A Quantum Communication Based Secure Road Condition Monitoring Application in Intelligent Internet of Vehicular Things

Kumar Prateek
Department of Information Technology
Indian Institute of Information Technology
Allahabad, Prayagraj, India.
Email: pcl2017003@iiita.ac.in

Soumyadev Maity
Department of Information Technology
Indian Institute of Information Technology
Allahabad, Prayagraj, India.
Email: soumyadev@iiita.ac.in

Neetesh Saxena
School of Computer Science
& Informatics, Cardiff University,
Cardiff, Wales, UK.
Email: nsaxena@ieee.org

***Abstract*—The expeditious and meteoric advancement in the ever-transforming transportation industry has paved the way for harmonizing and mellifluous development of the intelligent internet of vehicular things (IIoVT). Cloud computing and edge computing have resulted in numerous applications that are well deployed within smart cities to meet the spike in demand for low latency, coupled with mobility in practical IIoVT deployment. However, the underlying security of such applications depends on the time complexity of mathematical hard problems. The arrival of quantum computers has reduced computational time exponentially, thus making such applications vulnerable. Therefore, this article investigates the proposed quantum communication-based secure architecture for edge-driven IIoVT applications. The proposed architecture, utilizing quantum communication protocol, provides a new platform for developing IIoVT applications ensuring unconditional security and eavesdropper detection. Also, the paper presents a case study, namely, a quantum secured intelligent edge-driven road condition monitoring application that features automatic road conditions detection, subsequently recommending transport authorities periodically. Finally, future research directions are presented with a security perspective in IIoVT.**

***Index Terms*—Quantum Key Distribution, Security, Vehicular Things.**

I. Introduction

The internet of vehicles (IoV), which combines physical things and communication networks, could be used for providing advanced, intelligent, and secure services for humans [1]. Intelligent IoVT can transform existing IoVT services to the next level, thus envisioning the digitalization of physical things in the digital world. Now-a-days innovative communication technologies, along with physical things and human beings, are capable of facilitating numerous applications and services to be used in smart cities [2]. The IoVT can empower the design and development of smart applications and has been instrumental in collecting vast amounts of pervasive data for further analysis and decision-making. However, addressing security and privacy issues along with latency sensitivity and computational intensiveness is essential because of the low computational capabilities of the vehicle's onboard units (OBU) [3]. Cloud computing is prominent in delivering on-demand services such as data aggregation, data analysis, and data-based prediction using the abundance of computing capabilities. The different components of IIoVT with coordinated resource management can enhance the quality of service (QoS). Nevertheless, the different components of IIoVT generate a mammoth amount of data, thus confronting high latency and low transmission rate in standard cloud-based IoVT applications [4]. The enormous bandwidth requirement in standard cloud-based IoVT applications brings tremendous challenges, restraining the design and development of applications featuring high-quality experience and low latency. Edge computing utilizing computing resources at the edge solves problems of standard cloud-based IoVT applications [5]. Also, edge computing enables low latency, mobility, and scalability while facilitating real-time computation, response, and resource allocation in IoVT [6]. Despite several benefits of edge computing in IoVT applications, security threats remain challenging. With the cheap availability of computing resources, adversaries can quickly perform malicious attacks on each layer, even on the edge computing layer. Additionally, state-sponsored agencies are also active in destroying specific day-to-day services of any country to make them suffer from substantial economic loss and public unrest. The edge nodes store private information in the IoVT ecosystem; thus, a possible comprise of edge nodes will have a disastrous effect. Also, if two edge nodes collude, false messages exchanged with the rogue vehicles can easily threaten the whole IoVT system. Therefore, it is requisite to provide security and privacy in numerous applications utilizing edge computing in IIoVT [7]. In literature, almost all existing security protocols rely on mathematical hard problems such as Discrete log problem (DLP), computational Diffie hellman (CDH), or decisional Diffie hellman (DDH) to provide security.

The advent of quantum computers has significantly threatened the security protocols used nowadays for providing security in numerous applications. Peter Shor has shown that the computational time of hard problems is reduced from millions

978-1-6654-7350-7/22/$31.00 ©2022 IEEE

of years to a few seconds, thereby threatening all existing security protocols whose security depends on mathematical hard problems [8]. Additionally, quantum attacks make almost all applications employing security protocols whose security depends on mathematical hard problems vulnerable to the extent that time has now arrived to remove or update such protocols to make the application quantum resistant. Also, exponential interest in developing quantum computers by major corporations has anticipated that large bits quantum computers will arrive in the market much sooner than predicted. Quantum computing uses quantum key distribution (QKD) to exchange keys between parties. In the past, the QKD protocol has proved its technological advances through laboratory implementation [9]. Now, few-bit quantum computers are accessible to everyone to design and implement new quantum algorithms through the cloud. The users will use quantum computing as a service and subscribe to the pay-as-use model provided by different corporations. Nevertheless, not only is secure message communication essential, but eavesdropper detection and authentication play a pivotal role in providing security in many applications. The features of quantum computing include guaranteeing unconditional security-enabled eavesdropper detection by prohibiting copies of quantum states during communication, making it a perfect candidate for designing secure applications in the IIoVT ecosystem. Moreover, the use of quantum key distribution and quantum key-based authentication has the potential to guarantee unconditional security in real-time IIoVT applications. Therefore, with enough motivation in hand to safeguard the numerous applications from threats arising due to the arrival of few bits quantum computer, this article's contribution now follows:

A. Contribution

- We have proposed a novel security architecture for edge-driven IIoVT applications utilizing quantum key distribution. The proposed architecture uses properties of quantum mechanics such as superposition, entanglement, and measurement to guarantee unconditional security (security does not depend on computational hard problems).
- We have described the potential applications of the proposed security architecture. Also, we have provided a security analysis of the proposed architecture against five cyber attacks.
- We have designed and described a new road condition monitoring application using the proposed security architecture featuring security against said attacks. The designed application can assist officials of the transportation department in decision-making.

II. Related Work

The literature features many work that uses QKD for fulfilling numerous security goals spanned across multiple application areas [10]–[15]. A protocol by L. Wang et al. [10] divides the QKD-produced secrets into the segment and then reconstitutes the segment to form larger secret keys to guarantee secure communication. In the scheme, [11], a shared secret is used between the group of end devices to reduce QKD deployment cost. The scheme [12] uses both continuous variable QKD and discrete variable QKD between the device and aggregator. Notably, it uses CV-QKD between the device and aggregator separated over a short distance, whereas DV-QKD communicates over a long distance. In the scheme [13], Geeta et al. used QKD along with identity-based authentication to authenticate cloud infrastructure. Similarly, the scheme [14] utilizing QKD and classical identity authentication techniques describe a privacy-preserving authentication scheme for authenticating vehicle and roadside units in vehicular-ad-hoc networks. Besides, enrollment and verification of assets of IoV, such as RSU enrollment and verification and vehicle enrollment and verification, are well explained in [15]. Nevertheless, the wider availability of cheap computing power can compromise the IIoVT ecosystem in the future. Therefore, to address this gap, we propose a quantum secured edge-driven security architecture for IIoVT.

III. The Proposed Quantum Secured Edge driven IIoVT Architecture

A. Threat Model

The threat model describes the attacker's perspective detailing valuable assets and vulnerable points within the system. The details of various security threats are as follows:

Sybil Attack - The malicious vehicle can use a counterfeit identity to control the vehicular edge nodes, affecting the service provided to clients. The genuine vehicle cannot trust the services provided by a compromised edge-driven IIoVT. So, limitations ought to be forced on the production of identities.

Impersonation attack - Here the attacker effectively postulates the identity of any genuine vehicular edge nodes or any client vehicle by taking advantage of the media access control address and launching various attacks on the network.

Eavesdropping the Network - The adversary can eavesdrop the edge-driven IIoVT network thus can learn the unprotected message and may apply different cryptographic attacks such as ciphertext attacks and plain text attacks.

Communication Channel - In any IIoVT network, vehicles transfer messages either through V2V communication or V2I communication. The adversary can use these channels for the possible launch of attacks.

Impersonating Assets - In any IIoVT network, vehicle, RSU, and cloud infrastructure are assets. The adversary can get into the system through compromised RSU. Also, an adversary can pretend to be the legitimate vehicle in any IIoVT network to reveal important information of any assets, such as unprotected stored data and the storage space of RSU.

B. Quantum Secured Edge driven IIoVT Architecture

The proposed quantum secured edge-driven intelligent internet of vehicular things (IIoVT) architecture comprises four layers: data generating layer, edge computing layer, cloud computing layer, and application layer, as illustrated in Fig. 1. The details of each layer are as follows:

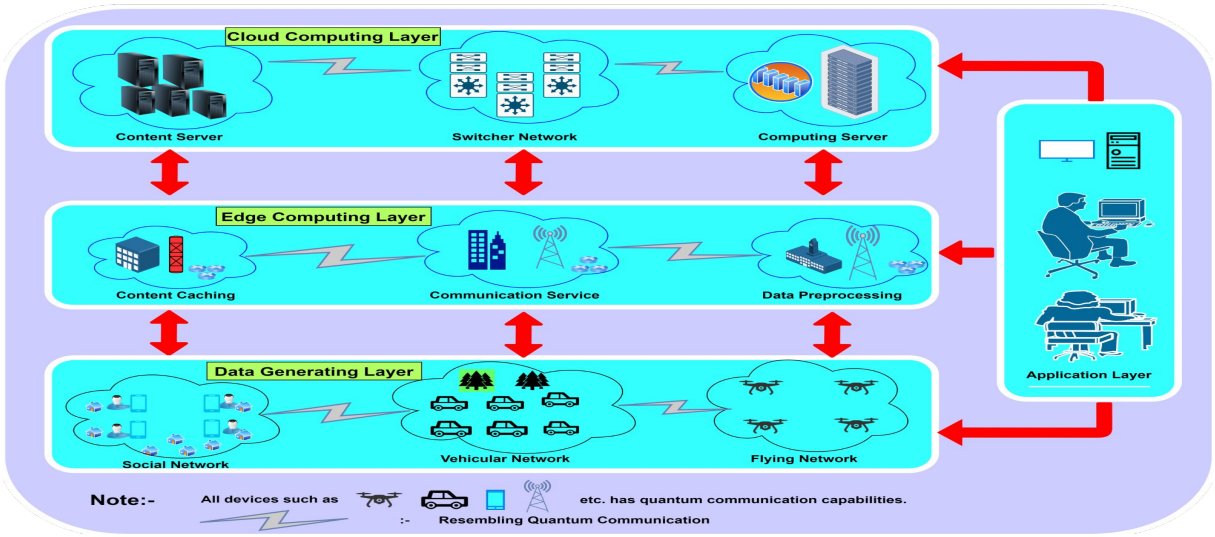

Fig. 1. Quantum Secured Edge Driven IIoVT Architecture

*1) **Data Generating layer**:* This layer corresponds to the OSI model's physical layer and acts as the proposed architecture's bottom layer. The widely known technologies such as RFID and WSN constitute the data generating layer. The RFID enables the application's efficient object identification and reliable data acquisition in different areas such as commodity transportation, public transportation, etc. In contrast, the application achieves reliability and efficiency while transmitting data from one node to another only because of WSN.

*2) **Edge Computing layer**:* This layer comprises multiple edge nodes equipped with communication capabilities, thus enabling communication between two edge nodes in addition to performing data pre-processing, content caching, etc. Also, these multiple edge nodes provide essential services effectively with low transmission delay. Sometimes, these edge nodes act as a base station for assisting numerous services in the IIoVT. These multiple edge nodes are generally categorized as stationary or movable. A smart city is generally divided into zones encompassing stationary edge nodes and movable edge nodes. Stationary edge nodes are positioned within the cell tower and installed at junctions, parking areas, or office areas. In contrast, while operational throughout the city, movable edge nodes are connected to the internet and empower neighboring vehicles in communication by providing WLAN. As these edge nodes contain processing power and transient storage, therefore, are responsible for gathering information from vehicles and performing computation (if needed), thereby reporting to the cloud server.

*3) **Cloud Computing layer**:* This layer is comprised of three sub-layers: infrastructure layer, platform layer, and software layer. The services offered at the infrastructure level are known as Infrastructure as a service (IaaS), mainly including communication and storage facilities, whereas development, testing, debugging, and numerous operations of a particular application are offered to IIoVT by the platform sub-layer. Additionally, software as a service (SaaS) is known for delivering software services through the internet. This layer, along with the edge computing layer, plays a critical role in facilitating communication and storage, delivering numerous services in IIoVT, such as traffic information, road monitoring, and large geographical area monitoring from a remote location.

*4) **Application layer**:* This layer comprises human beings and ubiquitous sensors, thus connecting the cyber and physical worlds, generating numerous opportunities for designing and implementing various applications and services. Also, the generation of an enormous amount of data from sensors not only fosters the need for efficient, meaningful extraction of information but secure and privacy-preserving communication is also desirable. Additionally, the abilities of evolving technologies such as AI and ML bring up enough opportunities for efficient statistical data analysis and prediction, thereby contributing to the decision-making process like never before.

C. Quantum Secured Edge driven IIoVT Applications

Traditionally, IIoVT applications utilizing cloud computing are designed to transfer data generated from the source to the cloud for analysis and decision-making. However, it suffers excessive bandwidth requirements and efficiency, particularly because of differences in political and geographical issues. The security of such applications depends on mathematical hard problems such as DLP, CDH, and DDH. Nevertheless, the entry of quantum computers has endangered the existing mathematical hard problems, jeopardizing all existing IIoVT applications that depend on mathematical hard problems to ensure security. Therefore, a new type of application must be developed and deployed using IIoVT that provides unconditional security, requires less bandwidth, and has a low transmission delay. What now follows is the description of the various quantum-secured edge-driven IIoVT applications.

*1) **Smart Healthcare Services**:* During a journey on the road, any quantum secure assets like movable edge vehicles

or stationary edge nodes (Roadside units) can assist the ambulance, emergency medical vehicles, and ordinary vehicles, thus contributing to saving human resources, i.e., the life of humans. Whenever any quantum secure edge node detects abnormal health data from an ambulance or ordinary vehicle, just after storing it in the driver's electronic health record (EHR) corresponding to a particular vehicle, it sends the EHR record to the doctor for medical advice. Finally, the quantum secure edge node sends the advice to an ambulance. Generally, medical data (such as heart rate, blood pressure) could be used by quantum secure edge nodes to detect unusual health conditions of the driver, generating a warning to the driver about his health so that a possible mishappening on the road could be prevented. Also, the quantum secure edge node can send a possible accident warning to vehicles and nearby transportation authorities to avoid serious accidents.

*2) **Smart Trip Services**:* IIoVT can enable smart trip services efficiently by saving energy and realizing the vision of green travel. Interactive interfaces could easily handle the integration of transportation modes and traffic management to meet the travel requirements of the vehicle while commuting a journey. Mobility as a service is in great demand now-a-days. These services generally help trip planners by providing real-time traffic monitoring and mobile communication utilizing various tools such as machine learning-based prediction, geographical information technologies, and satellite positioning. Smart trip services, with the help of quantum secure IIoVT, will not only save time and resources for the travelers but also notify them with a possible unconditionally secure real-time prediction of areas they are planning to commute.

*3) **Over Speed Regulation**:* During the journey on the road, any quantum secure movable edge vehicle or quantum secure stationary edge node (Roadside units) can assist each vehicle commuting in that area by observing the individual speed of the vehicle. Afterward, the quantum secure edge nodes can warn the driver to lower their speed per that area's speed regulation, thereby preventing possible accidents that could have materialized due to overspeeding. Specifically, the quantum secure edge node stores the speed data in the driver's vehicle record (VR) and sends the vehicle record to the speed control department of the transportation agency, corresponding to overspeeding vehicle commuting in a particular area. Afterward, the quantum secure edge nodes warn the driver of overspeeding along with instructions to lower the vehicle's speed. Generally, the quantum secure edge node could use speed-related data (if speed crosses 25km/h) to detect overspeeding, thereby warning the driver about the speed limit rule (max speed limit is 25Km/hr) so that fine could be imposed for violators.

*4) **Other Smart City Services**:* While commuting on the road, any vehicle can capture the environment and transfer the image to quantum secure edge nodes and subsequently to the cloud. Other vehicles can access real-time information regarding empty parking spots within the city. The quantum secure edge nodes could provide empty parking spot data, such as the location of parking spots and the distance from the location of the requested vehicle, enabling real-time identification of empty parking spots. Besides, installing cameras throughout the city for crime monitoring is not feasible. Many crimes occur alongside roads which could be captured and transferred using quantum communication by vehicles roaming nearby the crime location. Later, through a cloud server, crime regulation authorities could access records and punish the offenders if found guilty.

IV. Case Study and Experimental Design

This section describes a quantum secured edge-driven road condition monitoring application utilizing the proposed security architecture. The quantum secured edge-driven road condition monitoring application automatically detects road conditions and recommends the transportation department's officials for deciding on possible renovation.

A. Road Condition Monitoring Application

The reinforcement technique is widely used to solve various issues of IoVT systems with higher accuracy [16]. A model-free reinforcement learning technique, namely Q-learning, will be a perfect candidate to enable road monitoring applications that embrace low computation complexity. We designed a Q-learning-based edge-driven road monitoring IIoVT application that uses quantum communication protocol to guarantee secure communication. The designed system first uses a popular BB84 quantum key distribution algorithm to provide unconditional communication security. The Q-learning process is executed on the edge nodes at junctions and hotspot areas such as parking places. The BB84 protocol [17] uses the law of quantum mechanics such as superposition, interference, and entanglement to enable unconditional security during communication. Additionally, with the No cloning theorem, copying quantum states is prohibited during communication, thus allowing eavesdropper detection (if any) during communication. The work [18] very well explains the security of the BB84 protocol. The Q-learning method in the proposed application utilizes a trial and error mechanism to observe irregularities in the road (pitfalls, potholes, cracks). Specifically, all features of road information received from edge nodes are observed. Subsequently, extraction of essential features of road information is performed. Thereafter, proper analysis of extracted essential features is performed based on system specification, thus comparing with the ideal condition of roads. Finally, if the compared result is found to be abnormal, a recommendation to renovate the road is forwarded to the authorities.

Fig. 2 illustrates the proposed approach. Precisely, after exchanging road information through a quantum communication protocol, edge nodes use Q- learning to find road irregularities. The proposed approach with learning rate α, discount factor β, and reward function r(s,a) updates the Q value accordingly. The edge node across the city executes the entire process of Q- learning by dividing the time into multiple episodes. In every episode, with respect to accuracy about transformation, action a is chosen in state s, thereby receiving reward r(s,a). Subsequently, analysis of essential

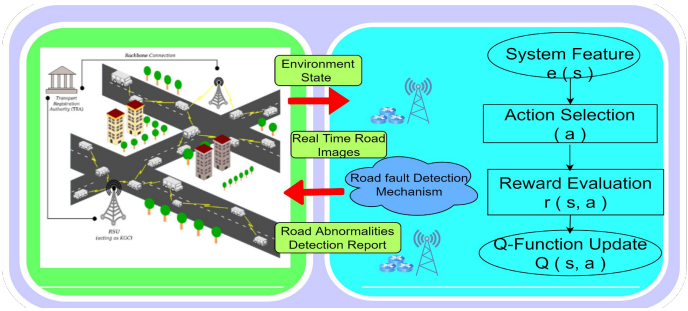

Fig. 2. Road Condition Monitoring framework in IIoVT

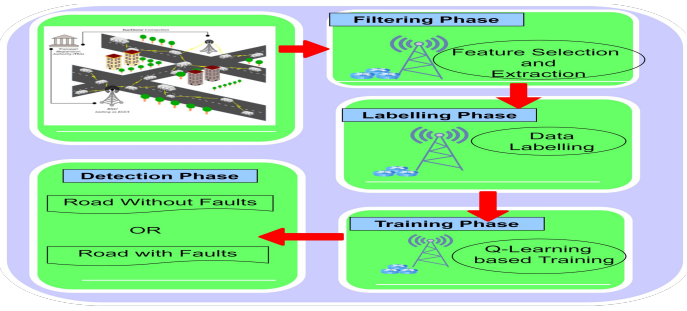

Fig. 3. Q learning Based Road Condition Monitoring

features of road information is performed in state s. If an uncommon road condition is noticed, the edge node executes an action during transformation to new state s'. Nevertheless, we may note that dependency of transformation probability P(s',a) relies on the current state, i.e., it is independent of the previous state and action. Besides, Fig. 3. clearly illustrates the road condition monitoring using edge computing. The entire process is completed using four phases: filtering, labelling, training, and detecting. In the filtering phase, edge nodes perform filtering on road images with a focus on carrying out feature selection and feature extraction. After successful feature extraction, each data is labelled in the labelling phase. Now, to classify the extracted features, Q learning training is performed. Finally, the detection phase results in the detection of road abnormalities by comparing ideal road conditions. Suppose the detection phase results produce some abnormalities (e.g., road cracks, road potholes). In that case, a report will be automatically sent to higher authorities through the cloud for a possible renovation of roads.

V. Result and Analysis

The proposed work utilizes the BB84 protocol to provide unconditional communication security in the discussed quantum secured edge-driven road condition monitoring application. Consequently, the simulation of the BB84 protocol has been performed on the quantum simulators. The details of the experimental setup are tabulated in Table I.

TABLE I
Experimental Setup

Components	Details
Virtual Environment	Anaconda Navigator
Operating System	Windows 10
Notebook Used	Jupyter Notebook
Clock Speed	3.20 GHz
Processor	Intel Core-i7
Simulator Used	QASM Simulator
Scripting Language	Python
Random Access Memory	16 GB
Software Development Kit	Qiskit

The experimental setup comprises of open source software development kit, namely QisKit [19], python scripting language, and jupyter notebook along with Windows 10 machine powered with core-i7 processor @ 3.20 GHz and 16 GB RAM. The Qiskit uses "$qasmsimulator$" in the backend. Through this experiment, we measured the simulation parameters such as information leakage, length of the established key before privacy amplification, the established final key length while switching eavesdropping rate, and an initial number of qubits one by one. The experiment is executed in a Jupyter notebook using Anaconda's virtual environment.

TABLE II
Simulation Results

Simulation Parameters	Values (in bits)					
Initial number of qubits	500	600	700	800	900	1000
Eavesdropping rate	0.2	0.2	0.2	0.2	0.2	0.2
Information leakage	52	48	46	48	48	48
Initial key length	190	240	260	290	374	390
Final key length	120	170	190	250	305	320
Final estimated error	0	0.02	0.05	0	0.11	0.03

A. Performance Evaluation

The simulation results are reported in Table II and illustrated in Fig. 4. & Fig. 5. Precisely, Fig. 4. shows the variation of performance parameters when the initial number of qubits is kept constant at 600. In contrast, Fig. 5. shows how the performance parameters vary when the eavesdropping rate is kept constant. It may be clear from the figures that the final key length and key length before privacy amplification increase linearly as the initial number of qubits are increased. Also, there is a linear decrement in key length and a linear increase in information leakage concerning an increase in eavesdropping rate. Therefore, the communication security of road monitoring applications is independent of the number of qubits.

B. Security Analysis

1) Mutual Authentication: Device-independent QKD-based authentication is well known to authenticate the sender and receiver with the freedom to choose any scheme. The BB84 protocol is used in the proposed security architecture to produce the secret keys. The BB84-produced keys could be divided into three parts: authentication, encryption, and confirmation, or into two parts: authentication and encryption. Also, quantum channels may use BB84-produced keys to prepare quantum states.

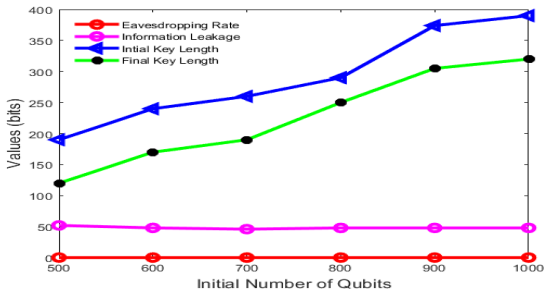

Fig. 4. Performance Parameters with constant initial number of qubits

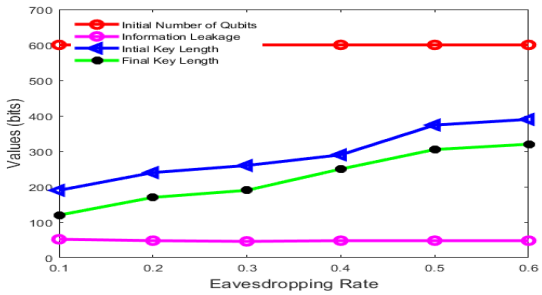

Fig. 5. Performance Parameters with constant eavesdropping rate

2) Resistance to Sybil attack: The QKD-based secret key cannot be reproduced or renewed without proper identity authentication from a trusted authority, thereby resisting the illegal production of identities.

3) Resistance to Impersonation attack: During vehicle registration, the BB84-produced secret could be shared as identification information. If any adversary tries to impersonate, he requires a quantum secret, which is impossible to regenerate.

4) Resistance to Man in the Middle attack: The No cloning theorem prohibits the creation of identical unknown quantum states, thus resisting Man in the Middle attack.

5) Communication Channel: The secret key generated and distributed using QKD protocols provides unconditional security using properties of quantum mechanics. As soon as qubits are measured in the communication channel, it collapses, allowing immediate eavesdropper detection.

6) Future Proof: QKD protocols are independent of the assumption of computational complexity to provide security; therefore, they are not threatened due to evergrowing computational power.

VI. Conclusion and Future Work

This article presents a quantum secured edge-driven security architecture for designing and developing numerous intelligent internet of vehicular things (IIoVT) applications. Besides, many quantum secured edge-driven intelligent IoVT applications are discussed. The article also narrates a case study on a quantum communication-based road condition monitoring application that uses Q learning and features automatic road conditions detection guaranteeing unconditional security. In the future, we will design a new privacy-preserving authentication protocol for vehicular communication in IIoVT featuring unconditional security and conditional privacy.

Acknowledgement

This work was supported by Ministry of Education, Government of India.

References

[1] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE internet of things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[2] Z. Su, Y. Wang, Q. Xu, and N. Zhang, "Lvbs: Lightweight vehicular blockchain for secure data sharing in disaster rescue," *IEEE Transactions on dependable and secure computing*, 2020.

[3] P. Bagga, A. K. Das, M. Wazid, J. J. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: taxonomy, analysis, and challenges," *Ieee Access*, vol. 8, pp. 54 314–54 344, 2020.

[4] X. Wang and Y. Li, "Content retrieval based on vehicular cloud in internet of vehicles," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 3, pp. 582–591, 2019.

[5] Y. Dai, D. Xu, S. Maharjan, G. Qiao, and Y. Zhang, "Artificial intelligence empowered edge computing and caching for internet of vehicles," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 12–18, 2019.

[6] J. Feng, Z. Liu, C. Wu, and Y. Ji, "Mobile edge computing for the internet of vehicles: Offloading framework and job scheduling," *IEEE vehicular technology magazine*, vol. 14, no. 1, pp. 28–36, 2018.

[7] J. Zhang and K. B. Letaief, "Mobile edge intelligence and computing for the internet of vehicles," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 246–261, 2019.

[8] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*. Ieee, 1994, pp. 124–134.

[9] R. Y. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution," *New Journal of Physics*, vol. 11, no. 4, p. 045024, 2009.

[10] L. Wang, D. Wang, J. Gao, C. Huo, H. Bai, and J. Yuan, "Research on multi-source data security protection of smart grid based on quantum key combination," in *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*. IEEE, 2019, pp. 449–453.

[11] R. Diovu and J. Agee, "Enhancing the security of a cloud-based smart grid ami network by leveraging on the features of quantum key distribution," *Transactions on Emerging Telecommunications Technologies*, vol. 30, no. 6, p. e3587, 2019.

[12] G. Bebrov, R. Dimova, and E. Pencheva, "Quantum approach to the information privacy in smart grid," in *2017 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) & 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP)*. IEEE, 2017, pp. 971–976.

[13] G. Sharma and S. Kalra, "Identity based secure authentication scheme based on quantum key distribution for cloud computing," *Peer-to-Peer Networking and applications*, vol. 11, no. 2, pp. 220–234, 2018.

[14] K. Prateek, F. Altaf, R. Amin, and S. Maity, "A privacy preserving authentication protocol using quantum computing for v2i authentication in vehicular ad hoc networks," *Security and Communication Networks*, vol. 2022, 2022.

[15] Z. Chen, K. Zhou, and Q. Liao, "Quantum identity authentication scheme of vehicular ad-hoc networks," *International Journal of Theoretical Physics*, vol. 58, no. 1, pp. 40–57, 2019.

[16] Z. Ning, K. Zhang, X. Wang, L. Guo, X. Hu, J. Huang, B. Hu, and R. Y. Kwok, "Intelligent edge computing in internet of vehicles: a joint computation offloading and caching solution," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2212–2225, 2020.

[17] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *arXiv preprint arXiv:2003.06557*, 2020.

[18] V. Scarani and R. Renner, "Security bounds for quantum cryptography with finite resources," in *Workshop on Quantum Computation, Communication, and Cryptography*. Springer, 2008, pp. 83–95.

[19] "Qiskit SDK," https://qiskit.org/, Accessed: 2022-01-19.