iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VIII **Month of publication:** Aug 2023

DOI: https://doi.org/10.22214/ijraset.2023.55012

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VIII Aug 2023- Available at www.ijraset.com

IAM-BDSS: A Secure Ciphertext-Policy and Identity- Attribute Management Data Sharing Scheme Based on Blockchain

Hariprasath[1], Sreerambabu[2], Kalidasan[3], Mohammed Riyaz[4]
[1]PG Scholar, [2]Head of the Department, [3, 4]Assistant Professor Dept of MCA

Abstract: ***This paper presents a Ciphertext-policy attribute-based encryption (CP-ABE) is widely recognized as a secure access control mechanism for data sharing. However, the generation of secret keys (SK) in most CP-ABE schemes relies on a centralized authority (CA), which can result in high costs for establishing trust and pose a single point of failure. To address these challenges and leverage the characteristics of blockchain technology, several blockchain-based schemes have been proposed to prevent data disclosure and protect user privacy attributes. In this paper, we propose IAM-BDSS, a novel CP-ABE identity-attribute management data sharing scheme based on blockchain, aimed at ensuring privacy through hidden policies and attributes. Additionally, we introduce a transaction structure to ensure the traceability of parameter transmission within the blockchain system. Through experimental results and security analysis, we demonstrate the effectiveness and feasibility of IAM-BDSS.***

Index Terms: ***IAM-BDSS, Blockchain, CP-ABE, identity-attribute management, security, privacy.***

I. INTRODUCTION

In recent times, attribute-based encryption (ABE) has gained significant traction for implementing fine-grained access control in data sharing. To ensure a streamlined and efficient data access control mechanism, most existing CP-ABE schemes rely on a centralized authority to generate users' secret keys. This approach necessitates users to disclose their set of attributes to the central authority. However, the effectiveness of data access control is heavily reliant on the centralized authority. Unfortunately, these centralized authorities are only partially trusted, which is impractical in real-world scenarios and can give rise to issues such as high trust establishment costs and vulnerability to single points of failure.

The rapid advancement of blockchain technology has instilled greater trust in data access control within both academic and industrial domains. The distributed nature of blockchain databases offers robust disaster recovery capabilities, as each node can rely on a consensus mechanism verified by honest nodes to fulfil necessary tasks. Notably, to achieve secure data sharing, previous efforts have focused on deploying access control policies on the blockchain. However, the transparent nature of the blockchain poses a risk of user privacy disclosure. This concern is particularly relevant in CP-ABE schemes where the generation of secret keys involves user communication with the central authority (CA), making user privacy vulnerable to potential attackers. Therefore, to establish a secure data sharing scheme based on the blockchain, it becomes essential to incorporate hidden access policies and attributes that ensure the security of the CP-ABE scheme.

In this research paper, we present IAM-BDSS, a data sharing scheme called Identity Attribute Management based on Blockchain with enhanced security. The scheme addresses challenges such as the high cost associated with trust establishment and the risk of single points of failure. Our contributions can be summarized as follows:

IAM-BDSS, a secure data sharing scheme that leverages blockchain technology to conceal access policies and attributes. In IAM-BDSS, users generate their secret keys locally, while the central authority (CA) manages the Master Secret Key (MSK) by matching hidden access control policies with user attributes. Within IAM-BDSS, we present an identity attribute management scheme based on CP-ABE to safeguard the confidentiality of access control and attribute procedures. To address privacy concerns in CP-ABE. The practicality and dependability of the algorithm are thoroughly examined through theoretical and experimental analyses, establishing its feasibility and reliability.

II. PROPOSED METHODOLOGY

In this project, our primary objective is to prevent unauthorized disclosure and safeguard the privacy of user properties.

©IJRASET: All Rights are Reserved

To achieve this, we propose a novel data sharing scheme called IAM-BDSS, which is based on the blockchain. IAM-BDSS ensures privacy by incorporating policies and properties while preserving confidentiality. Additionally, we introduce a transaction structure to facilitate parameter testing within the blockchain system.The proposed system, IAM-BDSS, is a secure data sharing scheme that combines ciphertext-policy attribute based encryption (CP-ABE) and identity-attribute management, all built on the foundation of blockchain technology. IAM-BDSS aims to address the limitations of traditional CP-ABE schemes, such as the reliance on a centralized authority for key generation and the associated costs and single point of failure. By leveraging the characteristics of blockchain, IAM-BDSS provides enhanced security and privacy protection for data sharing. The IAM-BDSS system comprises essential components such as:

Blockchain Integration: The integration of blockchain technology is a fundamental aspect of the IAM-BDSS system. By leveraging the decentralized and transparent nature of blockchain, we ensure secure and tamper-resistant data sharing.

Ciphertext-Policy Attribute Based Encryption (CP-ABE): IAM-BDSS incorporates CP-ABE as a key component. CP-ABE enables fine-grained access control by associating access policies with encrypted data, ensuring that only authorized users can access specific information.

Identity-Attribute Management: The IAM-BDSS system incorporates an identity-attribute management module. This component manages user attributes and access control policies to enforce secure data sharing.

Privacy Protection Mechanisms: IAM-BDSS employs various privacy protection mechanisms to safeguard user data. These mechanisms ensure that sensitive attributes and policies are encrypted and hidden, preventing unauthorized access and preserving user privacy.

Transaction Structure: The IAM-BDSS system includes a well-defined transaction structure. This structure ensures seamless parameter passing and facilitates testing within the blockchain system, enhancing the overall efficiency and reliability of the system.

III. SYSTEM COMPONENTS

A. Data Sharing And Send Data

In the IAM-BDSS (Identity Attribute Management-Blockchain-based Data Sharing Scheme), data sharing involves the secure transmission of encrypted data. Users can register and log into the system to initiate the process. The transmitted data is protected using a secure ciphertext-policy, ensuring its confidentiality. The encrypted data is then stored in a blockchain-based database, guaranteeing its integrity and immutability.

To access the shared data, users with trusted authority are granted permission by the data sharer. These authorized individuals can authenticate the file access for the intended patient. The authentication process utilizes identity attributes managed within the blockchain, further enhancing the security and privacy of the data sharing. Moreover, the data sharer has the capability to track and review the history of downloaded files. This feature enables monitoring and ensures accountability in the data sharing process. The IAM-BDSS provides a robust and trustworthy framework for data sharing, leveraging the security features of blockchain and ciphertext-policy. It ensures that data remains confidential, tamper-proof, and accessible only to authorized individuals.

B. Data Receiver Request Files

In the IAM-BDSS (Identity Attribute Management-Blockchain-based Data Sharing Scheme), the data receiver follows a specific process to request files. Initially, the receiver registers and logs into the system, gaining access to the platform. Within the system, they can view the shared data and identify the files they require. Once the desired file is selected, the receiver submits a formal request to the trusted authority associated with the IAM-BDSS. This request serves as a means to obtain authorization for accessing the requested file. The trusted authority evaluates the request and grants approval if deemed appropriate. After receiving approval, the receiver can proceed to download the requested file securely. The file's integrity and confidentiality are maintained by the secure ciphertext-policy employed in the IAM-BDSS, and its storage within the blockchain-based database ensures immutability.

Furthermore, the receiver has the ability to track and view their download history. This feature allows them to monitor their previous file downloads, providing an audit trail and promoting accountability within the data sharing process. The IAM-BDSS presents a reliable and secure framework for data receivers to request and access files, leveraging the capabilities of blockchain and ciphertext-policy to maintain data integrity and privacy.

C. Trusted Authority Authenticate The Request

The process begins with the trusted authority logging into the system. Once logged in, they can access the data and review the requests submitted by the receiver.

When the trusted authority receives permission from the data sharer, they proceed to authenticate the receiver's request. Upon successful authentication, the trusted authority securely provides the key to the receiver, enabling them to download the requested file.

The trusted authority logs into the IAM-BDSS system, gaining access to the platform's functionalities and features.

1) Within the system, the trusted authority can view the available data and the requests submitted by the receiver.

2) To authenticate the request, the trusted authority verifies the permissions granted by the data sharer. This step ensures that the receiver has been authorized to access the requested data.

3) Once the authentication process is successfully completed, the trusted authority securely provides the receiver with the necessary key or credentials to access the requested file. This key allows the receiver to decrypt and download the file securely.

4) Furthermore, the trusted authority has the ability to view the download history, which enables them to monitor and track the activities related to file downloads. This feature helps ensure transparency and accountability in the data sharing process.

5) By leveraging the secure ciphertext-policy and identity attribute management features of IAM-BDSS, the trusted authority can authenticate requests and facilitate secure and authorized data access for receivers. The utilization of blockchain technology ensures the integrity, transparency, and priv acy of the authentication process and data sharing activities.

D. BC Transaction Maintains Data

In the blockchain system, users can log in and take responsibility for maintaining shared data. The blockchain technology securely stores the data, ensuring its integrity and transparency throughout the process. In the IAM-BDSS (Identity Attribute Management-Blockchain-based Data Sharing Scheme), the blockchain plays a crucial role in maintaining shared data. Process of working:

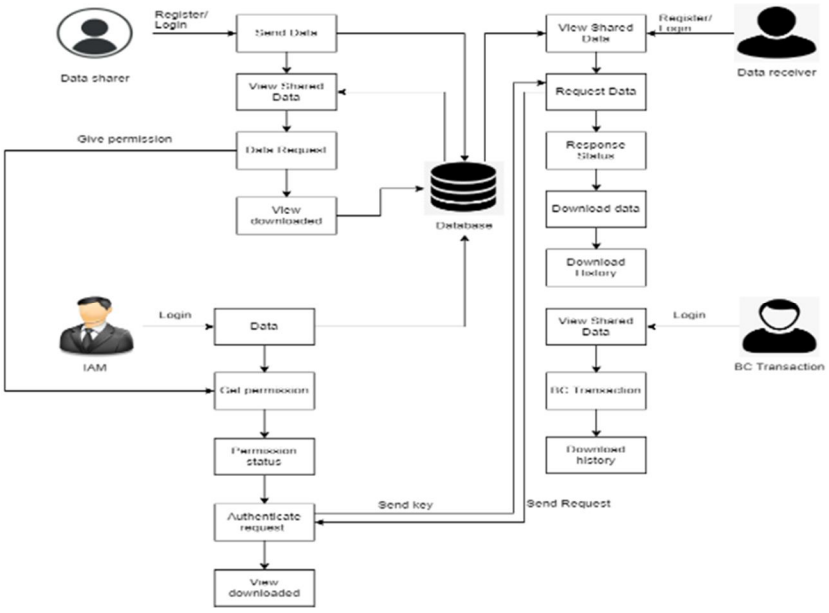
1) Users can log into the IAM-BDSS blockchain system, gaining access to its functionalities and features.

2) The shared data is securely stored within the blockchain, leveraging its inherent properties such as immutability and decentralized consensus. This ensures the integrity and confidentiality of the data throughout the sharing process.

3) The blockchain maintains a record of transactions, including the steps involved in the data sharing process. This transactional data provides a transparent and auditable trail, capturing the conversion and access activities.

4) Users can leverage the blockchain's features to view the download history of patients. This capability allows for tracking and reviewing past download activities, promoting accountability and facilitating monitoring within the data sharing scheme. The IAM-BDSS utilizes the power of blockchain technology, combined with secure ciphertext-policy and identity attribute management, to maintain data securely and transparently. By leveraging the blockchain's capabilities, the scheme ensures the integrity, privacy, and accountability of the shared data.

IV. ALGORITHM FORMULATION AND SYSTEM ARCHITECTURE



SYSTEM ARCHITECTURE

A. AES Algorithm

The Advanced Encryption Standard (AES) is currently the most popular and widely adopted symmetric encryption algorithm. In comparison to triple DES, AES has been found to be at least six times faster. DES needed to be replaced due to its small key size, which made it susceptible to exhaustive key search attacks as computing power increased. Although Triple DES was introduced as a solution, it was deemed slow.

Operation Of AES: AES operates as an iterative cipher, distinct from the Feistel cipher. It utilizes a structure known as a "substitution-permutation network." This network consists of a sequence of interconnected operations, involving both substitutions (replacing inputs with specific outputs) and permutations (shuffling bits). An interesting aspect of AES is that it operates on bytes rather than individual bits. Thus, a plaintext block of 128 bits is treated as 16 bytes. These bytes are organized into a 4x4 matrix, with four columns and four rows, to facilitate processing. In contrast to DES, the number of rounds in AES varies depending on the length of the key. For 128-bit keys, AES employs 10 rounds, while 192-bit keys require 12 rounds, and 256-bit keys demand 14 rounds. Each round employs a unique 128-bit round key, which is derived from the original AES key.

B. SHA-512 Algorithm

The SHA-512 algorithm is a widely used hashing algorithm that is responsible for performing a specific hashing function on input data. Hashing algorithms have various applications in internet security, digital certificates, and blockchain technology. Given the critical role of hashing algorithms in cryptography and digital security, this walkthrough aims to provide a clear and understandable explanation of SHA-512. It belongs to a family of hashing algorithms known as SHA-2, which also includes SHA-256. SHA-256 is extensively used in the hashing process of the Bitcoin blockchain.

Hashing Function: Hashing functions are designed to take input data and generate a fixed-length output known as a hash digest. For these functions to be useful, they must meet specific criteria:

1) Uniform distribution: It is crucial that the output hash digests are evenly distributed. Regardless of the input data, each possible output value should have an equal likelihood of being produced. This ensures that the hash function maintains a balanced distribution of hash digests.
2) Fixed Length: The output hash digests must have a consistent and predetermined length. This allows for easy comparison and storage of hash values. For example, a hashing function could produce hash digests of 20 characters or 12 characters, while SHA-512 generates a 512-bit output.
3) Collision Resistance: Collision resistance refers to the property where it is highly improbable, or practically infeasible, to find two distinct inputs that yield the same hash digest. A strong hashing function minimizes the possibility of collisions, ensuring that unique inputs produce unique hash digests.

In summary, a reliable hashing function ensures a uniform distribution of output values, fixed output length, and high collision resistance, making it a valuable tool in various applications such as data integrity verification and password storage.

V. CONCLUSION AND FUTURE WORK

In conclusion, we have presented a robust that ensures the security and privacy of medical data stored in the cloud. By employing hierarchical authority CP-ABE in conjunction with blockchain technology, our system effectively enforces access control policies while mitigating the risks associated with a single point of failure. This approach enhances user property privacy and strengthens key security. Furthermore, we have introduced a mechanism for the transfer of CP-ABE key parameters, utilizing blockchain for implementation and recording purposes, thereby enabling the testability of key parameter passing.

Scalability: As the volume of shared data continues to grow, enhancing the scalability of IAM-BDSS will be crucial. Research and development efforts can focus on optimizing the blockchain infrastructure to handle larger datasets efficiently and accommodate an increasing number of participants.

Interoperability: Enabling interoperability with other data sharing systems and standards can enhance the utility and compatibility of IAM-BDSS. Efforts can be directed towards integrating IAM-BDSS with existing healthcare information exchange frameworks and promoting seamless data sharing across different platforms.

Enhanced Privacy Measures: IAM-BDSS can further strengthen privacy measures to ensure secure and confidential data sharing. This can involve exploring advanced cryptographic techniques, such as homomorphic encryption and zero-knowledge proofs, to enhance data privacy without compromising the scheme's efficiency and functionality.

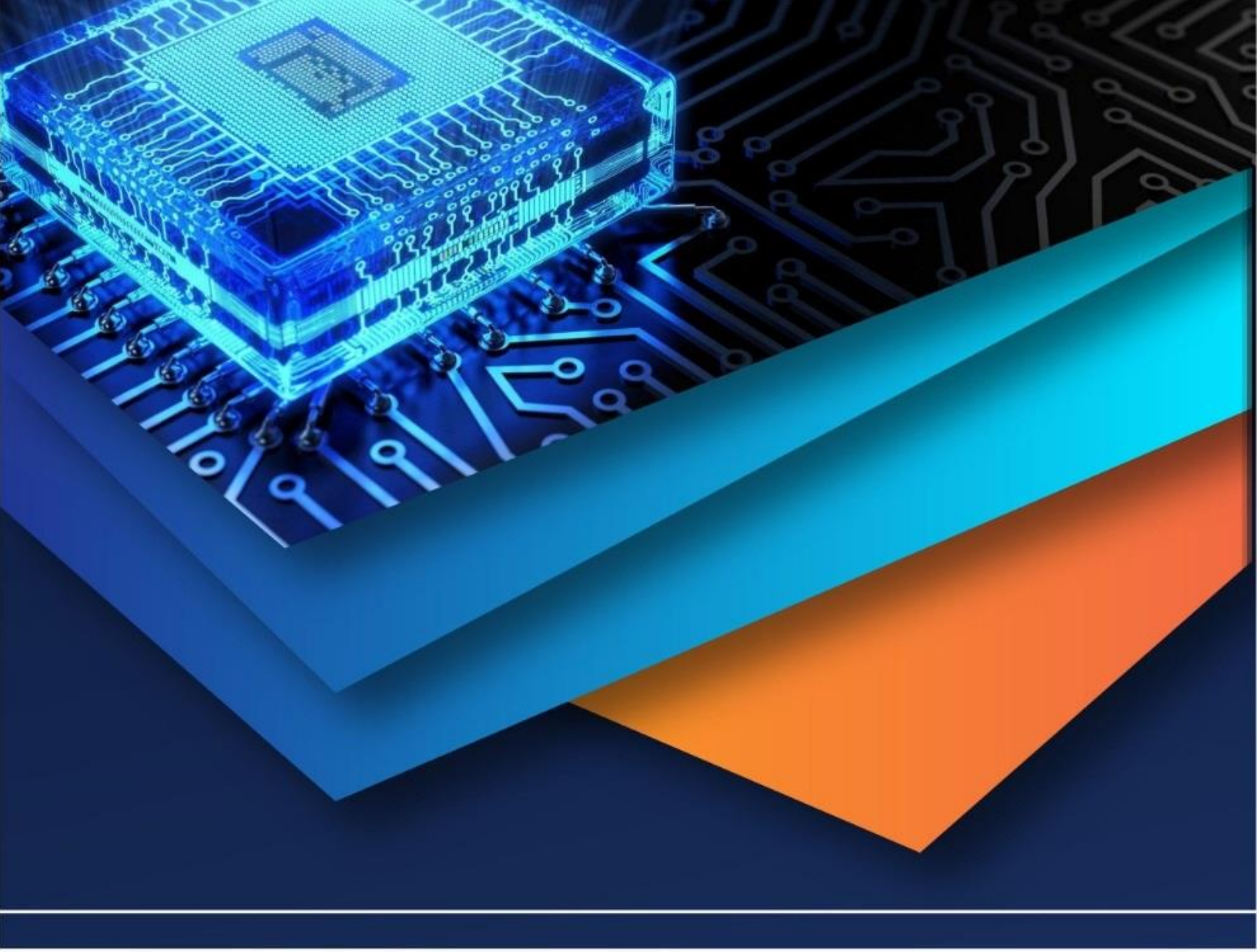
User-Friendly Interfaces: Improving the user experience and designing intuitive interfaces can enhance the accessibility and usability of IAM-BDSS. User-friendly interfaces can simplify data sharing processes and provide clear visibility into permissions, access history, and shared data.

The future scope of IAM-BDSS lies in its continued evolution to address scalability, interoperability, privacy enhancement, integration with emerging technologies, regulatory compliance, and improved user experience. These advancements will further establish IAM-BDSS as a robust and efficient solution for secure data sharing in healthcare and beyond.

REFERENCES

[1] Yu Guo; Chen Zhang; XiaohuaJia, "Verifiable and Forward-secure Encrypted Search Using BlockchainTechniques", 2020.
[2] Shunrong Jiang; Jianqing Liu; Liangmin Wang; Seong-Moo Yoo, "Verifiable Search Meets Blockchain: A Privacy-Preserving Framework for Outsourced Encrypted Data", 2019.
[3] Shengshan Hu; ChengjunCai; Qian Wang; Cong Wang; Xiangyang Luo; Kui Ren, "Searching an Encrypted Cloud Meets Blockchain: A Decentralized, Reliable and Fair Realization", 2018.
[4] Wenyuan Yang; Yuesheng Zhu, "A Verifiable Semantic Searching Scheme by Optimal Matching Over Encrypted Data in Public Cloud", 2020.
[5] Qiuyun Tong; Yinbin Miao; Ximeng Liu; Kim-Kwang Raymond Choo; Robert Deng; Hongwei Li, "VPSL: Verifiable Privacy-Preserving Data Search for Cloud-Assisted Internet of Things", 2020.
[6] Kun He; Jing Chen; Qinxi Zhou; Ruiying Du; Yang Xiang, "Secure Dynamic Searchable Symmetric Encryption With Constant Client Storage Cost", 2020.
[7] Xueqiao Liu; Guomin Yang; Willy Susilo; Joseph Tonien; Ximeng Liu; Jian Shen,"Privacy-Preserving Multi-Keyword Searchable Encryption for Distributed Systems", 2020.
[8] Jin Li; Yanyu Huang; Yu Wei; SiyiLv; Zheli Liu; Changyu Dong; Wenjing Lou, "Searchable Symmetric Encryption with Forward Search Privacy", 2021.
[9] Xixi Yan; Xiaohan Yuan; Qing Ye; Yongli Tang, "Blockchain-Based Searchable Encryption Scheme With Fair Payment", 2020

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)