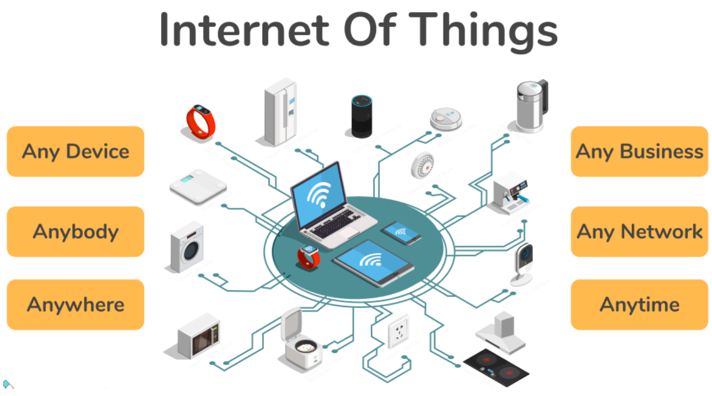
ATM Vehicle Location Privacy and Security using End-to-End Quantum Key Cryptosystems

G.Mariselvam,
ECE
Department,
PSNCET,
Tirunelveli.
India.
Selvamganesan840@gmail.com

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.

I.INTRODUCTION

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 airplane, 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

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 I analyses it to help us inform and automate our subsequent actions or decisions.

II. FIELD OF STUDY

Ghawar Said; Anwar Ghani **(**2022) [1] 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. 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.

Gabin Heo; Kijoon Chae **(**2022) [2] 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.

Nubila Nabeel; Mohamed Hadi Habaebi (2021) [3] 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.

Sungjin Yu (2020) [4] 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.

III. 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.

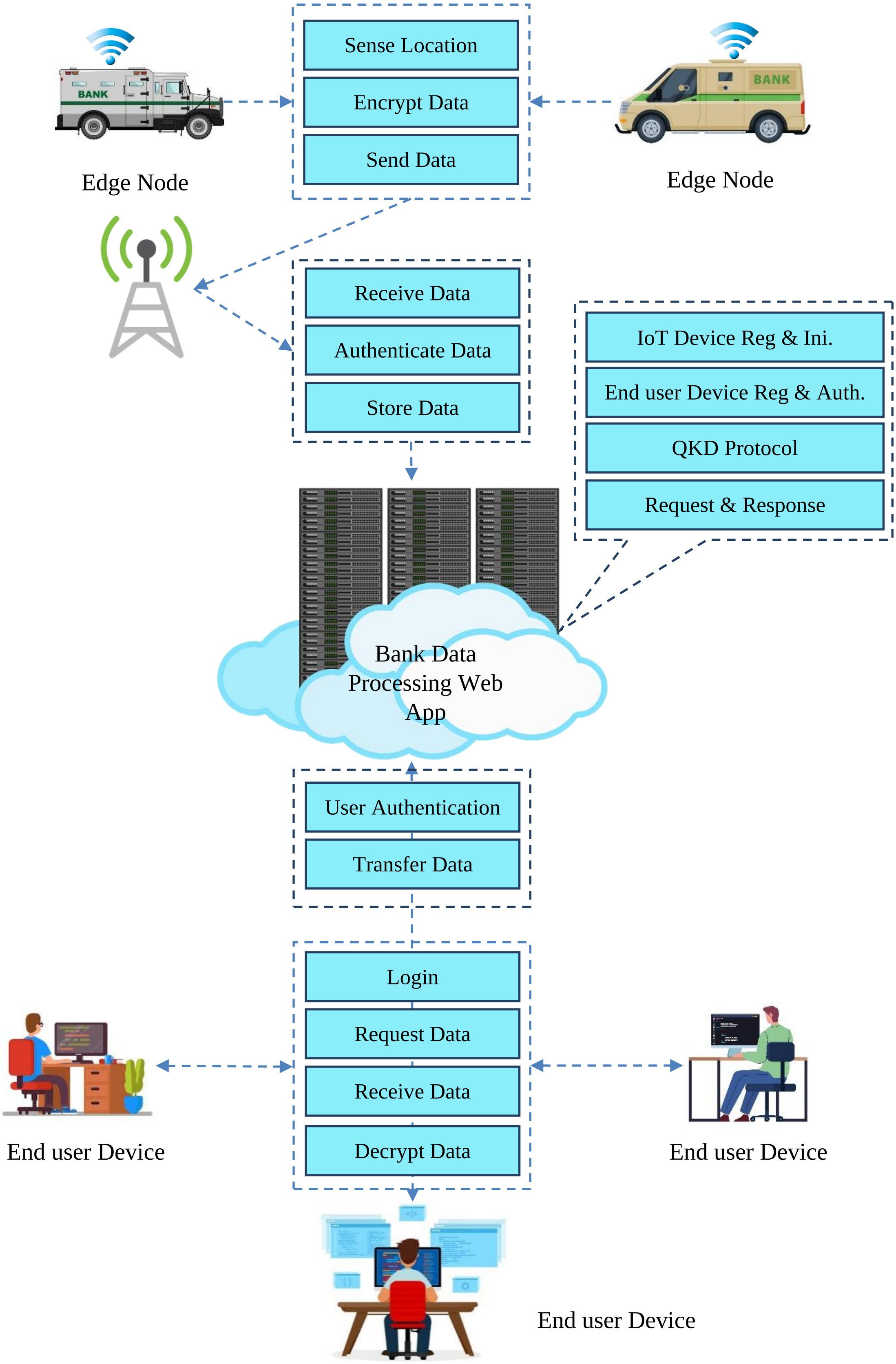
- **Private key authentication**

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.

IV. PROPOSED SYSTEMS

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 betweenthem.

SYSTEM ARCHITECTURE



4.1 system Architecture

V. RESULT

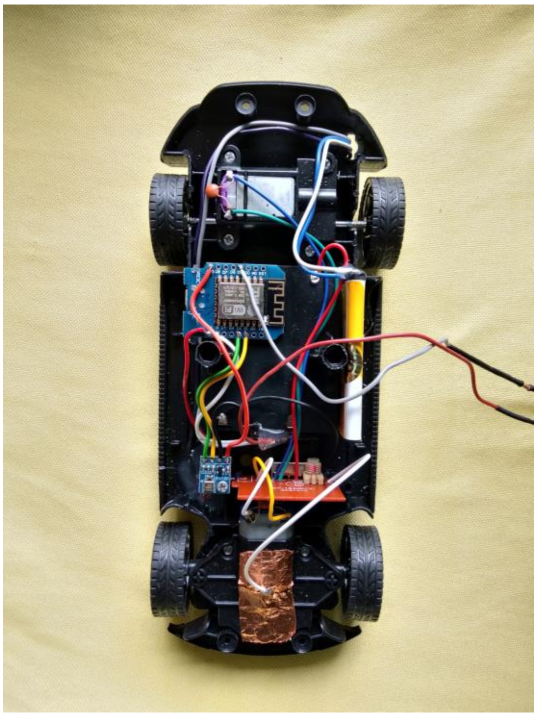
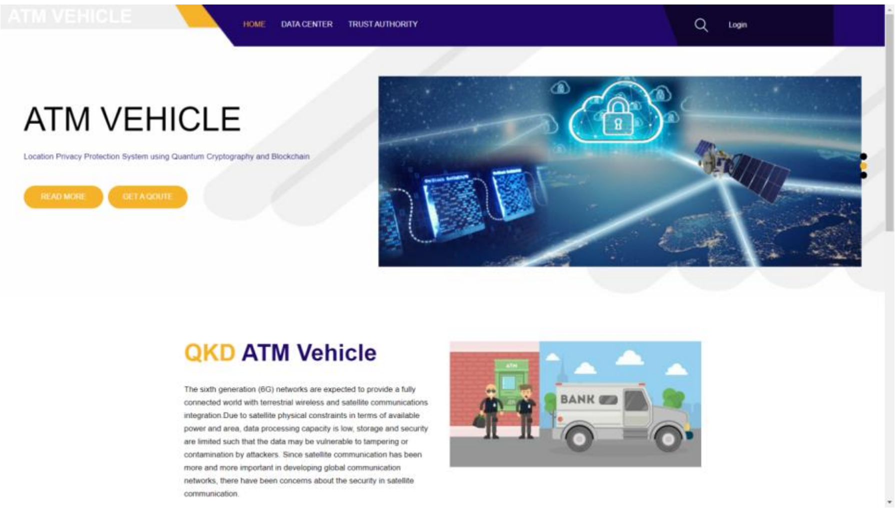


Fig 5.1 Output image



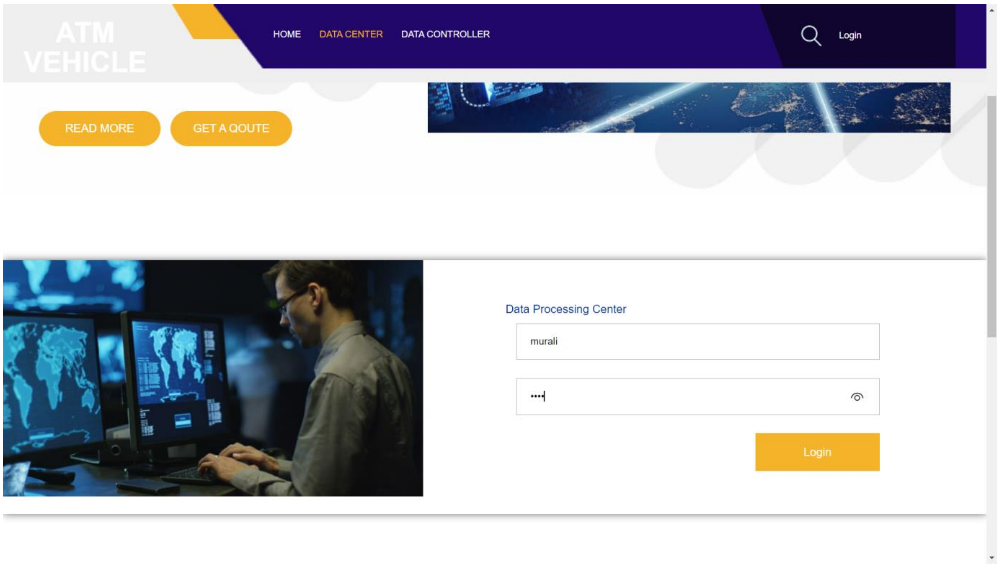
ATM VEHICLE

Location Privacy Protection System using Quantum Cryptography and Blockchain

QKD ATM Vehicle

The sixth generation (6G) networks are expected to provide a fully connected world with terrestrial wireless and satellite communications integration.Due to satellite physical constraints in terms of available power and area, data processing capacity is low, storage and security are limited such that the data may be vulnerable to tampering or contamination by attackers. Since satellite communication has been more and more important in developing global communication networks, there have been concerns about the security in satellite communication.

Fig 5.2 Home Page

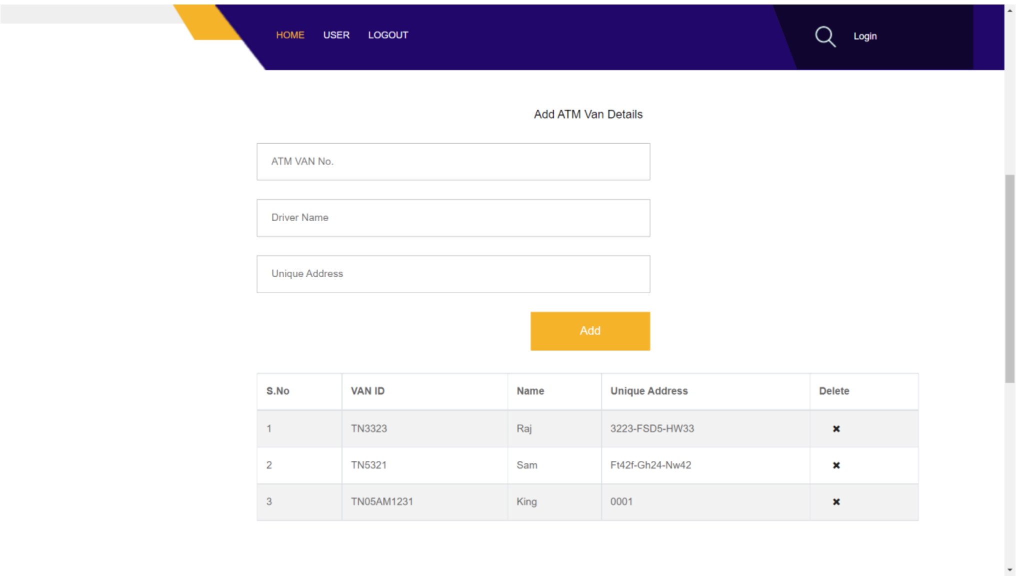


Data Processing Center

murali

••••

Fig 5.3 Data Center



Add ATM Van Details

ATM VAN No.

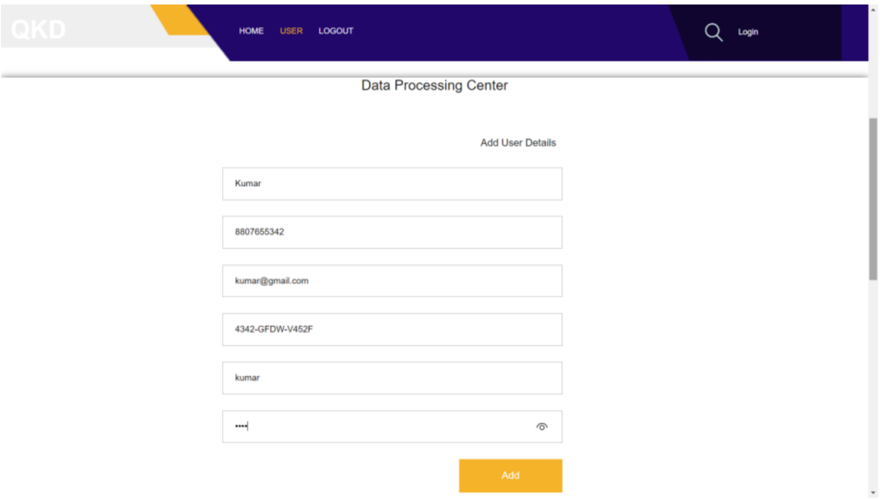
Driver Name

Unique Address

Add

S.No	VAN ID	Name	Unique Address	Delete
1	TN3323	Raj	3223-FSD5-HW33	✖
2	TN5321	Sam	Ft42f-Gh24-Nw42	✖
3	TN05AM1231	King	0001	✖

Fig 5.4 ATM Van Details



Data Processing Center

Add User Details

Kumar

8807655342

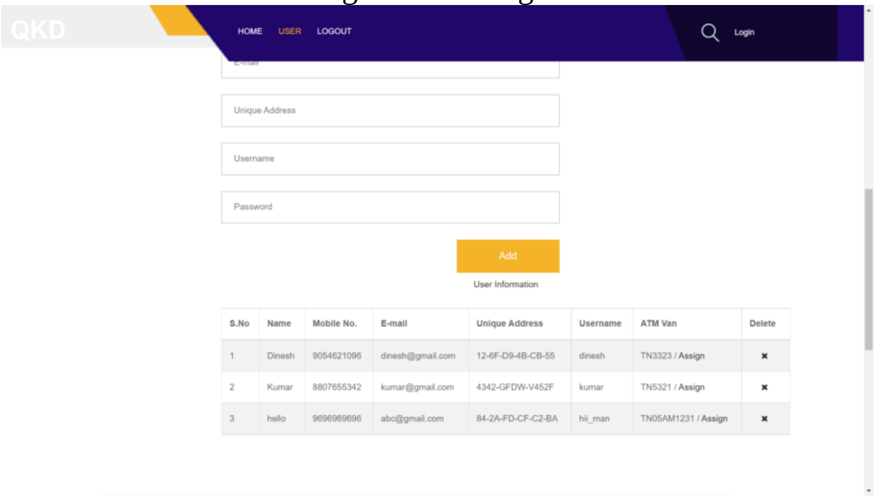
kumar@gmail.com

4342-GFDW-V452F

kumar

••••

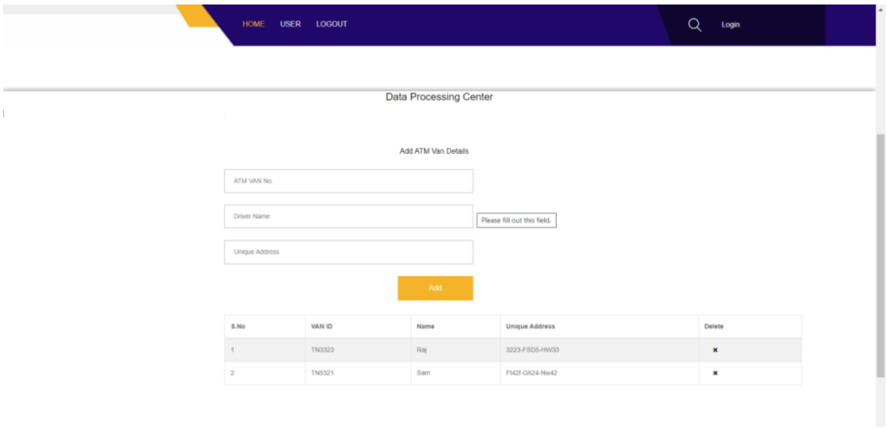
Fig 5.5 User Login



User Information

S.No	Name	Mobile No.	E-mail	Unique Address	Username	ATM Van	Delete
1	Dinesh	9054621096	dinesh@gmail.com	12-6F-D9-4B-CB-55	dinesh	TN3323 / Assign	✖
2	Kumar	8807655342	kumar@gmail.com	4342-GFDW-V452F	kumar	TN5321 / Assign	✖
3	hello	9696969696	abc@gmail.com	84-2A-FD-CF-C2-BA	hii_man	TN05AM1231 / Assign	✖

Fig 5.6 User Information



Data Processing Center

Add ATM Van Details

Please fill out this field.

S.No	VAN ID	Name	Unique Address	Delete
1	TN3323	Raj	3223-FSD5-HW33	✖
2	TN5321	Sam	Fl42f-Gh24-Nw42	✖

Fig 5.7 DATA Processing Center

VI. 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.

VII. 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. 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.
5. 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.