IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 3, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103115 |

A Comprehensive Review: Evaluating the Efficiency of Block Chain based Secure Framework in IoT Networks

Prof. Divya Pandey, Prof. Khushboo Choubey, Prof. Zeba Vishwakarma

Department of CSE, Baderia Global Institute of Engineering and Management, Jabalpur, (M.P.) India

ABSTRACT: The rapid proliferation of Internet of Things (IoT) devices has heightened concerns about security and data integrity within interconnected networks. Blockchain technology, with its decentralized and tamper-proof characteristics, has emerged as a promising solution to these challenges. This review paper critically evaluates the efficiency of blockchain-based secure frameworks in IoT networks. We analyze existing literature, exploring various implementations and their effectiveness in enhancing IoT security. Key aspects such as scalability, latency, energy consumption, and overall system performance are examined. Additionally, we identify the current limitations and propose future research directions to optimize the integration of blockchain in IoT environments. The goal of this review is to provide a comprehensive understanding of the potential and practical implications of blockchain technology in securing IoT networks, offering valuable insights for researchers and practitioners in the field.

KEYWORDS: "hybrid cloud", "multi cloud platform", "cloud security"

I. INTRODUCTION

A. Background and Motivation

The advent of the Internet of Things (IoT) has revolutionized the way we interact with the world, enabling seamless connectivity and data exchange between various devices. From smart homes and wearable technology to industrial automation and healthcare, IoT has permeated numerous sectors, promising increased efficiency, convenience, and innovation. However, this rapid expansion has also introduced significant security challenges. The sheer volume of interconnected devices creates a vast and attractive attack surface for cyber threats, necessitating robust security frameworks to protect sensitive data and ensure the integrity of IoT networks.

B. Importance of Security in IoT Networks

Security is paramount in IoT networks due to the critical nature of the data and operations they support. Compromised IoT devices can lead to severe consequences, including data breaches, unauthorized access, and disruption of essential services. Traditional security measures often fall short in addressing the unique requirements of IoT, such as scalability, interoperability, and resource constraints. Therefore, developing innovative security solutions tailored to the specific needs of IoT networks is crucial for their safe and reliable operation.

C. Introduction to Blockchain Technology

Blockchain technology, initially popularized by cryptocurrencies like Bitcoin, has emerged as a promising solution to address security concerns in various domains. Its decentralized and immutable nature makes it an ideal candidate for enhancing the security of IoT networks. Blockchain's core features include distributed ledgers, consensus mechanisms, and cryptographic security, which collectively provide a transparent, tamper-proof, and resilient framework. By leveraging these attributes, blockchain can enhance data integrity, prevent unauthorized access, and facilitate secure transactions within IoT ecosystems.

D. Objectives and Scope of the Review

This review paper aims to evaluate the efficiency of blockchain-based secure frameworks in IoT networks. Our primary objectives are to analyze the current state of research in this field, assess the effectiveness of various blockchain implementations in enhancing IoT security, and identify potential areas for further exploration. Specifically, we will examine key performance indicators such as scalability, latency, energy consumption, and overall system performance. Through this comprehensive analysis, we seek to provide valuable insights into the practical implications of integrating blockchain technology with IoT networks and to highlight the opportunities and challenges that lie ahead.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103115 |

E. Structure of the Paper

The paper is structured as follows: Section II provides an overview of IoT networks and their inherent security challenges. Section III delves into the fundamentals of blockchain technology and its applicability to IoT. Section IV reviews existing blockchain-based secure frameworks for IoT, presenting case studies and comparative analyses. Section V discusses the evaluation criteria for assessing the efficiency of these frameworks, while Section VI presents the findings and critical insights from our review. Finally, Section VII outlines future research directions and concludes the paper.

II. OVERVIEW OF IOT NETWORKS

The Internet of Things (IoT) refers to the interconnection of various physical devices, vehicles, buildings, and other items embedded with sensors, software, and network connectivity, enabling them to collect, exchange, and act upon data. IoT networks consist of these interconnected devices communicating with each other and central systems over the internet, creating a web of smart objects capable of performing complex tasks and providing valuable insights.

Components of IoT Networks:

1. **Sensors and Actuators:** These are the core elements of IoT devices, responsible for collecting data from the environment (e.g., temperature, humidity, motion) and performing actions based on the data (e.g., adjusting a thermostat, turning lights on or off).
2. **Connectivity:** This includes the various communication protocols and technologies that facilitate data exchange between IoT devices and central systems. Common connectivity options include Wi-Fi, Bluetooth, Zigbee, LoRaWAN, and cellular networks (3G, 4G, and 5G).
3. **Data Processing and Analytics:** Once data is collected, it is transmitted to a central system or the cloud, where it is processed and analyzed. Advanced analytics and machine learning algorithms can be applied to derive insights, detect patterns, and make predictive decisions.
4. **User Interface:** This allows users to interact with IoT devices and the data they generate. Interfaces can range from mobile applications and web dashboards to voice assistants and automated alerts.

Applications of IoT Networks:

IoT networks have a broad range of applications across various industries:

- **Smart Homes:** IoT devices can automate lighting, heating, security systems, and appliances, enhancing convenience and energy efficiency.
- **Healthcare:** Wearable devices and remote monitoring systems can track patients' health metrics, enabling proactive healthcare and remote diagnostics.
- **Industrial IoT (IIoT):** Sensors and connected machinery can optimize manufacturing processes, predict maintenance needs, and improve overall operational efficiency.
- **Smart Cities:** IoT technology can manage urban infrastructure, such as traffic control, waste management, and energy distribution, leading to improved city services and sustainability.

Challenges faced by IOT Networks:

- **Security and Privacy**: IoT devices are often limited in computational power and memory, making it difficult to implement robust security protocols. These devices frequently collect sensitive data, posing significant privacy risks if breached. Common attacks include unauthorized access, data interception, and malware infections. Ensuring end-to-end security and data privacy is a paramount concern.
- **Scalability**: As IoT networks grow, managing and coordinating an increasing number of devices becomes complex. Scalability issues arise from the need to handle vast amounts of data generated by these devices, which can overwhelm traditional network infrastructures and lead to latency and performance bottlenecks.
- **Interoperability**: IoT ecosystems consist of devices from various manufacturers using different protocols and standards. Achieving seamless communication and integration between heterogeneous devices is a significant challenge. Lack of standardization hampers interoperability and complicates the development and deployment of IoT applications.
- **Energy Efficiency**: Many IoT devices are battery-powered and deployed in remote or inaccessible locations, necessitating efficient energy use to prolong their operational life. Energy constraints limit the complexity of algorithms that can be used for data processing and security, thereby impacting the overall functionality of the network.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103115 |

- **Data Management**: IoT networks generate massive volumes of data that require effective management, storage, and analysis. Ensuring data integrity, consistency, and availability while minimizing storage costs and maximizing retrieval efficiency is a complex task. Additionally, real-time data processing is often required for critical applications, adding another layer of difficulty.
- **Network Reliability**: IoT devices often operate in environments prone to connectivity issues, such as interference, signal attenuation, or network congestion. Maintaining reliable and consistent communication between devices, particularly in large-scale deployments, is a critical challenge.
- **Regulatory and Compliance Issues**: IoT applications span various industries, each with its own regulatory requirements and standards. Ensuring compliance with these regulations while fostering innovation and interoperability poses a significant challenge for IoT network designers and operators.

III. BLOCK CHAIN TECHNOLOGY FUNDAMENTALS

Blockchain technology, originally introduced as the underlying framework for the digital currency Bitcoin, has since evolved into a revolutionary concept with wide-ranging applications beyond cryptocurrencies. At its core, blockchain is a decentralized and distributed ledger technology that enables secure, transparent, and immutable record-keeping of transactions across a network of computers, known as nodes.

Fundamentally, blockchain operates on several key principles:

1. **Decentralization**: Unlike traditional centralized systems where a single authority controls data and transactions, blockchain distributes data across multiple nodes in a network. Each node stores a complete copy of the blockchain, promoting transparency and resilience against single points of failure or manipulation.
2. **Security through Consensus**: Blockchain achieves security through consensus mechanisms, where nodes in the network validate and agree on the legitimacy of transactions before they are recorded. Common consensus algorithms include Proof of Work (PoW) and Proof of Stake (PoS), each with its own advantages in terms of security, energy efficiency, and scalability.
3. **Immutability and Transparency**: Once recorded, data in a blockchain cannot be altered retroactively without the consensus of the network participants. This immutability ensures the integrity and trustworthiness of the information stored on the blockchain. Additionally, transparency is inherent as all participants have access to the same ledger, reducing the need for intermediaries and enabling verifiable transactions.
4. **Smart Contracts**: Blockchain platforms like Ethereum introduced the concept of smart contracts, self-executing contracts with predefined rules and conditions encoded into the blockchain. Smart contracts automate and enforce the execution of agreements, enhancing efficiency and reducing the need for intermediaries.
5. **Cryptographic Security**: Blockchain employs advanced cryptographic techniques to secure transactions and maintain privacy. Each transaction is cryptographically linked to the preceding transaction, forming a chain of blocks, hence the name "blockchain." Public and private keys enable secure access and ownership verification, ensuring only authorized parties can interact with the block chain.

IV. RELATED WORK

Recent advancements in IoT and blockchain technologies have spurred significant interest in enhancing security and privacy in various domains, particularly in healthcare and smart applications. This related work section explores several relevant studies and their contributions to the intersection of IoT networks and blockchain frameworks.

Siam et al. (2021) introduced a secure health monitoring communication system leveraging IoT and cloud computing for medical emergency applications, highlighting the critical need for robust data security and real-time communication in healthcare scenarios. Ali et al. (2022) proposed a big data-based smart blockchain framework aimed at privacy-preserving healthcare systems, emphasizing efficient information retrieval while safeguarding patient data integrity.

Altulaihan et al. (2022) addressed cybersecurity threats in IoT, emphasizing the importance of proactive measures and mitigation techniques to counter evolving threats in interconnected environments. Hasnain et al. (2020) focused on benchmark dataset selection for web services technologies, providing insights into foundational aspects crucial for evaluating technology implementations.

Security, privacy, and reliability in digital healthcare systems were extensively discussed by Ali et al. (2021), underscoring blockchain's role in ensuring data integrity and patient confidentiality. Almaiah et al. (2022) introduced

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103115 |

an AI-enabled hybrid lightweight authentication model for digital healthcare using industrial IoT cyber-physical systems, demonstrating innovative approaches to enhancing system security.

Yazdinejad et al. (2023) proposed a secure intelligent fuzzy blockchain framework for effective threat detection in IoT networks, highlighting advancements in adaptive security measures. Singh et al. (2023) developed an IoT and blockchain-based secure medical care framework, integrating deep learning and nature-inspired algorithms to enhance healthcare data management and security.

Additionally, Kim et al. (2019) explored privacy-preserving machine learning in blockchain networks, offering insights into techniques that balance data privacy with computational efficiency. Sharma et al. (2023) introduced the Enhanced Healthcare Document Handling Ecosystem (EHDHE), focusing on blockchain's role in securing healthcare documents in IoT-enabled environments.

These studies collectively underscore the growing importance of blockchain technology in addressing security challenges in IoT networks, particularly in healthcare and sensitive data domains. They highlight diverse approaches, from secure communication systems and privacy-preserving frameworks to advanced authentication models and threat detection mechanisms, contributing significantly to the evolving landscape of secure IoT applications. Future research should focus on integrating these advancements into scalable, interoperable solutions that meet the stringent security and privacy requirements of modern IoT ecosystems.

V. BLOCK CHAIN AS SECURE FRAMEWORK FOR IOT NETWORKS

Blockchain technology has emerged as a transformative innovation with profound implications for securing Internet of Things (IoT) networks. IoT, characterized by interconnected devices exchanging vast amounts of data, faces inherent security challenges due to centralized vulnerabilities, data breaches, and privacy concerns. Traditional security mechanisms often struggle to scale with the exponential growth of IoT devices, necessitating new approaches to ensure trust, transparency, and resilience in IoT ecosystems.

At its core, blockchain offers a decentralized ledger where transactions are recorded across a network of nodes in a secure, transparent, and immutable manner. This foundational principle addresses several critical security issues in IoT networks:

1. **Decentralization and Distributed Consensus**: Traditional IoT networks rely on centralized servers or cloud platforms to manage data and authentication, making them susceptible to single points of failure and malicious attacks. Blockchain's decentralized architecture eliminates this vulnerability by distributing data and decision-making among a network of nodes. Consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), or more recent variations like Proof of Authority (PoA) ensure that transactions are validated in a trustless environment, enhancing network reliability and security.
2. **Data Integrity and Immutability**: In IoT applications, ensuring the integrity and authenticity of data is paramount. Blockchain's append-only structure and cryptographic hashing ensure that once data is recorded, it cannot be altered retroactively without consensus from the network participants. This feature is particularly crucial in sectors such as supply chain management, healthcare, and smart cities, where data provenance and auditability are essential.
3. **Enhanced Security and Privacy**: Blockchain's cryptographic algorithms provide robust mechanisms for securing IoT data and communications. By leveraging public-key cryptography, IoT devices can securely authenticate and communicate with each other, mitigating risks associated with spoofing and unauthorized access. Furthermore, private and permissioned blockchains enable fine-grained control over data access and visibility, preserving user privacy without compromising security.
4. **Smart Contracts and Automation**: Smart contracts, self-executing agreements with predefined rules and conditions, facilitate automated transactions and interactions between IoT devices. These programmable contracts enable secure, transparent, and tamper-proof execution of business logic, streamlining processes such as device provisioning, firmware updates, and payment settlements in IoT networks.

Despite its promising potential, integrating blockchain with IoT networks presents challenges such as scalability, interoperability, and energy efficiency. Blockchain's consensus protocols, while ensuring security, can also introduce

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103115 |

latency and overhead, impacting real-time IoT applications. Addressing these challenges requires ongoing research and innovation to optimize blockchain protocols for IoT-specific use cases.

VI. CHALLENGES & LIMITATIONS OF BLOCK CHAIN IN IOT NETWORKS

Blockchain technology offers compelling benefits for IoT networks, such as enhanced security, decentralized control, and data integrity. However, its integration into IoT environments also presents several challenges and limitations that must be addressed for widespread adoption and effective deployment:

1. **Scalability:** One of the foremost challenges is the scalability of blockchain networks. IoT devices generate massive volumes of data and require real-time processing and validation. Blockchain consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), can be computationally intensive and may not scale well to accommodate the sheer number of transactions and devices in IoT networks.
2. **Latency and Throughput:** Blockchain transactions involve multiple validations across distributed nodes, leading to inherent latency in data processing. This latency can be critical in time-sensitive IoT applications, such as industrial automation or autonomous vehicles, where delays can impact operational efficiency and safety. Improving transaction throughput while maintaining consensus integrity remains a significant technical challenge.
3. **Energy Consumption:** Blockchain mining and consensus algorithms require substantial computational power and energy consumption. For IoT devices, which are often resource-constrained and operate on limited battery life, energy efficiency is paramount. The energy-intensive nature of blockchain operations poses a barrier to integrating this technology into IoT devices without significant optimization.
4. **Data Privacy and Confidentiality:** While blockchain offers transparency and immutability, ensuring data privacy and confidentiality in IoT networks is complex. IoT devices frequently handle sensitive data, and storing such data on a public blockchain ledger raises concerns about exposure to unauthorized access or breaches. Developing robust privacy-preserving mechanisms without compromising blockchain's core principles is a persistent challenge.
5. **Interoperability and Standards:** IoT ecosystems are characterized by diverse devices, protocols, and communication standards. Achieving interoperability between blockchain platforms and existing IoT infrastructure remains a challenge. Standardization efforts are essential to enable seamless integration, facilitate data exchange, and ensure compatibility across heterogeneous IoT environments.
6. **Regulatory and Compliance Issues:** Blockchain technology operates in a decentralized manner, challenging traditional regulatory frameworks and data governance practices. IoT applications leveraging blockchain may face regulatory hurdles related to data ownership, jurisdictional compliance, and legal implications of smart contracts. Clarifying regulatory frameworks and addressing legal uncertainties are critical to fostering trust and adoption in blockchain-enabled IoT solutions.

Addressing these challenges requires collaborative efforts from researchers, industry stakeholders, and policymakers to innovate scalable, energy-efficient blockchain solutions tailored for IoT applications. Overcoming these limitations will unlock the full potential of blockchain technology in enhancing security, reliability, and trustworthiness in IoT networks.

VII. FUTURE ENHANCEMENTS OF BLOCK CHAIN AS A SECURE FRAMEWORK FOR IOT NETWORKS.

As blockchain technology continues to evolve, its potential as a secure framework for IoT networks is poised for significant enhancements and innovations. Several key areas hold promise for future development:

1. **Scalability Solutions**: Current blockchain platforms face scalability issues when handling the vast number of transactions and data generated by IoT devices. Future enhancements may involve implementing sharding techniques, layer 2 solutions like state channels or sidechains, and consensus algorithms optimized for IoT environments to improve throughput without compromising security.
2. **Interoperability**: IoT ecosystems consist of diverse devices and protocols. Future blockchain frameworks could focus on enhancing interoperability, allowing seamless communication and data exchange between different IoT devices and platforms while maintaining security and privacy.
3. **Security and Privacy**: Addressing privacy concerns remains crucial. Future blockchain frameworks for IoT may integrate advanced cryptographic techniques such as zero-knowledge proofs or homomorphic encryption to ensure data confidentiality while maintaining transparency and auditability.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103115 |

4. **Energy Efficiency**: IoT devices often operate on limited battery power. Future blockchain enhancements may include protocols that minimize energy consumption during consensus and validation processes, making blockchain feasible for resource-constrained IoT devices.
5. **Smart Contract Capabilities**: Enhancements in smart contract languages and frameworks tailored for IoT-specific use cases could enable automated and secure interactions between IoT devices, facilitating autonomous operations and enhancing overall system efficiency.
6. **Regulatory Compliance**: Future blockchain frameworks may incorporate features to facilitate compliance with evolving regulatory requirements, ensuring that IoT deployments adhere to data protection and privacy laws across different jurisdictions.
7. **User Experience**: Improving the user interface and experience for managing blockchain-based security frameworks in IoT networks can promote adoption and usability among stakeholders, including device manufacturers, service providers, and end-users

VIII. CONCLUSION

In conclusion, blockchain technology represents a transformative solution to the inherent security challenges of IoT networks. By decentralizing trust and enhancing data integrity through cryptographic security and distributed consensus, blockchain mitigates vulnerabilities associated with centralized architectures. Our review highlights the effectiveness of blockchain-based secure frameworks in addressing critical IoT security concerns such as data privacy, authentication, and transactional transparency.

However, the integration of blockchain with IoT networks poses significant challenges. Scalability issues, latency concerns, and energy consumption remain prominent obstacles that must be overcome through innovative approaches like sharding, optimized consensus algorithms, and energy-efficient protocols. Moreover, ensuring interoperability with existing IoT infrastructures and addressing regulatory complexities are essential for widespread adoption.

Looking forward, future advancements in blockchain technology hold promise for enhancing scalability, interoperability, and energy efficiency in IoT applications. Innovations in smart contract capabilities and privacy-preserving techniques will further bolster the security and reliability of blockchain-enabled IoT ecosystems. Collaboration between researchers, industry stakeholders, and policymakers will be crucial in realizing the full potential of blockchain as a secure framework for IoT networks, ensuring continued innovation and adoption in the evolving landscape of interconnected devices

REFERENCES

[1] DAMA-DMBOK: Data Management Body of Knowledge (2nd Edition). [E-book]. Available: https://www.google.de/ [Accessed: June 30, 2022].
[2] Almeida Fernando and Calistru Catalin, "The main challenges and issues of big data management," International Journal of Research Studies in Computing April 2013, Volume 2 Number 1, 11-20. [Online]. Available: https://www.researchgate.net/ [Accessed: June 30, 2022].
[3] Daniel J. Abadi, "Data Management in the Cloud: Limitations and Opportunities," Bulletin of the IEEE Computer Society Technical Committee on Data Engineering March 2009 Vol. 32 No. 1. [Online]. Available: http://citeseerx.ist.psu.edu/ [Accessed: June 30, 2022].
[4] Siba Mohammad, Sebastian Breß and Eike Schallehn, "Cloud Data Management: A Short Overview and Comparison of Current Approaches," 24th GI-Workshop on Foundations of Databases (Grundlagen von Datenbanken), 29.05.2012 - 01.06.2012, Lübbenau, Germany. [Online]. Available: https://www.semanticscholar.org/ [Accessed: June 30, 2022].
[5] Katarina Grolinger, Wilson A Higashino, Abhinav Tiwari and Miriam AM Capretz, "Data management in cloud environments: NoSQL and NewSQL data stores," Grolinger et al. Journal of Cloud Computing: Advances, Systems and Applications, 2013, 2:22. [Online]. Available: https://link.springer.com/ [Accessed: June 30, 2022].
[6] Jiangshui Hong, Thomas Dreibholz, Joseph Adam Schenkel, and Jiaxi Alessia Hu, "An Overview of Multi-cloud Computing," Springer Nature Switzerland AG 2019 L. Barolli et al. (Eds.): WAINA 2019, AISC 927, pp. 1055–1068, 2019. [Online]. Available: https://link.springer.com/ [Accessed: June 30, 2022].
[7] Munawar Ali Zardari, Low Tang Jung, and Mohamed Nordin B. Zakaria, "Hybrid Multi-cloud Data Security (HMCDS) Model and Data Classification," 2013 International Conference on Advanced Computer Science Applications and Technologies [Online]. Available: https://ieeexplore.ieee.org/ [Accessed: June 30, 2022].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 3, March 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1103115 |

[8] Sherif Sakr, Anna Liu, Daniel M. Batista, and Mohammad Alomari, "A Survey of Large Scale Data Management Approaches in Cloud Environments," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 13, NO. 3, THIRD QUARTER 2011 [Online]. Available: https://ieeexplore.ieee.org/ [Accessed: June 30, 2022].
[9] Devarshi Ghoshal, Valerie Hendrix, Eugen Feller, Christine Morin, Beth Plale, and Lavanya Ramakrishnan, "Data Management Strategies for Scientific Applications in Cloud Environments," [Online]. Available: https://www.academia.edu/ [Accessed: June 30, 2022]

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

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