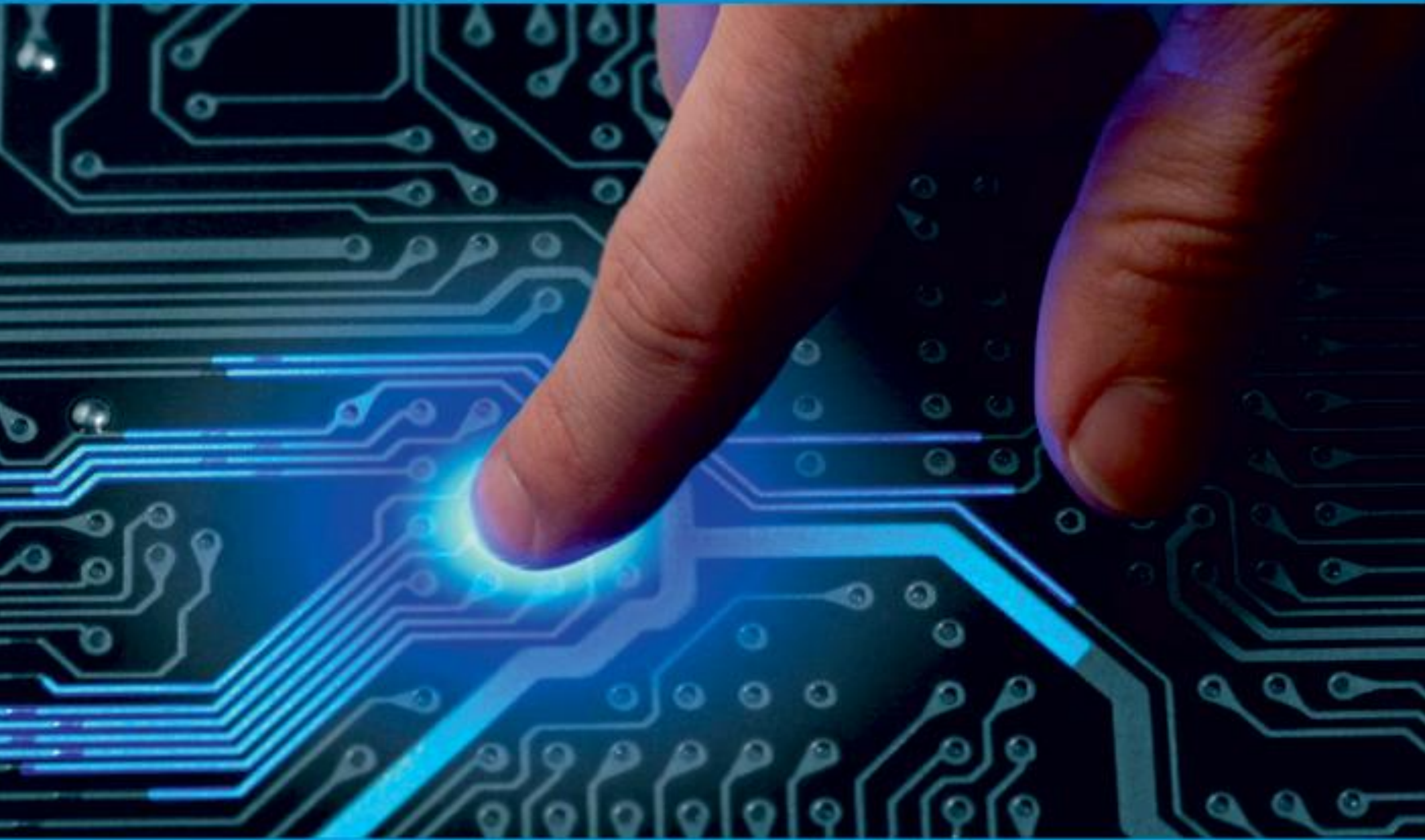
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 5, May 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| DOI: 10.15680/IJIRCCE.2024.1205210 |

Secure Satellite Communication Using Quantum-Secured Blockchain with QKD Protocol

Dr. G. Kavitha, G. Raghul, Dr. G. Kalaimani

Professor & HOD, Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Assistant Professor, Department of CSE, Muthayammal Engineering College (Autonomous), Rasipuram, Tamil Nadu, India

Professor, Department of CSE, Karpagam college of engineering, Coimbatore, India

ABSTRACT: The sixth generation (6G) networks are expected to provide a fully connected world with terrestrial wireless and satellite communications integration. The security of these transactions is essential. Blockchain is one of the most promising solutions because of its decentralized and distributed ledger technology, and has been employed to protect these transactions against such attacks. However, the security of blockchain relies on the computational complexity of certain mathematical functions, and because of the evolution of quantum computers, its security may be breached in real-time in the near future. Therefore, researchers are focusing on combining quantum key distribution (QKD) with blockchain to enhance blockchain network security. This new technology is known as quantum-secured blockchain. This article describes different attacks in optical networks and provides a solution to protect networks against security attacks by employing quantum-secured blockchain in optical networks. It provides a brief overview of blockchain technology with its security loopholes, and focuses on QKD, which makes blockchain technology more robust against quantum attacks. Next, the article provides a broad view of quantum-secured blockchain technology. It presents the network architecture for the future research and development of secure and trusted optical networks using quantum-secured blockchain. The article also highlights some research challenges and opportunities.

KEYWORDS: Block chain based access control, Quantum protocol, satellite Transaction, true negative rate, true positive rate, PoST, block chain authentication

I. INTRODUCTION

A satellite is a body that orbits around another body in space. There are two different types of satellites – natural and man-made. Examples of natural satellites are the Earth and Moon. The Earth rotates around the Sun and the Moon rotates around the Earth. A man-made satellite is a machine that is launched into space and orbits around a body in space.

Figure 1.1. Satellite

Man-made satellites come in many shapes and size and have different pieces of instruments on them to perform different functions while in space. Satellite Communication Satellite communication is the method of transporting information from one place to another using a communication satellite in orbit around the Earth. Watching the English Premier League every weekend with your friends would have been impossible without this. A communication satellite is an artificial satellite that transmits the signal via a transponder by creating a channel between the transmitter and the receiver located at different locations on the Earth.Telephone, radio, television, internet, and military applications use satellite communications. Believe it or not, more than 2000 artificial satellites are hurtling around in space right above your heads.

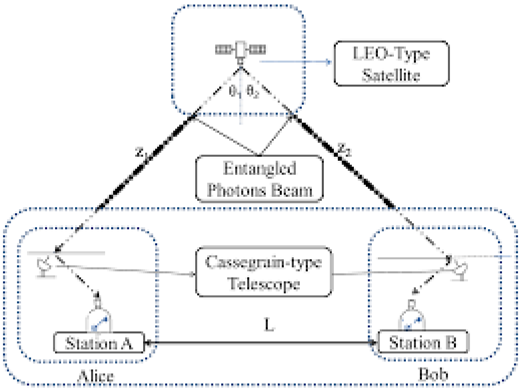


Figure 2 Satellite Communication

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.

II. LITERATURE SURVEY

Satellite Communication comes with many benefits and various risks. Cryptographic algorithms should develop security solutions that protect GEO Satellite networks and minimize security risks.As security is the prime concern for any communications, the traditional security techniques are 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 (Standard Encryption Standard) is a 64-bit symmetric block encryption algorithm. This algorithm works on 64-bit blocks 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. First, the transition is performed according to a fixed table (initial permutation), which divides a 64-bit block of plain text into two 32-bit blocks, each of which performs 16 identical operations, called rounds. The two halves are connected, and the first inversion of the permutation is performed. The purpose of the first implementation is clear. This does not affect the security of the algorithm. Therefore, small blocks of plain text and cipher text can be loaded into an 8-bit chip. Only half of the original 64-bit block is used in one run. The rounds alternate between the two halves.

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. "Brute force" is a painstaking effort (as opposed to an intelligent strategy) through repeated attempts and efforts. The Brute Force attack automatically uses automated tools and then it therefore it takes guesses various combinations until a hacker breaks the key.

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 subkeys with a total of 4168 bytes.

III. METHODS

There are essentially three types of orbits classified by the satellite altitude: geostationary earth orbit (GEO), medium earth orbit (MEO), and low earth orbit (LEO). Among them, GEO satellites are stationary relative to the earth’s surface so that the doppler shift is negligible and has a lower transmission outage probability than non-GEO satellites. The GEO satellites work at very high altitudes (≈35,786 km) and can offer the most extensive coverage. Thanks to the low outage probability and wide coverage, GEO satellites are preferred in our proposed protocol.

Satellite communications systems enable the sending and receiving of information worldwide, offering internet access, television, telephone, radio, and other civilian and military operations.The advent of HTS(high-throughput satellite) systems has greatly enhancedtechnical capabilities and offered wideband services at lowercosts. Significant improvements are expected on the forthcoming mega-constellations in low Earth orbits that willdeploy thousands of satellites, providing full earth coverageto minimize delays in addition to wide bandwidth. The use ofsatellites, given these characteristics, can increase efficiencyin providing large sets of services and applications that aresecurity-sensitive, such as telemedicine, banking, search andrescue, sensor networks, and content delivery network feed.However, in many cases, the security of satellite communication has been seriously compromised, resulting in covertdangers. In satellite communications (and even in terrestrial systems), hackers can interfere, intercept, or modifywireless network systems remotely, attack the equipment of flight crews, and control the positioning and transmissionof satellite communication antennas.According to satellite communication protocols, the use of space in satellitecommunications can be developed independently to enhancecommunication security. Recommendations have been proposed to further increase the unity and compatibility of communication protocols for space. A single security mechanismis insufficient to meet the security requirements for satellite communication services. In this project, Quantum Key Cryptography and blockchaintechnology is introduced to analyse the security of satellitecommunication networks in terms of access control, confidentiality, and security authentication.

Quantum 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.

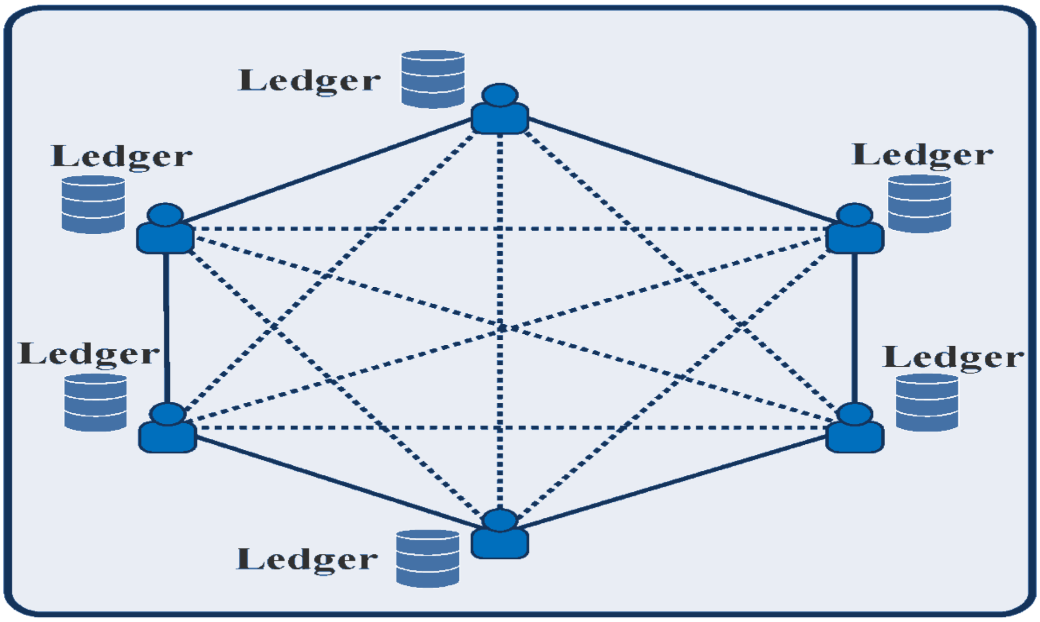


Fig 3: Securing Optical Networks Using Quantum-Secured Blockchain

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.

IV. RESULT ANALYSIS

Each modification in software impacts unmodified areas, which results serious injuries to that software. So the process of re-testing for rectification of errors due to modification is known as regression testing. Installation and Delivery Installation and Delivery is the process of delivering the developed and tested software to the customer. Refer the support procedures Acceptance and Project Closure Acceptance is the part of the project by which the customer accepts the product. This will be done as per the Project Closure, once the customer accepts the product; closure of the project is started. This includes metrics collection, PCD, etc….

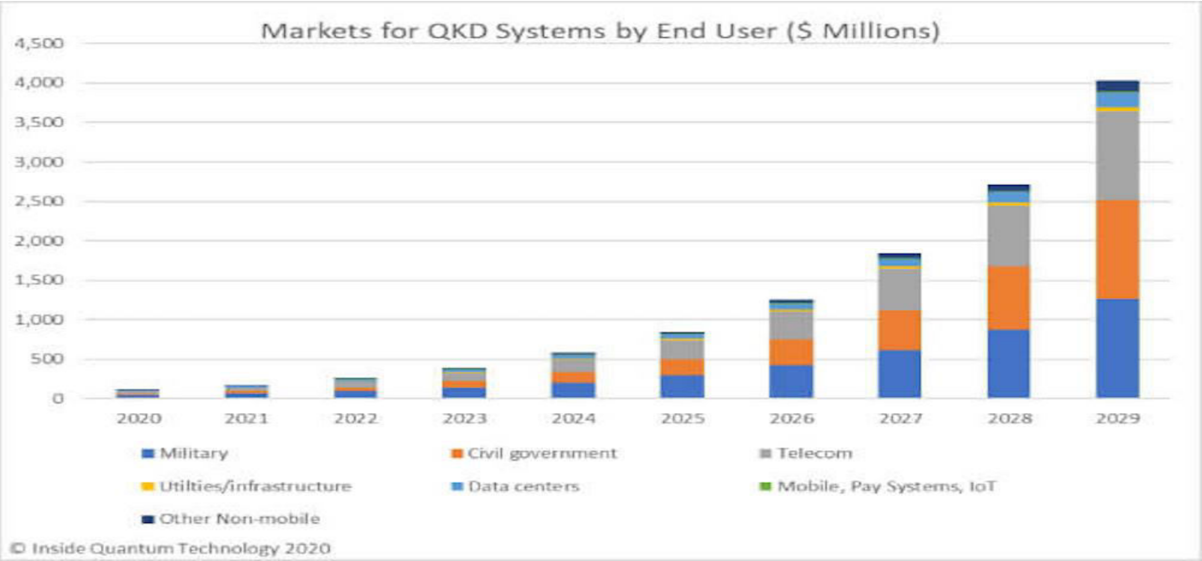


Fig 4: Result Analysis

This subsection discusses the research directions in the area of quantum-secured blockchain technology. In the area of communication and networking, artificial intelligence (AI), machine learning (ML), deep learning (DL), and reinforcement learning (RL) have been used as effective solutions to address various problems and challenges. AI/ML has the capability to take decisions and automate and optimize the system for better performance. For an improved security, speed, and scalability, AI/ML can help to construct an intelligent system on the quantum-secured blockchain. Additionally, recent advances in AI/ML, such as DL and RL, can be exploited to propose a secure and robust consensus in quantum-secured blockchain. AI/ML plays an important role in providing protection against node/link failures in quantum blockchain-based optical networks with confidentiality and privacy. A new combination of quantum-secured blockchain and AI/ML techniques will be able to build more robust and trusted optical networks against various security breaches. However, such a combination of security and intelligence is not currently developed and also might face various challenges in this domain. Hence, efforts are needed to combine quantum-assisted blockchain with AI/ML/DL/RL and design more secure, trusted, and intelligent optical networks.

V. CONCLUSION

The satellite communication channel is different not only from the common mobile channel but also from the ground station channel. The satellite communication channel is the fusion of the satellite channel and the mobile communication channel. Satellite communication channels are extremely vulnerable to hackers and external interference signals. Protecting satellite networks from illegal information access and use can be extremely challenging. In this project, Quantum Key Cryptography and blockchain technology is introduced to analyze the security of satellite communication networks in terms of access control, confidentiality, and security authentication. The proposed scheme is developed to solve the security problem of using a centralized database in satellite communication. The simulation results show that the proposed method was able to significantly improve security and protection for satellite communications. In the future, the blockchain-satellite system will depend on cloud constellations for managingdata centers in orbit, where companies can upload their data and bypass ground networks; this approach will help governments and companies obtain information from different sources and orbits in space20

REFERENCES

1. Y. Xue, ``Satellite-relayed intercontinental quantum network," J. Phys.,Conf. Ser., vol. 2229, no. 1, Mar. 2022, Art. no. 012028.
2. P. Tedeschi, S. Sciancalepore, and R. D. Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," Comput. Netw., vol. 216, Oct. 2022, Art. no. 109246.
3. H. D. Le, P. V. Trinh, T. V. Pham, D. R. Kolev, A. Carrasco-Casado,T. Kubo-Oka, M. Toyoshima, and A. T. Pham, ``Throughput analysis for TCP over the FSO-based satellite-assisted internet of vehicles," IEEE Trans. Veh. Technol., vol. 71, no. 2, pp. 1875-1890, Feb. 2022.
4. M. E. Sudip, A. Mukherjee, A. Roy, N. Saurabh, Y. Rahulamathavan, and M. Rajarajan, ``Blockchain at the edge: Performance of resource- constrained IoT networks," IEEE Trans. Parallel Distrib. Syst., vol. 32, no. 1, pp. 174-183, Jan. 2021.
5. T. Duan and V. Dinavahi, ``Starlink space network-enhanced cyberphysical power system," IEEE Trans. Smart Grid, vol. 12, no. 4,pp. 3673-3675, Jul. 2021
6. S. Nazir, S. Patel, and D. Patel, "Autoencoder based anomaly detection for SCADA networks," Int. J. Artif. Intell. Mach. Learn., vol. 11, no. 2, pp. 83–99, Jul. 2021.
7. S. Fu, J. Gao, and L. Zhao, ``Integrated resource management for terrestrial-satellite systems," IEEE Trans. Veh. Technol., vol. 69, no. 3, pp. 3256-3266, Mar. 2020.
8. K. Li, H. Zhou, Z. Tu, W. Wang, and H. Zhang, ``Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning," IEEE Access, vol. 8, pp. 214852-214865, 2020.
9. H.-N. Nguyen, N.-L. Nguyen, N.-T. Nguyen, A.-T. Le, N.-D. X. Ha, D.-T. Do, and M. Voznak, ``Reliable and secure transmission in multiple antennas hybrid satellite-terrestrial cognitive networks relying on NOMA," IEEE Access, vol. 8, pp. 215044-215056, 2020.
10. M. Q. Vu, T. V. Pham, N. T. Dang, and A. T. Pham, ``Design and performance of relay-assisted satellite free-space optical quantum key distribution systems," IEEE Access, vol. 8, pp. 122498-122510, 2020.
11. O. S. Badarneh, P. C. Sofotasios, S. Muhaidat, S. L. Cotton, K. M. Rabie,and N. Aldhahir, ``Achievable physical-layer security over composite fading channels," IEEE Access, vol. 8, pp. 195772-195787, 2020.
12. H. Yang, Y. Liang, Q. Yao, S. Guo, A. Yu, and J. Zhang, ``Blockchain-based secure distributed control for software defined optical networking," China Commun., vol. 16, no. 6, pp. 42-54, Jun. 2019.
13. L. Xu and F.Wu, ``A lightweight authentication scheme for multi-gateway wireless sensor networks under IoT conception," Arabian J. Sci. Eng., vol. 44, no. 4, pp. 3977-3993, Apr. 2019.
14. J. Li, Y. Yao, G. Wu, J. Hou, W. Yu, B. Liu, and J. Liu, ``Broadband laser Doppler frequency shift emulator for satellite laser communication," IEEE Photon. J., vol. 11, no. 6, pp. 1-12, Dec. 2019.
15. Y.-H. Gong, K.-X. Yang, H.-L. Yong, J.-Y. Guan, G.-L. Shentu, C. Liu,F.-Z. Li, Y. Cao, J. Yin, S.-K. Liao, J.-G. Ren, Q. Zhang, C.-Z. Peng, andJ.-W. Pan, ``Free-space quantum key distribution in urban daylight withthe SPGD algorithm control of a deformable mirror," Opt. Exp., vol. 26,no. 15, pp. 18897-18905, 2018.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 ☎ 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details