IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 12, December 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 12, December 2024| DOI: 10.15680/IJIRCCE.2024.1212008

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A Novel Approach for Authentication using Session QR-Code

Mohd Asim, Dr. Geetu Soni

Ph.D. Scholar, Department of Computer Science, Glocal School of Technology & Computer Science, Glocal University, Saharanpur (UP), India

Associate Professor, Glocal School of Technology & Computer Science, Saharanpur (UP), India

ABSTRACT: Authentication is confirming the identification of people or systems. This procedure allows only approved users, services, and applications with the proper access rights to use organizational resources. Information theft and forgeries are more likely because of inadequate authentication techniques. To address breaches in data security and privacy protection during authentication and authorization in the peer-to-peer (P2P) cloud network, a comprehensive and methodical literature research has been carried out. Researchers have discovered many security vulnerabilities associated with web browsers. In this work, we introduce a new QR-based authentication method that does away with the necessity of manual login procedures. This technique, which is quick and safe, facilitates peer connections in the P2P cloud.

Our method and algorithm are well-defined for both the client and server sides. Compared to the popular SSL Authentication Protocol (SAP), a comprehensive method created and tested in a Python simulation environment has shown significantly greater speed and efficiency. We have also conducted tests for man-in-the-middle attacks and session hijacking through Python simulation with the help of Scapy and other supported libraries. Our approach proved to be safe and efficient.

Our approach may stop session hijacking and man-in-the-middle attacks. All things considered, our strategy successfully tackles security and privacy issues in cloud computing, particularly in P2P cloud networks.

KEYWORDS: QR-code, P2P Cloud, SAP, Authentication & Authorization

I. INTRODUCTION

The foundational principles of cloud computing encompass diverse models such as cluster, grid, and cloud computing, each striving to embody the vision of computing utility (Armbrust et al., 2010) [4] & (Buyya et al., 2009) [1]. Cloud computing, an innovative technological paradigm, involves the distribution of software applications, computing resource services, and data storage services. In 2009, Gardner's definition characterized cloud computing as an advanced computing technique offering massively scalable IT-related capabilities provided as services, accessible through Internet technologies. (Erdogmus,2009) [2] described cloud computing as a reservoir comprising highly scalable and abstracted infrastructure capable of hosting applications for users, with billing based on resource consumption. Expanding upon this landscape, Peer-to-Peer (P2P) cloud computing introduces a unique set of core concepts, redefining the paradigm by enabling direct sharing of computing resources among interconnected devices within a network, eliminating the need for a central server. In contrast to traditional cloud models, P2P cloud computing emphasizes collaboration, augmenting scalability, fault tolerance, and resource utilization. This collaborative model takes center stage, leveraging a network of interconnected devices to cultivate a more distributed and resilient infrastructure. The crux lies in the direct interaction among devices, fostering a dynamic and cooperative environment for resource sharing. In summary, while cloud computing delivers scalable IT capabilities through centralized services, P2P cloud computing pioneers a decentralized approach, emphasizing direct collaboration among devices for resource sharing within a distributed network. Together, these concepts signify the evolution and diversification of computing models, offering tailored solutions for various technological landscapes.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. REVIEW OF LITERATURE

The user interface (UI) of the online page, the browser cache memory, extensions, and plug-ins are all subject to attacks that can be carried out on web browsers. Using these flaws, the attacker can launch malicious JavaScript to take advantage of the user's system. The threats addressed include buffer overflow, cross-site scripting, man-in-the-middle, extension vulnerability, extreme phishing, browser cache poisoning, session hijacking, drive-by download, and clickjacking. To protect the browser from attack, sandboxed processes and browsers with electrolysis systems are described (Satish & Chavan, 2017) [3]

Cloud computing has numerous conceivable benefits, and many business applications and data are moving to public or hybrid clouds. However, organizations, particularly big businesses, still wouldn't migrate some business-critical apps to the cloud. The market size for cloud computing is still very small compared to expectations.

Consumers' concerns about cloud computing security, particularly those related to data security and privacy protection, continue to be the principal barrier to the uptake of cloud computing services. This essay offers a succinct but comprehensive review of data security and privacy protection issues related to cloud computing at all data life cycle stages. This paper then covers some contemporary solutions. This report also discusses upcoming research on data security and privacy protection (Chen & Jhao, 2012) [4]

One of the key components of cloud computing is virtualization technology, and virtualization security is a key component of cloud computing security as well. This article presents the widely used virtualization technology, examines the security risks associated with virtualization in cloud computing, and suggests appropriate mitigation strategies (Chen et al., 2020) [5]

The cloud service provider (CSP) is accountable for ensuring the integrity, availability, privacy, and confidentiality of client data stored in the cloud. However, CSP does not deliver trustworthy data services to customers. The article addresses the problems with cloud data storage, including data breaches, data theft, and cloud data unavailability. Finally, we offer potential fixes for the aforementioned cloud concerns (Rao, 2016) [6]

(Jagdale & Bakal, 2020) [7] To provide security against many types of assaults that occur in P2P networks, this study offers a multi-level authentication and authorization system based on the fuzzy-enabled advanced encryption standard (AES). In this instance, the verification is completed using security considerations such as a hashing function, spatial information, location profile, one-time password, and so forth. After the user and the server register for the authentication process, multi-level authorization and authentication procedures are carried out using hashing functions and AES. Consequently, the suggested plan strengthens the P2P network's security. The success rate is 0.7666 and the hit ratio is 0.9 when the suggested system is used.

III. ARCHITECTURE OVERVIEW

Cloud computing offers flexible computation and garage services, but its centralized version can lead to bottlenecks and provider outages during system disasters. To triumph over these challenges, dispensed cloud assets the usage of based peer-to-peer (P2P) overlay networks have been proposed. However, protection problems, in particular peer authentication in decentralized settings, remain unaddressed. Therefore, we propose an authentication framework for P2P clouds. This framework integrates numerous entity and message authentication methods, leveraging cryptographic primitives and security mechanisms from present-based P2P networks. By improving peer authentication, the framework aims to strengthen the security and reliability of P2P-based cloud computing. It guarantees robustness and trustworthiness in dispensed environments, paving the manner for more resilient and stable cloud offerings.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

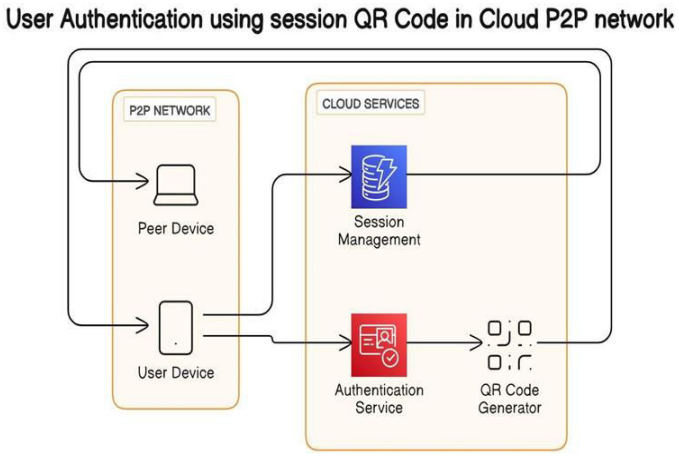


Figure-1: Architecture of Authentication Phase

IV. USER AUTHENTICATION PHASE

A. In QR code user authentication, cryptographic techniques generate and verify authentication tokens or session IDs.

i. Token Generation

The cloud server generates a unique authentication token or session ID for the user. This token is usually generated using cryptographic hash functions or encryption algorithms.

Token=hash_function(Data)

Data - session id. + user id.

Encrypted_Token=Encryption_Algorithm (token, key)

SHA256 and AES256 are used with a key length of 256 bits.

ii. QR-Code Generation

The authentication token is encoded into a QR code format after encryption of the hashed message. The QR code serves as a visual representation of the authentication token.Mathematical calculations involved in QR code generation are typically handled by QR code generation libraries and encoding standards, such as the QR Code Model.

iii. Token & QR-code Generation (Server Side)

Hash_Value = Hash_Function (user_id + session id)

Encrypted_Data=encryption (Hash_value, key)

QR-code - encoding (Encrypted_Data)

The user requests to log in using their user ID onto the P2P cloud via the cloud control module, such as their username or email address. A login request and user ID are sent to the cloud control module. In reply, the CCM creates a session ID for the relevant request and forwards it to the peer for validation on the peer side. The SHA256 technique is used to generate a hash value using the session and user IDs as data. The CCM will now use the AES256 encryption technique to create an encrypted value before encoding it into a QR code, and it will preserve this value for use in future validation processes. The AES256 technology is used to increase security and protect the data.

iv. Token and QR code Verification (Client Side)

The user's device confirms the token's integrity and authenticity after receiving it to make sure it hasn't been altered. After receiving the QR code from the user, it must be validated.

Computed_Hash = Hash_Function (user_id + session id)

Decrypted_Data=Decryption_Algorithm (QR-code, Key)

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

The peer will apply the SHA256 algorithm after combining the user ID and session data. As a result, the hash value will be produced and saved for verification. It's time to verify the QR code, though, as the peer also received one for a secure login. The AES256 method must be used to decode the QR code. In reality, the decoded message was a hash value or message digest that had been encrypted with AES. To ensure a safe login, these two values will be compared; if not, the login will be rejected.

v. Comparing Hashes (Server side)
Compare (Computed Hash, Stored Hash)
Comparing Decrypted Data: Compare (Decrypted Data, OriginalData)

The computed hash and decrypted data are compared with the pre-computed hash value or original data stored on the server to validate the token.

vi. Session Validation
If the token is validated successfully, the cloud server authenticates the user and grants access to the requested services. Otherwise, access is denied, and appropriate error handling is performed.

V. IMPLEMENTATION SETUP

The above algorithm is implemented in Python with multiple libraries and functions. We have created a virtual environment with three entity cloud control modules and two peers. These peers need to be connected securely to share data.
a. Libraries used to implement QR code generation and cryptographic capabilities qrcode-7.4.2, pypng-0.20220715.0 and pycryptodome-3.20.0.
We simulate an attacker intercepting and modifying the communication between two peers and the cloud control module to test for MITM attacks.
During the authentication process, a session ID for the peer and this session ID can be modified by the attacker so it can be easily tracked down by the algorithm on both sides' validation process. The following libraries are used to implement

- Scapy: For packet crafting and network attacks.
- Requests: For simulating web requests and session hijacking.
- Wireshark: For monitoring network traffic and detecting anomalies

Algorithm of Secure Communication Process:
1. **Peer1**
a) Sends username to **Cloud Server**.
2. **Cloud Server**:
a) Creates a session ID.
b) Generates an AES-256 key.
c) Combines username and session ID.
d) Applies SHA-256 to the combined data.
e) Encrypts the resulting hash using AES-256.
f) Generates a QR code of the encrypted message.
g) Sends the session ID and QR code to **Peer1**.
3. **Peer1**
a. Receives session ID and QR code.
b. Combines the received session ID with the username.
c. Applies SHA-256 to generate a hash.
d. Sends the hash to Cloud Server for storage.
4. **Cloud Server**
a. Stores the hash received from **Peer1**.
5. **Peer1**
a. Decodes the QR code.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

b. Decrypt the message using AES-256 and the session ID.
c. Verifies the hash against the stored hash on the **Cloud Server**.
6. **Verification**
a. If the hashes match, the connection is established securely.
b. If the hashes do not match, the connection fails.
7. **Peer2**
a. Connect Peer2 securely with Peer1 to share data and services.
8. **Calculate the time and memory consumption in each operation**
a. Such as Hash Generation, Encryption, QR-code generation, etc.
9. **Perform a man-in-the-middle attack using the Scapy library and other functions.**

We changed the session key after intercepting peer-to-cloud control module communication. This caused the peer validation process to fail, and the decoded value of the QR code was inconsistent. Because changing any value on the client or server side fails the verification process and halts connection, MITM attacks and session hijacking may be totally avoided in this method. This guarantees that any unwanted access is prevented, preserving the security and integrity of the shared data. Organizations may greatly lower the risk of cyberattacks and improve overall system resilience by putting such strong security measures in place.

VI. RESULTS AND DISCUSSION

1. FEASIBILITY AND PERFORMANCE

The performance analysis of the QR code-based authentication system demonstrates that the proposed system is both efficient and practical for real-world applications. The system successfully integrates key cryptographic operations, including hash generation, encryption, and QR code generation, to ensure secure and seamless authentication.

2. Hash Generation

The average time for generating a SHA-256 hash of the session data is very low, indicating that this step does not introduce significant overhead.

3. Encryption

The AES encryption step, including the generation of a random initialization vector (IV), is also performed efficiently. The time taken for encryption is minimal, ensuring that the session data is secured quickly.

4. QR Code Generation

Generating the QR code from the encrypted session data is slightly more time-consuming than the previous steps but remains within an acceptable range. The QR code generation is crucial as it forms the core of the user authentication process, providing a secure and user-friendly means of verifying identity.

5. Total Time

The cumulative time taken for all operations (hash generation, encryption, and QR code generation) is low, suggesting that the entire process from data preparation to QR code display can be completed swiftly. This ensures a smooth user experience without noticeable delays during authentication.

VII. COMPARATIVE ANALYSIS

The effectiveness and performance of the Session QR code-based authentication technique have been assessed in this section. The time spent on each component—hash generation, encryption, and QR code production—is measured for assessment purposes. We have taken the mean value as the final result after ten iterations of all the investigations. To demonstrate the CPU time consumption in each component, the individual average time of each component is also measured. Lastly, the suggested approach has recorded the total average time. Nevertheless, each component's memory usage as well as the overall memory usage of the suggested approach are noted. The following are the outcomes:

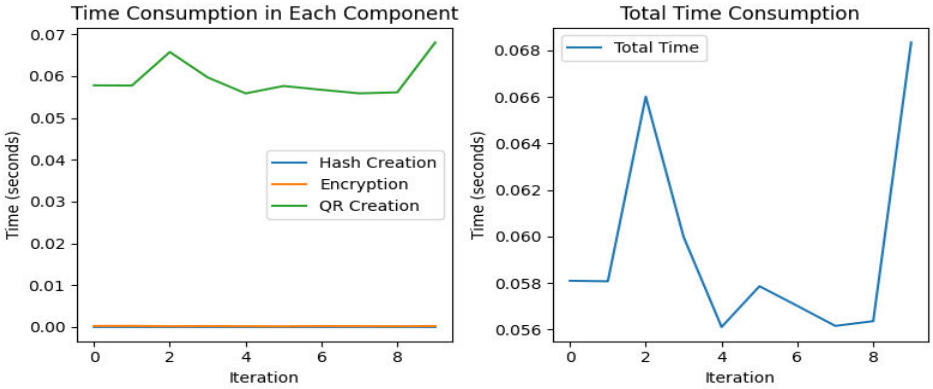
Performance Analysis over 10 iterations:
Average Hash Generation Time: 0.000029 seconds

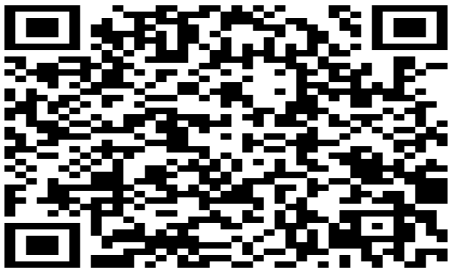
www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

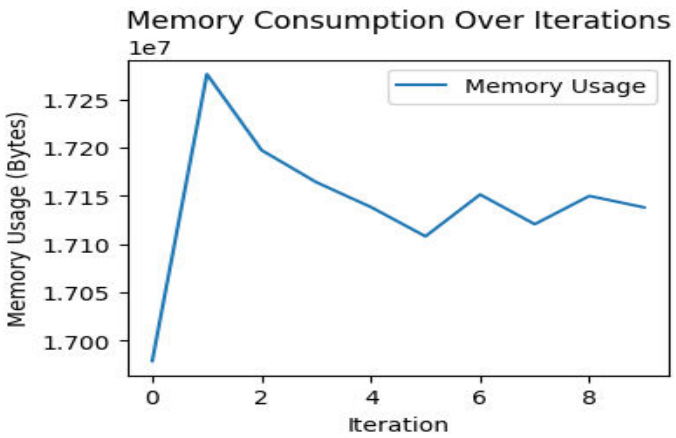
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Average Encryption Time: 0.000234 seconds
Average QR Code Generation Time: 0.059133 seconds
Average Total Time: 0.059399 seconds
Max Total Time: 0.068342 seconds
Min Total Time: 0.056107 seconds
Average Hash Generation Memory Usage: 61242.40 bytes
Average Encryption Memory Usage: 55330.90 bytes
Average QR Code Generation Memory Usage: 91131.20 bytes
Overall Average Memory Usage: 69234.83 bytes





QR-Code Generated by our system



www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Cloud Admin server running
Peer server running
Peer server running Peer received: AUTH asimmca2002@gmail.com
CloudAdmin received: AUTH asimmca2002@gmail.com
Peer received from cloud admin: AUTH
mgZh0Qy8QHwTE3Y7cKY9PpajYmHQ4AEMyyytG0IIzpjaNzkERIeaI2KXiohvLP6tnynrt/jw5GI3dUA4nOe+53lR7W/4GgysrVuDxTq8pyNNcdtclNIURSje8xSlQ+YB
Peer received from peer: AUTH_RESPONSE asimmca2002@gmail.com

Our findings have been contrasted with those of SAP (SSL Authentication procedure).
It takes 66.889 msec for our method to complete. Conversely, SAP has taken 315 msec on the server side and 275 msec on the client side. Consequently, 432 msec would be the average. compared to SAP, our authentication protocol is substantially faster. However, our authentication process uses a bit more memory than SAP does, indicating that our authentication technique has a comparatively higher communication cost.

We have also taken steps to mitigate the Man-in-the-Middle (MITM) attack, which aims to change the session key and affects client-side validation, halting the login process. Therefore, our approach may be quicker and safer against MITM.

VIII. SECURITY ANALYSIS

a. Robust Cryptographic Techniques

The use of SHA-256 for hashing and AES for encryption provides strong security guarantees. SHA-256 is resistant to collisions, making it suitable for generating unique session identifiers, while AES encryption ensures that the session data cannot be easily decrypted without the correct key.

b. Secure QR Code-Based Authentication

The QR code mechanism enhances security by ensuring that session data is encrypted before being encoded into a QR code. Users scan the QR code with their mobile device, which then decodes and decrypts the session data for authentication. This method reduces the risk of credential theft and phishing attacks, as there are no static passwords to compromise.

c. Mitigation of Replay and Man-in-the-Middle Attacks

The session data includes a timestamp, making it time-sensitive and reducing the window for replay attacks. Any intercepted session data would quickly become invalid. Additionally, the encrypted communication channel between peers and the cloud admin server helps protect against man-in-the-middle attacks.

IX. PRACTICAL IMPLICATIONS

a. User Experience

The QR code-based authentication system offers a user-friendly experience by simplifying the login process. Users can authenticate themselves quickly by scanning a QR code, eliminating the need to remember and input complex passwords.

b. Scalability

The performance metrics indicate that the system can handle multiple authentication requests efficiently, making it scalable for larger deployments. The low computational overhead ensures that the system remains responsive even under high load.

c. Cost Efficiency

By reducing the need for extensive password management and leveraging efficient cryptographic operations, the system can lower maintenance costs for service providers. The use of temporary session data instead of long-term credentials further reduces the risk and associated costs of data breaches.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

X. LIMITATIONS AND FUTURE WORK

a) Resource Consumption

While the performance analysis shows that the system is efficient, generating and displaying QR codes may consume additional resources on mobile devices. Future work could explore optimizations to further reduce the computational load and improve battery life on mobile devices.

b) User Device Security

The security of the authentication process depends on the integrity of the user's mobile device. Ensuring that the device is free from malware and unauthorized accessis crucial. Future enhancements could include additional layers of security, such as biometric authentication, to complement the QR code mechanism.

c) Broader Testing

The current performance analysis is based on a controlled environment. Testing the system in diverse, real-world scenarios with various network conditions and device types would provide more comprehensive insights and help identify potential areasfor improvement.

XI. CONCLUSION AND FUTURE WORK

The Proposed method for P2P Cloud, focusing on QR code-based user authentication, demonstrates a robust and efficient approach to securing user authentication. The performance metrics validate the system's feasibility, while the security analysis highlights its resilience against common attacks. The practical implications of enhanced user experience, scalability, and cost efficiency make this system a promising solution for secure authentication in modern P2P cloud environments.

REFERENCES

1.Buyya, R., Yeo, C., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25(6), pp.599-616.

2.Erdogmus, H. (2009). Cloud Computing: Does Nirvana Hide behind the Nebula? IEEE Softw., 26, 4-6.

3.Satish, P. S., & Chavan, R. K. (2017). Web browser security: different attacks detection and prevention techniques. International Journal of Computer Applications, 170(9), 35-41.

4.Chen, D., & Zhao, H. (2012, March). Data security and privacy protection issues in cloud computing. In 2012 International Conference on Computer Science and Electronics Engineering (Vol. 1, pp. 647-651). IEEE.

5.Chen, L., Xian, M., Liu, J., & Wang, H. (2020, April). Research on virtualization security in cloud computing. In IOP conference series: materials science and engineering (Vol. 806, No. 1, p. 012027). IOP Publishing.

6.Rao, B. T. (2016). A study on data storage security issues in cloud computing. Procedia Computer Science, 92, 128-135

7.Jagdale, B.N and Bakal, B.W (2020). A novel authentication and authorization scheme in P2P networking using location-based privacy. Volume 15, pages (1251-1264),2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

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