RESEARCH ARTICLE OPEN ACCESS

SECULSION CONSERVE SYSTEM USING PUBLIC KEY

B.Saritha*,K.Anjugam**,C.Narmatha***,P.Roja kanmani****

**(Assistant Professor,Department of Electronics and communication,Anna university/K.S.K College of engineering and technology,India.)*
Email:saritha.dsp@gmail.com

***(Assistant Professor,Department of Electronics and communication,Anna university/K.S.K College of engineering and technology,India.)*
Email:anjugamanjana@gmail.com

****(Department of Electronics and communication, Anna University /K.S.K College of engineering and technology,India.)*
Email: narmathachittrarasan@gmail.com

*****(Department of Electronics and communication,Anna University/K.S.K College of engineering and technology,India.)*

Email: rojakanmani369@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 dominates in IoT, because a large portion of world population use it. Major 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.

Keywords --QKD protocol ,Block chain technology,Advanced cryptographic technology.

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 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.

II. 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 as shown in Fig 1. 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.

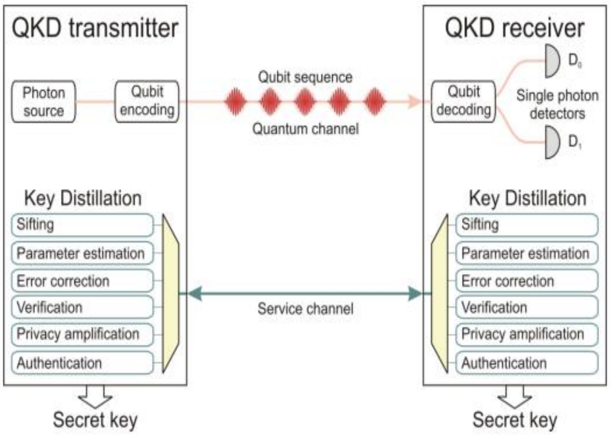


Fig.1. QKD Transmitter and Receiver

III. SYSTEM DESIGN

A. NanoGPS

Fig2. Nano GPS carries the Nano Hornet module from OriginGPS. It's the smallest GPS module with an integrated patch antenna (measuring just 10x10x3.8mm).

Despite its size, it offers superior sensitivity and outstanding performance, with time to first fix (TTFF) of less than 1 second, accuracy of approximately 1m, and tracking sensitivity down to -163dBm.

Multi Micro Hornet ORG1510-MK05 module is introducing the industry's lowest energy per fix ratio, unparalleled accuracy, and extremely fast fixes even under challenging signal conditions, such as in built-up urban areas, dense foliage or even indoor.

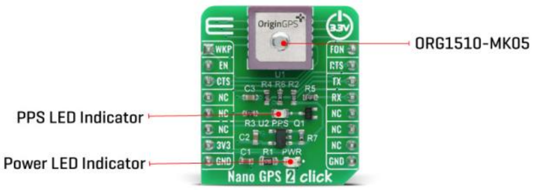


Fig.2 Nano GPS

B. ESP8266

The ESP8266 is a low-cost Wi-Fi microchip, with built-in TCP/IP networking software, and microcontroller capability.This small module allows microcontrollers to connect to a Wi-Fi network and make simple TCP/IP connections using Hayes-style commands.

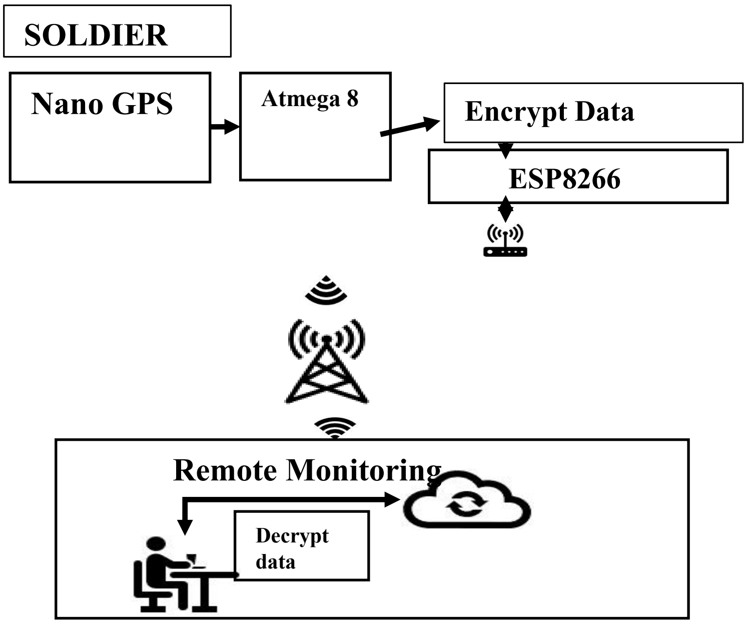
A cost-effective and highly integrated Wi-Fi MCU for IoT applications.

The ESP8266 is capable of either hosting an application or offloading all WiFi networking functions from another application processor.

C. ATMEGA8

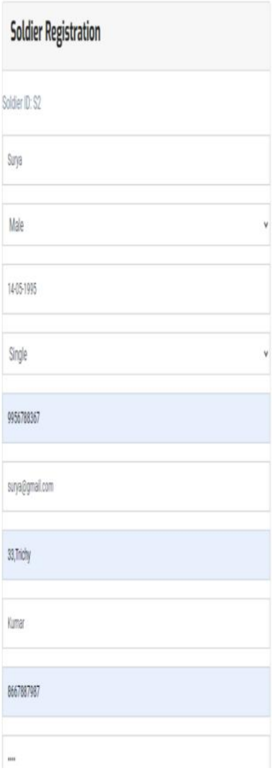
The ATmega8 is a low-power CMOS 8-bit microcontroller based on the AVR RISC architecture. ATmega8 microcontroller consists of 1KB of SRAM, 8KB of flash memory and 512 bytes of EEPROM.The ATmega8 is supported with a full suite of program and system development tools, including C compilers, macro assemblers, program simulators, and evaluation kits.ATmega8 is a powerful microcontroller that provides a highly-flexible and cost-effective solution to many embedded control applications.

D. .BLOCK DIAGRAM



E. TRACKING AND SIMULATION

I. *SOLDIER REGISTRATION*



Soldier Registration

Soldier ID: S2

Surya

Male

14-05-1995

Single

9956788367

surya@gmail.com

33,Trichy

Kumar

8667887987

....

Fig.3 Soldier Registration

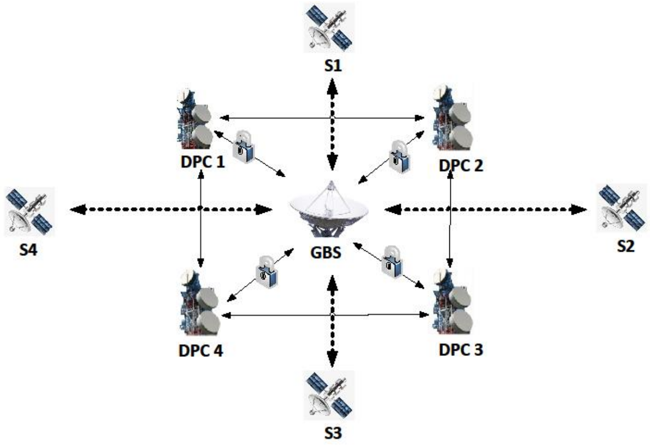
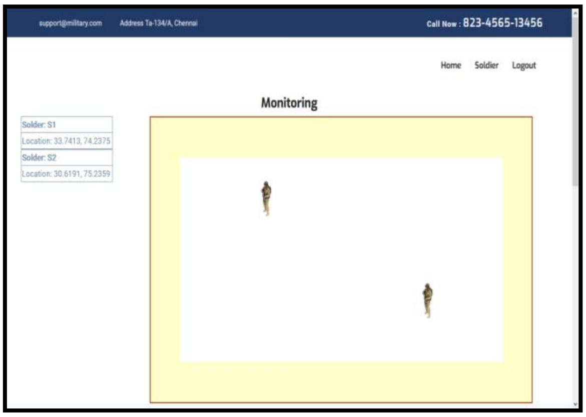


Fig.4 Encryption and data transmission

II. SOLDER TRACKING SIMULATION



support@military.com Address Ta-134/A, Chennai Call Now : 823-4565-13456

Monitoring

Solder: S1
Location: 33.7413, 74.2375
Solder: S2
Location: 30.6191, 75.2359

Fig.5 Soldier tracking system

This QKD Protocol is used in Soldier trackingas shown in Fig.5 by Encrypt and Decrypt exact location of the army soldier in defence .we can use it in any IOT Device communication.

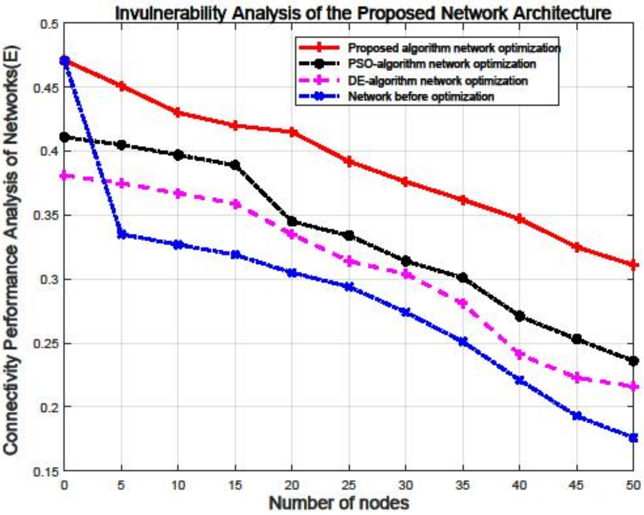


Fig.6 Invulnerability analysis of the Proposed network architecture

F. 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 cybersecurity. Two popular, yet distinctly different cryptographic applications that are under development using quantum properties include:

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 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. 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

G. USE CASES

- **Encryption and authentication of endpoint devices**

Endpoint devices include any piece of hardware that a user utilizes to interact with a distributed computing system or network. This can include canonical examples such as personal computers and mobile phones, as well as kiosks/terminals in banks, stores, and airports, as well as any kind of embedded technology connected to a broader network. Encryption of endpoint devices refers to the practice of making the contents of the device unreadable to unauthorized parties through the use of cryptography and security protocols. This is an important practice to prevent unauthorized data transfer and access, to ensure that only approved devices are allowed access to the system, and to deal appropriately with rogue or compromised devices that threaten system security through intrusions such as malware, key loggers, or viruses.

- **Cloud Storage and computing**

Options for quantum-safe cloud computing are subsumed by quantum-safe server, endpoint, and network infrastructure security. Key exchange parameters for protocols such as HTTPS should no longer make use of RSA, DSA, or ECDSA. Fortunately, cloud computing offers the distinct advantage of having a centralized IT security management system across many applications and businesses, reducing security overhead for individual enterprises and consequently offering easier transition to quantum-safe protocols. This transition is essential in particular due to both the fact that cloud storage is – by definition – remotely accessed, requiring data to traverse a public network between the user and the cloud. The need for strong encryption is further amplified by the multitude of distinct and untrusted users sharing the infrastructure.

1. 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 communicate 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. Many commercial applications have regulated security requirements, often with unique and constrained cryptographic key management needs.

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

IV. CONCLUSIONS

IoT is essentially important to improve the quality of human life by the interconnection of different technologies, smart devices, and applications. At present, 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.

ACKNOWLEDGMENT

Seculsion conserve system using public key Project by guidance bestowed by Ms.K.Anjugam Assistant Professor and support extended by the team of Instrumentation laboratory ,K.S.K college of engineering and technology. Sincere thanks to my fellow mates who collaborated in my achievement of the Project.

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 edge assisted 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 and robust 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, and A. Jindal, ''FESDA: Fog-enabled secure data aggregation in smart grid IoT network,'' 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 blockchain based secure device-to-device communication in Internet of Military Things,'' in Proc. Int. Conf. Inf. Commun. Technol. Converg., Oct. 2020, pp. 1896–1898.