ATM Vehicle Location Privacy and Security using End-to-End Quantum Key Cryptosystems

A UG PROJECT REPORT

Submitted by

MARISELVAM G (1905017)

in partial fulfilment for the award of the degree

of

BACHELOR OF ENGINEERING

in

ELECTRONICS AND COMMUNICATION ENGINEERING

PSN COLLEGE OF ENGINEERING AND TECHNOLOGY

(AUTONOMOUS)

MELATHEDIYOOR, TIRUNELVELI-627152

ANNA UNIVERSITY::CHENNAI 600025

APRIL 2023

BONAFIDE CERTIFICATE

This is to certify that this UG project report titled **"ATM Vehicle Location Privacy and Security using End-to-End Quantum Key Cryptosystems"** is a bonafide work of **MARISELVAM. G** (1905017) who carried out the UG project work under supervision. Certified further, that to the best of my knowledge the work reported herein does not form part of my any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this any other candidates.

SIGNATURE
Dr. T. RAJESH., M.E., PhD.,
HEAD OF THE DEPARTMENT,
Professor,
Department of ECE,
PSN College of Engineering
and Technology,
Melathediyoor,
Tirunelveli – 627152.

SIGNATURE
Mr. K. JEBASTIN., M.E.,
SUPERVISOR,
Associate Professor,
Department of ECE,
PSN College of Engineering
and Technology,
Melathediyoor,
Tirunelveli – 627152.

Submitted for the UG project viva-voce Examination held at the PSN College of Engineering and Technology, Tirunelveli on _____ .

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

I regard my grateful thanks to god almighty and beloved parents for their marvelous blessing showered on us to complete this dissertation successful. I would like to thank my honorable Chairman **Dr.P.SUYAMBU,** for providing all the facilities.

I am so grateful to express my heartfelt thanks and gratitude to Executive Director **Dr. P.SELVAKUMAR, Ph.D.,**

I furnish my special and profound gratitude to **Dr.V. MANIKANDAN,** Principal, PSN College of Engineering and Technology for giving opportunity to undertake this project work.

I would like to thank **Dr. T. RAJESH**, Head of the Department, Department of Electronics and Communication Engineering, for his support in completing my project.

The Project would have been a dream of darkness for me without the sparkle of guidance by my guide **Mr.K.JEBASTIN**, Department of Electronics and Communication Engineering. I am always thankful for his blessings, motivation, confidence, ideas and encouragement for doing this project.

I would like to thank the staff members of my department of their valuable suggestions in bringing out this project in the successful way.

ABSTRACT

Internet-of-things (IoT) is the latest revolution in electronic industry after internet. Smart appliances, portable computing devices, mobile phones and handheld system dominate in IoT, because large portions of world population use it. UG applications, mainly financial, e-commerce, information security and sensitive data-communication need special attention in terms of security. Device authentication, encryption, and key distribution are of vital importance to any Internet-of-Things (IoT) systems, such as the new smart city infrastructures. This is due to the concern that attackers could easily exploit the lack of strong security in IoT devices to gain unauthorized access to the system or to hijack IoT devices to perform denial-of-service attacks on other networks. This creates a strong requirement for providing security solutions into these devices. However, although scholars have designed a variety of authentication protocols for IoT environment, the resource costs of these protocols and security impact are still expensive for resource-constrained devices. In this project, we propose a novel lightweight IoT device authentication, encryption, and key distribution approach using Quantum Key Cryptosystems. The Quantum Key Cryptosystems adopt three types of end-to-end encryption schemes: Asymmetric, Device-key, and without keys. The experimental results demonstrate the potential of this novel approach as a promising security and privacy solution for the next-generation of IoT systems.

TABLE OF CONTENT

CHAPTER NO.	TITLE	PAGE
	ABSTRACT	v
	LIST OF FIGURES	v
	LIST OF ABBREVIATIONS	v
1	**INTRODUCTION**	
	1.1 Overview	1
	1.2 IoT Works	2
	1.3 Internet of Things Security	3
	1.4 Ojective of the project	3
2	**LITERATURE SURVEY**	
	2.1 Cryptography	5
	2.2 Types of Cryptography	5
	2.3 Quantum Cryptography	7
	2.4 Fields of application	8
	2.5 Literature survey	9
3	**SYSTEM ANALYSIS**	
	3.1Existing system	17
	3.2 Quantum Key Cryptography	18
	3.3 Proposed System	20
	3.4 Disadvantage	21
	3.5 Block Diagram	22
	3.6 System Architecture	23

4	**System specification** 4.1 Software specification 4.1.1 PHP 5 4.1.2 MySQL 4.1.3 WAMP Server 2.0 4.1.4 Bootstrap 4 4.1.5 Embedded C	 24 25 26 26 27
5	**Hardware specification** 5.1 Hardware specification 5.1.1 Arduino UNO. 5.1.2 Nano GPS 5.1.3 Esp8266 5.1.4 OLED Display	 28 30 31 34
6	**RESULTS AND DISCUSSION** 6.1 screenshots	35 37
7	**CONCULSION AND REFERENCES**	41

LIST OF FIGURES

FIGURE NO	TITLE	PAGE NO
Figure 1.1.	IoT	1
Figure 1.2	IoT Works	2
Figure 1.3	Secure Data in IoT Systems	3
Figure 3.2.1	QKD service channel	20
Figure 3.4	. Block Diagram	22
Figure 3.5	System Architecture	23
Figure 5.1	Arduino UNO	28
Figure 5.2	Nano GPS	30
Figure 5.3	ESP8266-01 Wi-Fi Module	32
Figure 5.4	ESP8266-01 Wi-Fi Module Pins	33
Figure 5.5	OLED	34
Figure 6.1	Output Image	35
Figure 6.2	Data Center	37
Figure 6.3	ATM Van Details	38
Figure 6.4	User Login	39
Figure 6.5	User Info	39
Figure 6.6	Data Processing Center	40

LIST OF ABBREVIATIONS

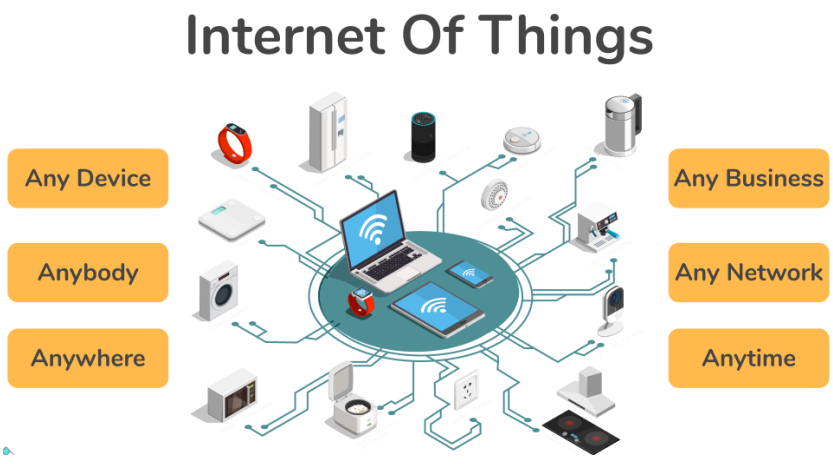
APPREVATIONS	EXPLANATIONS
IOT	Internet-of-things
MQTT	Message Queuing Telemetry Transport protocol
DOS	Denial-of-service
DOS	Denial-of-sleep
PKI	public key infrastructure
ARMA	AN Receiving Message Algorithm
RME	Receiving Message Extractor
UAV	Unmanned aerial vehicle
LNMNT	Lightweight New Mersenne Number Transform
HIL	Hardware -in-the-loop
AES	Advanced Encryption Standard
ECC	Elliptic curve cryptography
QKD	Quantum key distribution
VPN	Virtual Private Network
IKE	Internet Key Exchange
RTC	Real time clock
RF	Radio frequency
PWM	Pulse -width modulation
DIP	Dual -inline-package

CHAPTER 1

INTRODUCTION

1.1 Overview

The Internet of Things, or IoT, refers to the billions of physical devices around the world that are now connected to the internet, all collecting and sharing data. Thanks to the arrival of super-cheap computer chips and the ubiquity of wireless networks, it's possible to turn anything, from something as small as a pill to something as big as an aeroplane, into a part of the IoT. Connecting up all these different objects and adding sensors to them adds a level of digital intelligence to devices that would be otherwise dumb, enabling them to communicate real-time data without involving a human being. The Internet of Things is making the fabric of the world around us smarter and more responsive, merging the digital and physical universes.



1.1 IoT

1.2 IoT Works

IoT devices are empowered to be our eyes and ears when we can't physically be there. Equipped with sensors, devices capture the data that we might see, hear, or sense. They then share that data as directed, and we analyse it to help us inform and automate our subsequent actions or decisions. There are four key stages in this process:

1.2 IoT Works

1.3 Internet of Things Security

Internet of Things security is a set of approaches and practices towards protecting physical devices, networks, processes, and technologies that comprise an IoT environment from a broad spectrum of IoT security attacks.

The two key goals of IoT security are to:

- Make sure all data is collected, stored, processed, and transferred securely.
- Detect and eliminate vulnerabilities in IoT components.

However, developing secure IoT systems and keeping them protected from attacks is not an easy task.

1.3.1 Secure data

`1.3 Secure Data in IoT Systems

Protect sensitive information. Install unique default passwords for each product or require immediate password updates on the first use of a device. Apply robust authentication to ensure that only valid users have access to data. To go the extra mile for better privacy protection, you can also implement a reset mechanism to allow the deletion of sensitive data and clearing of configuration settings if the user decides to return or resell the product.

Collect only necessary data. Ensure that your IoT product collects only data necessary for its operation. This will reduce the with various data protection regulations, standards, and laws.

Secure network communications. For better security, restrict your product's unnecessary communication within the IoT network. Don't rely entirely on the network firewall, and ensure secure communication by making your product invisible via inbound connections by default. Moreover, use encryption methods optimized to the needs of IoT systems, such as the Advanced Encryption Standard, Triple DES, RSA, and Digital Signature Algorit.

1.4 Objective of the project

- A new lightweight cryptographic in terms of 3D position and lattices as a suitable alternative key for fifth-generation and sixth-generation systems and beyond is proposed by taking into account the performance and energy consumption.

- The main benefit of the proposed cryptosystem is solving public key distribution problems and the ridding of public key infrastructure (PKI) because of the very expensive cost and complexity of building PKIs. We solve problems of public key distribution and management by using Quantum cryptography, i.e., we do not need to use digital certificates, certificate authorities, a private key generator or a key generation centre in our proposed cryptosystem, unlike existing protocols.
- We demonstrate that for attackers that are not restricted to any state or condition, secure localizations practicable.
- To the best of our knowledge, the proposed cryptosystem is the first secure position-driven cryptosystem without any restrictions, and it is secure against any number of collusion attackers in the pre- and post quantum IoMT world, unlike existing schemes. Furthermore, it guarantees mutual authentication process. This means that the proposed cryptosystem not only enhances the level of confidentiality but also enhances the level of authentication.
- The proposed cryptographic approach is not only for NB-IoT but also a generic cryptosystem for any network.
- The proposed position-based cryptographic protocol could produce more secure communications between devices, in particular in critical (mobile/static) situations established by using only a party's physical location as its credential. For instance, the worldwide corona virus (COVID-19) pandemic profoundly affected everyday activities. Combining position verification processes and lattice theory with the internet of (moving) things (IoMT) leads to an efficient protocol to improve security for the IoT in the pre- and post quantum world.

CHAPTER 2

2.1 Cryptography

It is technique of securing information and communication through use of codes so that only those people for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”. In cryptography the techniques which are used to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it .These algorithms are used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on internet and to protect confidential transaction such as credit card and card transactions.

2.2 Types of Cryptography

Cryptography can be broken down into three different types:

- Secret Key Cryptography
- Public Key Cryptography
- Hash Functions

Secret Key Cryptography, or symmetric cryptography, uses a single key to encrypt data. Both encryption and decryption in symmetric cryptography use the same key, making this the easiest form of cryptography. The cryptographic algorithm utilizes the key in a cipher to encrypt the data, and when the data must be accessed again, a person entrusted with the secret key can decrypt the data. Secret Key Cryptography can be used on both in-transit and at-rest data, but is commonly only used on at-rest data, as sending the secret to the recipient of the message can lead to compromise.

Examples:

- AES
- DES
- Caesar Cipher

Public Key Cryptography, or asymmetric cryptography, uses two keys to encrypt data. One is used for encryption, while the other key can decrypt the message. Unlike symmetric cryptography, if one key is used to encrypt, that same key cannot decrypt the message, rather the other key shall be used.

One key is kept private, and is called the "private key", while the other is shared publicly and can be used by anyone, hence it is known as the "public key". The mathematical relation of the keys is such that the private key cannot be derived from the public key, but the public key can be derived from the private. The private key should not be distributed and should remain with the owner only. The public key can be given to any other entity.

Examples:

- ECC
- Diffie-Hellman
- DSS

Hash functions are irreversible, one-way functions which protect the data, at the cost of not being able to recover the original message. Hashing is a way to transform a given string into a fixed length string. A good hashing algorithm will produce unique outputs for each input given. The only way to crack a hash is by trying every input possible, until you get the exact same hash. A hash can be used for hashing data (such as passwords) and in certificates.

Some of the most famous hashing algorithms are:

1. MD5
2. SHA-1
3. SHA-2 family which includes SHA-224, SHA-256, SHA-384, and SHA-512

4. SHA-3
5. Whirlpool
6. Blake 2
7. Blake 3

2.3 Quantum Cryptography

Quantum cryptography is a science that applies quantum mechanics principles to data encryption and data transmission so that data cannot be accessed by hackers – even by those malicious actors that have quantum computing of their own. The broader application of quantum cryptography also includes the creation and execution of various cryptographic tasks using the unique capabilities and power of quantum computers. Theoretically, this type of computer can aid the development of new, stronger, more efficient encryption systems that are impossible using existing, traditional computing and communication architectures. While many areas of this science are conceptual rather than a reality today, several important applications where encryption systems intersect with quantum computing are essential to the immediate future of cyber security.

Quantum-safe cryptography: The development of cryptographic algorithms, also known as post-quantum cryptography, that is secure against an attack by a quantum computer and used in generating quantum-safe certificates.

Quantum key distribution: The process of using quantum communication to establish a shared key between two trusted parties so that an untrusted eavesdropper cannot learn anything about that key.

2.4 Fields of application

- **Medicine and health**

Medicine and health services in industrialized countries share core values of patient confidentiality, which is increasingly important giving the rising ubiquity of regional and national public health information networks, as well as multi-clinic information systems for centralized patient records.

- **Financial Services**

Banks and financial services rely heavily on information technology in their operations, and as a consequence are extensive users of cryptography to guarantee authenticity, integrity and confidentiality of the information they process.

- **Mobile Applications**

Mobile applications may or may not be owned and controlled by a Mobile Network Operator (MNO),the availability of these applications and services are often a deciding factor for users as to which handset they will purchase and to which mobile network they will subscribe.

- **Mobile Network Operator Wholesale**

Internet of Things - M2M, sensors are used everywhere to remotely monitor assets and communi cate back to their owners. Electrical meters, vending machines, shipping containers, medical monitoring equipment are some of the examples of embedded devices that require remote connectivity that either uses a proprietary dedicated wireless network or purchases wireless cellular bandwidth from an MNO as a wholesale application.

Connected Vehicles, telemetric and emerging vehicle-to-vehicle communications used for fleet logistics and public safety applications. Many of these applications rely on confidential and authentic communications.

2.5 LITERATURE SURVEY

1. Title: Light-weight Secure Aggregated Data Sharing in IoT-enabled Wireless Sensor Networks

Author: Ghawar Said; Anwar Ghani

Year: 2022

Cross Ref:https://ieeexplore.ieee.org/document/9737147

Methodology

This paper presents a lightweight Secure Aggregation and Transmission Scheme (SATS) for secure and lightweight data computation and transmission. SATS provides a lightweight XOR operation for obtaining batch keys instead of the expensive multiplication operation. Furthermore, the AN Receiving Message Algorithm (ARMA) is presented at the AN to aggregate data generated by sensor nodes. The Receiving Message Extractor (RME) algorithm is presented to decrypt the message and perform batch verification at the Fog-Server. SATS protects against several security threats such as denial of service attacks, the man in the middle attack, and reply attacks.

Findings

The proposed scheme is simulated using NS 2.35 where the TCL files are used for placement and message sending. The C files contain independent classes for configuring sensing devices, AN, and the FoG- Server. The experimental results show that the proposed scheme performs better than its competitors in terms of computation and communication cost as well as it has low storage requirements.

2. Title: Hierarchical Blockchain-Based Group and Group Key Management Scheme Exploiting Unmanned Aerial Vehicles for Urban Computing

Author: Gabin Heo; Kijoon Chae

Year: 2022

Cross Ref: https://ieeexplore.ieee.org/document/9729848

Methodology

This work proposes a hierarchical block chain-based group and group key management scheme to establish an efficient communication environment in urban computing. We adopted block chains to track the movement and density of IoT and secure node authorization. Using the upper layer block chain, the unmanned aerial vehicle (UAV) determines the movement and density of IoTs. Using the lower-layer block chain, base stations (BSs) identify the IoT's movement of information in each group. We included only nodes determined to be safe in the group. Through the hierarchical block chain, while protecting the IoT's privacy, we can record the information in the block chain to determine the mobility of nodes and the node density of a group.

Findings

In simulation, when considering communication and computation overhead, group combination is efficient when the number of group membership changes is greater than 30.After the group combination, when the node movement ratio decreases for a certain time, the groups need to be separated again for better performance. This research scope did not include group separation.

3. Title: Security Analysis of LNMNT-Lightweight Crypto Hash Function for IoT

Author: Nubila Nabeel; Mohamed Hadi Habaebi

Year: 2021

Cross Ref: https://ieeexplore.ieee.org/document/9638508

Methodology

This paper introduces a new Lightweight (LWT) hash function termed Lightweight New Mersenne Number Transform (LNMNT) Hash function, suitable for many IoT applications. The proposed LWT hash function is evaluated in terms of randomness, confusion, diffusion, distribution of hash function, and different attacks.

The randomness analysis is performed using the NIST test suit. The LNMNT LWT hash function has been benchmarked against other LWT hash functions in terms of execution time, cycles per byte, memory usage, and consumed energy.

Findings

The NMNT has a good diffusion property and a fast computation algorithm. The proposed hash function generates a transform with a variable length (powers of two). These characteristics make the New LWT Hash Function design suitable for a wide range of IoT applications. The proposed hash function passed the NIST test suite for randomness, confusion, diffusion, and attack types. Cooja Simulator was used to assess its computational complexity and energy consumption.

4. Title: Lightweight Three-Factor-Based Privacy- Preserving Authentication Scheme for IoT-Enabled Smart Homes

Author: Sungjin Yu

Year: 2021

Cross Ref: https://ieeexplore.ieee.org/document/9531969

Methodology

In this paper the author designs a secure and lightweight three-factor based privacy-preserving user authentication scheme in IoT-enabled smart home environments to provide secure home services for legitimate users. The proposed AKA scheme resists various security attacks such as impersonation attack, and session key disclosure attack, and also provides the security functionalities such as mutual authentication, anonymity, and privacy. Then perform formal (simulation) security of the proposed protocol using the Automated Verification of Internet Security Protocols and Applications (AVISPA), which evaluates security against various security attacks.

Findings

Threat modelling is employed to prove the robustness of the proposed cryptosystem. Additionally, simulation results compare an insecure NB-IoT network (without any security consideration)and a secure NB-IoT network (via the proposed cryptosystem). These results prove that the proposed cryptography improves IoT security without compromising its performance features, including the energy consumption of advanced and normal nodes, time consumption at the BS, stability period, throughput and elapsed time for the whole network in the presence of cyber security computational costs and transmission costs.

5. Title: A Quantum Chaotic Image Cryptosystem and Its Application in IoT Secure Communication

Author: Heping Wen; Chongfu Zhang

Year: 2021

Cross Ref: https://ieeexplore.ieee.org/document/9336671

Methodology

This paper proposes a secure image cryptosystem using quantum chaos and verifies its feasibility on the IoT experimental platform. A quantum logistic chaotic map is selected to generate the PRNS (pseudo-random number sequence) for encryption. The PRNS has been verified to have better randomness, and is suitable for information security protection in cryptographic systems. To enhance the ability of encryption algorithms against cryptographic attacks, the author proposes an image cryptosystem of the structure ‘‘diffusion-permutation diffusion’’. By means of permutation, the confusion and diffusion performance of encryption algorithm are enhanced, and the ability of cipher image to resist various noise attacks is improved.

Findings

The proposed image cryptosystem uses a diffusion-permutation-diffusion structure and introduces a plaintext association mechanism to enhance the security. Theoretical security analysis and experimental results both demonstrate the excellent performance of our proposed cryptosystem.

It is both sensitive to plain image sand secret keys, and has robust ability to resist differential attacks as well as other various common attacks.

6. Title: Security Architecture and Protocols for Secure MQTT-SN

Author: Chang-Seop Park

Year: 2020

Cross Ref: https://ieeexplore.ieee.org/document/9296847

Methodology

This paper proposes security architecture and protocols to bootstrap MQTT security in the wireless sensor network. Security bootstrapping for MQTT includes security credential generation and distribution; registration protocol for joining MQTT entities such as publishers, subscribers, and brokers to the security controller; and rekeying protocol for group membership management. Special attention is given to the end-to-end security between the publishers and subscribers because the data from the publishers should not be corrupted by, and exposed to, the compromised broker.

Findings

Especially, based on two security models for the broker, malicious broker and honest but-curious broker, the necessity of establishing end-to-end security between the publishers and subscribers was also investigated. Both device and topic certificates constructed using the ECQV certificate could establish a framework to provide end-to-end security, as well as fine-grained access control, for the devices.

7. Title: A Cyber-Physical System to Detect IoT Security Threats of a Smart Home Heterogeneous Wireless Sensor Node

Author: Chang-Seop Park

Year: 2020

Cross Ref: https://ieeexplore.ieee.org/document/9296847

Methodology

In this paper, the author proposes to use a smart IoT system as the platform for developing a CPS for detecting an IoT security threat by behavioural power monitoring of the wireless sensor devices. Developed a smart Cyber-Physical System (CPS) to detect cyber security threats through behavioural power profiling .Proposed proactive and provable monitoring of power uses in smart IoT devices using a Smartphone.

Findings

The proposed approach can detect cyber-attacks through behavioural power profiling of a wireless smart home hardware-in-the-loop (HIL) devices. This research provides a non-invasive system that allows users to better understand the security state of a CPS-based system. The results from different sensor data sets are also resented to show that this approach provides a high rate of classification correctness in power profiling for security monitoring. The system may also have multiple applications such as security analytics of a smart grid or a smart home energy management system.

8. Title: An Authentic-Based Privacy Preservation Protocol for Smart e-Healthcare Systems in IoT

Author: B. D. Deebak,Fadi Al-Turjman

Year: 2019

Cross Ref: https://ieeexplore.ieee.org/document/8839043

Methodology

In this work, a substantial thought is made to investigate the underlying adversarial model that tries to eliminate the deficiencies such as redundancies, insufficiencies, ambiguities, etc. using the evaluation criteria set. As for systematic methodology, a broad set of 12 independent criteria is characterized to analyse the pra ctical capabilities of adversary model. Though it is completely not available to examine, it is expected to provide a solid analysis of requirement definition.

Findings

The proposed SAB-UAS scheme shows the formal security model, resource and performance efficiency analysis to prove the security, storage and performance efficiencies. The former proof demonstrates that the proposed scheme can protect the sensitive information of a user from adversary to achieve the property of perfect forward secrecy. The latter analysis shows that the proposed SAB-UAS scheme can substantially reduce the storage, computation and communication cost to improve the performance efficiency of any real-time based healthcare application systems.

9. Title: A Secure Trust-Based Key Distribution with Self-Healing for Internet of Things

Author: Song Han; Mianxue Gu

Year: 2019

Cross Ref: https://ieeexplore.ieee.org/document/8804180

Methodology

In this paper, the author proposes a framework of key management with self-healing and trust for IoT objects of community healthcare.

Our system model which contains three kinds of devices can be divided into two layers, i.e., the top layer: between MS and AD, and the bottom layer: between AD and IoTDs.

In the top layer, the author uses a polynomial based key agreement approach; while in the bottom layer, then propose a polynomial based self-healing group key distribution method, which meets the requirements of our secret model.

Findings

At last, the author conducts security analysis which shows our proposed scheme meets all the requirements we presented in the security model. Then also conduct performance analysis which shows the overheads in term of storage, computation and communication, and some experiments which relate to the healing rate of the proposed scheme

10. Title: PROS: A Privacy-Preserving Route-Sharing Service via Vehicular Fog Computing

Author: Meng Li; Liehuang Zhu

Year: 2018

Cross Ref:https://ieeexplore.ieee.org/document/8517131

Methodology

Privacy-preserving Route Sharing (PROS) scheme via vehicular fog computing is proposed to protect user and group privacy. The author introduces fog computing into the route-sharing service model where fog nodes i.e., road-side units (RSUs) pre-process the users' group formation/participation requests for the SP. We provide the definition of group privacy.

Findings

The PROS scheme not only provides users with route planning and group formation but also protects user and group privacy. Finally, the author proved the security and privacy of the PROS scheme and evaluated its performance by comparing it with existing work. In the future work, the author will consider the possibility that the RSUs can be compromised.

CHAPTER 3

SYSTEM ANALYSIS

3.1 Existing System

IoT also comes with many benefits and various risks. Cryptographic algorithms should develop security solutions that protect IoT networks and minimize security risks. As security is the prime concern for any communications, the traditional security techniques are

- **AES**

AES Rijndael's proposal for AES (Advanced Encryption Standard) uses 128, 192, and 256 bits to decode a number that allows the block length and key length to be specified independently of each other. The key length determines some parameters of the AES algorithm.

- **DES**

DES (Standard Encryption Standard) is a 64-bit symmetric block encryption algorithm. This algorithm works on 64-bitblocks of plain text. Due to the symmetry, the same key can be used for encryption and decryption. In most cases, the same algorithm is used for encryption and decryption.

- **Triple-DES**

Triple-DES is a type of computer encryption algorithm in which each data block receives three passes. Triple DES is currently considered obsolete, but some IoT products use it for compatibility and flexibility. Triple DES is a good encryption algorithm that can be used to protect against brute force attacks.

- **Blowfish**

Blowfish is a block cipher and is a part of symmetric key encryption. It encrypts data in blocks of 8 bytes. The algorithm consists of two parts, a key extension part and a data encryption part. The key extension converts a key with a maximum length of 56 bytes (448 bits) into several tables with sub keys with a total of 4168 bytes.

- **Hash functions.**

New cryptographic hash algorithm “SHA-3” competition attracts many people’s attention. SHA-3 is expected to be a general-purpose hash function, and none of the current finalists do not satisfy lightweight properties.

- **Elliptic curve cryptography (ECC)**

It is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

- **Private key authentication**

Private key cryptography is asymmetric encryption which provides two keys, one public and one private. If data are encrypted with the private key, it can only be decrypted with the public key, and vice versa. Doing so preserves the security of the system and makes communications with other devices safer. This can be useful when a new device needs to connect to the IoT network and in the verification of messages passed between devices.

3.2 Quantum Key Cryptography

Quantum cryptography, also called quantum encryption, applies principles of quantum mechanics to encrypt messages in a way that it is never read by anyone outside of the intended recipient. It takes advantage of quantum’s multiple states, coupled with its "no change theory," which means it cannot be unknowingly interrupted.

- **Quantum-safe cryptography**:

The development of cryptographic algorithms, also known as post-quantum cryptography, that are secure against an attack by a quantum computer and used in generating quantum-safe certificates. Quantum cryptography uses the same physics principles and similar technology to communicate over a dedicated communications link.

The goal of post-quantum cryptography (also called quantum-resistant cryptography) is to develop cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks.

- **Post Quantum Cryptography**

PQC links private keys to public keys without using problems that quantum computers can easily solve. In other words, it aims to deliver the benefits of today's public-key encryption without the vulnerability to quantum hacking.

Approaches to PQC include building encryption around mathematical "structures" called lattices, using systems purely based upon code, solving complicated problems involving multiple variables, and much more.

- **Quantum key distribution**:

The process of using quantum communication to establish a shared key between two trusted parties so that an untrustedvc eavesdropper cannot learn anything about that key. Quantum key distribution utilizes the unique properties of quantum mechanical systems to generate and distribute cryptographic keying material using special purpose technology.

Quantum Key Generation: Internet key exchange version 2 (IKEv2) Internet Key Exchange (IKEv2) is a protocol used to establish keys and security associations (SAs) for the purpose of setting up a secure Virtual Private Network (VPN) connection that protects network packets from being read or intercepted over a public Internet connection. This allows a remote computer on a public network to access resources and benefit from the security of a private closed network without compromising security. The IKE protocol standard is rigid and does not permit VPN designers to choose beyond a small set of cryptographic algorithms.

The shared secrets provided by QKD may either be used with conventional encryption ciphers, or for one-time pad encryption in high security applications' may also be used for the second pass to solve the key management problem of distributing shared secret keys for message authentication. Instead of calculating shared secrets and computing secret keys, QKD keys could be used to protect integrity

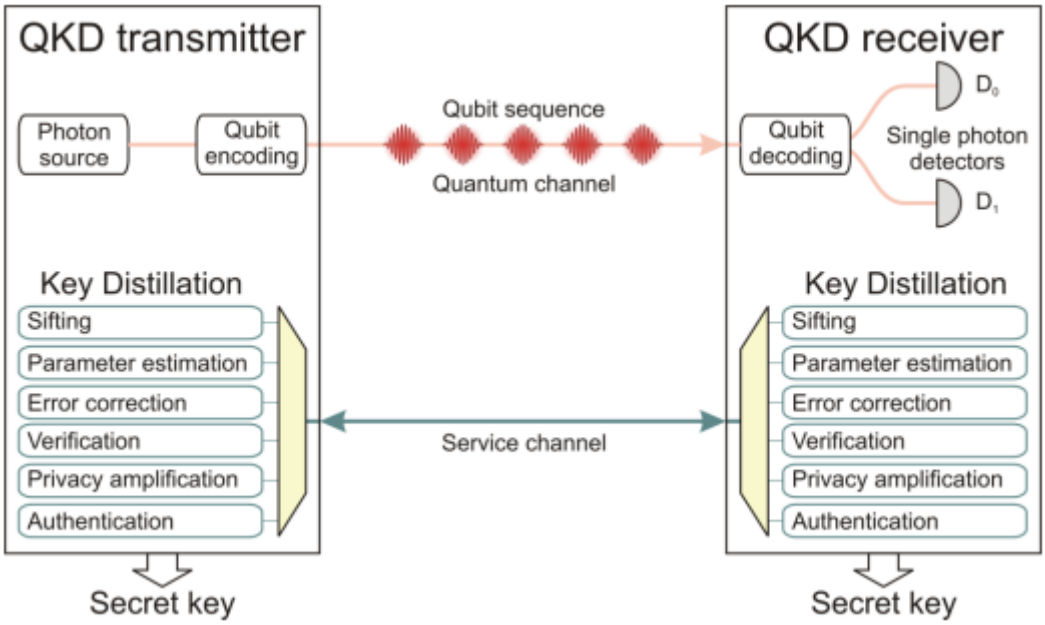


Figure 3.2.1 QKD service channel

3.3 Proposed System

The Internet of Things (IoT) connects billions of machines that can interact with each other. IoT is one of the fastest-growing areas in the history of computing, and will continue in this direction in the 6G era. New security problems have been raised, however, since implementing protection mechanisms for IoT devices, such as encryption, authentication, and so on, is inefficient, due to their inherent flaws. Therefore, a new method of protecting IoT devices needs to be sought.

Quantum security depends on the natural physical phenomenon (quantum mechanics) and offers an appropriate and powerful security technique. This paper suggests a new approach for simulating the quantum key distribution between IoT devices and a server to encrypt the data sent to the server.The area of Quantum Cryptography is a new and upcoming field in terms of security of data. Unlike the normal Cryptography techniques this technique is faster and also can handle large amount of data as it works on qubits and on the principle of Heisenberg Uncertainty. This project proposes the use of quantum cryptography techniques in order to protect IoT devices in the beyond 5G and 6G era. The approach proposed in this project consists of performing quantum key distribution (QKD) between the remote server and the IoT device controllers. Afterwards, Bank Server can distribute the generated keys to the IoT devices and remote server connected to it. Then, these IoT devices can encrypt their data while transmitting it to the controller over the traditional radio frequency (RF) communication links between them.

3.4 Disadvantages

- Encryption methodologies are becoming less reliable as the eavesdroppers and attackers are gaining powerful computing ability.
- Many of these solutions employ static authentication, which verifies the user/device just once at the beginning of each session.
- Does not prevent man-in-the middle attack and fails to prevent a collision attack.
- Does not provide backward and forward secrecy as the attacker can gain the ID of the devices, and then sniff other values from the current session to find the previous and future secret keys.
- Does not provide anonymity and untraced ability.
- Initialization and computation cost high.

3.5 Block Diagram

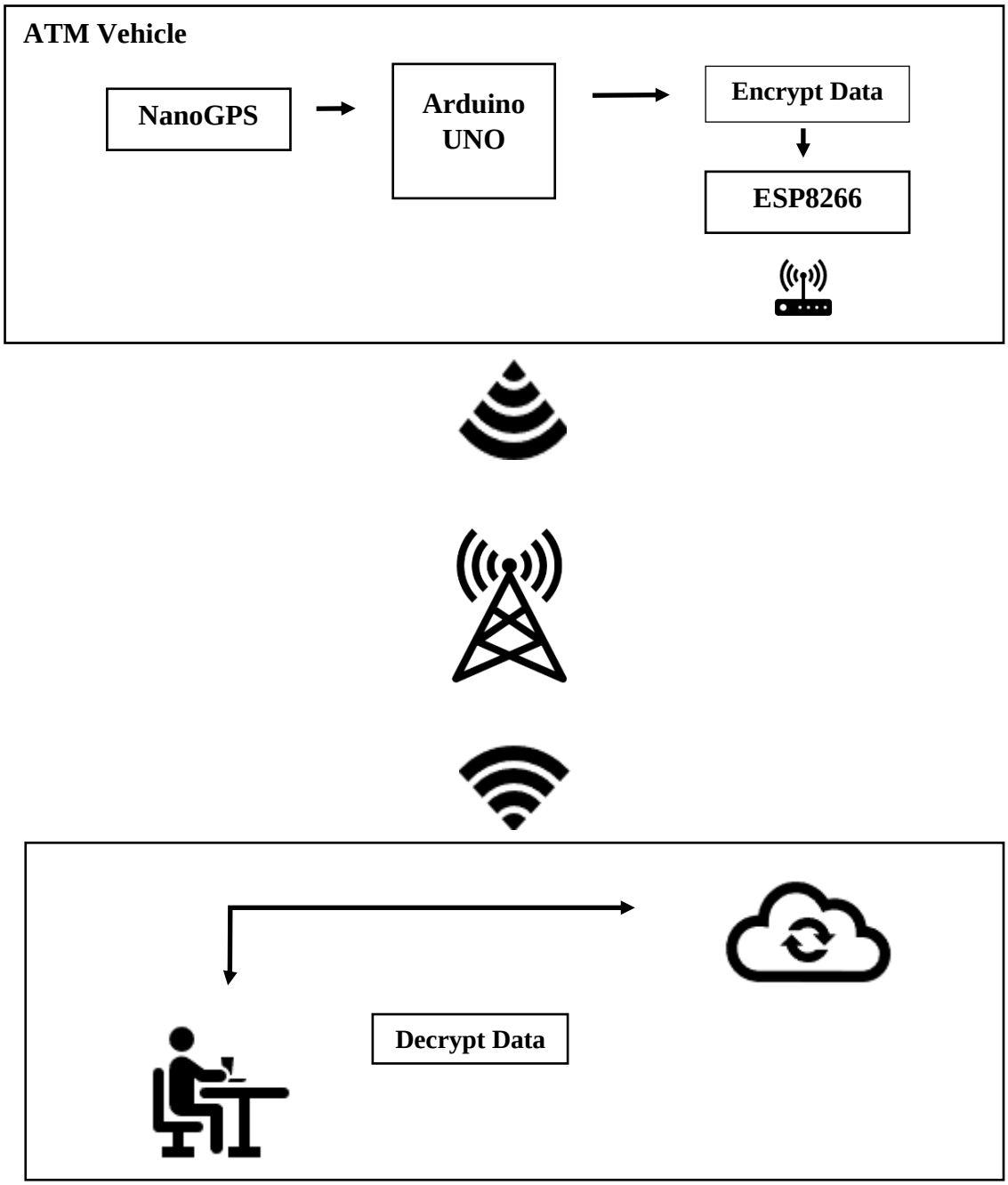
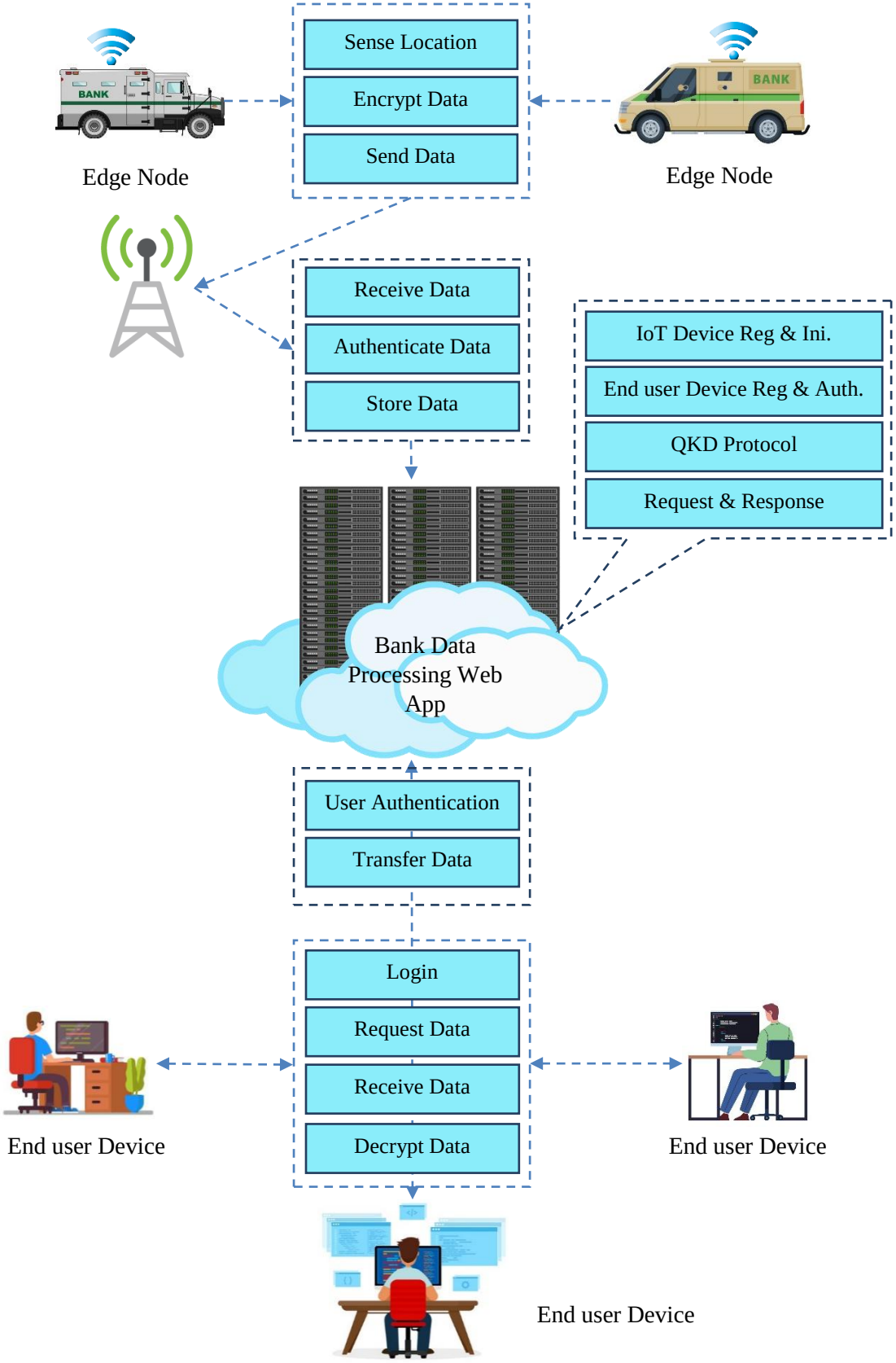


Fig 3.4 Block Diagram

3.6 System Architecture



3.5 system Architecture

Chapter 4

System Specification

4.1 Software specification

- PHP 5
- MySQL
- WAMP Server 2.0
- Embedded C
- Arduino IDE

4.1.1 PHP

The PHP Hypertext Preprocessor (PHP) is a programming language that allows web developers to create dynamic content that interacts with databases. PHP is basically used for developing web-based software applications. This tutorial helps you to build your base with PHP.

PHP is a flexible, dynamic language that supports a variety of programming techniques. It has evolved dramatically over the years, notably adding a solid object-oriented model in PHP 5.0 (2004), anonymous functions and namespaces in PHP 5.3 (2009), and traits in PHP 5.4 (2012).

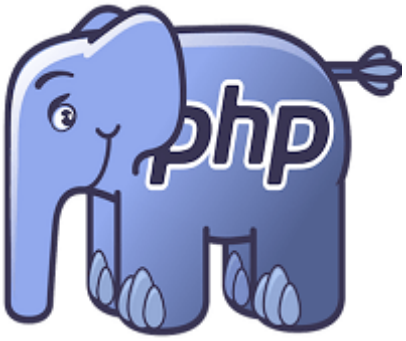
Object-oriented Programming

PHP has a very complete set of object-oriented programming features including support for classes, abstract classes, interfaces, inheritance, constructors, cloning, exceptions, and more.

Functional Programming

PHP supports first-class functions, meaning that a function can be assigned to a variable. Both user-defined and built-in functions can be referenced by a variable and invoked dynamically.

Functions can be passed as arguments to other functions (a feature called Higher-order Functions) and functions can return other functions.



4.1.2 MySQL

MySQL is a relational database management system based on the Structured Query Language, which is the popular language for accessing and managing the records in the database. MySQL is open-source and free software under the GNU license. It is supported by Oracle Company.

MySQL is currently the most popular database management system software used for managing the relational database. It is open-source database software, which is supported by Oracle Company. It is fast, scalable and easy to use database management system in comparison with Microsoft SQL Server and Oracle Database. It is commonly used in conjunction with PHP scripts for creating powerful and dynamic server-side or web-based enterprise applications.

4.1.3 WampServer

WampServer is a Windows web development environment. It allows you to create web applications with Apache2, PHP and a MySQL database. Alongside, PhpMyAdmin allows you to manage easily your database.

WAMPServer is a reliable web development software program that lets you create web apps with MYSQL database and PHP Apache2. With an intuitive interface, the application features numerous functionalities and makes it the preferred choice of developers from around the world. The software is free to use and doesn't require a payment or subscription.

4.1.4 Bootstrap 4

Bootstrap is a free and open-source tool collection for creating responsive websites and web applications. It is the most popular HTML, CSS, and JavaScript framework for developing responsive, mobile-first websites.

It solves many problems which we had once, one of which is the cross-browser compatibility issue. Nowadays, the websites are perfect for all the browsers (IE, Firefox, and Chrome) and for all sizes of screens (Desktop, Tablets, Phablets, and Phones). All thanks to Bootstrap developers -Mark Otto and Jacob Thornton of Twitter, though it was later declared to be an open-source project.

Easy to use: Anybody with just basic knowledge of HTML and CSS can start using Bootstrap

Responsive features: Bootstrap's responsive CSS adjusts to phones, tablets, and desktops

Mobile-first approach: In Bootstrap, mobile-first styles are part of the core framework

Browser compatibility: Bootstrap 4 is compatible with all modern browsers (Chrome, Firefox, Internet Explorer 10+, Edge, Safari, and Opera).

4.1.5 Embedded C

Embedded C is most popular programming language in software field for developing electronic gadgets. Each processor used in electronic system is associated with embedded software. Embedded C programming builds with a set of functions where every function is a set of statements that are utilized to execute some particular tasks. Both the embedded C and C languages are the same and implemented through some fundamental elements like a variable, character set, keywords, data types, declaration of variables, expressions, statements. All these elements play a key role while writing an embedded C program. The embedded system designers must know about the hardware architecture to write programs. These programs play a prominent role in monitoring and controlling external devices.

Embedded C programming plays a key role in performing specific function by the processor. In day-to-day life we used many electronic devices such as mobile phone, washing machine, digital camera, etc. These all-device working is based on microcontroller that are programmed by embedded C. In every embedded system-based project, Embedded C programming plays a key role to make the microcontroller run & perform the preferred actions.

Chapter 5

5.1 Hardware specification

- Arduino UNO.
- Nano GPS
- Esp8266
- OLED Display.

5.1.1 ARDUINO UNO

The Arduino UNO is a standard board of Arduino. Arduino UNO is based on an ATmega328P microcontroller. It is easy to use compared to other boards, such as the Arduino Mega board, etc. The board consists of digital and analog Input/output pins (I/O), shields, and other circuits. The Arduino UNO includes 6 analog pin inputs, 14 digital pins, a USB connector, a power jack, and an ICSP (In-Circuit Serial Programming) header. It is programmed based on IDE, which stands for Integrated Development Environment. It can run on both online and offline platforms.

Fig 5.1 Arduino UNO

Components of Arduino Uno:

- **ATmega328 Microcontroller**- It is a single chip Microcontroller of the ATmega family. The processor code inside it is of 8-bit. It combines **Memory (SRAM, EEPROM, and Flash), Analog to Digital Converter, SPI serial ports, I/O lines, registers, timer, external and internal interrupts, and oscillator.**
- **ICSP pin** - The In-Circuit Serial Programming pin allows the user to program using the firmware of the Arduino board.
- **Power LED Indicator**- The ON status of LED shows the power is activated. When the power is OFF, the LED will not light up.
- **Digital I/O pins**- The digital pins have the value HIGH or LOW. The pins numbered from D0 to D13 are digital pins.
- **TX and RX LED's**- The successful flow of data is represented by the lighting of these LED's.
- **AREF-** The Analog Reference (AREF) pin is used to feed a reference voltage to the Arduino UNO board from the external power supply.
- **Reset button**- It is used to add a Reset button to the connection.
- **USB**- It allows the board to connect to the computer. It is essential for the programming of the Arduino UNO board.
- **Crystal Oscillator**- The Crystal oscillator has a frequency of 16MHz, which makes the Arduino UNO a powerful board.
- **Voltage Regulator**- The voltage regulator converts the input voltage to 5V.
- **GND**- Ground pins. The ground pin acts as a pin with zero voltage.
- **Vin**- It is the input voltage.

- **Analog Pins**- The pins numbered from A0 to A5 are analog pins. The function of Analog pins is to read the analog sensor used in the connection. It can also act as GPIO (General Purpose Input Output) pins

4.2.2 Nano GPS Protocol:

Original GPS have launched the Nano Spider (ORG4400), a fully integrated, highly sensitive GPS receiver module.

5.2 Nano GPS

1. **Designed to support ultra-compact applications**

Measuring only 4.1 x 4.1 x 2.1mm and with minimal power consumption, the Nano Spider is an ideal match for smart watches, wearable devices, trackers, and digital cameras. A double-sided circuit design reduces footprint size and makes the Nano Spider 47% smaller than previous solutions.

2. Fully integrated features

Unlike other miniature GPS modules, the Nano Spider includes a low noise amplifier (LNA), surface acoustic wave (SAW) filter, temperature-controlled crystal oscillator (TCXO) and real time clock (RTC) crystal, a power management unit, and radio frequency (RF) shielding.

3. Superior sensitivity and performance

The Nano Spider module offers accuracy of approximately 1 meter, achieves a rapid time to first fix (TTFF) of less than 1 second, and tracking sensitivity of -163dBm.

4. Continuous connectivity with minimal power consumption

The module achieves a state of near continuous availability by detecting changes in context, temperature and satellite signals. By maintaining and opportunistically updating its internal fine time, frequency, and satellite data, the Nano Spider consumes mere microwatts of battery power.

5. Improving marginal signal conditions

The module also features OriginGPS' proprietary Noise Free Zone (NFZ™) system. Increasing noise immunity even under marginal signal conditions, it allows the module to provide high accuracy in dense urban areas, under thick foliage, or when the receiver rapidly changes position.

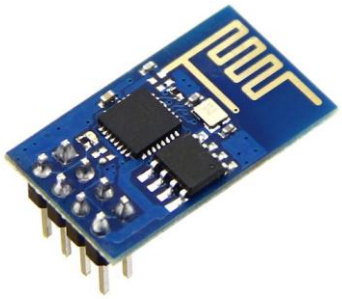
4.2.3 ESP8266 Wi-Fi Module

The ESP8266 is a System on a Chip (SoC), manufactured by the Chinese company Espressif. It consists of a Tensilica L106 32-bit micro controller unit (MCU) and a Wi-Fi transceiver. It has 11 GPIO pins* (General Purpose Input/output pins), and an analog input as well. This means that you can program it like any normal Arduino or other microcontroller. And on top of that, you get Wi-Fi communication, so you can use it to connect to your Wi-Fi network, connect to the Internet, host a web server with real web pages, let your Smartphone connect to it, etc..

.

Introduction

ESP8266 is Wi-Fi enabled system on chip (SoC) module developed by Espressif system. It is mostly used for development of IoT (Internet of Things) embedded applications.



5.3 ESP8266-01 Wi-Fi Module

ESP8266 comes with capabilities of

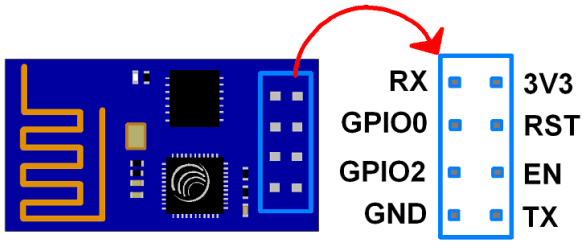
- 2.4 GHz Wi-Fi (802.11 b/g/n, supporting WPA/WPA2),
- general-purpose input/output (16 GPIO),
- Inter-Integrated Circuit (I^2C) serial communication protocol,
- analog-to-digital conversion (10-bit ADC)
- Serial Peripheral Interface (SPI) serial communication protocol,
- I^2S (Inter-IC Sound) interfaces with DMA (Direct Memory Access) (sharing pins with GPIO),
- UART (on dedicated pins, plus a transmit-only UART can be enabled on GPIO2), and
- Pulse-width modulation (PWM).

It employs a 32-bit RISC CPU based on the Tensilica Xtensa L106 running at 80 MHz (or over clocked to 160 MHz). It has a 64 KB boot ROM, 64 KB instruction RAM and 96 KB data RAM. External flash memory can be accessed through SPI. ESP8266 module is low-cost standalone wireless transceiver that can be used for end-point IoT developments. To communicate with the ESP8266 module, microcontroller needs to use set of AT commands.

Microcontroller communicates with ESP8266-01 module using UART having specified Baud rate. There are many third-party manufacturers that produce different modules based on this chip. So, the module comes with different pin availability options like,

- ESP-01 comes with 8 pins (2 GPIO pins) – PCB trace antenna. (shown in above figure)
- ESP-02 comes with 8 pins, (3 GPIO pins) – U-FL antenna connector.
- ESP-03 comes with 14 pins, (7 GPIO pins) – Ceramic antenna.
- ESP-04 comes with 14 pins, (7 GPIO pins) – No ant.etc.
-

ESP8266-01 Module Pin Description

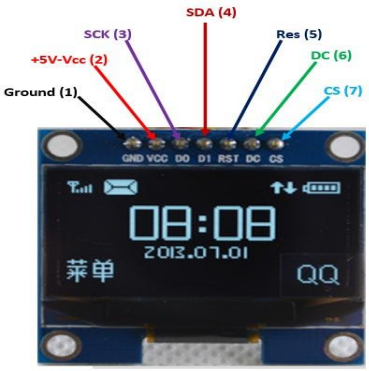


5.4 ESP8266-01 Module Pins

- **3V3**: - 3.3 V Power Pin.
- **GND**: - Ground Pin.
- **RST**: - Active Low Reset Pin.
- **EN**: - Active High Enable Pin.
- **TX**: - Serial Transmit Pin of UART.
- **RX**: - Serial Receive Pin of UART.
- **GPIO0 & GPIO2**: - General Purpose I/O Pins. These pins decide what mode (boot or normal) the module starts up in. It also decides whether the TX/RX pins are used for Programming the module or for serial I/O purpose.

4.2.4 OLED

OLED (Organic Light Emitting Diodes) is a flat light emitting technology, made by placing a series of organic thin films between two conductors. When electrical current is applied, a bright light is emitted. OLEDs are emissive displays that do not require a backlight and so are thinner and more efficient than LCD displays (which do require a white backlight).



5.5 OLED

There are two main families of OLED: those based on small molecules and those employing polymers. Adding mobile ions to an OLED creates a light-emitting electrochemical cell (LEC) which has a slightly different mode of operation. An OLED display can be driven with a passive-matrix (PMOLED) or active-matrix (AMOLED) control scheme. In the PMOLED scheme, each row and line in the display is controlled sequentially, one by one, where as AMOLED control uses a thin-film transistor (TFT) backplane to directly access and switch each individual pixel on or off, allowing for higher resolution and larger display size.

Chapter 6

RESULTS AND DISCUSSION

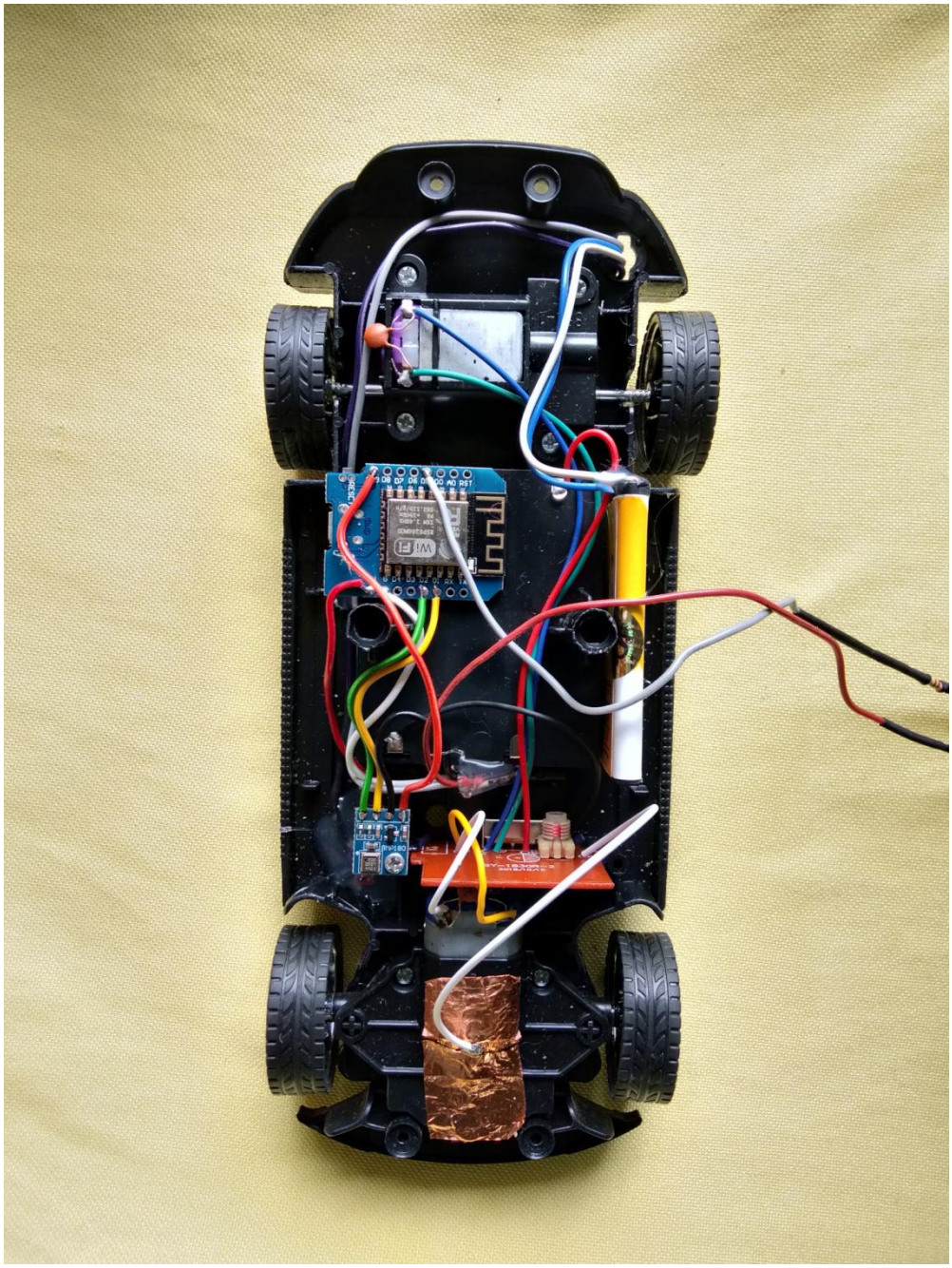


Fig 6.1 Output image

This section provides an analysis of the communication and computational costs of our proposed scheme.

A. Communication Overhead

The message sent by ATM Vehicle to BDP Location Server is

$$\mathrm{Dec}_{CAR_i}\begin{pmatrix}\mathrm{Enc}_{TA}\left(\mathrm{Star}_{\mathrm{ID,j}},\mathrm{End}_{\mathrm{ID,j}}\right),T_{\mathrm{ID,j}}\\ \mathrm{h}(\mathrm{h}\,(\mathrm{ID})+\mathrm{r}_{\mathrm{ID}}+T)\end{pmatrix}$$

The length of the message is 2048 bits. Therefore, the length of the message is 2048 bits. Therefore, the total size of the message received by all BS is about 2048 X $n_{Message}$ Xn_{Car} X n_{BDPLS} bits.

$$\mathrm{h}\left(\mathrm{h}\,(\mathrm{ID_{BS}})+\mathrm{r_{BS}}+T,\mathrm{CNum}'\right)||\mathrm{CNum}'$$

The total size of message sent by ATMV to BDP Location Server is about 1200 X (z + 1) X n_{BDPLS} bits, where z = 2. So the total communication overhead is approximately

$$\left(2\times \mathrm{n_{Message}}\times \mathrm{n_{CAR}}\times \mathrm{n_{BS}}+3\times \mathrm{n_{BS}}\right)kb \ll (100030)\,kb \ll 100Mb$$

Therefore, the communication overhead is acceptable.

B. Communication overhead

$t_{HLP\text{-}ENC}$ and $t_{HLP\text{-}DEC}$ respectively represent the time of one round of encryption and decryption using Hidden Lattice Problem lattice password; $t_{RSA\text{-}TA\text{-}ENC}$ and $t_{RSA\text{-}TA\text{-}DEC}$ respectively represent the time of one round of encryption and decryptionm using the public and private keys of ATMV and BBA Device; $t_{RSA\text{-}CAR\text{-}DEC}$ and $t_{RSA\text{-}CAR\text{-}ENC}$ respectively represent the average time for around of signing and verification using the CAR and BBA Device public and private keys. Thrash indicates the average time for a round of signatures.

Other simple addition operations cost much less than those above, so this can be ignored. Hence the total computational cost of the aggregation process is approximately

$$((t_{RSA-TA-ENC} + t_{RSA-CAR-DEC} + t_{RSA-CAR-ENC} + t_{hash}) \times n_{Message} \times n_{CAR} + t_{HLP-ENC} + t_{hash}) \times n_{BS} + t_{HLP-DEC}$$

Then, the parallelization computation overhead time is

$$(t_{RSA-TA-ENC} + t_{RSA-CAR-DEC} + (t_{RSA-CAR-ENC} + t_{hash}) \times n_{CAR}) \times n_{Message} + t_{HLP-ENC} + t_{hash} + t_{HLP-DEC}.$$

Through the experimental calculation, we know that under the premise of n_{BDPLS}= 10; $n_{Message}$= 50, the total computation cost is about 3175s, and the computation time after parallelization is about 53s, which is an extremely short and acceptable parallel computation time.

6.1 SCREENSHOTS

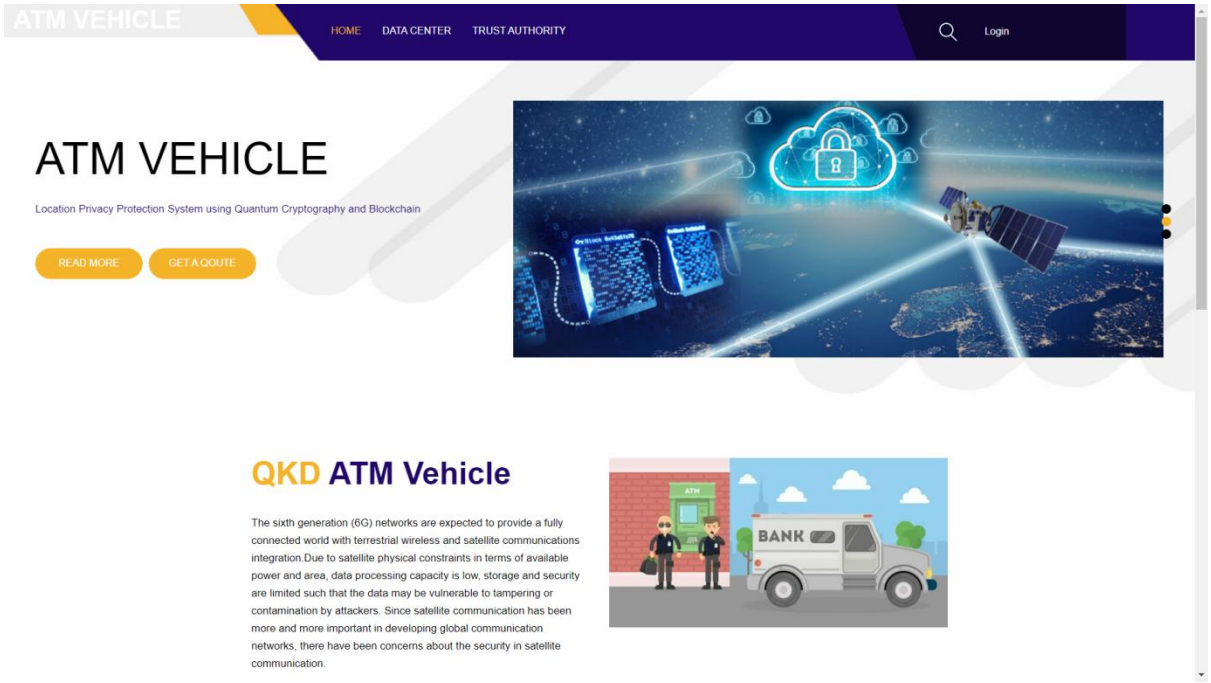


Fig 6.2 Home Page

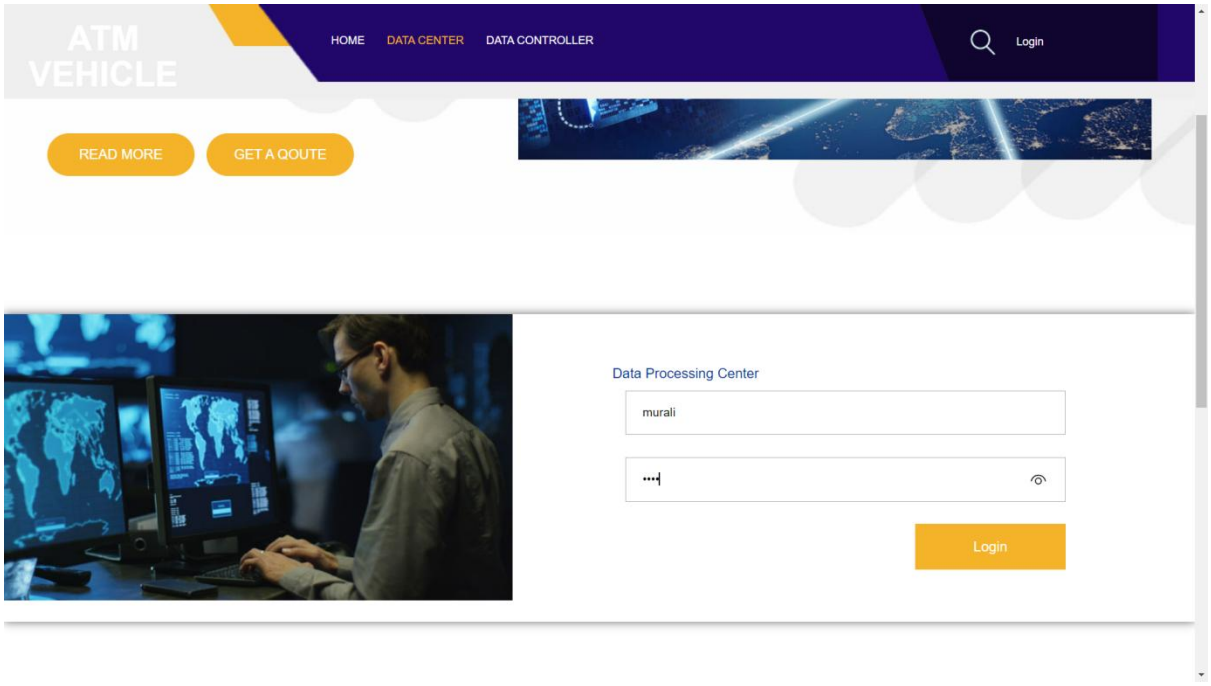


Fig 6.3 Data Center

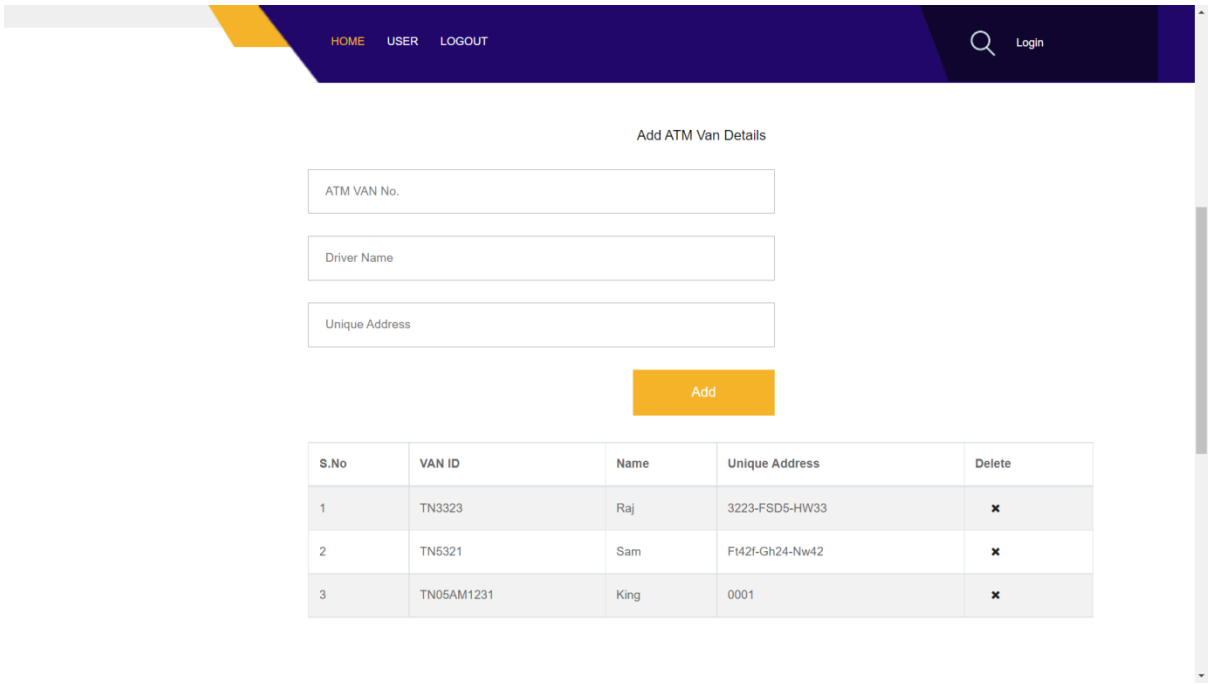


Fig 6.4 ATM Van Details

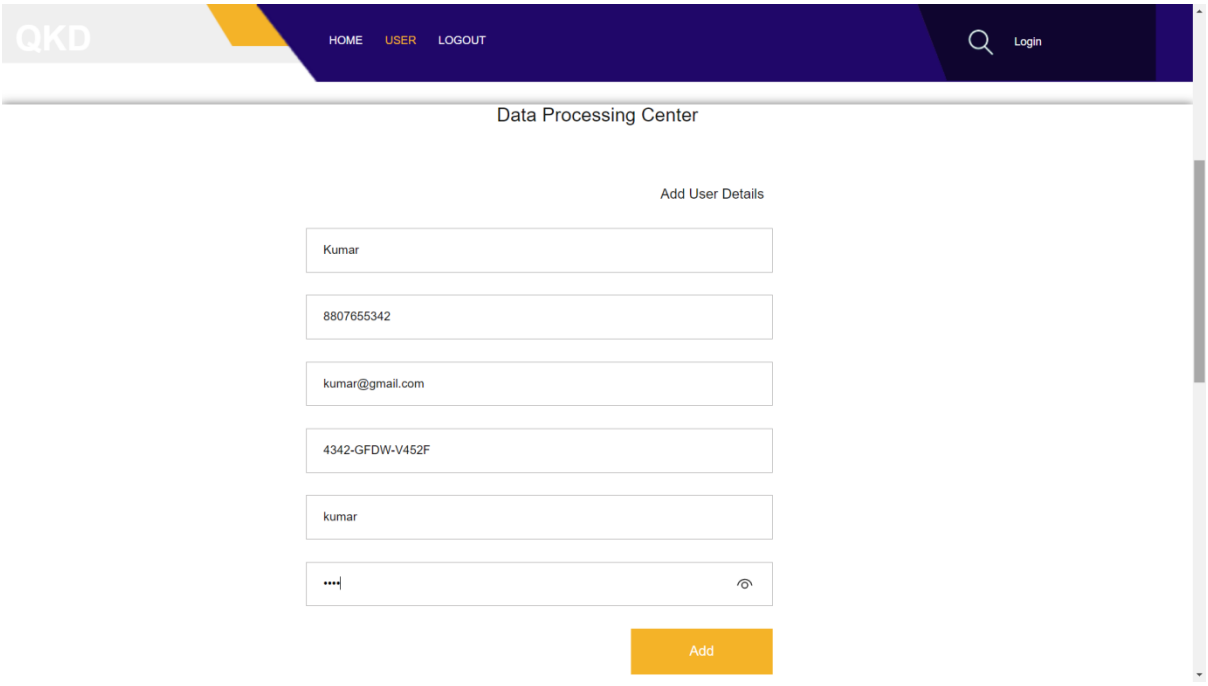


Fig 6.5 User Login

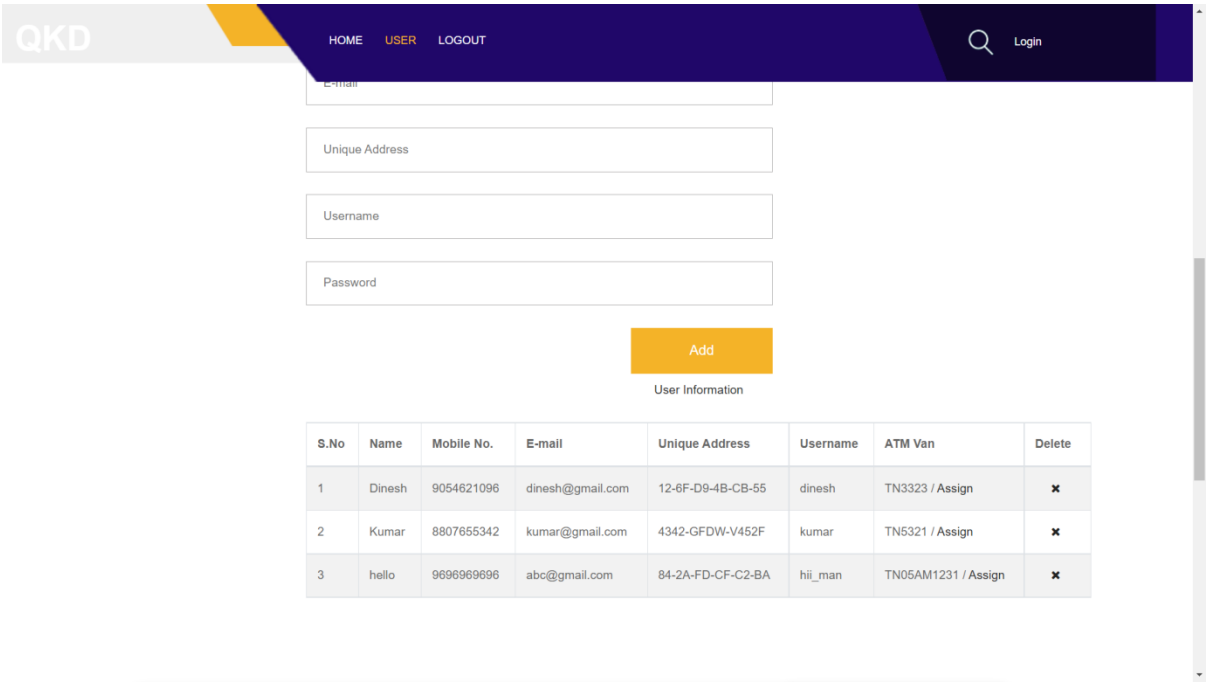


Fig 6.6 User Information

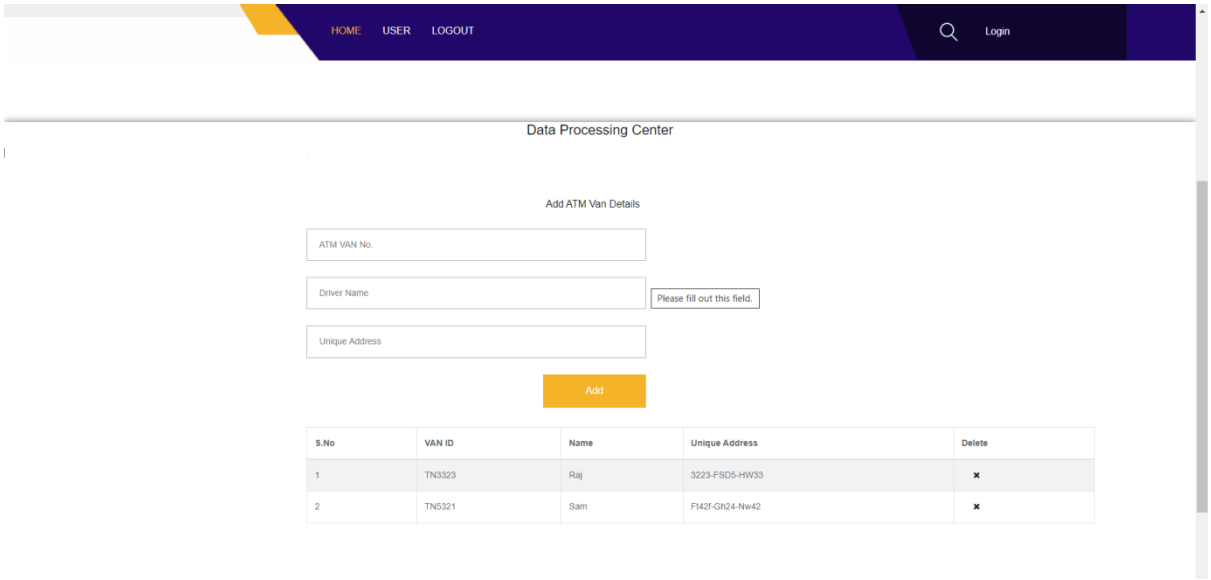


Fig6.7 DATA Processing Center

Chapter 7

Conclusion

IoT is essentially important to improve the quality of human life by the interconnection of different technologies, smart devices, and applications. At present, ATM vehicle location privacy protection methods play an important role in IoV systems, as they can improve the system and increase Banks' viscosity. Based on a post-quantum cryptography system, this project proposes a practical privacy protection scheme for ride hailing route information, which can make the statistical aggregation operation of the route and frequency from the starting point to the destination complete without the visibility of the ride-hailing platform, and ensure the data privacy security of a single vehicle. Compared with representative multi-vehicle aggregation solutions, we not only achieve message privacy, confidentiality, integrity, forward and backward security, anti-man in attack and redial attack, but also achieve multi-dimensional aggregation, CCA security and anti-quantum attack. In addition, through the analysis of the experiment, the cost of our scheme is reasonable, thus, the scheme is practical in this scenario.

References

1. J. Qian, Z. Cao, X. Dong, J. Shen, Z. Liu, and Y. Ye, ‘‘Two secure and efficient lightweight data aggregation schemes for smart grid,’’ IEEE Trans. Smart Grid, vol. 12, no. 3, pp. 2625–2637, May 2021.

2. J. Qian, Z. Cao, M. Lu, X. Chen, J. Shen, and J. Liu, ‘‘The secure lattice-based data aggregation scheme in residential networks for smart grid,’’ IEEE Internet Things J., vol. 9, no. 3, pp. 2153–2164, Feb. 2022.

3. J. Lin and J. Qian, ‘‘A multi-party secure SaaS cloud accounting platform based on lattice-based homomorphic encryption system,’’ in Proc. Int. Conf. Public Manage. Intell. Soc. (PMIS), Feb. 2021, pp. 1–4.

4. Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, ‘‘A practical privacy preserving data aggregation (3PDA) scheme for smart grid,’’ IEEE Trans .Ind. Informat., vol. 15, no. 3, pp. 1767–1774, Mar. 2019.

5. J. Song, Y. Liu, J. Shao, and C. Tang, ‘‘A dynamic membership data aggregation (DMDA) protocol for smart grid,’’ IEEE Syst. J., vol. 14, no. 1,pp. 900–908, Mar. 2020.

6. X. Li, J. Li, S. Yiu, C. Gao, and J. Xiong, ‘‘Privacy-preserving edgeassisted image retrieval and classification in IoT,’’ Frontiers Comput. Sci.,vol. 13, no. 5, pp. 1136–1147, Oct. 2019.

7. K. Xue, B. Zhu, Q. Yang, D. S. L. Wei, and M. Guizani, ‘‘An efficient androbust data aggregation scheme without a trusted authority for smart grid,’’IEEE Internet Things J., vol. 7, no. 3, pp. 1949–1959, Mar. 2020.

8. A. Saleem, A. Khan, S. U. R. Malik, H. Pervaiz, H. Malik, M. Alam, andA. Jindal, ‘‘FESDA: Fog-enabled secure data aggregation in smart grid IoTnetwork,’’ IEEE Internet Things J., vol. 7, no. 7, pp. 6132–6142, Jul. 2020.

9. S. Dahiya and M. Garg, ‘‘Unmanned aerial vehicles: Vulnerability to cyber-attacks,’’ in Proc. Int. Conf. Unmanned Aerial Syst. Geomatics. Springer,2019, pp. 201–211.

10. M. Golam, J.-M. Lee, and D.-S. Kim, ‘‘A UAV-assisted blockchainbased secure device-to-device communication in Internet of MilitaryThings,’’ in Proc. Int. Conf. Inf. Commun. Technol. Converg., Oct. 2020,pp. 1896–1898.