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 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104234 |

Blockchain Enabled Secured Storage System for Forensic Data: Secured Storage System for Crime Evidences

Adarsh T N[1] ,Anjana S Ramanahalli[2] ,Gagana H S[3],Chandana G A[4],Dr..Chetana Prakash[5], Prof. Rachana G Sunkad[6]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[1]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[2]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[3]

B.E Student, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[4]

Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology, Davangere, Karnataka, India[5]

Assistant Professor, Department of Computer Science and Engineering, Bapuji Institute of Engineering and Technology,Davangere, Karnataka, India[6]

ABSTRACT: Nowadays data is most important in every phase of work. The storage and processing on data with security is the need of each and every application field. Data need to be tamper resistant due to possibility of alteration. There are chances of attack on information which is vital for organization. One such challenge is securing forensic data. With rapid increase in cyber crime, attackers behave maliciously to alter those data. But it is having great impact on forensic evidences which is required for provenance. Therefore, it is required to maintain the reliability and provenance of digital evidences as it travels through various stages during forensic investigation. Blockchain technology provides the transfer of assets or evidence reports in transparent environment without central authority. A blockchain based secure system for forensic evidence is proposed. The proposed system is implemented on Ethereum platform. The tampering of forensic evidence can be easily traced at any stage by anyone in the forensic chain. The security enhancement of forensic evidences is achieved through implementation on Ethereum platform with high integrity, traceability and immutability.

I. INTRODUCTION

Forensic evidence is defined as criminal evidence acquired through scientific methods, including blood tests DNAtests to be used in court. Alternatively, forensic evidence can be holistically defined as the application of science within legal proceedings. Forensic evidence is gathered through photographs and measurements taken at the crime scene. In thecase of violent crimes, these are obtained along with fingerprints, footprints, tire tracks, blood and other body fluids, hairs, fibres, and fire debris. Each of these elements is useful in understanding what took place during the commission of the crime. Forensic analysis is usually carried out by experts working individually or in teams. Advanced techniques often require laboratories where the investigative conditions can be carefully controlled and monitored. Private laboratories and government agencies support small and large forensic labs. Analysis of forensic evidence is used in the investigation and prosecution of civil and criminal proceedings. Often, it can help to establish the guilt or innocence of possible suspects Forensic evidence is also used to link crimes that are thought to be related to one another. For example, DNA evidence can link one offender to several different crimes or crime scenes (or exonerate the accused). Linking crimes helps law enforcement authorities to narrow the range of possible suspects and to establish patterns of for crimes,

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

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104234 |

which are useful in identifying and prosecuting suspects. Forensics would not exist without transparency and access to data. In this approach, there is a forensic chain in which generated report passes through various levels or intermediaries such as pathology laboratory, doctor, police department etc. To build the transparent system with immutability of forensicevidences, blockchain technology is more suitable. Blockchain technology provides the transfer of assets or evidence reports in transparent environment without central authority. A blockchain based secure system for forensic evidences is proposed. The proposed system is implemented on Ethereum platform. The tampering of forensic evidence can be easily traced at any stage by anyone in the chain. The security enhancement of forensic evidences is achieved through implementation on Ethereum platform with high integrity, traceability and immutability.

The Forensic Evidence Management System is a web evidence management system. It is mainly targeted for law enforcement agencies and analysis labs for managing large volumes of forensic evidence including the chain of custody. It shall also be used for enterprises or government departments, who must handle forensic evidence. The current legal position of blockchain transactions is that they can only be used as documentary evidence if they are provided with a qualified electronic signature. The term evidence refers to any digital images that may be utilized for organizational, legal, or criminal investigations. Digitalization of forensic evidence management system is a need of time as it is an environment friendly model. Blockchains are digitally distributed ledgers of transactions signed cryptographically in chronological order that are sorted into blocks and is completely open to anyone in the blockchain network. Blockchain forensics is the use of science and technology to investigate and establish facts in criminal or civil courts of law. In other words, blockchain forensics deals primarily with the recovery and analysis of latent evidence left on the blockchain digital ledger as the results of transaction activities on a blockchain. Blockchain forensics brings user trust to the blockchain ecosystem and provides transparency to the blockchain transactions to deter possible usage from illicit transactions.

II. LITERATURE SURVEY

Lone and Mir-"Forensic-chain: A blockchain-based digital forensics chain of custody (2019)" [1] The authors main aim is to build a tamperproof chain of custody for digital forensics. A prototype of a blockchain-based digital forensics chain of custody is discussed. ForensicChain is a blockchain based solution for maintaining and tracing digital forensics chain of custody.

Al-Khateeb, Epiphaniou, and Daly-"The admissibility of digital evidence in a court of law and the importance ofchain of custody(2019)"[2] The research work presented focuses on the implementation of chain of custody using distributed ledger. The authors have presented the practical scenario that how chain of custody preserved on blockchain makes the overall system forensically ready and enables better investigation.

Li, Qin, and Min- "Evidence identification, preservation, analysis, and presentation recorded in the chain of blocks(2019)" [3] The prototype that is discussed is developed using Hyperledger Composer. Hyperledger is a Linux foundation project that develops blockchain technologies for business supporting only registered members. It is an open-source collaborative effort created to advance cross industry blockchain technologies.

Bonomi, Casini, and Ciccotelli "A blockchain-based chain of custody (B-CoC) (2018)"[4] The work presented ismainly focused on the evidence management to guarantee its suitability, integrity, and traceability of the owner. It discusses the prototype implementation of B-CoC architecture based on Ethereum.
Tasatanattakool,P.,&Techapanupreeda.C-"Blockchain:Challenges,applications"(2017, January)[5] Presented in 2018 International Conference on Information Networking (ICOIN). Blockchain is a form of database storage that is non-centralized, reliable, and difficult to use for fraudulent purposes. Transactions are made with no middle men. There are no transaction fees and no need to give your real name. The blockchain can be adopted for various applications. The adoption of blockchain-based applications in e-Government is still very limited and there is a lack of empirical evidence.

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

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104234 |

The main challenges faced in blockchain adoption are predominantly presented as technological aspects such as security, scalability and flexibility. From an organizational point of view, the issues of acceptability and the need of new governance models are presented as the main barriers to adoption. Moreover, the lack of legal and regulatory support is identified as the main environmental barrier of adoption.

A Porat, A Pratap, P Shah, V Adkar - scs.stanford.edu. Blockchain Consensus: "An analysis of Proof-of-Work and its applications." (2017) Blockchain Technology, having been around since 2008, has recently taken the world by storm. Industries are beginning to implement blockchain solutions for real world services. Author mainly focuses to build a Proof of Work based Blockchain consensus protocol and evaluate how major applications can run on the underlying platform. The proof of work (PoW) consensus algorithm faces the 51% attack risk. The proof-based consensus algorithm is defending spam attack that wastes up the computer's processing and the denial-of-service and other network service exploitations.

Halpin, H., &Piekarska, M. "Introduction to Security and Privacy on the Blockchain." (2017, April). Proposed in 2017 IEEE European Symposium on Security and Privacy Workshops (Euros PW). The blockchain has fueled one of themost enthusiastic bursts of activity in applied cryptography in years, but outstanding problems in security and privacy research must be solved for blockchain technologies to go beyond the hype and reach their full potential. The major concern for blockchain technology's security and privacy is routing attacks. A blockchain network and application rely on the real-time movement of massive amounts of data. Hackers can use an account's anonymity to intercept data as it isbeing transmitted to internet service providers.

III. PROPOSED SYSTEM

An increasing number of forensic crime cases find the need to manage evidence for investigation proceedings. All these investigations will benefit from more systematic evidence management. The system proposed to help this systematic evidence management is "Blockchain enabled secured storage system for forensic data: Secured storage system for crime evidences. " The actual node setup is done for investigators. Given the need for security, the chain involves the storage of information with regards to the physical media containing forensic evidence in the form of forensic report. The nodes will be added manually to the chain and turnoff auto-discovery for nodes. This proposed system will help efficiently in securing forensic evidences.

IV. METHODOLOGY

Forensic investigation is the gathering and analysis of all crime related physical evidences in order to conclude about a suspect. Forensic evidence is one of the most prominent aspects of today's judicial system. Forensic evidence is collected by way of Forensic investigation. Forensic investigation encompasses many different fields of science including Anthropology, Biology, Chemistry, Engineering, Genetics, Medicine, Pathology and Toxicology. This includes analysis of any kinds of materials including blood, fibres, bullets, fingerprints, footprints, palm prints. These are several types of Forensic evidences which are collected and examined in the laboratory to find out the real culprit involved in the crime. These evidence data is stored in the blocks of blockchain along with unique identifier value hash and previous hash values.This chain setup is difficult to be changed, hacked or manipulated thus providing security for forensic evidences.

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

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104234 |

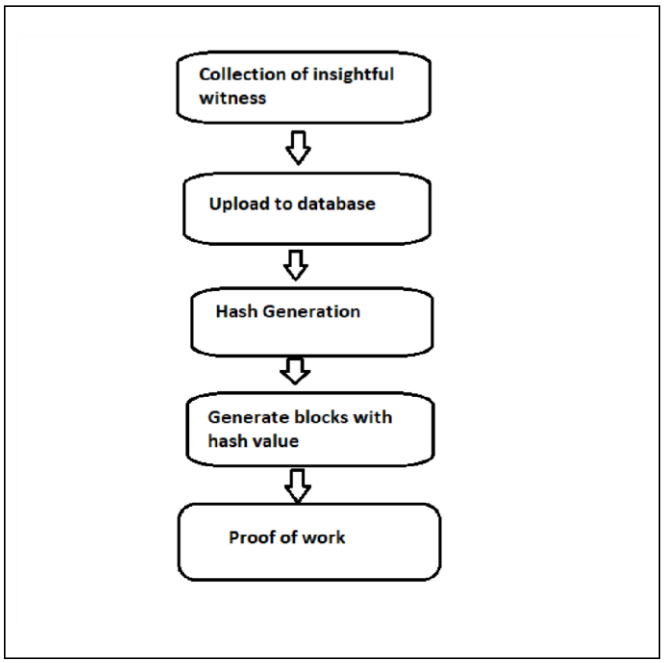


Fig 4.1: Workflow

Step1: The evidences, from the crime scene or the place of investigation, are collected in form of DNA analyser, video, audio, text, images or even system logs including the time of the evidence collected to make a timeline. Step2:The collecteddata are uploaded to the MySQL database which helps to store the case details. Case details are stored in the form of Forensic reports. Step3: A hash function turns an input (for example text) into a string of bytes with a fixed length and structure. Theoutput or value created is called a 'Hash value' or 'checksum.' Any hash value created from data using a specific hashing algorithm such as SHA-256 is always the same length and one-way - it cannot be reversed. A secure hashing algorithm or commonly referred to as SHA-256, is an unkeyed cryptographic hashing function that takes an input of variable length andproduces a 256-bit long hash output. Step4: The process of verifying and adding blocks to a blockchain ledger using a proofof work consensus mechanism is referred to as mining. The block is created along with timestamp. Thetimestamp helps to find when the evidence was uploaded to the blockchain. In case of any tamper it will change, which leads to breaking of chain. If the chain is not broken, it ensures the block is in proper state. Step5:POW is a method to ensure the accuracy of new transactions that are added to blockchain. The algorithm is used to verify these transactions and create a new block in the blockchain. POW is employed to ensure the integrity of new data. Actual node setup is as follows. Given the need for security as the chain involves the storage of information with regards to the storage media containing forensic evidences, thenodes are manually added to the chain and auto discovery for nodes is turned off. After the chain setup, public wallet addresses of each of the nodes is gathered. Once having all the public wallet addresses of each of the nodes, the genesis filecan be created. The genesis file defines the first block in the chain, and the first block defines which chain you want to join.In order for the nodes to find one another, need to get the enode id of every node, which kind of provides a way for other nodes to connect to them. To connect the nodes to the Ethereum python APIs, to perform actions on the blockchain, the contract must be deployed.

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 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104234 |

V. RESULTS

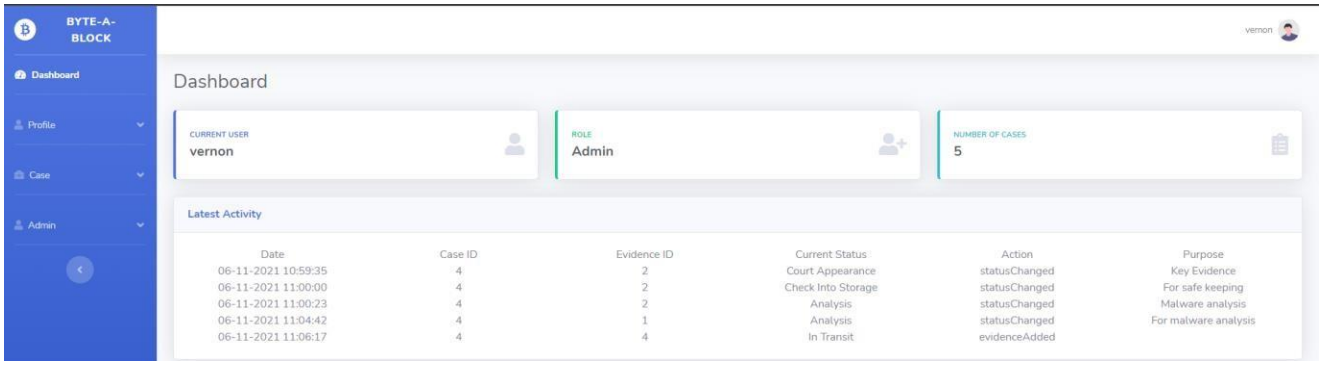


Fig 5.1: Home Page

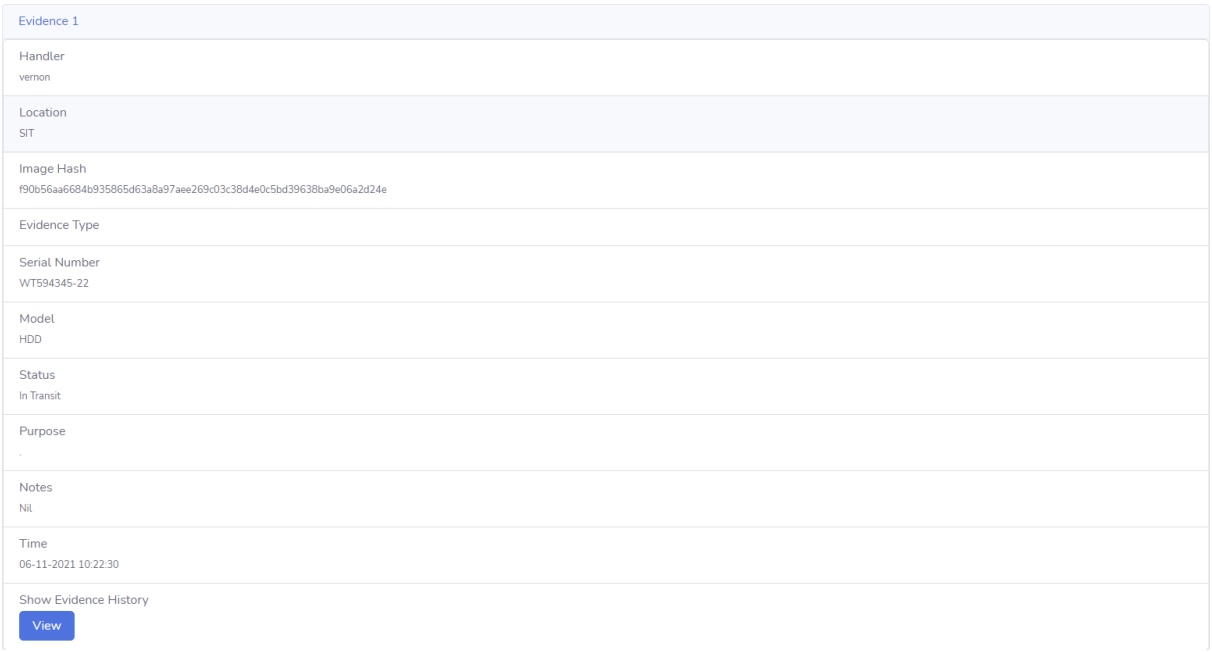
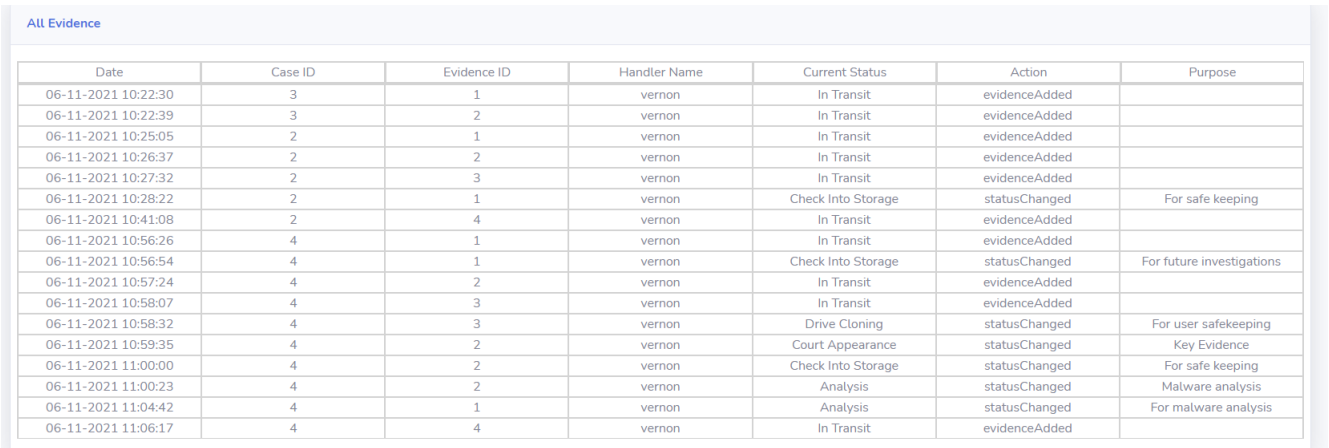


Fig 5.2: Case Details



All Evidence

Date	Case ID	Evidence ID	Handler Name	Current Status	Action	Purpose
06-11-2021 10:22:30	3	1	vernon	In Transit	evidenceAdded	
06-11-2021 10:22:39	3	2	vernon	In Transit	evidenceAdded	
06-11-2021 10:25:05	2	1	vernon	In Transit	evidenceAdded	
06-11-2021 10:26:37	2	2	vernon	In Transit	evidenceAdded	
06-11-2021 10:27:32	2	3	vernon	In Transit	evidenceAdded	
06-11-2021 10:28:22	2	1	vernon	Check Into Storage	statusChanged	For safe keeping
06-11-2021 10:41:08	2	4	vernon	In Transit	evidenceAdded	
06-11-2021 10:56:26	4	1	vernon	In Transit	evidenceAdded	
06-11-2021 10:56:54	4	1	vernon	Check Into Storage	statusChanged	For future investigations
06-11-2021 10:57:24	4	2	vernon	In Transit	evidenceAdded	
06-11-2021 10:58:07	4	3	vernon	In Transit	evidenceAdded	
06-11-2021 10:58:32	4	3	vernon	Drive Cloning	statusChanged	For user safekeeping
06-11-2021 10:59:35	4	2	vernon	Court Appearance	statusChanged	Key Evidence
06-11-2021 11:00:00	4	2	vernon	Check Into Storage	statusChanged	For safe keeping
06-11-2021 11:00:23	4	2	vernon	Analysis	statusChanged	Malware analysis
06-11-2021 11:04:42	4	1	vernon	Analysis	statusChanged	For malware analysis
06-11-2021 11:06:17	4	4	vernon	In Transit	evidenceAdded	

Fig 5.3: Transcation detail in the blockchain

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

|| Volume 11, Issue 4, April 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1104234 |

VI. CONCLUSION

Blockchain by design enforces integrity, transparency, authenticity, security and auditability thus making it possibly the best choice for maintaining and tracing forensic evidences. Blockchain helps in friction reduction through increased trust and thus brings the real promise for forensic community. Blockchain is the most effective solution for the digital era of forensics. The future work aims at developing complete Ethereum based smart digital forensic chain for securing forensic evidences.

REFERENCES

1. Lone and Mir (2019) have proposed forensic-chain: a blockchain-based digital forensics chain of custody.
2. Al-Khateeb, Epiphaniou, and Daly (2019) have briefly discussed the admissibility of digital evidence in a court oflaw and the importance of chain of custody.
3. Li, Qin, and Min (2019) have presented the work focused on evidence identification, preservation, analysis, andpresentation recorded in the chain of blocks.
4. Bonomi, Casini, and Ciccotelli (2018) have proposed a blockchain-based chain of custody (BCoC).
5. Tasatanattakool,P.,&Techapanupreeda,C"Blockchain: Challenges, applications"(2018, January)
6. A Porat, A Pratap, P Shah, V Adkar - scs.stanford.edu. Blockchain Consensus: "An analysis of Proof-of-Work andits applications." (2017)
7. Halpin, H., &Piekarska, M. "Introduction to Security and Privacy on the Blockchain." (2017, April).
8. Flores, D. A., &Jhumka, A. "Implementing Chain of Custody Requirements in Database Audit Records for ForensicPurposes"(2017, August)
9. Ryu et al. (2019) have proposed a blockchain-based forensics framework for IoT environment.
10. F. Wang and L.Xu and W. Gao, "Comments on SCLPV: Secure Certificate less Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors," IEEE Transactions on Computational Social Systems, vol. 5, no. 3, pp. 854–857, Sep. 2018.
11. A. Shah, R. Ganesan, S. Jajodia, and H. Cam, "Understanding trade-offs between throughput, quality, and cost of alert analysis in a csoc," IEEE Transactions on Information Forensics and Security, pp. 1–1, 2018.
12. Y. Teing, D. Ali, K. Choo, M. T. Abdullah, and Z. Muda, "Greening cloud-enabled big data storage forensics: Syncany as a case study," IEEE Transactions on Sustainable Computing, pp. 1– 1, 2018.
13. S. Li, L. Da Xu, and S. Zhao, "5g internet of things: A survey," Journal of Industrial Information Integration, 2018.

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