0.647	1440	0.056	5.8716
15kB	435	0.510	2148	0.056	5.8733
20kB	683	0.418	2868	0.056	5.873
25kB	973	0.379	3574	0.056	5.8736
30kB	1419	0.256	4314	0.056	5.873

Table 4.5: DES-SHA256 hybrid algorithm results under different plane text sizes.

Plane text size (kB)	DES – AHA256 Encryption time (msec)	Throughput of Encryption (Mbps)	DES – SHA256 Decryption time (msec)	Throughput of Decryption (Mbps)	Entropy
5kB	1.1451	48.373	0.8693	47.118	5.995
10kB	1.6496	66.692	1.4019	58.434	5.998
15kB	2.1071	78.120	1.9613	62.652	5.997
20kB	2.6149	83.839	2.5236	64.923	5.998
25kB	3.1227	87.698	3.0259	67.682	5.999
30kB	3.6227	90.663	3.5539	69.152	5.998

Table 4.6: AES-SHA256 hybrid algorithm results under different plane text sizes.

Plane text size (kB)	**AES-SHA256 Encryption time (msec.)**	**Throughput of Encryption (kbps.)**	**AES – SHA256 Decryption time (msec.)**	**Throughput of Decryption (kbps.)**	**Entropy**
5kB	0.8053	68.903	0.6236	65.683	5.997
10kB	1.2337	89.227	1.1749	69.725	5.997
15kB	1.5523	106.103	1.5089	81.436	5.997
20kB	1.9818	110.671	1.9562	83.754	5.998
25kB	2.2591	121.251	2.4231	84.519	5.998
30kB	2.5757	127.555	2.8725	85.556	5.999

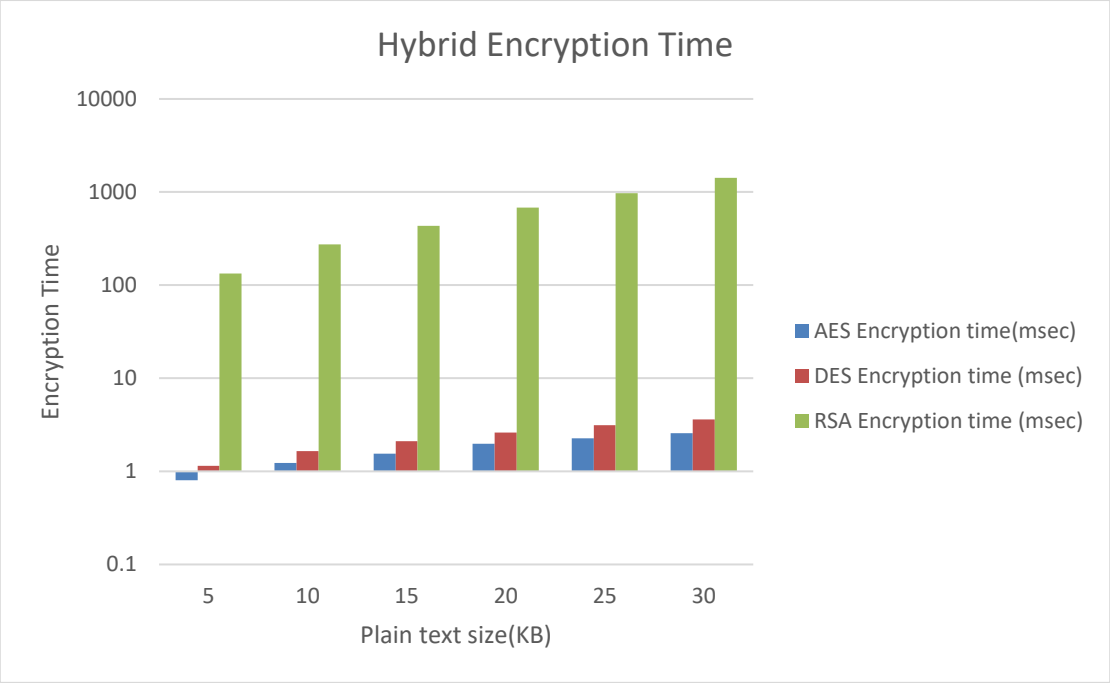


Figure 4.5. Comparative performance of encryption time among RSA-SHA256, DES-SHA256, and AES-SHA256.

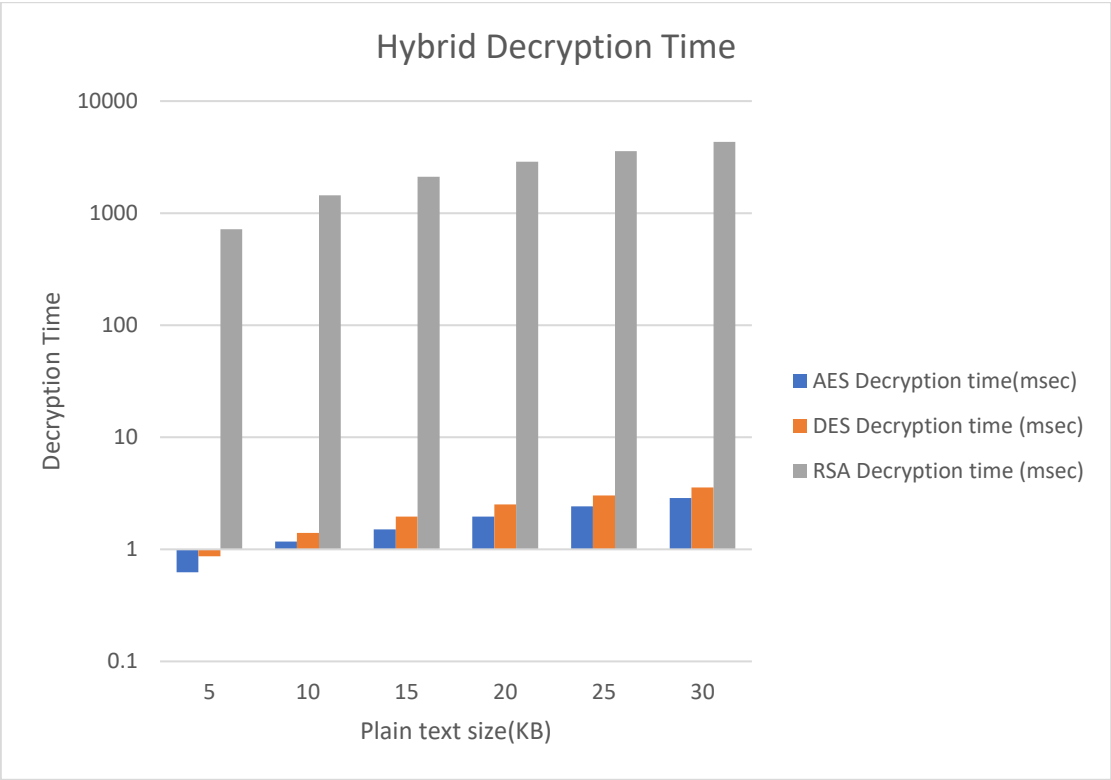


Figure 4.6. Comparative performance of decryption time among RSA-SHA256, DES-SHA256, and AES-SHA256.

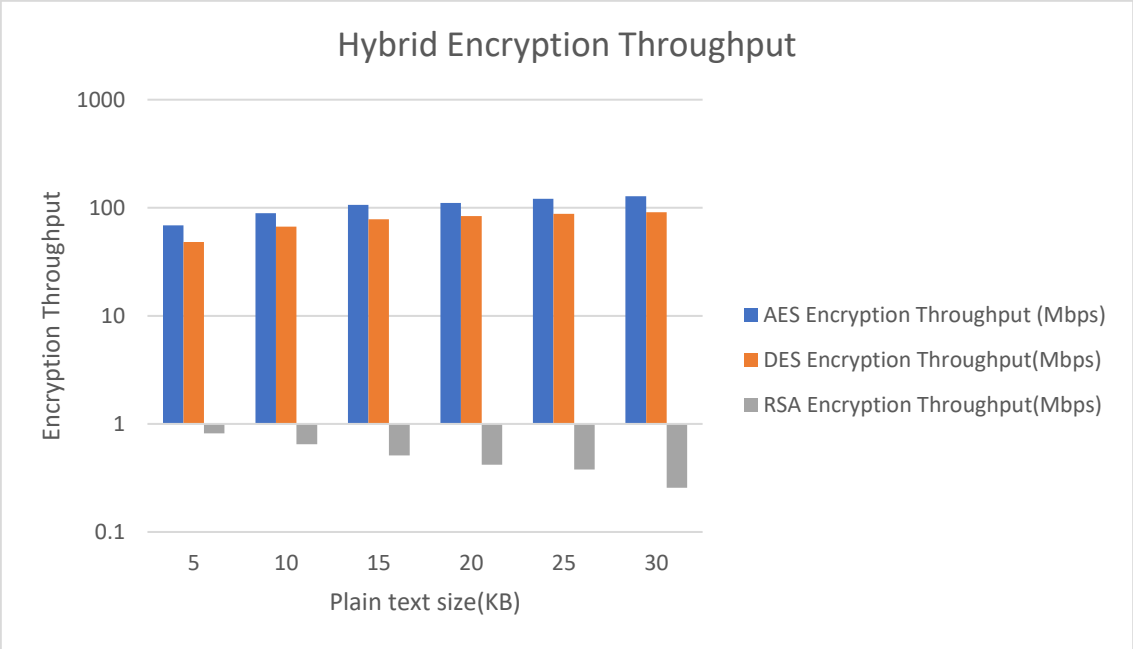


Figure 4.7. Comparative performance of encryption throughput among RSA-SHA256, DES-SHA256, and AES-SHA256.

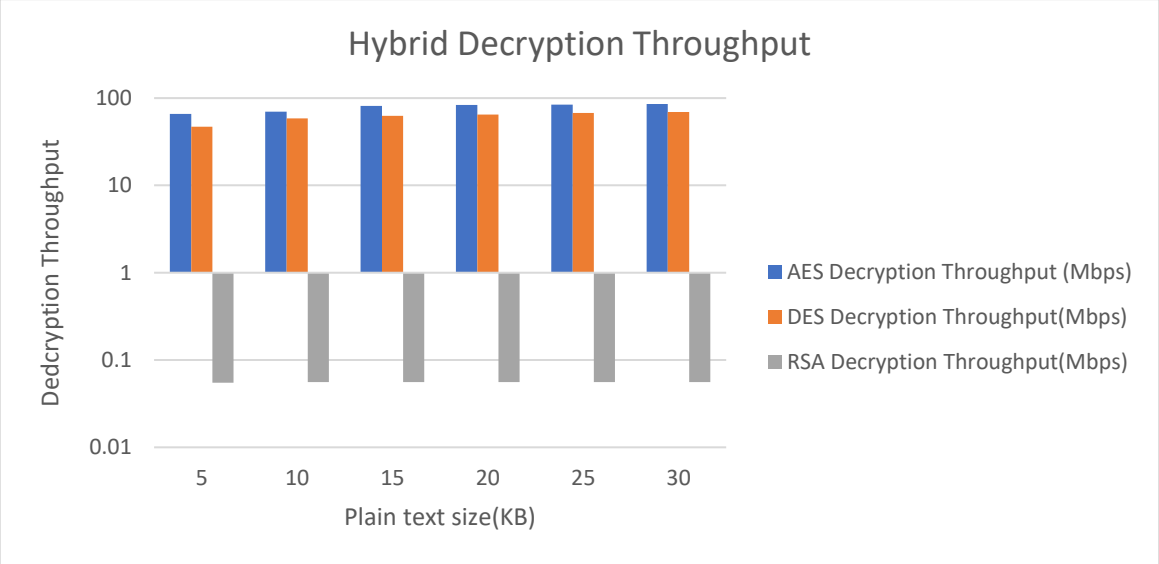


Figure 4.8. Comparative performance of decryption throughput among RSA-SHA256, DES-SHA256, and AES-SHA256.

4.4. Results of Proposed Fingerprint Algorithms

These results are related to fingerprint recognition and comparison using the FVC2002 (Fingerprint Verification Competition 2002) dataset. The dataset is often used to benchmark the performance of fingerprint recognition systems, as demonstrated in Figure (4.9).

In this scenario, a particular fingerprint image, '102-2.tif', was compared with multiple other fingerprint images in the dataset. The comparison yielded similarity scores between '102_2.tif' and each other images. A higher score represents more remarkable similarity, suggesting a higher probability that both fingerprints come from the same individual.

From the provided results, the fingerprints most similar to '102_2.tif' were those indexed as 102-1, 102-2, 102-3, 102-4, 102-5, 102-6, 102-7, and 102-8 in the Matched Fingerprints array. These fingerprints had the highest similarity scores with '101_2.tif', suggesting they may have come from the same person or similar fingerprints. Among all compared fingerprints, the one with the highest similarity score was '102-2' from the FVC2002 dataset. This suggests that '102-2' is likely from

the same individual who provided the fingerprint '102_2.tif', assuming the fingerprint comparison algorithm is highly accurate.

Figure 4.9. The FVC2002 database has eight copies of the same fingerprint in each row[139].

However, remember that the similarity scores depend on the specific fingerprint recognition algorithm used, as different algorithms may emphasize different features or characteristics of the fingerprints. Therefore, the actual certainty of a match depends on the reliability and performance of the algorithm.

For any biometric identification or verification system, it is essential to consider both the false acceptance rate (FAR) and false rejection rate (FRR). The FAR measures the likelihood that the system incorrectly accepts an access attempt by an unauthorized user. At the same time, the FRR is the likelihood that the system incorrectly rejects an access attempt by an authorized user. An ideal system minimizes both these rates.

If the results shown are part of a security system, further steps might be done to provide access or deny it based on the matched fingerprints. Alternatively, these results might narrow down suspects or link one crime scene to another in a criminal investigation.

Table (4.7) represents the results of the fingerprint image investigation with the database for the fingerprint, as demonstrated in Figure (4.10). The Table contains three columns, with the first being the fingerprint image compared with '102_2.tif', the second being the similarity score, and the third being whether it is considered a match or not based on the highest similarity scores:

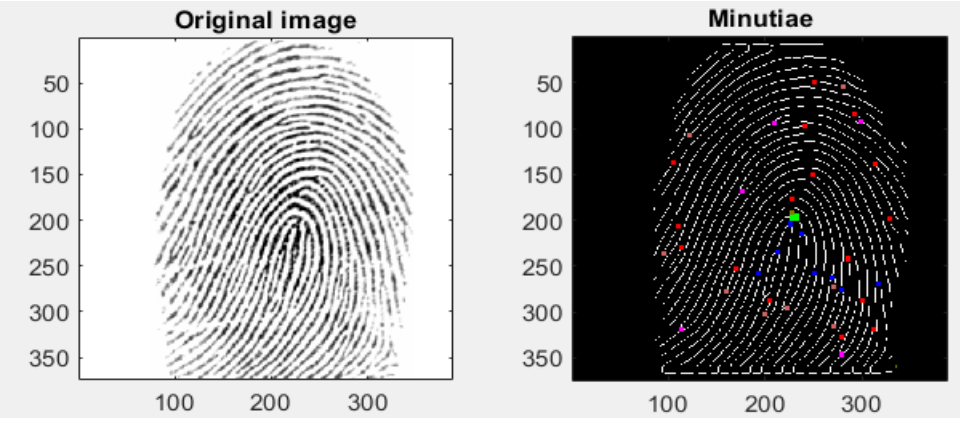


Figure 4.10. image 102_2 from the dataset.

Table 4.7: Comparison matching for image 102_2 with another dataset.

Compared Image	Similarity Score	Match
101_1	0.2804	No
101_2	0.21224	No
101_3	0.18858	No
101_4	0.21525	No
101_5	0.20795	No
101_6	0.27475	No
101_7	0.22231	No
101_8	0.2349	No
102_1	0.71028	Yes
102_2	1	Yes
102_3	0.60987	Yes
102_4	0.79723	Yes
102_5	0.48712	Yes
102_6	0.69322	Yes
102_7	0.65131	Yes
102_8	0.68559	Yes
103_1	0.2501	No
103_2	0.33558	No
103_3	0.20568	No
103_4	0.28475	No
103_5	0.23016	No
103_6	0.21011	No
103_7	0.3248	No
103_8	0.19936	No
104_1	0.23346	No
104_2	0.23745	No
104_3	0.2302	No
104_4	0.32219	No
104_5	0.22555	No
104_6	0.24166	No
104_7	0.21462	No
104_8	0.21582	No
105_1	0.22564	No
105_2	0.22564	No
105_3	0.25071	No

105_4	0.24855	No
105_5	0.3148	No
105_6	0.2349	No
105_7	0.30567	No
105_8	0.27475	No
106_1	0.36833	No
106_2	0.34531	No
106_3	0.26362	No
106_4	0.28475	No
106_5	0.27027	No
106_6	0.27027	No
106_7	0.38512	No
106_8	0.33581	No
107_1	0.34874	No
107_2	0.32432	No
107_3	0.25071	No
107_4	0.28183	No
107_5	0.24855	No
107_6	0.38904	No
107_7	0.26663	No
107_8	0.35135	No
108_1	0.2611	No
108_2	0.26509	No
108_3	0.25259	No
108_4	0.26601	No
108_5	0.23543	No
108_6	0.22337	No
108_7	0.24101	No
108_8	0.25917	No
109_1	0.24855	No
109_2	0.31639	No
109_3	0.29062	No
109_4	0.27962	No
109_5	0.27475	No
109_6	0.30015	No
109_7	0.27475	No
109_8	0.24012	No

This Table gives a clear overview of all the comparison results and which fingerprints were identified as matches based on the similarity scores.

Similarly, for fingerprint 102_3, as shown in Figure (4.11), the matching results are presented in Table (4.8). We can conclude from the Table that the algorithm has excellent performance in recognizing the fingerprint in different orientations for the same person.

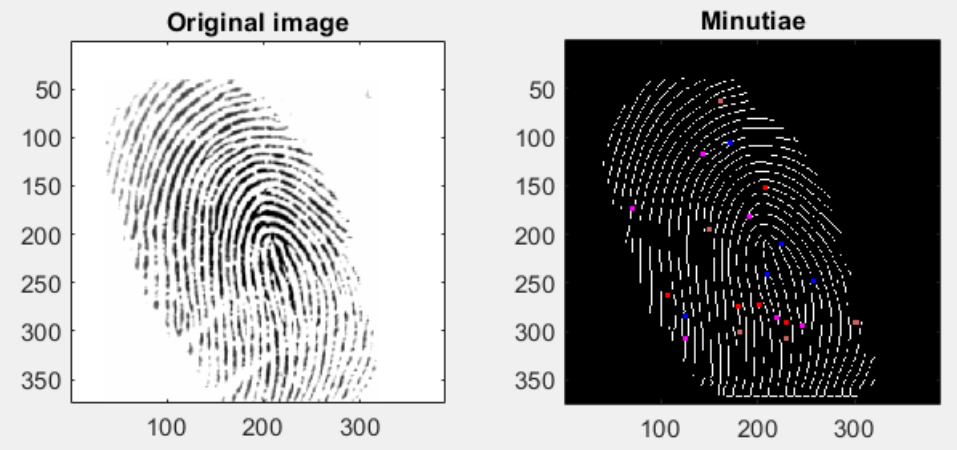


Figure 4.11. image 102_3 from the dataset.

Table 4.7: Comparison matching for image 102_3 with another dataset.

Compared Images	Similarity Score	Match
101_1	0.23262	No
101_2	0.28172	No
101_3	0.25031	No
101_4	0.28571	No
101_5	0.27603	No
101_6	0.24313	No
101_7	0.22131	No
101_8	0.22272	No
102_1	0.53875	Yes
102_2	0.574	Yes
102_3	1	Yes
102_4	0.70548	Yes

102_5	0.50395	Yes
102_6	0.47712	No
102_7	0.68252	Yes
102_8	0.77353	Yes
103_1	0.18443	No
103_2	0.22272	No
103_3	0.22751	No
103_4	0.25198	No
103_5	0.26186	No
103_6	0.23905	No
103_7	0.19597	No
103_8	0.2117	No
104_1	0.25355	No
104_2	0.20057	No
104_3	0.18334	No
104_4	0.19739	No
104_5	0.22454	No
104_6	0.26245	No
104_7	0.18128	No
104_8	0.19098	No
105_1	0.19967	No
105_2	0.23295	No
105_3	0.23295	No
105_4	0.24744	No
105_5	0.26591	No
105_6	0.22272	No
105_7	0.29508	No
105_8	0.32418	No
106_1	0.30557	No
106_2	0.27501	No
106_3	0.23328	No
106_4	0.25198	No
106_5	0.21525	No
106_6	0.17937	No
106_7	0.27264	No
106_8	0.32418	No
107_1	0.27003	No
107_2	0.25112	No
107_3	0.23295	No
107_4	0.21822	No

107_5	0.2062	No
107_6	0.2582	No
107_7	0.28957	No
107_8	0.21525	No
108_1	0.31991	No
108_2	0.29773	No
108_3	0.2794	No
108_4	0.26482	No
108_5	0.34091	No
108_6	0.2965	No
108_7	0.21328	No
108_8	0.23817	No
109_1	0.28868	No
109_2	0.20998	No
109_3	0.23146	No
109_4	0.28868	No
109_5	0.24313	No
109_6	0.27889	No
109_7	0.24313	No
109_8	0.27889	No

In both cases, accuracy measures how correctly the fingerprints are identified.

First case:

There are 8 accurate matches (102_1.tif through 102_8.tif for FVC2002). Let us assume our system has correctly matched 8 out of these 8 (from the 'Matched_Fingerprints' output: 102_1, 102_2, 102_3, 102_4, 102_5, 102_6, 102_7 and 102_8).

The formula calculates accuracy:

$$accuracy = (Total\ Correct\ Matches\ /\ Total\ Matches)\ \times 100 \qquad (4.1)$$

For this case, accuracy would be:

$$(8/8)\ \times\ 100\ =\ 100\%$$

Second case:

In this case, there are 8 true matches (102_1.tif through 102_8.tif for FVC2002). The 'Matched_Fingerprints' output shows 7 matches (102_1, 102_2, 102_3, 102_4, 102_6, 102_7, and 102_8).

Using the same formula as above:

$$(7/8) \times 100 = 87.5\%$$

So, the fingerprint matching accuracy for the first case is 100%, and for the second case is 87.5%.

These approximate calculations could vary depending on the actual count and ground truth. Also, the system considers any similarity score > 0.48 as a match. In reality, the threshold for considering a match can vary depending on the specificity and sensitivity of the system. The choice of threshold can also significantly affect the final accuracy. Finally, the Average Accuracy (%) is almost 93.2%-96.6% for all person fingerprints.

4.5. Results of Proposed car number recognition Algorithms

Figure (4.12) demonstrates the capture car number. At the same time, Figure (4.13) shows the initial binary image generated from the input image. The image is first converted to grayscale, then the noise is added and filtered out, and then thresholding is used to convert it to a binary image. Small objects in the binary image are then removed. The output should be a clean, binary image of the number plate.

Figure(4.14) displays the binary image after more extensive removal of objects. The size of objects to be removed depends on the size of the image. The output image will have fewer small objects and noise, primarily leaving the number plate characters.

Figure (4.15) shows the result of subtracting Figure (4.14) from the initial binary image. It highlights the differences between the two noise and object removal stages. The output image will show the elements removed from the first binary image to obtain a smooth image.

Figure (4.16) Here is displayed again, but this time after removing smaller objects with a size of less than 200 pixels. This step further cleans up the image and reduces noise, leaving a cleaner representation of the characters on the number plate. The bounding box is drawn with the rectangle function: The green rectangles represent the boundaries of the identified separate objects (characters) in the image. These are the regions that are subsequently processed for character recognition.

Simalritly, when testing the proposed algorithm on the new car number in Iraq, the proposed algorithm is effective and extraction number without error character or in number as shown in figures (4.17-4.21) respectively.

Figure 4.12. capture of car number

Figure 4.13. binary image after converted to grayscale and filtered out.

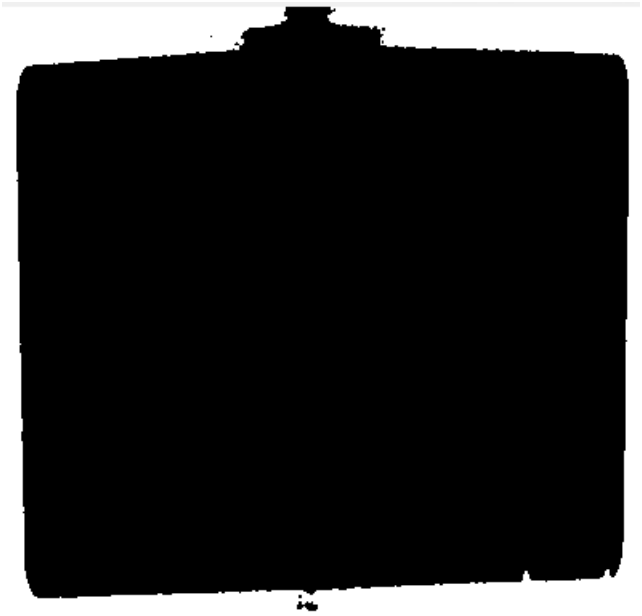


Figure 4.14. binary image after more extensive removal of objects.

Figure 4.15. binary image after subtracting from the initial binary image.

Figure 4.16. binary image after removing smaller objects with a size of less than 200 pixels with boundaries of characters.

Figure 4.17. capture of car number of Iraq system

Figure 4.18. binary image after converted to grayscale and filtered out.

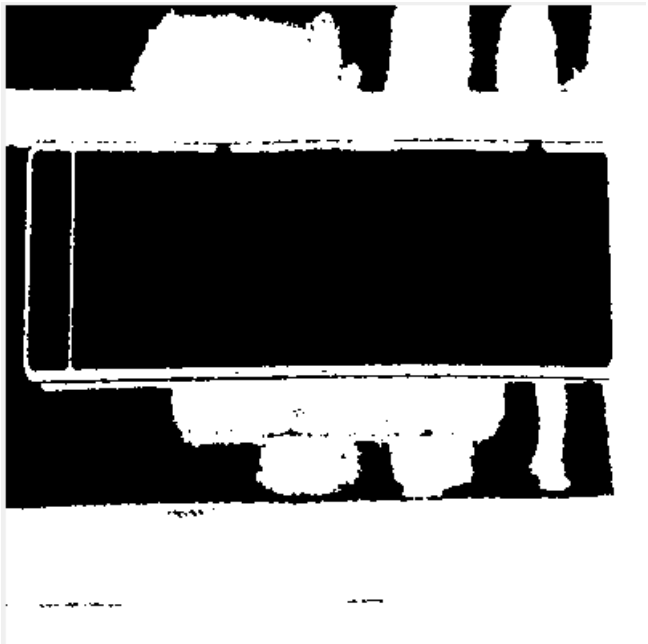


Figure 4.19. Binary image after more extensive removal of objects.

Figure 4.20. binary image after subtracting from the initial binary image.

Figure 4.21. binary image after removing smaller objects with boundaries of characters.

4.6. Simulation Results of Smart Port Gate Automation

The provided results represent a MATLAB simulation of a smart gate system. This system presented three gates, each containing information about car license IDs, fingerprint IDs, RFID, driver names, and other related attributes, as shown in Figure (4.22).

The main graphical window presented in Figure (4.22) is created with a light gray background, housing the controls for interacting with the gates. There are three gate IDs ('Gate1', 'Gate2', and 'Gate3'), and a corresponding status map is initialized with zeros, likely indicating that all gates are initially closed. Two buttons are created for each gate: one to open the gate and one to close the gate. Three sets of input boxes are created for each gate to allow users to enter car license IDs, fingerprint IDs, and RFID. These be used for matching with the stored IDs and may open the gate if matched or closed if not matched.

A structured database is created for each gate, containing detailed information such as:

- Car license IDs
- Fingerprint IDs
- RFIDs
- Driver names
- Departure times and dates
- Destinations
- Expected times of reach
- Container details (serial, weight, line, etc.)
- Type of goods
- Type and size of containers
- Ship agents
- Degree of danger

Each gate is Open, and Close buttons are created dynamically based on the number of gate IDs. Their positions are calculated to place them neatly in the window. The labels for the buttons include the gate IDs. The input boxes for car license IDs, fingerprint IDs, and RFID are aligned vertically and placed dynamically for each gate.

Three comprehensive databases are stored in a container. Map object, one for each gate. This allows for convenient lookup and manipulation of gate-specific information.

The main steps to implement a matching system are to retrieve the information entered in the carLicenseIDBoxes, fingerprintIDBoxes, and rfidIDBoxes for the particular gate. Then, it would access the corresponding stored information from the storedInfo container for the gate in question. Next, it compares the entered information with the stored information. This will typically involve checking if the entered Car License ID, Fingerprint ID, and RFID match any stored details for that gate.

Based on the comparison, it would make a decision. If the information matches, you could permit the gate operation (open or close) and display a message confirming the match. If the information does not match, it could deny the gate operation and display an error or warning message. Depending on the outcome, it may want to update the GUI by turning on or off certain buttons or displaying relevant messages. The status of open and closed with indicating messages are demonstrated in Figures (4.23) and (4.24).

Finally, when the car accesses the barrier within a range of 3m, the gate will have closed and generated a report with a tracking link for each gate, as shown in Figure (4.25).

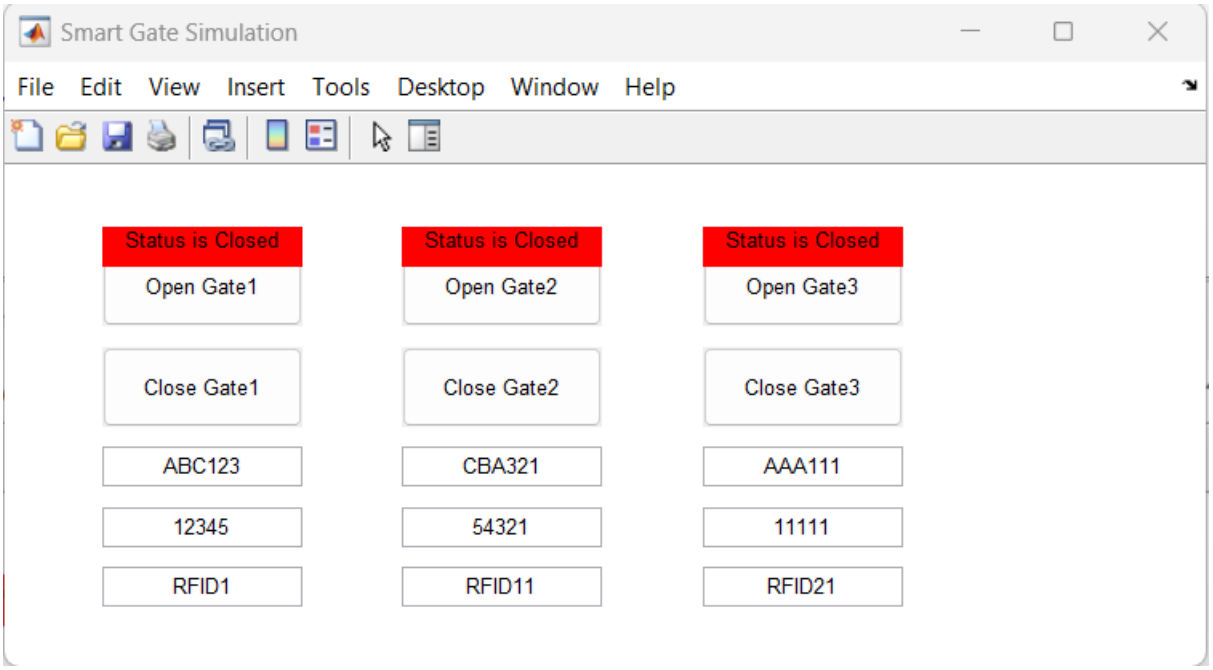


Figure 4.22. Three smart gates GUI based on IoT.

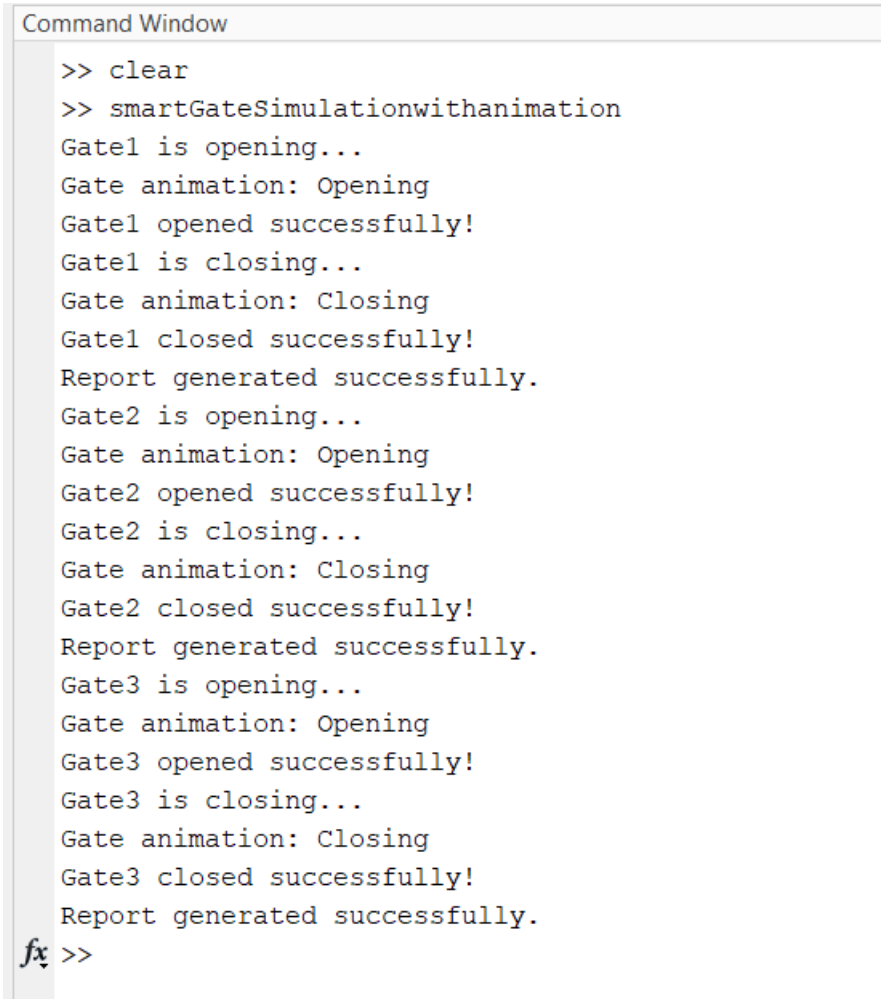
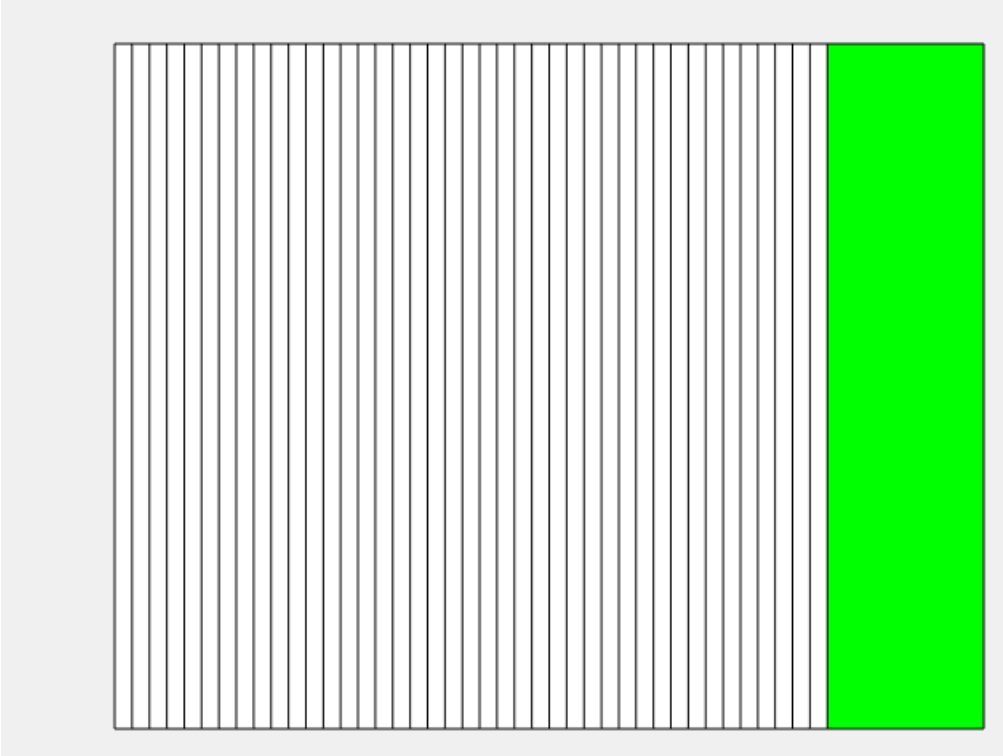
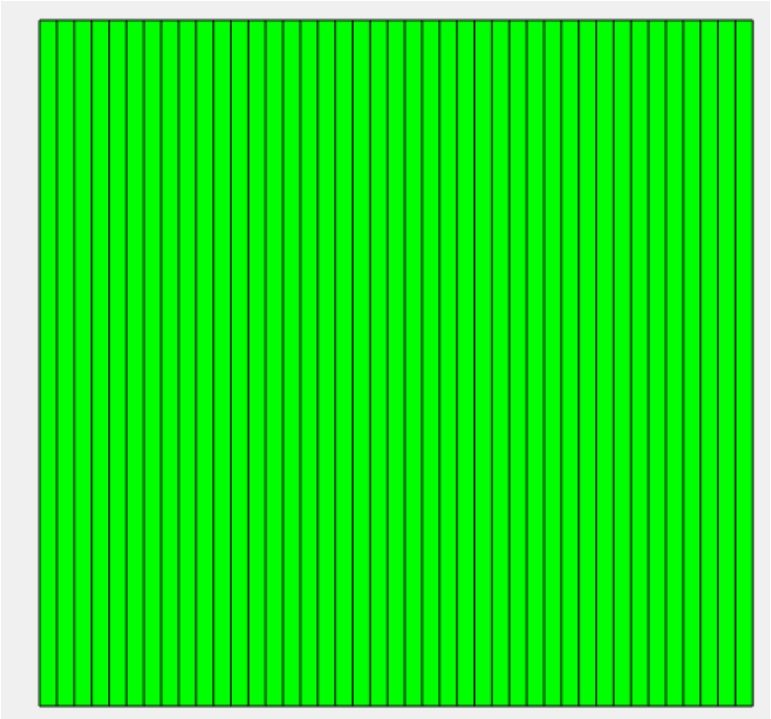


Figure 4.23. The status of each gate.

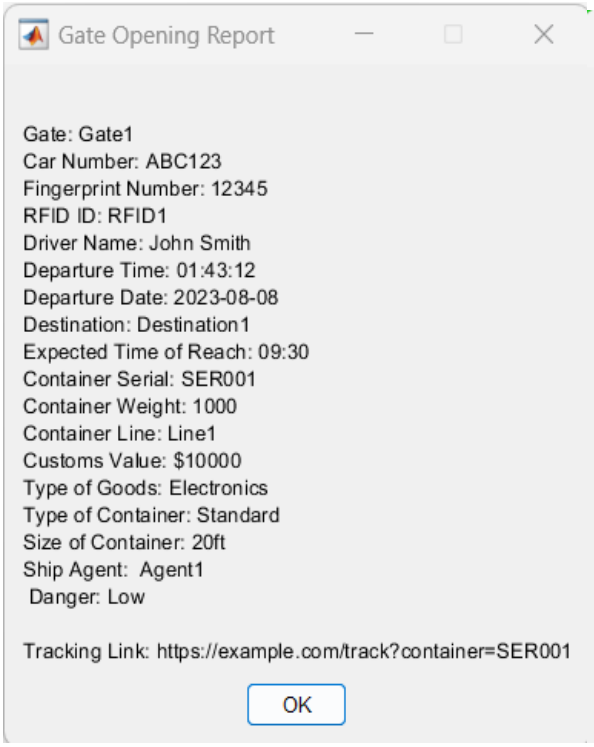


(a)

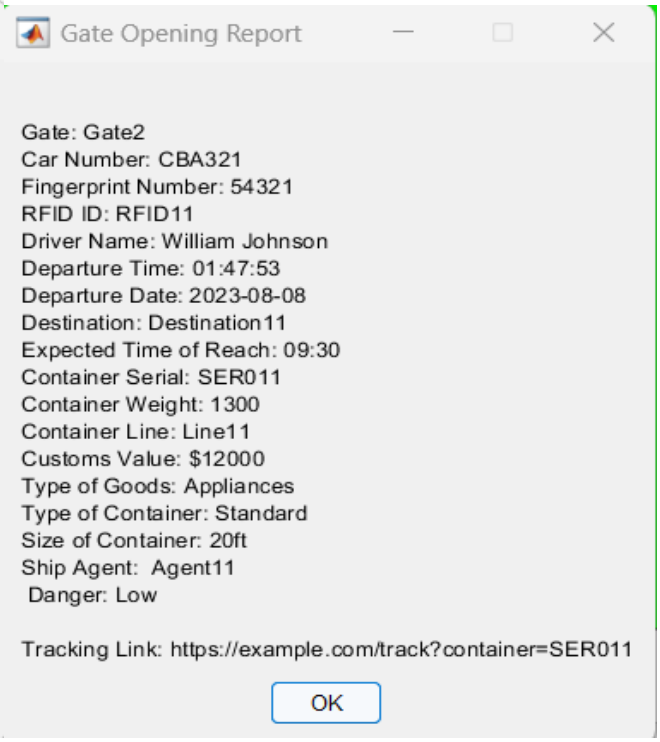


(b)

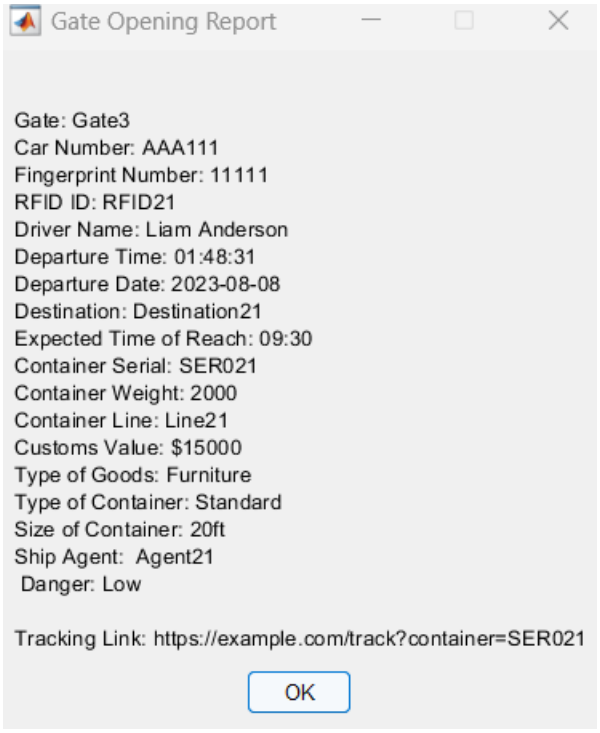
Figure 4.24. Simulation of status (a) open gate, (b) closed.



(a)



(b)



(c)

Figure 3.25. The output generated report (a) gate 1, (b) gate 2, and (c) gate three.

4.7. Experimental Results of Smart Port Gate

In order to add and update the data required to implement the project, a graphical interface was created, as shown in Figure (4.26).

All system components (RFID reader, ultrasonic sensors, camera, fingerprint sensor) are connected to the P.C. The PC. was accessed to the database via the cloud platform. The system was tested using the SUV vehicle type due to the difficulties of using a truck. When the vehicle approaches the gate at a certain distance (within the range of the RFID reader), the reader will read the I.D. of the tag, as shown in Figure (4.27).

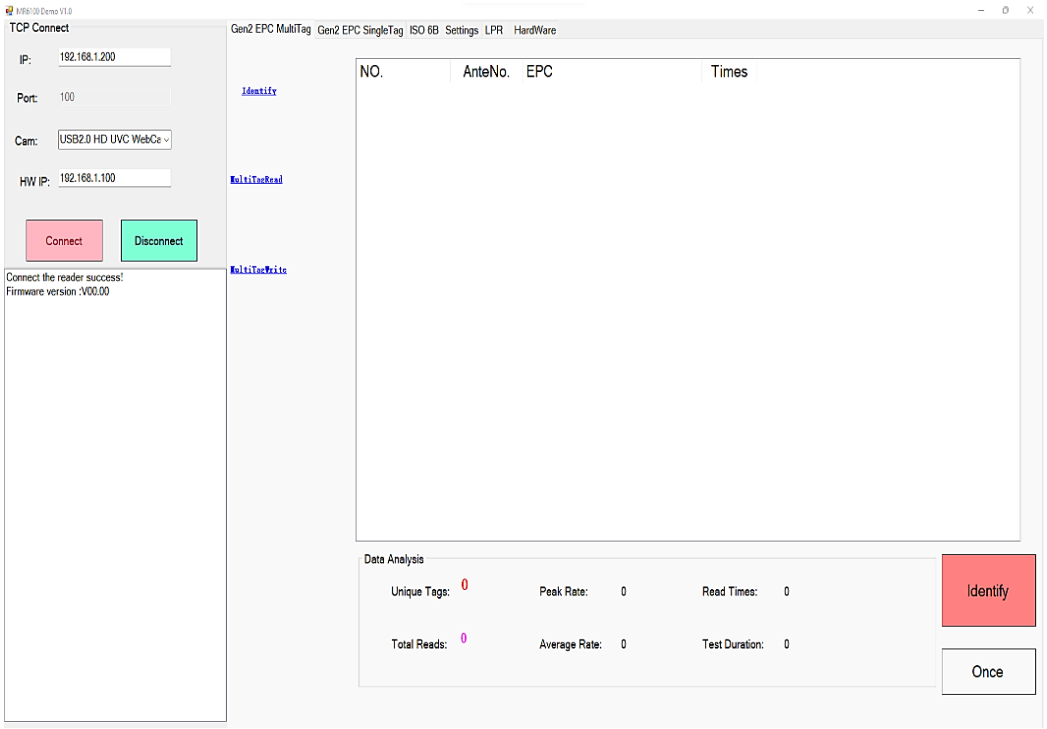


Figure 4.26. Graphical interface for executing the gate operation.

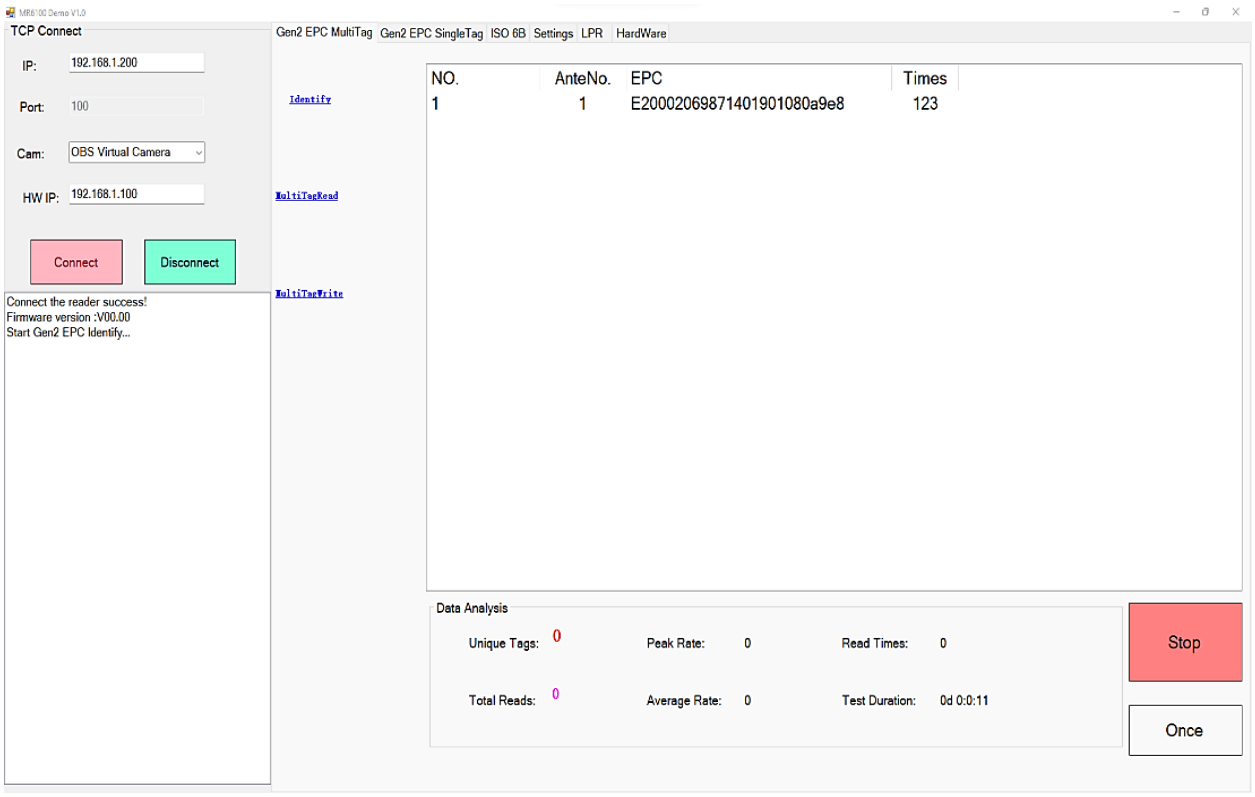


Figure 4.27. RFID reader for I.D. tags

At that moment, the fingerprint sensor becomes ready to take the driver's fingerprint. Figure (4.28) shows the driver's fingerprinting process. When the fingerprint process is completed, the camera takes a picture of the vehicle number plate to read the vehicle number using Rekor's OpenALPR suite. Figure (4.29) shows the process of capturing the vehicle number plate and reading the plate number.

When the vehicle number detection is completed, the information is matched with the database to decide whether to open the gate. Figures (4.30) and (4.31) show the gate-opening process after ensuring that the information received from the sensors matches the information installed in the database.

Figure 4.28. Driver fingerprinting process.

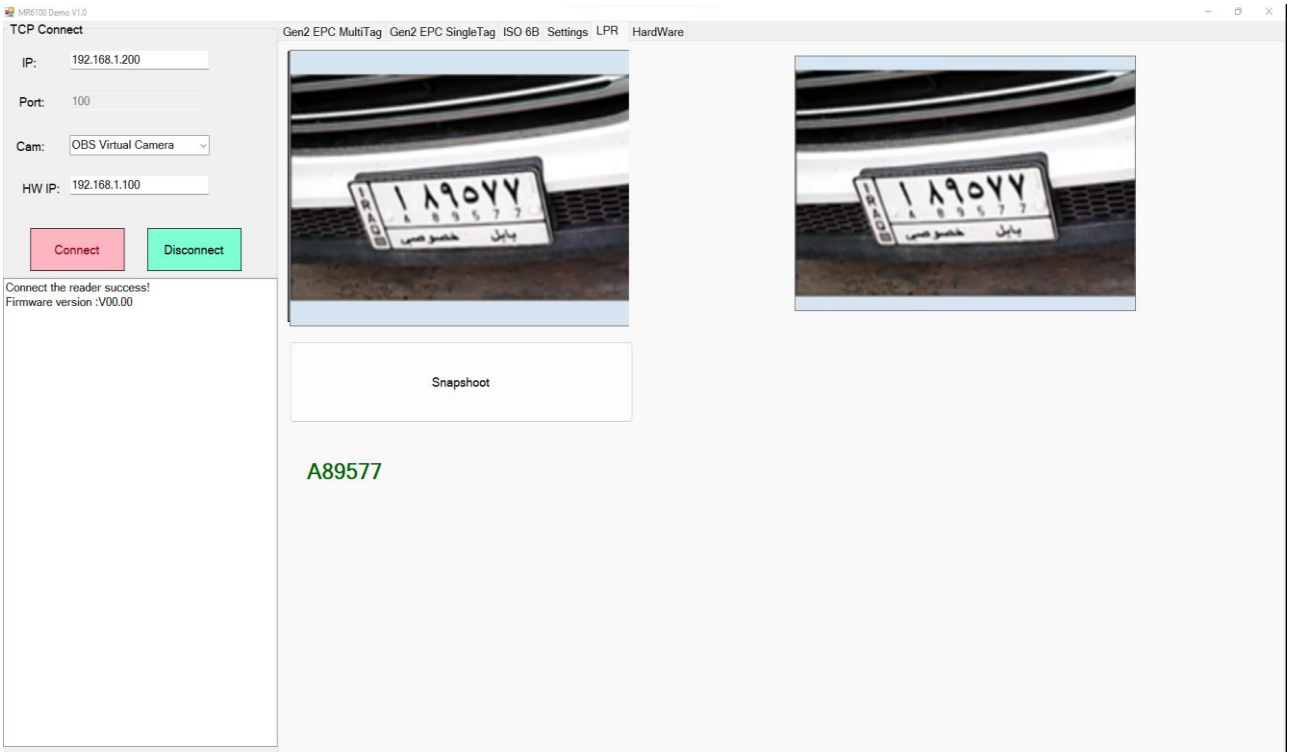


Figure 4.29. Capturing the vehicle plate image and reading the plate number.

Figure 4.30. Gate barrier closed

Figure 4.31. Gate barrier open

This proposed system can send a report to the Monitoring and Control Centre showing the I.D. of the containers leaving the gate with all relevant information (date and time, container description, car number, fingerprint I.D., and name of the driver) stored in the database as in Figure 4.32. The time taken for reading and matching the results with the data previously stored in the cloud database for opening the gate was less than 10 seconds, which depended on the speed of the internet. The work of this smart gate is very fast compared to the traditional gate, which leads to a high flow of goods and thus increases the financial revenues of the port in addition to an increase in security, the prevention of human errors, and an improvement in the appearance of the port and the city.

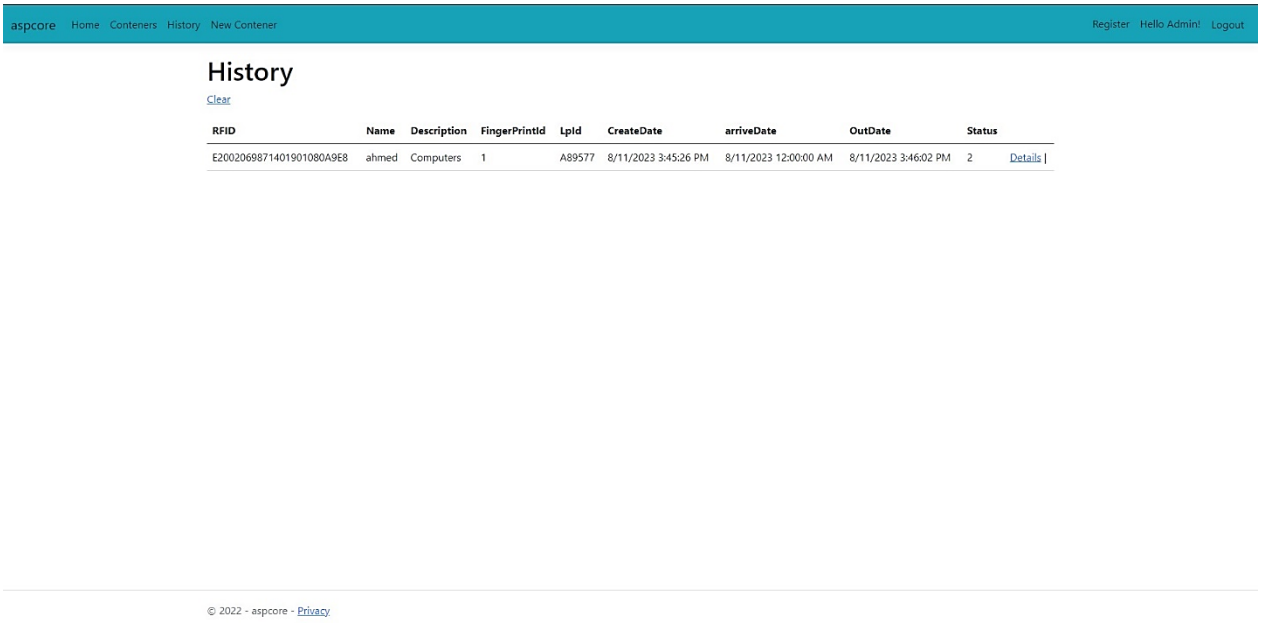


Figure 4.32: The report sent from the database after comparison and matching.

4.8. Discussion

Chapter 4 of the document discusses the testing and outcomes of proposed security algorithms, focusing on RSA encryption and decryption. The performance of these algorithms is evaluated for different plaintext sizes, and several metrics are analyzed to understand their behavior.

For RSA encryption, it is observed that the encryption time increases as the plaintext size grows, indicating that larger plaintexts require more computational effort to encrypt. However, the throughput of encryption, which measures the encryption speed, remains relatively consistent across different plaintext sizes. This suggests that the plaintext size does not significantly impact the encryption speed. Similar trends are observed for RSA decryption, where the decryption time increases with larger plaintexts while the decryption throughput remains relatively stable.

Entropy, which measures the randomness of the plaintext, is found to be constant across different plaintext sizes. This indicates that the randomness of the plaintext data remains unchanged regardless of the size.

The chapter also explores the application of the proposed algorithms to fingerprint recognition and comparison using the FVC2002 dataset. The results identify fingerprints most similar to a particular fingerprint image and suggest possible matches.

In addition to security algorithms, the chapter presents the process of capturing car numbers and converting them into clean binary images using various image processing techniques. The step-by-step process involves grayscale conversion, noise removal, thresholding, and object removal to isolate the number plate characters.

Finally, the proposed algorithm is tested on a new car number in Iraq, and it is reported to be effective in extracting the number without errors in characters or numbers in simulation and experimental results.

Overall, the proposed system has been tested experimentally and has proven to be compatible with simulation results.

Chapter Five

Conclusion and Recommendations for Future Work

5.1. Conclusions

By analyzing case studies and real-world implementations, it is evident that Smart Port Gate Automation offers substantial advantages in reduced operational costs, improved cargo handling, minimized human errors, and enhanced environmental sustainability.

Smart Port Gate Automation offers numerous advantages that positively impact the entire port ecosystem. The most notable benefits include:

1. Increased Efficiency: Automation eliminates manual processes, reducing human error and expediting cargo handling, resulting in faster turnaround times and increased port throughput.
2. Enhanced Security: Advanced biometric authentication, video surveillance, and access control systems bolster port security, minimizing the risk of unauthorized access and ensuring a safe operating environment.
3. Cost Optimization: By streamlining operations and reducing dependency on manual labor, Smart Port Gate Automation helps ports reduce operational costs, boosting overall profitability.
4. Prevent bribery of relevant personnel and forgery of official documents, such as invoices, certificates of origin, standardization and quality control certificates, to reduce or evade taxes
5. Environmental Sustainability: Improved operational efficiency reduces energy consumption and emissions, contributing to greener port practices and environmental conservation.
6. Real-Time Visibility: IoT-based monitoring provides real-time visibility into port operations, enabling stakeholders to make informed decisions promptly.

7. Regulatory Compliance: Automation assists in adhering to stringent international security and safety standards, ensuring regulatory compliance and reducing penalties.

5.2. Future Work Recommendations

Recommendations for Future Work for Smart Port Gate Automation:

1. Usability and User Experience Improvement: Future work should focus on enhancing the usability and user experience of Smart Port Gate Automation systems. User-friendly interfaces and intuitive design will facilitate easier adoption by port personnel and truck drivers, reducing the learning curve and potential resistance to change.
2. Integration with Supply Chain Ecosystem: Smart Port Gate Automation should seamlessly integrate with the broader supply chain ecosystem. Collaborating with logistics providers, shipping companies, and other stakeholders will enable end-to-end visibility and optimization of cargo movement from the point of origin to the final destination.
3. Cross-Border and Multi-Port Integration: Ports situated nearby or belonging to the same region can collaborate to implement cross-border and multi-port integration of Smart Port Gate Automation. This will facilitate smoother cargo movements across different port facilities.
4. Environmental Sustainability Initiatives: As part of Smart Port Gate Automation projects, ports should invest in sustainable practices. This may include integrating renewable energy sources, electric vehicle charging infrastructure, and eco-friendly materials in gate construction.
5. Standardization and Interoperability: To promote the widespread adoption of Smart Port Gate Automation, industry stakeholders should work together to develop standardized protocols and ensure interoperability between different systems and ports.

6. Integration of Autonomous Vehicles: As autonomous trucking technology advances, integrating autonomous vehicles with Smart Port Gate Automation will further streamline the movement of goods, reduce human error, and enhance safety.
7. Continuous Cybersecurity Enhancement: Given the increasing threat of cyberattacks, ongoing efforts to improve cybersecurity measures, including regular audits, vulnerability assessments, and employee training, are crucial to safeguarding Smart Port Gate Automation systems.
8. Diversity in the use of sensors: Other types of sensors can be used at the gate to detect prohibited materials such as explosives and drugs, as well as using sensors to know the state of the goods and their weights.

By focusing on these recommendations, the future of Smart Port Gate Automation will see improved efficiency, sustainability, and security. Embracing technological advancements, fostering collaboration, and prioritizing user needs will unlock the full potential of Smart Port Gate Automation, driving the maritime industry towards a more connected and intelligent future.

References:

[1] A. Othman, S. El Gazzar, and M. Knez, "Investigating the influences of smart port practices and technology employment on port sustainable performance: the Egypt case," *Sustainability*, vol. 14, no. 21, p. 14014, 2022.

[2] B. Belmoukari, J.-F. Audy, and P. Forget, "Smart port: a systematic literature review," *European Transport Research Review*, vol. 15, no. 1, pp. 1-12, 2023.

[3] J. Keshta, H. Elmesmary, and M. Obrecht, "Investigating the impact of covid-19 on maritime supply chain sustainability and technology: A review," in *Proceedings of the ICAMS International Conference on Advanced Materials and Systems, Bucharest, Romania*, 2020, pp. 1-3.

[4] A. Sepehri, H. R. Vandchali, A. W. Siddiqui, and J. Montewka, "The impact of shipping 4.0 on controlling shipping accidents: A systematic literature review," *Ocean Engineering*, vol. 243, p. 110162, 2022.

[5] A. Karaś, "Smart port as a key to the future development of modern ports," *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 14, no. 1, 2020.

[6] M. Heikkilä, J. Saarni, and A. Saurama, "Innovation in Smart Ports: Future Directions of Digitalization in Container Ports," *Journal of Marine Science and Engineering*, vol. 10, no. 12, p. 1925, 2022.

[7] Y. Triska, E. M. Frazzon, V. M. D. Silva, and L. Heilig, "Smart port terminals: Conceptual framework, maturity modeling and research agenda," *Maritime Policy & Management*, pp. 1-24, 2022.

[8] Y. Boullauazan, C. Sys, and T. Vanelslander, "Developing and demonstrating a maturity model for smart ports," *Maritime Policy & Management*, vol. 50, no. 4, pp. 447-465, 2023.

[9] W. Mi and Y. Liu, *Smart Ports*. Springer, 2022.

[10] H. Min, "Developing a smart port architecture and essential elements in the era of Industry 4.0," *Maritime Economics & Logistics*, vol. 24, no. 2, pp. 189-207, 2022.

[11] A. F. Aljawareen, "Current state and projections of the maritime transport sector for economic development in Iraq," *International Journal of Economics, Business and Accounting Research (IJEBAR)*, vol. 4, no. 02, 2020.

[12] D. Xisong, X. Gang, L. Yuantao, G. Xiujiang, and L. Yisheng, "Intelligent ports based on Internet of Things," in *Proceedings of 2013 IEEE International Conference on Service Operations and Logistics, and Informatics*, 2013: IEEE, pp. 292-296.

[13] N. Bahnes, B. Kechar, and H. Haffaf, "Cooperation between intelligent autonomous vehicles to enhance container terminal operations," *Journal of Innovation in Digital Ecosystems*, vol. 3, no. 1, pp. 22-29, 2016.

References

[14] J. Odiete, A. Agbeyangi, and O. Olatinwo, "An automated door control system using biometric technology," *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN*, pp. 2278-0661, 2017.

[15] Y. Yang, M. Zhong, H. Yao, F. Yu, X. Fu, and O. Postolache, "Internet of things for smart ports: Technologies and challenges," *IEEE Instrumentation & Measurement Magazine,* vol. 21, no. 1, pp. 34-43, 2018.

[16] H. Ohal, C. Lalwani, S. Jadhav, and N. Parikh, "Smart gate," in *2018 2nd International Conference on Inventive Systems and Control (ICISC)*, 2018: IEEE, pp. 1069-1073.

[17] T. N. D. P. Holkar Vaijayanti, "Automatic Gate Control System Using Image Processing," *International Journal Of Innovative Research In Technology,* vol. 6, no. 11, pp. 579–583, 2020.

[18] A. Molavi, G. J. Lim, and B. Race, "A framework for building a smart port and smart port index," *International journal of sustainable transportation,* vol. 14, no. 9, pp. 686-700, 2020.

[19] N. Prabhakaran, V. Srivaishnavi, V. Srinaya, T. Preethi, S. Aishwarya, and M. Dinesh, "Automatic gate control for highly secure organization using RFID and GSM Technology," in *2020 International Conference on Computer Communication and Informatics (ICCCI)*, 2020: IEEE, pp. 1-4.

[20] S. Shanthi, "Automatic Gate using Face Recognition Technique using HAAR Cascade Algorithm," *International Journal of Engineering and Advanced Technology (IJEAT),* vol. 9, no. 3, pp. 1302-1305, 2020.

[21] S. Jalapur and A. Maniyar, "Door lock system using cryptographic algorithms based on IOT," *International Research Journal of Engineering and Technology,* 2020.

[22] P. Elechi, C. Ahiakwo, and S. Shir, "Design and implementation of an automated security gate system using global system for mobile communication network," *Journal of Network and Computer Applications,* vol. 7, no. 1, pp. 1-10, 2021.

[23] A. Y. Cil, D. Abdurahman, and I. Cil, "Internet of Things enabled real time cold chain monitoring in a container port," *Journal of Shipping and Trade,* vol. 7, no. 1, pp. 1-26, 2022.

[24] M. A. Ben Farah *et al.*, "Cyber security in the maritime industry: A systematic survey of recent advances and future trends," *Information,* vol. 13, no. 1, p. 22, 2022.

[25] D. Barki and L. Deleze-Black, "Review of maritime transport 2016," 2016.

[26] S. Bessid, A. Zouari, A. Frikha, and A. Benabdelhafid, "Smart ports design features analysis: A systematic literature review," in *13ème CONFERENCE INTERNATIONALE DE MODELISATION, OPTIMISATION ET SIMULATION (MOSIM2020), 12-14 Nov 2020, AGADIR, Maroc*, 2020.

References

[27] K. Douaioui, M. Fri, and C. Mabrouki, "Smart port: Design and perspectives," in *2018 4th International Conference on Logistics Operations Management (GOL)*, 2018: IEEE, pp. 1-6.

[28] https://www.nauticexpo.com/prod/konecranes/product-30447-189111.html (accessed.

[29] E. A. Bouman, E. Lindstad, A. I. Rialland, and A. H. Strømman, "State-of-the-art technologies, measures, and potential for reducing GHG emissions from shipping–A review," *Transportation Research Part D: Transport and Environment*, vol. 52, pp. 408-421, 2017.

[30] S. Saxon and M. Stone, "Container shipping: The next 50 years," 2017.

[31] M. Jović, N. Kavran, S. Aksentijević, and E. Tijan, "The transition of Croatian seaports into smart ports," in *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2019: IEEE, pp. 1386-1390.

[32] G. Giuliano and T. O'Brien, "Reducing port-related truck emissions: The terminal gate appointment system at the Ports of Los Angeles and Long Beach," *Transportation Research Part D: Transport and Environment*, vol. 12, no. 7, pp. 460-473, 2007.

[33] L. Heilig and S. Voß, "A cloud-based SOA for enhancing information exchange and decision support in ITT operations," in *Computational Logistics: 5th International Conference, ICCL 2014, Valparaiso, Chile, September 24-26, 2014. Proceedings 5*, 2014: Springer, pp. 112-131.

[34] D. Ashbrook and T. Starner, "Using GPS to learn significant locations and predict movement across multiple users," *Personal and Ubiquitous computing*, vol. 7, pp. 275-286, 2003.

[35] S. Aslam, M. P. Michaelides, and H. Herodotou, "Internet of ships: A survey on architectures, emerging applications, and challenges," *IEEE Internet of Things journal*, vol. 7, no. 10, pp. 9714-9727, 2020.

[36] K.-L. A. Yau, S. Peng, J. Qadir, Y.-C. Low, and M. H. Ling, "Towards smart port infrastructures: Enhancing port activities using information and communications technology," *Ieee Access*, vol. 8, pp. 83387-83404, 2020.

[37] N. Zrnić, Z. Petković, and S. Bošnjak, "Automation of ship-to-shore container cranes: A review of state-of-the-art," *FME Transactions*, vol. 33, no. 3, pp. 111-121, 2005.

[38] A. Bhimani and M. Sisson, "Increasing quayside productivity," in *Pan Pacific Conference, Oakland, CA, USA*, 2002.

[39] P. Sun and P. Sun, "5GtoB enables enterprise production," *Unleashing the Power of 5GtoB in Industries*, pp. 41-58, 2021.

[40] ed.

[41] "5G Smart Port White Paper," White paper, 2019.

References

[42] P. Blaiklock. (2017) Automated Stacking Cranes In Port Terminals. *The E-Journal of Port and Terminals*.

[43] ABB, ed, 2019https://new.abb.com/news/detail/24698/next-level-remote-operations-the-remote-crane-operator-and-beyond.

[44] https://www.gs-yuasa.com/en/newsrelease/article.php?ucode=gs180311554116_522 (accessed.

[45] P. S. Pratama, T. H. Nguyen, H. K. Kim, D. H. Kim, and S. B. Kim, "Positioning and obstacle avoidance of automatic guided vehicle in partially known environment," *International Journal of Control, Automation and Systems*, vol. 14, pp. 1572-1581, 2016.

[46] J. Zhang, P. A. Ioannou, and A. Chassiakos, "Automated container transport system between inland port and terminals," *ACM Transactions on Modeling and Computer Simulation (TOMACS)*, vol. 16, no. 2, pp. 95-118, 2006.

[47] P. Doan, T. Nguyen, V. Dinh, H. Kim, and S. Kim, "Path tracking control of automatic guided vehicle using camera sensor," in *Proceedings of the 1st International Symposium on Automotive and Convergence Engineering*, 2011, pp. 20-26.

[48] P. S. Pratama, B. T. Luan, T. P. Tran, H. K. Kim, and S. B. Kim, "Trajectory tracking algorithm for automatic guided vehicle based on adaptive backstepping control method," in *AETA 2013: Recent Advances in Electrical Engineering and Related Sciences*, 2014: Springer, pp. 535-544.

[49] C. Chao, W. Bing, and Y. Qingtai, "Application of automated guided vehicle (AGV) based on inductive guidance for newsprint rolls transportation system [J]," *Journal of Donghua University*, vol. 21, no. 2, pp. 88-92, 2004.

[50] Y.-S. Chen and L. Yao, "Robust type-2 fuzzy control of an automatic guided vehicle for wall-following," in *2009 International conference of soft computing and pattern recognition*, 2009: IEEE, pp. 172-177.

[51] S.-Y. Lee and H.-W. Yang, "Navigation of automated guided vehicles using magnet spot guidance method," *Robotics and Computer-Integrated Manufacturing*, vol. 28, no. 3, pp. 425-436, 2012.

[52] C. I. Liu, H. Jula, K. Vukadinovic, and P. A. Ioannou, "Comparing different technologies for containers movement in marine container terminals," in *ITSC2000. 2000 IEEE Intelligent Transportation Systems. Proceedings (Cat. No. 00TH8493)*, 2000: IEEE, pp. 488-493.

[53] J. Riedl, F.-X. Delenclos, and A. Rasmussen, "To Get Smart, Ports Go Digital," *Boston Consulting Group*, vol. 11, 2018.

[54] L. Heilig and S. Voß, "Information systems in seaports: a categorization and overview," *Information Technology and Management*, vol. 18, pp. 179-201, 2017.

References

[55] J. Zhang and C. Zhang, "Smart container security: the E-seal with RFID technology," *Modern Applied Science,* vol. 1, no. 3, pp. 16-18, 2007.

[56] "E-Seal," ed.

[57] Ç. Iris and J. S. L. Lam, "A review of energy efficiency in ports: Operational strategies, technologies and energy management systems," *Renewable and Sustainable Energy Reviews,* vol. 112, pp. 170-182, 2019.

[58] J.-K. Woo, D. S. Moon, and J. S. L. Lam, "The impact of environmental policy on ports and the associated economic opportunities," *Transportation Research Part A: Policy and Practice,* vol. 110, pp. 234-242, 2018.

[59] G. Wilmsmeier and T. Spengler, "Energy consumption and container terminal efficiency," 2016.

[60] T. Zis, R. J. North, P. Angeloudis, W. Y. Ochieng, and M. G. Harrison Bell, "Evaluation of cold ironing and speed reduction policies to reduce ship emissions near and at ports," *Maritime Economics & Logistics,* vol. 16, pp. 371-398, 2014.

[61] E. A. Sciberras, B. Zahawi, and D. J. Atkinson, "Electrical characteristics of cold ironing energy supply for berthed ships," *Transportation Research Part D: Transport and Environment,* vol. 39, pp. 31-43, 2015.

[62] T. Coppola, M. Fantauzzi, S. Miranda, and F. Quaranta, "Cost/benefit analysis of alternative systems for feeding electric energy to ships in port from ashore," in *2016 AEIT International Annual Conference (AEIT)*, 2016: IEEE, pp. 1-7.

[63] W. J. Hall, "Assessment of CO2 and priority pollutant reduction by installation of shoreside power," *Resources, Conservation and Recycling,* vol. 54, no. 7, pp. 462-467, 2010.

[64] T. K. Tran, "Study of electrical usage and demand at the container terminal," Deakin University, 2012.

[65] G. Parise and A. Honorati, "Port cranes with energy balanced drive," in *2014 AEIT Annual Conference-From Research to Industry: The Need for a More Effective Technology Transfer (AEIT)*, 2014: IEEE, pp. 1-5.

[66] D. Colarossi and P. Principi, "Technical analysis and economic evaluation of a complex shore-to-ship power supply system," *Applied Thermal Engineering,* vol. 181, p. 115988, 2020.

[67] J. C. Rijsenbrij and A. Wieschemann, "Sustainable container terminals: a design approach," in *Handbook of terminal planning*: Springer, 2011, pp. 61-82.

[68] M. Acciaro *et al.*, "Environmental sustainability in seaports: a framework for successful innovation," *Maritime Policy & Management,* vol. 41, no. 5, pp. 480-500, 2014.

[69] S. Song and K. Poh, "Solar PV leasing in Singapore: enhancing return on investments with options," in *IOP Conference Series: Earth and Environmental Science*, 2017, vol. 67, no. 1: IOP Publishing, p. 012020.

References

[70] M. Acciaro, H. Ghiara, and M. I. Cusano, "Energy management in seaports: A new role for port authorities," *Energy Policy,* vol. 71, pp. 4-12, 2014.

[71] Y. Du, Q. Chen, J. S. L. Lam, Y. Xu, and J. X. Cao, "Modeling the impacts of tides and the virtual arrival policy in berth allocation," *Transportation Science,* vol. 49, no. 4, pp. 939-956, 2015.

[72] https://www.jp.com.sg/about-us/awards-and-milestones, "Jurong port," ed.

[73] H. Im, J. Yu, and C. Lee, "Truck appointment system for cooperation between the transport companies and the terminal operator at container terminals," *Applied Sciences,* vol. 11, no. 1, p. 168, 2020.

[74] T. Pious, K. Sujina, and K. Sneha, "Finger print based automatic door lock system," *Int. J. Adv. Res. Electr. Electron. Instrum. Eng,* vol. 6, no. 4, 2017.

[75] I. Vasim, K. Akshay, and M. P. SB, "Rack and pinion operated automatic sliding gate," *Global Journal of engineering science and researchers*, pp. 111-114, 2016.

[76] S. Yadav, "RFID Implemented Parking System," *International Journal of Information and Computation Technology,* vol. 4, no. 4, pp. 369-372, 2014.

[77] F. Chetouane, "An overview on RFID technology instruction and application," *IFAC-PapersOnLine,* vol. 48, no. 3, pp. 382-387, 2015.

[78] D. Kaur and J. Sengupta, "Survey paper on RFID: radio frequency identification," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 39, no. 2, pp. 72-78, 2016.

[79] M. Chen and S. Chen, *RFID technologies for internet of things*. Springer, 2016.

[80] S. Nainan, R. Parekh, and T. Shah, "RFID technology based attendance management system," *arXiv preprint arXiv:1306.5381,* 2013.

[81] D. Parkash, T. Kundu, and P. Kaur, "The RFID technology and its applications: a review," *International Journal of Electronics, Communication & Instrumentation Engineering Research and Development (IJECIERD),* vol. 2, no. 3, pp. 109-120, 2012.

[82] K. Ahsan, H. Shah, and P. Kingston, "The role of enterprise architecture in healthcare-IT," in *2009 Sixth International Conference on Information Technology: New Generations*, 2009: IEEE, pp. 1462-1467.

[83] S. Samadi, "Applications and opportunities for radio frequency identification (RFID) technology in intelligent transportation systems: A case study," *International Journal of Information and Electronics Engineering*, vol. 3, no. 3, pp. 341-345, 2013.

[84] M. Massoud, M. Sabee, M. Gergais, and R. Bakhit, "Automated new license plate recognition in Egypt," *Alexandria Engineering Journal*, vol. 52, no. 3, pp. 319-326, 2013.

[85] M. S. Rahman, M. Mostakim, M. S. Nasrin, and M. Z. Alom, "Bangla license plate recognition using convolutional neural networks (CNN)," in *2019 22nd*

International Conference on Computer and Information Technology (ICCIT), 2019: IEEE, pp. 1-6.

[86] H. Rajput, T. Som, and S. Kar, "An automated vehicle license plate recognition system," *Computer*, vol. 48, no. 8, pp. 56-61, 2015.

[87] C. Patel, D. Shah, and A. Patel, "Automatic number plate recognition system (anpr): A survey," *International Journal of Computer Applications*, vol. 69, no. 9, 2013.

[88] N. K. Ibrahim, E. Kasmuri, N. A. Jalil, M. A. Norasikin, S. Salam, and M. R. M. Nawawi, "License plate recognition (LPR): a review with experiments for Malaysia case study," *arXiv preprint arXiv:1401.5559*, 2014.

[89] Z. Saad, M. S. Sulaiman, R. Seman, Z. H. C. Soh, and F. Pazli, "SMART AUTOGATE USING OPTICAL CHARACTER RECOGNITION (OCR) AND COLOR DETECTION," *PalArch's Journal of Archaeology of Egypt/Egyptology*, vol. 17, no. 10, pp. 946-956, 2020.

[90] Lubna, N. Mufti, and S. A. A. Shah, "Automatic number plate Recognition: A detailed survey of relevant algorithms," *Sensors*, vol. 21, no. 9, p. 3028, 2021.

[91] I. S. Ahmad, B. Boufama, P. Habashi, W. Anderson, and T. Elamsy, "Automatic license plate recognition: A comparative study," in *2015 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, 2015: IEEE, pp. 635-640.

[92] R. Diarah, D. Egbune, and B. A. Adedayo, "Design and implementation of a microcontroller based automatic door and vistors counter," 2014.

[93] O. Shoewu and S. O. Olatinwo, "Design and Implementation of a Microcontroller Based Automatic Gate," *African Journal of Computing & ICT*, vol. 6, no. 1, pp. 21-32, 2013.

[94] S. Kumar, D. Rasaily, M. Mukhia, and A. Ashraf, "Biometric Attendance System using Microcontroller," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 32, no. 6, pp. 306-308, 2016.

[95] M. G. Vargas, F. E. Hoyos, and J. E. Candelo, "Portable and efficient fingerprint authentication system based on a microcontroller," *International journal of Electrical and Computer Engineering*, vol. 9, no. 4, p. 2346, 2019.

[96] J. Wan and L. Zhang, "Design of embedded fingerprint identification system based on TMS320C5515," in *2011 International Conference on Computer Science and Service System (CSSS)*, 2011: IEEE, pp. 3160-3163.

[97] D. K. Yadav, S. Singh, S. Pujari, and P. Mishra, "Fingerprint based attendance system using microcontroller and LabView," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 4, no. 6, pp. 5111-5121, 2015.

[98] D. Valdes-Ramirez *et al.*, "A Review of Fingerprint Feature Representations and Their Applications for Latent Fingerprint Identification: Trends and Evaluation," *IEEE Access*, vol. 7, no. 1, pp. 48484-48499, 2019.

References

[99] I. Rahman, A. Razzaq, and U. Ali, "A review on fingerprints recognition system," *J Comput Sci Syst Biol,* vol. 11, pp. 286-9, 2018.

[100] A. S. Abdalkafor and S. A. Aliesawi, "Applying of (SOM, HAC, and RBF) algorithms for data aggregation in wireless sensors networks," *Bulletin of Electrical Engineering and Informatics,* vol. 11, no. 1, pp. 354-363, 2022.

[101] A. Y. Ardiansyah and R. Sarno, "Performance analysis of wireless sensor network with load balancing for data transmission using xbee zb module," *Indones. j. electr. eng. comput. sci,* vol. 18, pp. 88-100, 2020.

[102] S. J. Ramson and D. J. Moni, "Applications of wireless sensor networks—A survey," in *2017 international conference on innovations in electrical, electronics, instrumentation and media technology (ICEEIMT)*, 2017: IEEE, pp. 325-329.

[103] P. Dhillon and H. Sadawarti, "A review paper on zigbee (ieee 802.15. 4) standard," *International journal of engineering research and technology,* vol. 3, 2014.

[104] R. Sudarmani, K. Venusamy, S. Sivaraman, P. Jayaraman, K. Suriyan, and M. Alagarsamy, "Machine to machine communication enabled internet of things: a review," *International Journal of Reconfigurable and Embedded Systems,* vol. 11, no. 2, p. 126, 2022.

[105] S. Schaefer, "Secure trade lane: a sensor network solution for more predictable and more secure container shipments," in *Companion to the 21st ACM SIGPLAN symposium on Object-oriented programming systems, languages, and applications*, 2006, pp. 839-845.

[106] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future generation computer systems,* vol. 29, no. 7, pp. 1645-1660, 2013.

[107] M. M. Subashini, S. Das, S. Heble, U. Raj, and R. Karthik, "Internet of things based wireless plant sensor for smart farming," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 10, no. 2, pp. 456-468, 2018.

[108] I. Salehin, S. Noman, I. J. Baki-Ul-Islam, P. Bishnu, U. Habiba, and N. Nessa, "IFSG: Intelligence agriculture crop-pest detection system using IoT automation system," *November 2021, Indonesian Journal of Electrical Engineering and Computer Science,* vol. 24, no. 2, p. 1091, 2021.

[109] J. Mona, "Data communication in internet of things: Vision, challenges and future direction," *Telkomnika (Telecommunication Computing Electronics and Control),* vol. 16, no. 5, pp. 2057-2062, 2018.

[110] R. H. Putra, F. T. Kusuma, T. N. Damayanti, and D. N. Ramadan, "IoT: smart garbage monitoring using android and real time database," *TELKOMNIKA (Telecommunication Computing Electronics and Control),* vol. 17, no. 3, pp. 1483-1491, 2019.

References

[111] F. Kamaruddin, N. N. N. Abd Malik, N. A. Murad, N. M. a. A. Latiff, S. K. S. Yusof, and S. A. Hamzah, "IoT-based intelligent irrigation management and monitoring system using arduino," *TELKOMNIKA (Telecommunication Computing Electronics and Control),* vol. 17, no. 5, pp. 2378-2388, 2019.

[112] M. Eriyadi, A. G. Abdullah, H. Hasbullah, and S. B. Mulia, "Internet of things and fuzzy logic for smart street lighting prototypes," *Int J Artif Intell ISSN,* vol. 2252, no. 8938, p. 8938, 2021.

[113] H. Ouldzira, A. Mouhsen, H. Lagraini, M. Chhiba, A. Tabyaoui, and S. Amrane, "Remote monitoring of an object using a wireless sensor network based on NODEMCU ESP8266," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 16, no. 3, pp. 1154-1162, 2019.

[114] J. Panigrahi, C. Padhy, D. Sen, J. Swain, and O. Larsen, "Optimal ship tracking on a navigation route between two ports: a hydrodynamics approach," *Journal of marine science and technology,* vol. 17, pp. 59-67, 2012.

[115] C.-M. Yeoh *et al.*, "Ubiquitous containerized cargo monitoring system development based on wireless sensor network technology," *International Journal of Computers Communications & Control,* vol. 6, no. 4, pp. 779-793, 2011.

[116] A. Belfkih, C. Duvallet, and B. Sadeg, "The Internet of Things for smart ports: Application to the port of Le Havre," *Proceedings of IPaSPort,* vol. 2017, no. May, 2017.

[117] R. Jamshidi and M. M. S. Esfahani, "A novel hybrid method for supply chain optimization with capacity constraint and shipping option," *The International Journal of Advanced Manufacturing Technology,* vol. 67, pp. 1563-1575, 2013.

[118] H.-C. Burmeister, W. Bruhn, Ø. J. Rødseth, and T. Porathe, "Autonomous unmanned merchant vessel and its contribution towards the e-Navigation implementation: The MUNIN perspective," *International Journal of e-Navigation and Maritime Economy,* vol. 1, pp. 1-13, 2014.

[119] S. Jain and M. A. Alam, "Comparative Study of Traditional Database and Cloud Computing Database," *International Journal of Advanced Research in Computer Science,* vol. 8, no. 2, 2017.

[120] W. Al Shehri, "Cloud database database as a service," *International Journal of Database Management Systems,* vol. 5, no. 2, p. 1, 2013.

[121] A. Kousalya and N.-k. Baik, "Enhance cloud security and effectiveness using improved RSA-based RBAC with XACML technique," *International Journal of Intelligent Networks,* vol. 4, pp. 62-67, 2023.

[122] M. A. Omer, A. A. Yazdeen, H. S. Malallah, and L. M. Abdulrahman, "A Survey on Cloud Security: Concepts, Types, Limitations, and Challenges," *Journal of Applied Science and Technology Trends,* vol. 3, no. 02, pp. 47-57, 2022.

References

[123] Y. Alghofaili, A. Albattah, N. Alrajeh, M. A. Rassam, and B. A. S. Al-Rimy, "Secure cloud infrastructure: A survey on issues, current solutions, and open challenges," *Applied Sciences*, vol. 11, no. 19, p. 9005, 2021.

[124] P. Sonia and R. Malika, "A hybrid cloud security model for securing data on cloud," in *Proceedings of the Workshop on Computer Networks and Communications, Chennai, India*, 2021, vol. 1.

[125] S. Kumar, G. Karnani, M. S. Gaur, and A. Mishra, "Cloud security using hybrid cryptography algorithms," in *2021 2nd international conference on intelligent engineering and management (ICIEM)*, 2021: IEEE, pp. 599-604.

[126] Z. Luo, K. Shen, R. Hu, Y. Yang, and R. Deng, "Optimization of AES-128 Encryption Algorithm for Security Layer in ZigBee Networking of Internet of Things," *Computational Intelligence and Neuroscience*, vol. 2022, 2022.

[127] I. K. Dutta, B. Ghosh, and M. Bayoumi, "Lightweight cryptography for internet of insecure things: A survey," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019: IEEE, pp. 0475-0481.

[128] M. F. Mushtaq, S. Jamel, A. H. Disina, Z. A. Pindar, N. S. A. Shakir, and M. M. Deris, "A survey on the cryptographic encryption algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 11, 2017.

[129] K. Logunleko, O. Adeniji, and A. Logunleko, "A comparative study of symmetric cryptography mechanism on DES AES and EB64 for information security," *Int. J. Sci. Res. in Computer Science and Engineering*, vol. 8, no. 1, 2020.

[130] N. A. Al-gohany and S. Almotairi, "Comparative study of database security in cloud computing using AES and DES encryption algorithms," *Journal of Information Security and Cybercrimes Research*, vol. 2, no. 1, pp. 102-109, 2019.

[131] S. Ghosh, D. T. Biradar, G. Shinde, S. D. Bhojaned, and M. R. Shirapure, "Performance analysis of AES, DES, RSA and AES-DES-RSA hybrid algorithm for data security," *International Journal of Innovative and Emerging Research in Engineering*, vol. 2, no. 5, pp. 83-88, 2015.

[132] S. Fatima, T. Rehman, M. Fatima, S. Khan, and M. A. Ali, "Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing," *Engineering Proceedings*, vol. 20, no. 1, p. 14, 2022.

[133] M. Kannan, C. Priya, and S. VaishnaviSree, "A comparative analysis of DES, AES and RSA crypt algorithms for network security in cloud computing," *J Emerg Technol Innov Res (JETIR)*, vol. 6, no. 3, pp. 574-582, 2019.

[134] I. Al_Barazanchi, S. A. Shawkat, M. H. Hameed, and K. S. L. Al-Badri, "Modified RSA-based algorithm: A double secure approach," *TELKOMNIKA*

(Telecommunication Computing Electronics and Control), vol. 17, no. 6, pp. 2818-2825, 2019.

[135] O. Taylor and T. Victor, "Comparative analysis of cryptographic algorithms in securing data," *Int J Eng Trend Technol,* vol. 58, no. 3, 2018.

[136] R. Sobti and G. Geetha, "Cryptographic hash functions: a review," *International Journal of Computer Science Issues (IJCSI),* vol. 9, no. 2, p. 461, 2012.

[137] R. Chattamvelli, "A Symmetric Scheme for Securing Data in Cyber-Physical Systems/IoT Sensor-Based Systems based on AES and SHA256," *International Journal of Information Security and Cybercrime (IJISC),* vol. 11, no. 1, pp. 49-58, 2022.

[138] P. P. Pittalia, "A comparative study of hash algorithms in cryptography," *International Journal of Computer Science and Mobile Computing,* vol. 8, no. 6, pp. 147-152, 2019.

[139] D. Maltoni, D. Maio, A. K. Jain, and J. Feng, "Latent Fingerprint Recognition," *Handbook of Fingerprint Recognition,* pp. 339-383, 2022.

Appendix A

Customs declarations show the administrative and bureaucratic procedures that entail obtaining many licenses and long waits for the release of goods, resulting in additional costs for exporters.

كمارك العراق

التاريخ 12/02/2023
رقم منفذ الكمارك 9
رقم التسلسل الحدودي 38331
رقم التصريحة الكمركية الآلي 2302120980015

عنوان موقع
البريد الالكتروني

القسم أ : بيانات المستورد او الوكيل

رقم المستورد او الوكيل ---
اسم المستورد وزارة النفط/شركة المشاريع النفطيه
العنوان
بغداد
منيورتي 83
ح معن احمد

اسم الوكيل ----------
رقم هوية الوكيل
تاريخ هوية الوكيل

القسم ب : تحديد رسم

تفاصيل الارسالية	قيمة البضائع المعفاة	قيمة البضائع الخاضعة للضريبة
عدد 3 حاويه × 20 قدم 2129255+2723377+3857836 محمله على السيارات # 147192+155454+166206	198,000.00	0.00
تحتوي على 48 طرد مواد معالجة والعائده الى وزارة النفط/شركة المشاريع النفطيه وحسب الفاتوره ارساليه جديده المنشا الامارات العربيه تزن جمعا 62880 كغم	0.00	0.00
قرار 167 لسنة 2010 معفاة حسب كتاب العامه المرقم 10847 في 2022/8/11 وكتاب الجنوبيه المرقم 24942 في 2022/12/7 وحسب الوصل المرقم 6935544 في 2023/2/12	0.00	0.00

: تم تعديل حالة البضاعة الاصلية من قبل المشرف

المجموع بعملة القائمة: 198,000.00 0.00
المجموع بعد التعديل : 0.00
قيمة البضاعة (د. ع): 0.00
قيمة الرسم ####% بعملة القائمة : 0.00

القسم ج : سداد الضريبة

العملة دولار امريكي — سعر الصرف 1,320.00
رقم خطاب الضمان --- — اسم المصرف ---
رقم الصك --- — اسم المصرف ---
المخمن احمد طه — المدقق عباس محسن
المفتش بركات خلف/فواد طارق/خالد حسين
رقم وصل امين الصندوق

1- الضريبة المدفوعة (2+3): 0.00 (د. ع)
2- المبلغ النقدي : 0.00 (د. ع)
3- مبلغ الصك : 0.00 (د. ع)
4- المبلغ المؤجل : 0.00 (د. ع)

12/02/2023 11:58:45 Page 1 of 1

Appendix

القسم أ : بيانات المستورد او الوكيل

التاريخ 12/02/2023
رقم منفذ الكمارك 9
رقم التسلسل الحدودي 2276
رقم التصريحة الكمركية الآلي 2302120980016

رقم المستورد او الوكيل ---
اسم المستورد وزارة النفط/شركة المشاريع النفطيه
العنوان
بغداد
يوميفيمنت 63
ح معن احمد

الموقف من الاعفاء غير معفى
نوع النقل تجارة
وسيلة الاتصال
رقم الهاتف
رقم الفاكس
رقم الموبايل
عنوان موقع
البريد الالكتروني

اسم الوكيل ---------- رقم هوية الوكيل تاريخ هوية الوكيل

القسم ب : تحديد رسم

تفاصيل الارسالية	قيمة البضائع المعفاة	قيمة البضائع الخاضعة للضريبة
عدد 5 حاويه × 20 قدم 2138490+2527065+2856922+8126748+2502826 # محمله على السيارات 147348+130640+165555+38351+44380	373,250.00	0.00
تحتوي على 92 طرد مواد معالجه والعائده الى وزارة النفط شركة المشاريع النفطيه وحسب الفاتوره تزن جمعا 105620 كغم ارساليه جديده المنشا الامارات العربيه	0.00	0.00
قرار 167 لسنة 2010 معفاة حسب كتاب العامه المرقم 7966 في 2022/12/21 وكتاب الجنوبيه المرقم 24937 في 2022/12/7 وحسب الوصل المرقم 6935543 في 2023/2/12	0.00	0.00

: تم تعديل حالة البضاعة الاصلية من قبل المشرف

المجموع بعملة القائمة: 373,250.00 0.00
المجموع بعد التعديل : 0.00
قيمة البضاعة (د. ع): 0.00
قيمة الرسم ####% بعملة القائمة : 0.00

القسم ج : سداد الضريبة

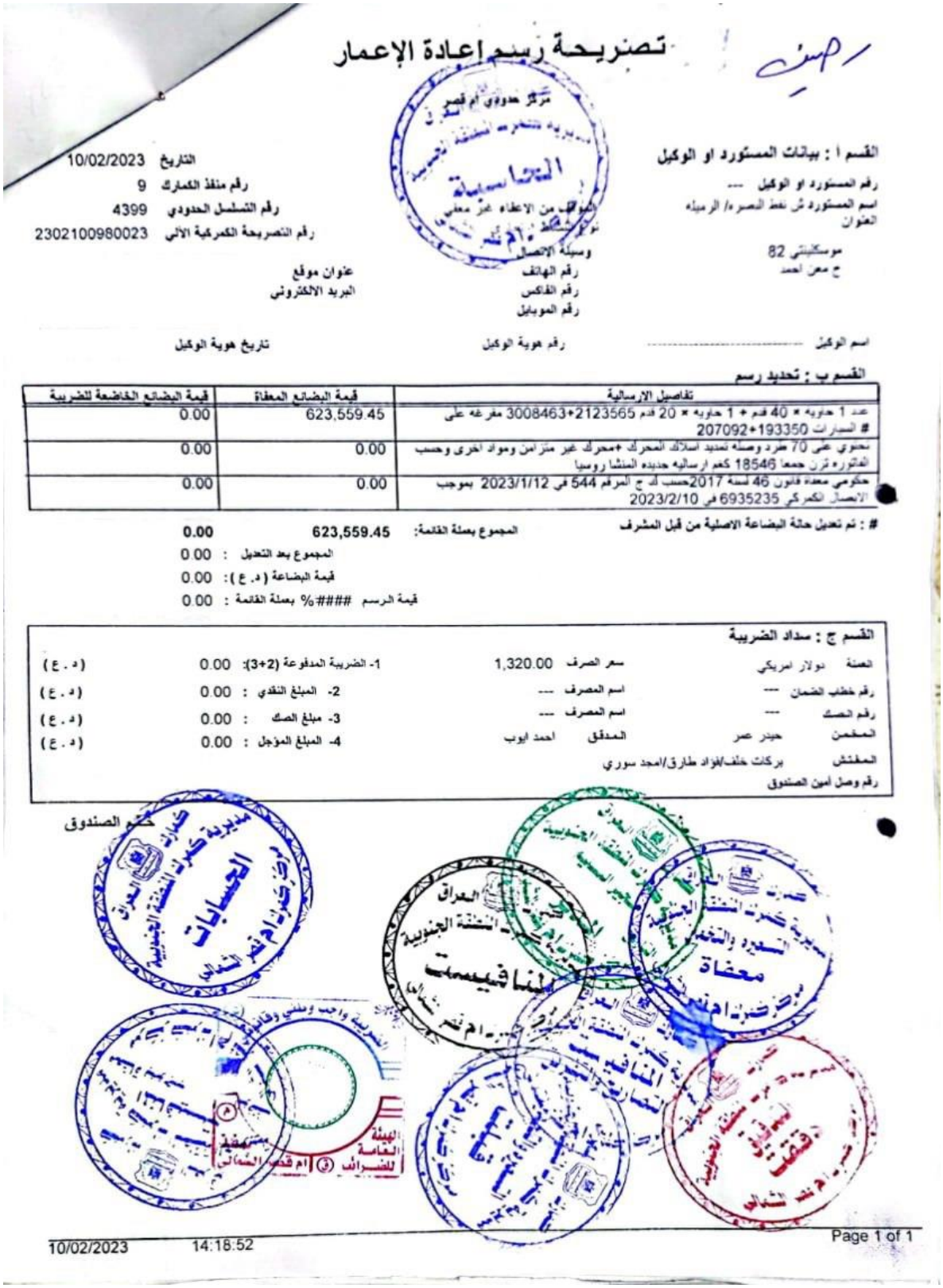
العملة دولار امريكي — سعر الصرف 1,320.00
رقم خطاب الضمان --- — اسم المصرف ---
رقم الصك --- — اسم المصرف ---
المخمن احمد طه — المدقق عباس محسن
المفتش بركات خلف/فواد طارق/خالد حسين
رقم وصل أمين الصندوق

1- الضريبة المدفوعة (2+3): 0.00 (د. ع)
2- المبلغ النقدي : 0.00 (د. ع)
3- مبلغ الصك : 0.00 (د. ع)
4- المبلغ المؤجل : 0.00 (د. ع)

ختم الصندوق

12/02/2023 11:59:50 Page 1 of 1

Appendix



تصريحة رسم إعادة الإعمار

مركز حدودي أم قصر

التاريخ 10/02/2023
رقم منفذ الكمارك 9
رقم التسلسل الحدودي 4399
رقم التصريحة الكمركية الآلي 2302100980023

القسم أ : بيانات المستورد او الوكيل

رقم المستورد او الوكيل ---
اسم المستورد ثن نفط المصرد/ الرميله
العنوان
موسكلينتي 82
ح معن احمد

عنوان موقع
البريد الالكتروني

وسيلة الاتصال
رقم الهاتف
رقم الفاكس
رقم الموبايل

اسم الوكيل ..... رقم هوية الوكيل تاريخ هوية الوكيل

القسم ب : تحديد رسم

تفاصيل الارسالية	قيمة البضائع المعفاة	قيمة البضائع الخاضعة للضريبة
عدد 1 حاويه × 40 قدم + 1 حاويه × 20 قدم 2123565+3008463 مفرغه على # السيارات 193350+207092	623,559.45	0.00
يحتوي على 70 طرد وصله تمديد اسلاك المحرك +محرك غير منزامن ومواد اخرى وحسب الفاتوره ترن جمعا 18546 كغم ارساليه جديده المنشا روسيا	0.00	0.00
حكومي معفاء قانون 46 لسنة 2017حسب اد ج المرقم 544 في 2023/1/12 بموجب الاتصال الكمركي 6935235 في 2023/2/10	0.00	0.00

: تم تعديل حالة البضاعة الاصلية من قبل المشرف

المجموع بعملة القائمة: 623,559.45 0.00
المجموع بعد التعديل : 0.00
قيمة البضاعة (د . ع): 0.00
قيمة الرسم ####% بعملة القائمة : 0.00

القسم ج : سداد الضريبة

العملة دولار امريكي — سعر الصرف 1,320.00
رقم خطاب الضمان --- — اسم المصرف ---
رقم الحسك --- — اسم المصرف ---
المخلص حيدر عصر — المدقق احمد ايوب
المفتش بركات خلف/فؤاد طارق/امجد سوري
رقم وصل امين الصندوق

1- الضريبة المدفوعة (2+3): 0.00 (د . ع)
2- المبلغ النقدي : 0.00 (د . ع)
3- مبلغ الصك : 0.00 (د . ع)
4- المبلغ المؤجل : 0.00 (د . ع)

ختم الصندوق

10/02/2023 14:18:52 Page 1 of 1

Appendix B

A sample of the real-time data obtained from the Umm Qasr Port Administration.

رقم الحاوية container no	FWRU0116023	CMAU6765352	CMAU4276270	CMAU4201543	FCIU9284037
الحجم size	40	40	40	40	40
نوع الحاوية type	HC	HC	HC	HC	HC
المستفيد customer	TARIQ AL RAIDA LI TIJARIT	GREEN PEARL COMPANY	GOODS CONSIGNED	GOODS CONSIGNED	GOODS CONSIGNED
البضاعة good	850213/Generating sets with compression-ignition internal combustio	382311/Stearic acid industrial	843629/Poultry-keeping machinery (excl. machines for sorting or gra	843629/Poultry-keeping machinery (excl. machines for sorting or gra	843629/Poultry-keeping machinery (excl. machines for sorting or gra
الوزن weight	22290	28966	17024.35	19775.5	17021.55
طبيعة الحاوية Danger					
وكيل الباخرة SHIP AGENT	STATE AGENT	STATE AGENT	STATE AGENT	STATE AGENT	STATE AGENT
خط الحاوية line Container	CMA	CMA	CMA	CMA	CMA

Appendix C

Pictures of the port of Umm Qasr in Iraq and another of the port of Rotterdam in the Netherlands showing the difference between the two ports.

Umm Qasr Port

Rotterdam: One of Today's Smartest Ports

Rotterdam: One of Today's Smartest Ports

Appendix D

HC-SR04 Ultrasonic Sensor

Elijah J. Morgan

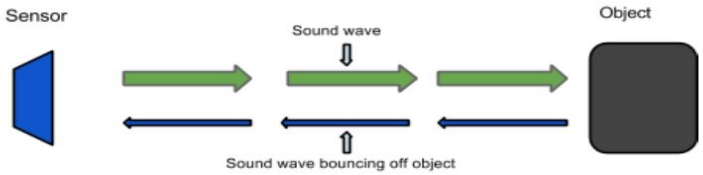
Nov. 16 2014

The purpose of this file is to explain how the HC-SR04 works. It will give a brief explanation of how ultrasonic sensors work in general. It will also explain how to wire the sensor up to a microcontroller and how to take/interpret readings. It will also discuss some sources of errors and bad readings.

1. **How Ultrasonic Sensors Work**
2. **HC-SR04 Specifications**
3. **Timing chart, Pin explanations and Taking Distance Measurements**
4. **Wiring HC-SR04 with a microcontroller**
5. **Errors and Bad Readings**

1. How Ultrasonic Sensors Work

Ultrasonic sensors use sound to determine the distance between the sensor and the closest object in its path. How do ultrasonic sensors do this? Ultrasonic sensors are essentially sound sensors, but they operate at a frequency above human hearing.



The sensor sends out a sound wave at a specific frequency. It then listens for that specific sound wave to bounce off of an object and come back (Figure 1). The sensor keeps track of the time between sending the sound wave and the sound wave returning. If you know how fast something is going and how long it is traveling you can find the distance traveled with equation 1.

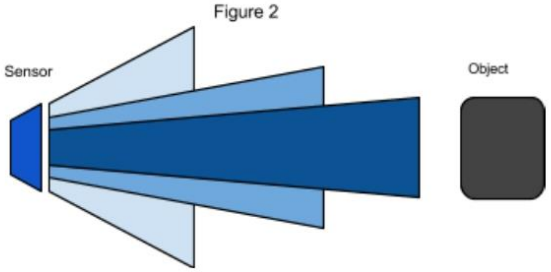
Equation 1. $d = v \times t$

The speed of sound can be calculated based on the a variety of atmospheric conditions, including temperature, humidity and pressure. Actually calculating the distance will be shown later on in this document.

It should be noted that ultrasonic sensors have a cone of detection, the angle of this cone varies with distance, Figure 2 show this relation. The ability of a sensor to

detect an object also depends on the objects orientation to the sensor. If an object doesn't present a flat surface to the sensor then it is possible the sound wave will bounce off the object in a way that it does not return to the sensor.

Figure 2



2. HC-SR04 Specifications

The sensor chosen for the Firefighting Drone Project was the HC-SR04. This section contains the specifications and why they are important to the sensor module. The sensor modules requirements are as follows.

- Cost
- Weight
- Community of hobbyists and support
- Accuracy of object detection
- Probability of working in a smoky environment
- Ease of use

The HC-SR04 Specifications are listed below. These specifications are from the Cytron Technologies HC-SR04 User's Manual (source 1).

- Power Supply: +5V DC
- Quiescent Current: <2mA
- Working current: 15mA
- Effectual Angle: <15º
- Ranging Distance: 2-400 cm
- Resolution: 0.3 cm
- Measuring Angle: 30º
- Trigger Input Pulse width: 10uS
- Dimension: 45mm x 20mm x 15mm
- Weight: approx. 10 g

The HC-SR04's best selling point is its price; it can be purchased at around $2 per unit.

3. Timing Chart and Pin Explanations

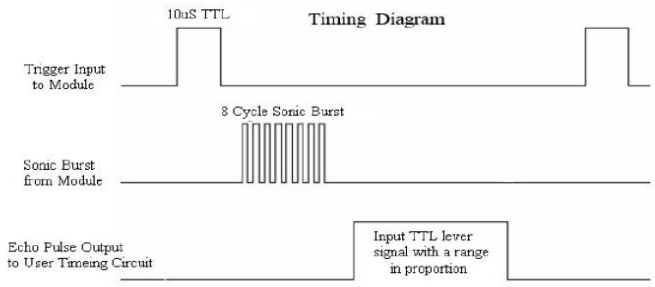
The HC-SR04 has four pins, VCC, GND, TRIG and ECHO; these pins all have different functions. The VCC and GND pins are the simplest -- they power the HC-SR04. These pins need to be attached to a +5 volt source and ground respectively. There is a single control pin: the TRIG pin. The TRIG pin is responsible for sending the ultrasonic burst. This pin should be set to HIGH for 10 μs, at which point the HC-SR04 will send out an eight cycle sonic burst at 40 kHZ. After a sonic burst has been sent the ECHO pin will go HIGH. The ECHO pin is the data pin -- it is used in taking distance measurements. After an ultrasonic burst is sent the pin will go HIGH, it will stay high until an ultrasonic burst is detected back, at which point it will go LOW.

Taking Distance Measurements

The HC-SR04 can be triggered to send out an ultrasonic burst by setting the TRIG pin to HIGH. Once the burst is sent the ECHO pin will automatically go HIGH. This pin will remain HIGH until the the burst hits the sensor again. You can calculate the distance to the object by keeping track of how long the ECHO pin stays HIGH. The time ECHO stays HIGH is the time the burst spent traveling. Using this measurement in equation 1 along with the speed of sound will yield the distance travelled. A summary of this is listed below, along with a visual representation in Figure 2.

1. Set TRIG to HIGH
2. Set a timer when ECHO goes to HIGH
3. Keep the timer running until ECHO goes to LOW
4. Save that time
5. Use equation 1 to determine the distance travelled

Figure 3
Source 2



Source 2

To interpret the time reading into a distance you need to change equation 1. The clock on the device you are using will probably count in microseconds or smaller. To use equation 1 the speed of sound needs to determined,which is 343 meters per second at standard temperature and pressure. To convert this into more useful form use equation 2 to change from meters per second to microseconds per centimeter. Then equation 3 can be used to easily compute the distance in centimeters.

Equation 2. $Distance = \frac{Speed}{170.15\ m} \times \frac{Meters}{100\ cm} \times \frac{1e6\ \mu S}{170.15\ m} \times \frac{58.772\ \mu S}{cm}$

Equation 3. $Distance = \frac{time}{58} = \frac{\mu s}{\mu s/cm} = cm$

4. Wiring the HC-SR04 to a Microcontroller

This section only covers the hardware side. For information on how to integrate the software side, look at one of the links below or look into the specific microcontroller you are using.

The HC-SR04 has 4 pins: VCC, GND, TRIG and ECHO.

1. VCC is a 5v power supply. This should come from the microcontroller
2. GND is a ground pin. Attach to ground on the microcontroller.
3. TRIG should be attached to a GPIO pin that can be set to HIGH
4. ECHO is a little more difficult. The HC-SR04 outputs 5v, which could destroy many microcontroller GPIO pins (the maximum allowed voltage varies). In order to step down the voltage use a single resistor or a voltage divider circuit. Once again this depends on the specific microcontroller you are using, you will need to find out its GPIO maximum voltage and make sure you are below that.

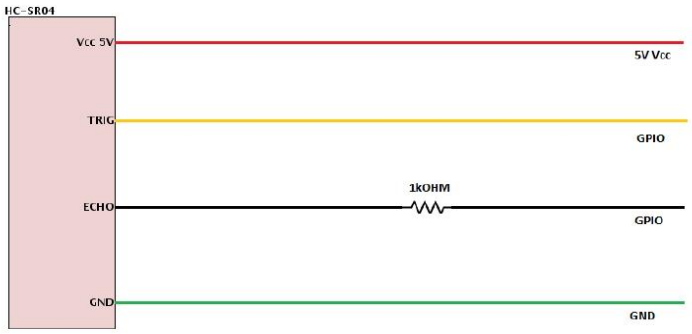
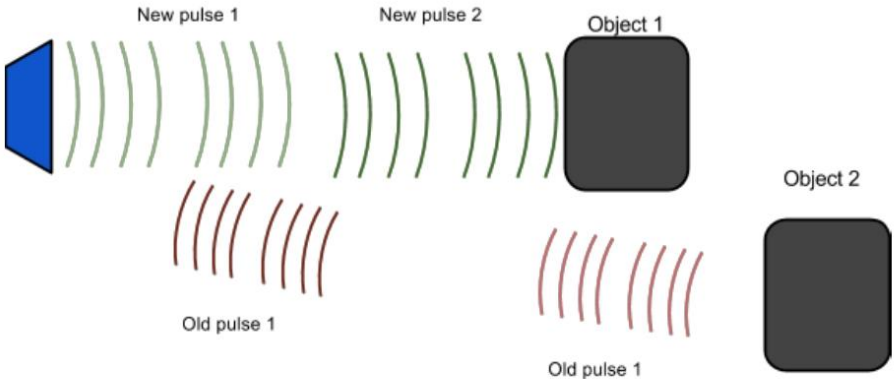


Figure 4

5. Errors and Bad Readings

Ultrasonic sensors are great sensors -- they work well for many applications where other types of sensors fall short. Unfortunately, they do have weaknesses. These weaknesses can be mitigated and worked around, but first they must be understood. The

first weakness is that they use sound. There is a limit to how fast ultrasonic sensors can get distance measurements. The longer the distance, the slower they are at reporting the distance. The second weakness comes from the way sound bounces off of objects. In enclosed spaces it is possible, if not probable that there will be unintended echos. The echos can very easily cause false short readings. In Figure 2 a pulse was sent out. It bounced off of object 1 and returned to the sensor. The distance was recorded and then a new pulse was sent. There was another object farther away, so that when the new pulse reaches object 1, the first signal will reach the sensor. This will cause the sensor to think that there is an object closer than is actually true. The old pulse is smaller than the new pulse because it has grown weaker. The longer the pulse exists the weaker it grows until it is negligible. If multiple sensors are being used, the number of echos will increase along with the number of errors. There are two main ways to reduce the number of errors. The first is to provide shielding around the sensor. This prevents echos coming in from angle outside what the sensor should actually pick up. The second is to reduce the frequency at which pulses are sent out. This gives more time for the echos to dissipate.



Appendix E

R307 Fingerprint Module

R307 Fingerprint Module consists of optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other functions.

FEATURES:

• Perfect function: independent fingerprint collection, fingerprint registration, fingerprint comparison (1: 1) and fingerprint search (1: N) function.

• Small size: small size, no external DSP chip algorithm, has been integrated, easy to install, less fault.

• Ultra-low power consumption: low power consumption of the product as a whole, suitable for low-power requirements of the occasion.

• Anti-static ability: a strong anti-static ability, anti-static index reached 15KV above.

• Application development is simple: developers can provide control instructions, self-fingerprint application product development, without the need for professional knowledge of fingerprinting.

• Adjustable security level: suitable for different applications, security levels can be set by the user to adjust.

Appendix

• Finger touch sensing signal output, low effective, sensing circuit standby current is very low, less than 5uA.

SPECIFICATIONS:

• Supply voltage: DC 4.2 ~ 6.0V

• Supply current: Working current: 50mA (typical) Peak current: 80mA

• Fingerprint image input time: <0.3 seconds

• Window area: 14x18 mm

• Matching method: Comparison method (1: 1)

• Search method (1: N)

• Characteristic file: 256 bytes

• Template file: 512 bytes

• Storage capacity: 1000 pieces

• Security Level: Five (from low to high: 1,2,3,4,5)

• Fake rate (FAR): <0.001%

• Refusal rate (FRR): <1.0%

• Search time: <1.0 seconds (1: 1000 hours, mean value)

• Host interface: UART \ USB1.1

• Communication baud rate (UART): (9600xN) bps Where N = 1 ~ 12 (default N = 6, ie 57600bps)

• Working environment: Temperature: -20 ℃ - +40 ℃ Relative humidity: 40% RH-85% RH (no condensation)

• Storage environment: Temperature: -40 ℃ - +85 ℃ Relative humidity: <85% H (no condensation).

للمرور عبر البوابة الذكية بنسبة ١٠٪ تقريبًا، وهو ما يعتمد على نوع السيارة. وتتوافق النتائج التجريبية مع النتائج التي تمت محاكاتها، مما يدل على أن النظام المقترح قوي وآمن وفعال للغاية في الاعتراف. ويساعد هذا النهج المبتكر على تخفيف تحديات الموانئ التقليدية من خلال تسهيل المعالجة، وبالتالي تعزيز الكفاءة والأداء.

وخلصت الدراسة إلى أن التطبيق التدريجي لتقنيات الموانئ الذكية في العراق يعد حلاً ممكناً لمواجهة التحديات القائمة ومساراً واعداً لتعزيز القدرة التنافسية العالمية للموانئ بشكل كبير. إن إطلاق البوابة الذكية لا يؤدي إلى زيادة الموثوقية والأمن فحسب، بل يساعد أيضًا في منع الفساد والتهريب، مما يجعلها خطوة أساسية نحو نظام موانئ حديث وفعال في العراق.

الخلاصة

أدى الارتفاع العالمي في التجارة البحرية الدولية إلى دفع الطبيعة التنافسية لإدارة الموانئ البحرية، مع التركيز على الكفاءة والأداء وخفض التكاليف. تستهدف هذه الدراسة على وجه التحديد التحديات والفرص داخل الموانئ العراقية، وتسليط الضوء على إنخفاض إدائها وانتاجيتها بسبب الحرب والعقوبات الاقتصادية، وارتفاع الفساد وعدم الكفاءة. ويتم اقتراح الحل الأمثل من خلال اعتماد تقنيات الموانئ المبتكرة لمواءمة الموانئ العراقية مع المنافسين العالميين.

محور البحث هو اقتراح البوابة الذكية لميناء أم قصر، ووضعها كخطوة أولى في نقل الموانئ العراقية إلى وظائف أكثر ابتكارا. تم بناء البوابة الذكية المقترحة بناءً على تقنيةRFID ، وأجهزة استشعار بصمات الأصابع، ونظام التعرف التلقائي على لوحة الترخيص للمصادقة، مع استخدام الحوسبة السحابية لتخزين البيانات ومعالجتها. يتم تبادل المعلومات بين البوابة الذكية والسحابة من خلال نظام أمني هجين لضمان السرية وسلامة المعلومات.

تمت محاكاة آلية بوابة المنفذ الذكية المبتكرة باستخدام MATLAB، مع خطوات فردية مصممة وفقًا لمجموعات بيانات محددة، مثل استخدام مجموعة بيانات FVC2002 لدقة بصمات الأصابع. وقد لوحظ أن دقة مطابقة بصمات الأصابع تصل إلى ٩٦,٦٪ عبر مجموعات البيانات المختلفة. بالإضافة إلى ذلك، تم تقييم التعرف على رخصة المركبة على الأرقام الأوروبية والعراقية باستخدام طريقة التعرف على القالب، وكانت الخوارزمية ناجحة في كلتا الحالتين. وتم بعد ذلك إجراء محاكاة شاملة، بما في ذلك البوابات الثلاث، والتحقق من عملها بصورة صحيحة.

تمت محاكاة أنظمة الأمان الهجينة، والتي تتكون من خوارزميات شائعة الاستخدام وهي AES، DES، وRSA، وتهجينها بخوارزمية التجزئة SHA256. أظهرت نتائج المحاكاة أن وقت التشفير وفك التشفير لـ RSA أبطأ بحوالي ١٠٠٠ مرة من وقت التشفير لـ AES. ولذلك، فإن الإنتاجية ستكون حوالي ١٠٠٠ مرة أقل من إنتاجية AES. أما قيمة العشوائية فكانت متساوية لجميع الخوارزميات، حوالي ٥,٩.

تم تنفيذ النظام المقترح عملياً باستخدام لغة البرمجة C# مع استخدام لغة SQL-Server لبرمجة قاعدة البيانات السحابية. لقد ثبت أن التنفيذ العملي لأتمتة منفذ البوابة الذكية يؤدي إلى تحسين الوقت الذي تستغرقه السيارة

جمهورية العراق
وزارة التعليم العالي والبحث العلمي
جامعة بابل
كلية الهندسة
قسم الهندسة الكهربائية

تصميم وتنفيذ منظومة بوابات لمنافذ ذكية آمنة

اطروحة

مقدمة إلى كلية الهندسة في جامعة بابل

وهي جزء من متطلبات الحصول على درجة الدكتوراه

فلسفة في هندسة الالكترونيك والاتصالات

من قبل

حيدر علي حسون

باشراف

الاستاذ الدكتور حسن جاسم مطلك

٢٠٢٣م **١٤٤٥ هـ**