RECENT ADVANCES IN IoT AND BLOCKCHAIN TECHNOLOGY

Editors:
Koyel Datta Gupta
Deepak Kumar Sharma
Rinky Dwivedi
Fadi Al-Turjman

Bentham Books

Advances in Computing Communications and Informatics

(Volume 4)

Recent Advances in IoT and Blockchain Technology

Edited by

Koyel Datta Gupta
Department of Computer Science & Engineering
Maharaja Surajmal Institute of Technology
New Delhi
India

Deepak Kumar Sharma
Department of Information Technology
Indira Gandhi Delhi Technical University for Women
Delhi, India

Rinky Dwivedi
Department of Computer Science & Engineering
Maharaja Surajmal Institute of Technology
C-4 Janakpuri, New Delhi 100058
India

&

Fadi Al-Turjman
Department of Artificial Intelligence Engineering
Near East University
North Cyprus

Advances in Computing Communications and Informatics

Volume # 4

Recent Advances in IoT and Blockchain Technology

Series Editors: Pradeep Kumar Singh, Bharat Bhargava and Wei-Chiang Hong

Volume Editors: Koyel Datta Gupta, Deepak Kumar Sharma, Rinky Dwivedi & Fadi Al-Turjman

ISSN (Online): 2737-5730

ISSN (Print): 2737-5722

ISBN (Online): 978-981-5051-60-5

ISBN (Print): 978-981-5051-61-2

ISBN (Paperback): 978-981-5051-62-9

First published in 2022.

need for a court order if at any point you breach any terms of this License Agreement. In no event will any delay or failure by Bentham Science Publishers in enforcing your compliance with this License Agreement constitute a waiver of any of its rights.

3. You acknowledge that you have read this License Agreement, and agree to be bound by its terms and conditions. To the extent that any other terms and conditions presented on any website of Bentham Science Publishers conflict with, or are inconsistent with, the terms and conditions set out in this License Agreement, you acknowledge that the terms and conditions set out in this License Agreement shall prevail.

Bentham Science Publishers Pte. Ltd.
80 Robinson Road #02-00
Singapore 068898
Singapore
Email: subscriptions@benthamscience.net

CONTENTS

PREFACE

It is of immense pleasure to launch our book entitled Recent Advancements In Iot And Block chain that explores the idea of the Internet of Things and Blockchain Technology.

Recent advancements in the fields of block chaining for enterprises, block chaining in financial services, block chaining in supply chain, IoT in healthcare, and other industries and technologies have resulted in the integration of block chaining and the Internet of Things (IoT). Blockchain, whether public or private, is capable enough to maintain the integrity of transactions by decentralizing the records among involved users. Many IoT companies are using blockchain technology to make the world a better-connected place. Many companies are exploring how to make this technology more and more efficient service provider for IoT. Blockchain and IoT are certainly revolutionary technologies that are changing the world around us. Therefore, the major focus of this book is to present the recent advancements in these two technologies and how these technologies, when merged together, provide a transparent, reliable, and secure model for data processing by intelligent devices in various domains.

The book chapters have been contributed by scholars, researchers, academicians, and engineering practitioners. The book received plenteous abstract-articles that were subjected to rigorous review procedures to ensure that the selected articles met the required quality standards.

We would extend our gratitude to everyone who has contributed directly or indirectly to the book. We express our sincere gratitude to all the authors and reviewers who ve been committed to shaping this book even after facing hardships due to the current pandemic situation. Our earnest thanks to the publisher Bentham Science for accepting our book proposal.

ACKNOWLEDGEMENTS

Our gratitude belongs to all the co-authors without whom these pages would be blank. We would also like to thank all the referees for their useful suggestions.

Koyel Datta Gupta
Department of Computer Science and Engineering
Maharaja Surajmal Institute of Technology
New Delhi
India

Deepak Kumar Sharma
Department of Information Technology
Indira Gandhi Delhi Technical University for Women
Delhi
India

Rinky Dwivedi
Department of Computer Science and Engineering
Maharaja Surajmal Institute of Technology
C-4 Janakpuri, New Delhi 100058
India

&

Fadi Al-Turjman
Department of Artificial Intelligence Engineering
Near East University
North Cyprus

List of Contributors

Aarti Goel Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India

Aayush Bhatnagar Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India

Aditya Gupta Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India

Arjun Khera Department of Information Technology, Netaji Subhas University of Technology, New Delhi 110078, India

Ayush Kumar Singh Department of Information Technology, Netaji Subhas University of Technology (Formerly known as Netaji Subhas Institute of Technology), New Delhi, India

Bhuvneshwar Sharma Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India

Deepak Kumar Sharma Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India

Harshit Mittal Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India

Koyel Datta Gupta Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India

Manik Agarwal Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India

Muskan Gupta Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India

Nipunika Department of Information Technology, Netaji Subhas University of Technology (Formerly known as Netaji Subhas Institute of Technology), New Delhi, India

Pardeep Kumar Department of Computer Systems and Engineering, QUEST University, Nawabshah, Pakistan

Rinky Dwivedi Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India

Rohit Rastogi Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India

Sachin Singh Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India

Sahil Dwivedi Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India

Salman Azeez Syed Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India

Tanmay Sharma Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India

Vimal Gaur Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India

Vivaswat Sinha Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India

CHAPTER 1

Blockchain Framework for Data Storage and Security

Salman Azeez Syed[1,*], **Vivaswat Sinha**[1], **Sachin Singh**[1] and **Aarti Goel**[1]

[1] *Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India*

Abstract: In this age of sensitive information where knowledge is power, our data has become an invaluable resource. Easy and public access to information makes it vulnerable to adulteration. The ever-increasing cases of cyber-attacks are causing organizations to spend an exorbitant amount on security. General cloud storage systems are considered efficient for data storage and sharing, but it has multiple limitations such as data centralization, data leakage, and high maintenance cost. Data centralization makes it a hotspot for cyber-attacks, making it prone to data outflows and tampering. An effective alternative is a decentralized system. With advancements in information technology and cyber security, the need for authenticity and verification is highly sought after, making blockchain technology an extremely indispensable tool in the hands of many organizations and enterprises. It solves the problem of security by encrypting its data storing it as a "Hash" or encoded data so that only the user with the key can access the data. The finance sector is being overwhelmed by the ever-increasing reliability of blockchain and the implementation of its framework and architecture. Blockchain is a distributed ledger system across a network of users. The blockchain technology, being decentralized, is proposed as a disseminated and diffused or distributed approach which is testified to decipher and decode the security requirements of the new digital era as well as serve as a platform and a jump pad for advancements in various other fields such as Internet of Things (IoT), data storage, biometric security, healthcare facilities, smart grids, and many more.

This chapter begins with a basic outline of all you need to know about blockchain, an upcoming evolutionary technology that ameliorates the world of data decentralization and security. It further explains its use, features, areas of implementation, architecture, as well as its limitations that are detrimental to be cognizant of how the blockchain system works/is implemented. It then explores P2P networks and interplanetary file systems (IPFS) followed by its current use cases in the form of Filecoin. Next, the chapter explores the privacy and security aspects of the blockchain. It showcases some of the faults of blockchain ledgers like Sybil and discusses some techniques that are implemented to fix them. It discusses bitcoin, one of the most secure blockchain architecture to date, and describes private and public keys, peer to peer network, hash.

[*] **Correspondence author Salman Azeez Syed:** Department of Information Technology, Netaji Subhas University of Technology, New Delhi, India; Tel: 7428030776; E-mail: azeezsalman1@gmail.com

Koyel Datta Gupta, Deepak Kumar Sharma, Rinky Dwivedi and Fadi Al-Turjman (Eds.)

chained storage, digital signature, and consensus algorithms implemented by bitcoin to prevent any fraudulent transactions from taking place.

Keywords: Attribute Based Encryption (ABE), Blockchain, Consensus, Digital signature, Filecoin, IPFS, P2P network, Sharding.

INTRODUCTION

Nowadays, computers have found their way into many fields. This process of digitalization or more appropriately computerization, has now been adopted by all the departments ranging from hospitals, schools, railways, and many more areas. Why? This is because computers have huge advantages over paper-based systems, which has led to the proliferation of computers in almost all organizations and enterprises. Some of these advantages include:.

- **Compact**

In contrast to recording data on paper, storage as a digital copy massively reduces space, which is generally a constraint for small organisations.

- **Ease of Accessibility**

All the data stored on the cloud can be accessed easily and remotely by any person around the world, making it a good means of sharing data. Otherwise, the person would have to look at the papers himself in person.

- **Readability**

Papers can easily be lost or damaged. Even if it is kept safely, over time, the ink fades away and this requires the need for constant updating and refreshing of the data. With digitalization, the need for such is eliminated, saving money, time, resources, and most importantly, the environment.

- **Speed and Efficiency**

Accessing and organizing data on computers is much easier, resulting in faster and easier access to data from anywhere around the world.

- **Cost-effectiveness**

When a single computer can be used instead of a room full of papers for the current and the future data, which requires much more maintenance, and doesn't provide as much accessibility, the computer is a cost-effective and modern alternative in the long run.

Having corroborated the supremacy of computerization, we then come to the problems faced by it. Some of the major problems include security of data, storage space, and other miscellaneous problems such as cost of maintenance and health issues. For the first two problems, many solutions have been devised, which include a database or a data archive where all the information is stored. This database can be centralized or decentralized. We shall now discuss each of them in the next section.

Centralized Database System

A centralized database is a type of database where storage, management, and manipulation of data are done at a single central location. This center may be a server or even a mainframe computer, depending on the requirements of the network. All the data from each computer is stored at this single location which often runs around the clock and must be properly maintained. For example, a company implements a centralized database system, then all data processed or produced from its various branches and from each workstation is stored at this sole location.

In a centralized system, users rely on a central authority that can alter or change the system by altering the database. These do not distribute authority and the legitimacy of the system depends solely on the accountability of this central authority.

Advantages

- Data is easily portable and accessible since it is kept in a single location.
- Maximum data integrity as data can be easily coordinated consistently and accurately.
- Storing data in a single location reduces data redundancy and saves space.
- Cost effective, suitable for small organizations and businesses.
- Effortless debugging, simulation, and deployment for application development.

Disadvantages

- Major disadvantage is the breakdown of the central location, which affects all the associated workstations.

CHAPTER 2

Blockchain Based Hybrid Framework for Identity Management in Healthcare

Deepak Kumar Sharma[1,*], Arjun Khera[2], Koyel Datta Gupta[3] and **Rinky Dwivedi[3]**

[1] *Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India*

[2] *Department of Information Technology, Netaji Subhas University of Technology, New Delhi 110078, India*

[3] *Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India*

Abstract: Healthcare systems face numerous impediments due to the unavailability of proper mechanisms to track the transactions related to patient's medical records. The maintenance and privacy of patient records are one of the key requirements of the healthcare system. Blockchain can be the potential solution to these problems. Blockchains have made a tremendous impact ever since their invention barely a decade ago. This paper delves into how blockchain can be used to solve the problem of patient record management by constructing scalable decentralised key systems with inbuilt sharing of credentials in a safe, secure, and digitally verifiable way. The work presents a hybrid scalable system capable of managing personal identity in a decentralized manner with no dependence on central authorities along with a rapid and simplistic way of exchanging claims among the users. The system overcomes potentially all problems associated with SOVRIN and blockchains in general by splitting itself into two symbiotic versions, one centralised and the other, decentralised.

Keywords: Blockchain, Healthcare, Identity management, Decentralized applications, IoT.

INTRODUCTION

With the rapid growth in the field of information technology, the changes in the worldwide healthcare system are eminent. IoT based medical system [1, 2] is gaining popularity because of improved coordination between healthcare personnel and patients. The patient's data recorded in the form of images, videos, text, and audio by IoT devices [3] needs to be processed and stored through

[*] **Correspondence author Deepak Kumar Sharma:** Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India; Tel: 9868861080; E-mail: dk.sharma1982@yahoo.com

multimedia techniques. The devices are connected to the internet for subsequent storage of information at the cloud level, which can be accessed by different entities like doctors, insurance companies, research wings, and pharmaceutical companies (Fig. **1**). However, healthcare record contains private information that may be viable to cyber-attacks. Hence, securing such large-scale multimedia data and maintaining the privacy of the patient records is important.

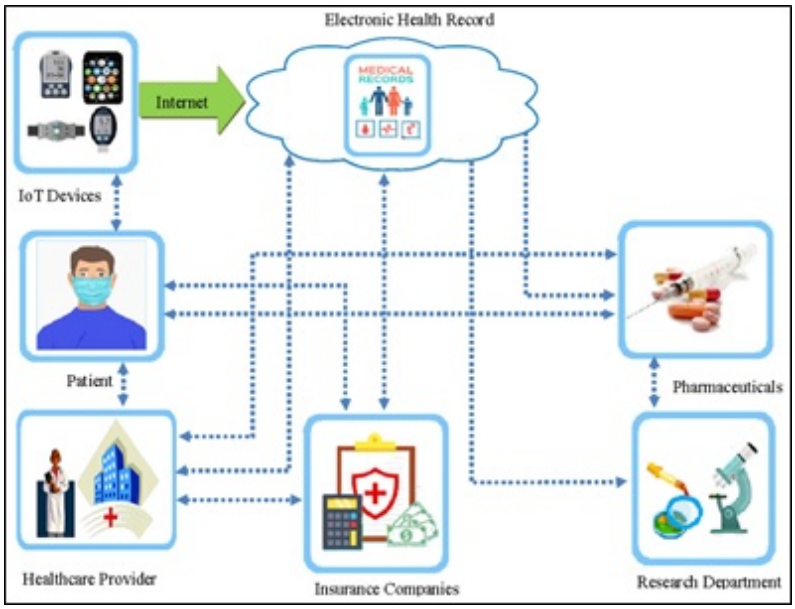

Fig. (1). IoT enabled Healthcare System.

The online transfer and storage of this sensitive record require a robust credential system. In this context, blockchain technology [4 - 7] can be used as a secure way to save and distribute information. The smallest unit of data that is linked with one another is called a block. The blockchain is a linear list of these blocks which are linked to one another using cryptographic hash functions, as depicted in Fig. (**2**). Evidently, the blockchain is nothing but an immutable ledger of records maintained across several computers which are linked together in peer-to-peer manner. Large number of participating entities maintain the ecosystem by storing, updating, and exchanging data among each other.

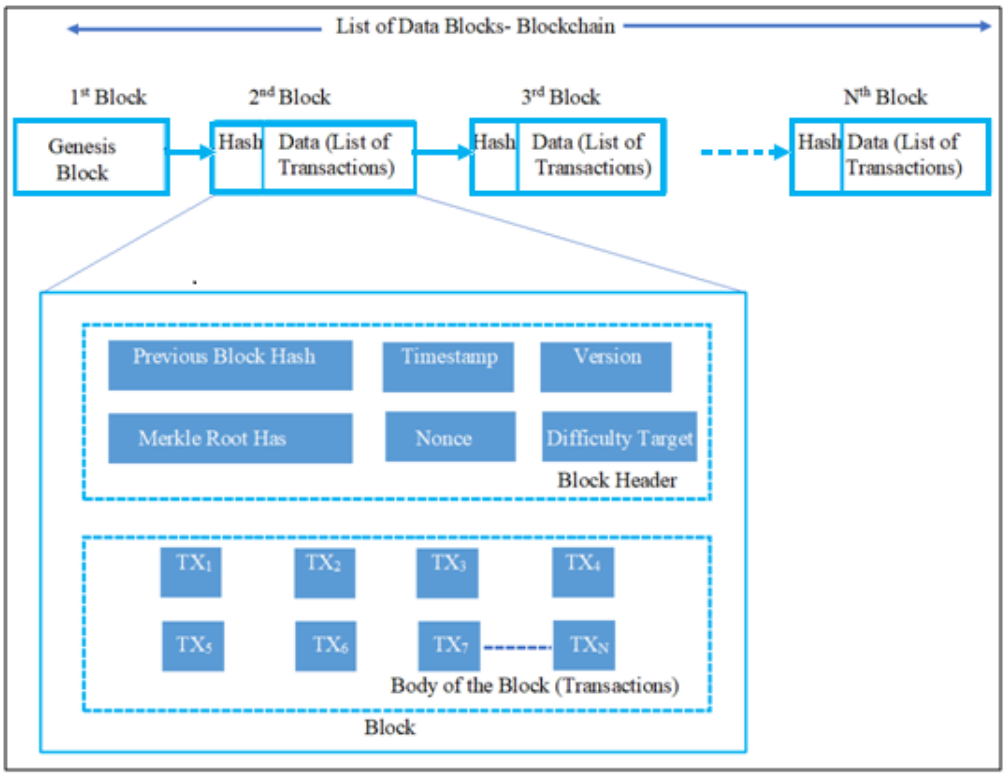

Fig. (2). List of Data Blocks.

However, like any new invention, blockchain also had its flaws, the most pervasive being scalability. Decentralization and the associated benefits come at the cost of performance and scaling. When Bitcoin experienced a surge in popularity, the associated transaction fees shot through the roof as the system was capable of processing only a single every 10 minutes, which pales in comparison to other payment processing platforms such as Visa, which processes up to 2000 transactions per second. This was not the only problem. Bitcoin also consumed a lot of energy for mining, so much so that it has come under scrutiny for wastage of resources due to consumption charting more than even what cities draw. Many variations and changes to this structure, particularly to the consensus algorithms, have been introduced since then to overcome these shortcomings. Most of the implementations of blockchain to date have been around cryptocurrencies, and there is good reasoning behind that. Blockchain or decentralisation is a novel service, and running this service without any form of commitment by a central authority means other participants need something in return for operating the chain and its operations. Monetary rewards solve this problem better than

CHAPTER 3

Blockchain in Smart Healthcare Facility

Ayush Kumar Singh[1], Nipunika [1] and **Deepak Kumar Sharma[2,*]**

[1] *Department of Information Technology, Netaji Subhas University of Technology (Formerly known as Netaji Subhas Institute of Technology), New Delhi, India*

[2] *Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, India*

Abstract: Healthcare is an indispensable system whose efficiency and robustness are reliable indicators of a nation's prosperity. This sector has seen technological advancements not only in terms of medical equipment and drugs but also in varied fields such as Electronic Medical Records, wearable health monitoring devices, and telemedicine. In this chapter, we explore the aspects of utilising the disruptive technology of blockchain in healthcare. Ever since its initial use in cryptocurrency and finance, aiming to shift the industry from institute-centric to patient-centric, blockchain technology has found its use in healthcare. This chapter analyzes its use cases along with the limitations posed by traditional healthcare systems and how blockchain alleviates them. Furthermore, we will also walk through the roadblocks in implementing blockchain-based healthcare services and discuss a few implemented as well as proposed blockchain-based healthcare frameworks, highlighting their successes and failures.

Keywords: Applications, Blockchain, Electronic medical records, Electronic health records, Healthcare, Services, Supply chain.

INTRODUCTION

Blockchain technology came into existence in 2008 after Satoshi Nakamoto, a pseudonym for a developer or a group of developers, released a whitepaper with the title “Bitcoin: A Peer to Peer Electronic Cash System” [1]. Bitcoin became the first major cryptocurrency, with its peak market capitalization reaching 238 billion USD in the fourth quarter of 2017 [2]. Since its conception, Blockchain has been thoroughly researched for implementation in fields other than cryptocurrency and finance. The key features of blockchain include immutability, privacy, incorruptibility, and transparency, which makes it a suitable framework for implementing healthcare based applications. In this section, we will explore.

* **Correspondence author Deepak Kumar Sharma:** Department of Information Technology, Indira Gandhi Delhi Technical University For Women, Delhi, India; Tel: 8743075567; E-mail: dk.sharma1982@yahoo.com

Koyel Datta Gupta, Deepak Kumar Sharma, Rinky Dwivedi and Fadi Al-Turjman (Eds.)

the working of blockchain and its prominent use-cases. This will be followed by analyzing the traditional systems in healthcare and then we will look at an overview of how blockchain technology can reform the healthcare industry.

Technical Aspects of Blockchain

In its essence, Blockchain is a distributed public ledger. In other words, it is a decentralized database. There is no central authority in charge of its functioning and maintenance. This is the reason it enables peer-to-peer transactions, eliminating the need for a middleman. As the name suggests, a blockchain is a linear arrangement of blocks, which are its data units. These blocks can store data ranging from transaction records to medical records and even media. This linear arrangement is like an append-only data structure. New blocks can only be added to one of the ends of this chain. Every block has a hash value that uniquely identifies it. Further, the block also contains the hash value of the block previous (otherwise known as the parent block), which forms a link. The very first block of a blockchain, which has no parent block, is known as the genesis block.

Since there is no entity to verify which blocks are to be added to the ledger, blockchain makes use of various consensus algorithms to validate new blocks. All participating users agree to abide by a pre-defined consensus algorithm to decide on the concurrent state of the ledger and allow the blockchain to facilitate "trustless" transactions within the network. Every new block needs to be verified by the consensus algorithm before being introduced into the blockchain. The time it takes to verify and append a new block is known as the Block time of the network. It is about 10 minutes for the Bitcoin blockchain and about 20 seconds for the Ethereum blockchain [3]. Proof of Work (PoW) is a widely used and robust consensus algorithm that is used in the Bitcoin blockchain. It uses cryptographic hash functions, like SHA 256 to enforce security and integrity. A cryptographic hash function uniquely maps input data to a corresponding hash value. Also, it is a non-reversible function, so it is practically not possible to compute the input data from a given hash value. PoW protocol requires the users to put in some computational work to obtain a hash value for a block that satisfies some predefined condition. This condition is usually a number known as a nonce, which sets the "difficulty" for computing the hash. For example, the nonce can define the number of zeros with which the hash value must begin. Due to the "Avalanche Effect", even a small change in the input data completely alters the corresponding hash value. Hence, the users who want to add a block have no other option but to brute-force till they find a combination that satisfies the given hash condition. Once a combination is found, other users in the network can simply run this combination with the cryptographic hash function and confirm

whether it satisfies the condition or not. This process of adding blocks to the blockchain is known as mining and the users who put in the computational effort to add the blocks are known as miners (see Fig. **1**).

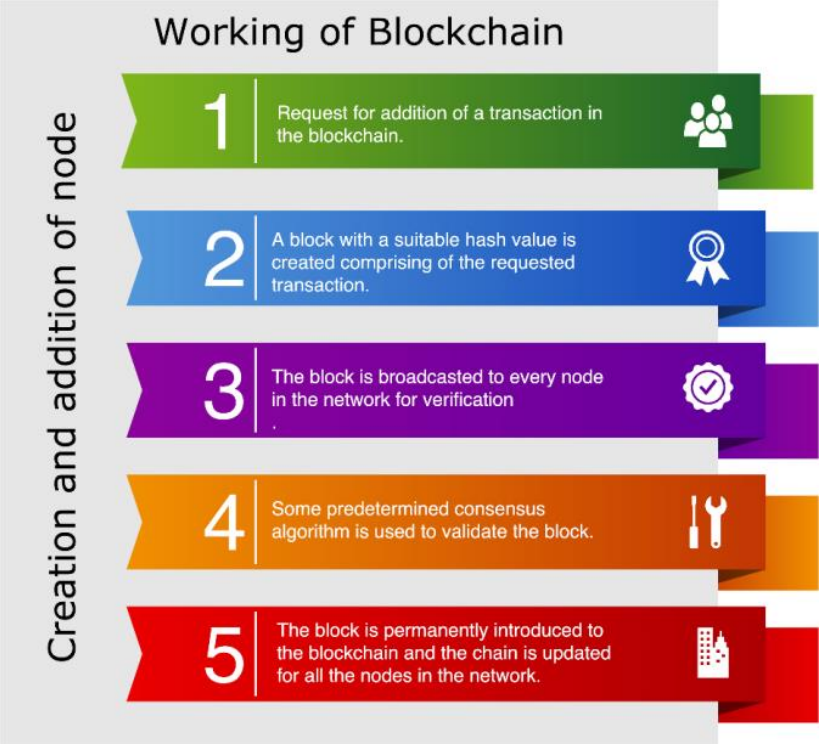

Fig. (1). Sequential working of Blockchain.

Some other consensus algorithms are Proof of Stake, Proof of Burn, and Practical Byzantine Fault Tolerance. While these algorithms differ in the way they are implemented, their functions remain the same; to validate new blocks and to make sure that only one version of the database exists in the entire network [4].

Applications of Blockchain

As of 2020, blockchain has been researched and implemented in numerous fields, proving the versatility of this technology. Following are some examples.

Voting

Blockchain has the potential to revolutionise voting. A blockchain-based voting

CHAPTER 4

Application of IoT in Patient Health Monitoring System

Rinky Dwivedi[1,*], **Harshit Mittal**[1], **Manik Agarwal**[1] and **Sahil Dwivedi**[1]

[1] *Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India*

Abstract: The Internet of Things (IoT) is the infrastructure that enables the process of collecting data using various devices which in turn communicate with each other and store this data over the cloud. This helps to retrieve, analyze, and communicate data to any part of the world faster with great efficiency. IoT has indeed opened the doors to endless new possibilities in different areas and industries. From smart home appliances to remotely observing and controlling different objects to self-driven cars and whatnot. The healthcare industry has still not leveraged the true power of this modern IoT revolution. Specifically, when it comes to monitoring the health of elderly people, the techniques used today are still not robust and lack conviction. This has been an area of concern for a long time, and it is an even bigger challenge to remotely monitor the health condition. In this paper, our goal is to depict the current situation of the technology of the health monitoring projects based on IoT and propose an improvement in the actual practices currently prevalent in remote monitoring of the health of elderly people. We will also try to forecast the trend of various health parameters demonstrated in the paper beforehand to make the concerned people aware with precision if any alarming situation is spotted so that instant action can be taken, thus ensuring a reduction of casualties.

Keywords: Ardiuno, Internet of Things (IoT), Remote monitoring, Forecasting, Moving Averages, Health Assistant.

INTRODUCTION

The phrase “Internet of Things” is thought to have been coined at the beginning of the century, when work on the MIT Auto-ID Center [1] was underway to develop a smart identification system that would help minimize error rates while boosting efficiency and automating the process. However, the notion of IoT has grown rapidly in many ways since then, such as with the help of a large number of small networks that can stay linked to each other and transfer data to the main network without the need for human interaction.

[*] **Correspondence author Rinky Dwivedi:** Department of Computer Science and Engineering, Maharaja Surajmal Institute of Technology, C-4 Janakpuri, New Delhi 100058, India; Tel: 9958433922; E-mail: rinkydwivedi@msit.in

Koyel Datta Gupta, Deepak Kumar Sharma, Rinky Dwivedi and Fadi Al-Turjman (Eds.)

Quality of service in healthcare has always been under constant criticism in the modern era, as it is a very touchy subject. Monitoring the health of elderly people specifically has been a concern for a long time. In this modern world, most people have a hectic work life with long hours of continuous work, due to which the elderly are left neglected and vulnerable. It is difficult to keep a constant check on the elderly people in the house. Also, keeping an attendant or a servant is very expensive nowadays. In this situation, remote health monitoring based on IoT can help solve the problem.

IoT provides the means by which it is possible to collect and analyze data remotely without any human interaction. So, this helps us to possibly foresee and minimize any future hazard with precision and further notify the concerning authority like the family member or the physician if there is an alarming situation. IoT is important for this project for two main reasons. Firstly, it is automated, so no human intervention is needed. And secondly, because of automation, the process is less prone to errors, *i.e*., having a more robust system indicating a better quality of service.

In this paper, we describe how we collected data regarding three health parameters, namely temperature, heartbeat, and lung capacity, and used the time series algorithm to forecast these parameters to cope with any alarming situation looming in the future and take necessary actions beforehand to prevent it.

The paper is structured in the following way; the introduction is included in section 1. In section 2, previous works related to IoT in healthcare being discussed. The proposed system is described in section 3, which includes the methodology, block diagram, and system architecture. section 4 describes the equipment details. Section 5 contains the performance measurements and section 6 includes the conclusion. Finally, section 7 contains the future scope.

RELATED WORK

Extensive research on the topic related to the system shows a very few of the related works could build their preliminary framework and prototype of the system. Some of the works like the research conducted on **Ambient Assisted Living (AAL)** [2] did more of a literature survey of the state of its present condition of the monitoring system *via* IoT. They also tried to identify and highlight the critical issues and the quality of service as well as the user-driven experiences in their work. Some others worked on showing or highlighting the importance of IoT in the health sector and some proposals for the health monitoring architectures.

Some related findings used specific models for the health monitoring aspect. Like the abstraction of the **Model-Driven Tree Reference Model (MDTRM)** [3], where they explained the necessity of this model in the health field as well as identifying the complexities of the models. They also benched marked the models which came in handy for the initial phase of this research.

One of the other related models we found is **General Domain Model Architecture (GDMA)** [3], the health monitoring and sensing with cloud processing was also a helpful source behind the research, as it was useful for generating ideas to get raw data from wearable devices which are compatible and capable of measuring many physical values which we can be used to obtain meaningful results.

Masimo Radical-7 [4], a health monitor for the clinical environment helps to collect data and wirelessly transmit it for ongoing display. This provides high-resolution display of information with higher graphical capabilities. It also has a touch-based user interface. But as it can already be assumed how cost-effective it is, it can't send an alarm message to notify of any emergencies. **Free Scale Home Health Hub reference platform** [4] stores patient data in the cloud *via* various sensors, which the people related to the patient can have access to. This platform too can't notify about any alarming situations to the people engaged with the patient.

Some surveys of ours also lead us to projects which even discussed monitoring the health whole area through wireless network sensors [5, 6]. They also tried to share their ideas by giving a model of their frameworks like cloud-based processing [7] and big data [8 - 14]. However, these systems face several attacks, and research works are being carried out to detect such activities [15].

SYSTEM ARCHITECTURE

A. System Structure

In this paper, we used three health parameters that we will monitor using three different sensors namely body temperature, heartbeat, and lung capacity as shown in Fig. (**1**). Once we have collected all the sensors, the first step is to integrate these sensors into the microcontroller. A microcontroller is a cheap, small-sized computer, that can be portable and multitasking. We have used Arduino Uno as our microcontroller in the paper. Also, to keep a check on the values that are being collected by the sensors in real-time we have attached an LCD to our microcontroller for this purpose.

CHAPTER 5

IoT Based Verified and Public Vehicle Registration through BlockChain: Future Smart Cities based Applications with Sustainable Approach

Rohit Rastogi[1,*], Bhuvneshwar Sharma[1], Pardeep Kumar[2] and **Muskan Gupta[1]**

[1] *Department of CSE, ABES Engineering College, Ghaziabad, U.P. 201009, India*

[2] *Department of Computer Systems and Engineering, QUEST University, Nawabshah, Pakistan*

Abstract: Blockchain technology replaces centralized applications with distributed computing. Modern economy is estimated by the place of motor transport in the infrastructure of the national economy. An automobile registration system is a unified information system. This information system takes care of every information about automobile registration. It is administrated by a national registry entity and has access to other government and non-government services that handle automobile information. Cyber Physical System (CPS) is defined as the combination of computation and physical process. It is mainly used in the ICT section. It is also focused on resolving the problems related to authors of the data regarding transparency, media, and storage problems by technical handling.

The presented chapter uses all the above concepts in one place and integrates them to build a useful application. The presented frame allows car manufacturers, owners, repairing companies, and insurance agencies to register and add new car entries through a simple method. In addition, database technology has been leveraged to cache intermediate data. It efficiently uses the Industrial IoT and 5G technologies.

Many researchers have called for rules and applications to draw old maps based on distributed applications into the blockchain. New protocols are available in this work for the International Automated Vehicle Management System, called DriveLoop, which were proposed and developed.

Keywords: Driveloop, Blockchain, Peer to Peer (P2P), Hashing Algorithms, Car Registration, Overlay Network.

[*] **Correspondence author Rohit Rastogi:** Department of CSE, ABES Engineering College, Ghaziabad, U.P., 201009, India; Tel: 9818992772; E-mail: rohit.rastogi@abes.ac.in

Koyel Datta Gupta, Deepak Kumar Sharma, Rinky Dwivedi and Fadi Al-Turjman (Eds.)

INTRODUCTION

Anyone who has purchased or sold a car, or who has worked in the automobile manufacturing or distribution industry at any point, is familiar with the complication that is the Vehicle Registration process. Given the fact that all vehicles in the market have been sold and resold as they passed through multiple hands, it becomes a cumbersome task to maintain a legitimate record of the history of each vehicle and make it available when needed.

But before one goes on to talk about the problems of the process of Vehicle Registration, one first needs to understand why Vehicle Registration is such an important aspect of automobile dealing. Car ownership changes as many times as you can imagine.

Whether you look at it in terms of dealing in spare parts or in assembled vehicles, dealings by the middlemen or by the retailer who makes the final sale to a consumer, or in terms of the resale of a second-hand vehicle, some stakeholders are interested in learning everything there is to know about the car they are purchasing. Not to mention the insurance agencies, the police, and other authorities, and the government too needs to keep tabs on the automobiles for various reasons.

The fact of the matter is that all these stakeholders need information about the vehicles, starting from its manufacturing story, covering its first sale, the accidents, if any, that it has been in, and any and all repairs and maintenance. This is crucial not just to maintain a track record of the vehicle in question to determine its market value but also for legal and insurance purposes.

Vehicle Registration is a way to facilitate this record keeping by maintaining a link between the vehicle and its owner. It might be or not be compulsory, depending on the law of the land. This helps the authorities with regard to taxation, insurance, or crime detection purposes. Also, it is a way for automobile dealer to keep track of their vehicles [1 - 3].

Concept of Smart Cities

The urban development has resulted in a change of archetype in the 21st century. Research activities for smarter cities became a priority task. The life was improved in the last century in terms of technologies and services. Smart City is the demanding solution to sustainability and urbanization. Smart Cities may lead to a dystopian world that is regulated by technocratic governments, which propel citizens to subaltern roles. However, the massive industrialization and the

increasing population in the big cities has been a big challenging for urban planner, architects, and administrators.

The service platforms of smart cities are the Internet of Things (IoT), big data systems, and mobility. Connected automobile with their advanced technology reduces the chances of accident and help drivers save time and gasoline within their limits. An increase in population in urban areas often leads to the problem of parking spaces. Smart parking is one of the most important parts of smart city. Sensors are placed in smart cities with good internet connectivity. More urban our planet becomes, the smarter the cities have to be. The cities of tomorrow will be more prone to transformation embellishment than the cities of yesterday [4].

Problem of Car Registration and Motivation

The process of registering a car has always been difficult. This is a lengthy process involving several parties, and there is also the risk of manipulating information, replicating data and various errors. In this case, critical information can be very vulnerable to fraud or data falsification, or even available for tracking.

By bringing the power of Distributed Ledger Technology called Blockchain into the picture and moving the entire process of registering a car on to Blockchain, a lot of these vulnerabilities can easily be resolved [5].

Research Objectives

Blockchain comes to the rescue by reducing the average response time. The Blockchain will allow parties to send data in the form of an intellectual contract or chain code, which will eventually become the single source of unchanged data for all parties. In addition, the Blockchain in the vehicle registration ecosystem will help reduce the risk of fraud and aggression, since only authorized personnel can use the data when updating the private key in the province.

In fact, any attempt to track fake data can be easily done on the Blockchain. The best part is that Blockchain provides one single idea of the lifecycle of the car in one book, which is not currently available [6].

Scope of the Research Work

This research experiment is a generalized project implemented using open source technologies developed by Linux Foundation called hyper ledger Fabric in a permission model. Anyone can use this project by taking the authorization and adding their stakeholders into the system.

CHAPTER 6

Identification of Counterfeit Drugs Using Decentralized Supply Chain

Koyel Datta Gupta[1,*], Aditya Gupta[1], Tanmay Sharma[1] and **Aayush Bhatnagar[1]**

[1] *Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi 110058, India*

Abstract: This research attempts to overcome the problems faced by the medical healthcare system by using the advancing technology of blockchains. Pharma companies that manufacture and sell medicines face difficulties in tracking drugs, which in turn allows the counterfeiters to exploit the system. The decentralized abilities of blockchain technology enable us to counter the problems in existing centralized systems. The blockchain helps us to make sure that the quality is maintained throughout the decentralized supply chain. The use of blockchains in the medicine supply chain solution entails tracking the validity of the medicine from the producer to the distributor to the pharmacy. It assures that the pharmacist receives the original medication and does not reach the grey market. In this paper, the decentralized application which we created works using Ethereum and is based on blockchain technology. The medicine discovered by a pharmaceutical company is to be validated by an officer in a decentralized manner using smart contracts over Ethereum transactions. The validated drugs can then be produced and sold on the platform, where the entire data and the stages of the drug/medicine are tracked and stored. Research and development of such a system are necessary to facilitate the proper supply and tracking of medicines and to avoid counterfeiting.

Keywords: Blockchain, Ethereum, Amart contracts, Decentralized application (DApp).

INTRODUCTION

According to recent findings, drug counterfeiting is one of the significant problems in second and third-world countries. Individuals and the general public are in danger due to the effects of this occurrence. They are especially common in countries where surveillance and regulation ought to be enhanced or are inadequate, as well as in nations where drugs are in great demand but remain

[*] **Correspondence author Koyel Datta Gupta:** Department of Computer Science & Engineering, Maharaja Surajmal Institute of Technology, New Delhi, 110058, India; Tel: 9999061790; E-mail: koyel.dg@msit.in

Koyel Datta Gupta, Deepak Kumar Sharma, Rinky Dwivedi and Fadi Al-Turjman (Eds.)

mostly expensive. They are also prevalent during disease outbreaks and epidemics when vital pharmaceuticals are in limited supply and counterfeiting is widespread. Unauthorized pharmaceutical companies employ their cunning minds and expertise to develop identical replicas of the real pharmaceuticals that are undetectable. Fake drugs are harmful to the consumers as they might contain false ingredients and the patients are unable to identify them. Overdosage of the ingredients is also a common issue. Toxins and pollutants have the potential to cause allergic responses as well as adverse medicinal responses. Counterfeit pharmaceuticals squander people's money and raise the government's financial burden. Additionally, it may undermine public trust in the effectiveness of genuine treatments.

The Indian government presently lacks an efficient strategy for dealing with the problem of fraudulent medications made in India. Despite some progress, there has been no major innovation in combating the country's fraudulent medicines economy. A thorough study of the world's pharmacy business indicated that many of the substandard pharmaceuticals originate in India. India is among the leading exporters of drugs worldwide. Thus, there is a scope for intermixing fraudulent medicines and original medicines. This makes it arduous for government authorities to detect fraudulent drugs. This makes India one of the biggest fraud medicine markets worldwide. It is found that this problem is the result of complexity in the medication supply chain and a lack of process integrity.

Another obstacle faced by the customer is the monitoring of medications that can only be obtained through a prescription. While the selling of medicines without a prescription is against the law, keeping track of wholesaler honesty, in addition to the challenge of counterfeit drugs, is difficult and requires a unique strategy. Blockchain medication inventory might give major benefits with barcode-tagged medications scanned and placed into secure digital blocks anytime they change hands. Every exchange of hands is deemed a transaction, and it is recorded on blockchain technology, which is unchangeable, decentralized, and global.

Blockchain

Satoshi Nakamoto first created blockchain in the form of the popular cryptocurrency ‘Bitcoin’ [1]. In a peer-to-peer (P2P) network, each user is referred to as a node, and the transactions that take place are categorized as blocks. The blocks are then interconnected in an order. One pair of public-private keys is associated with each node. The public key is used to recognize the node as a sender or a recipient, while the associated private key is used by a sender to sign transactions and by a recipient to validate them. In addition to enabling the appropriate key to decrypt and collect the information, a deal among the

participating nodes must be attained before adjustments can be implemented. This guarantees that all blockchain ledger replicas are synchronized across the network. Users can always get the most up-to-date or, in other words, the most recent copy of a transaction when a transaction occurs, thanks to the blockchain's build architecture (Fig. **1**). Whenever a transaction occurs in the chain, the entire network is updated. This is possible as all other network participants are provided with a copy of the transaction. Blockchain has been used in several applications [2 - 4].

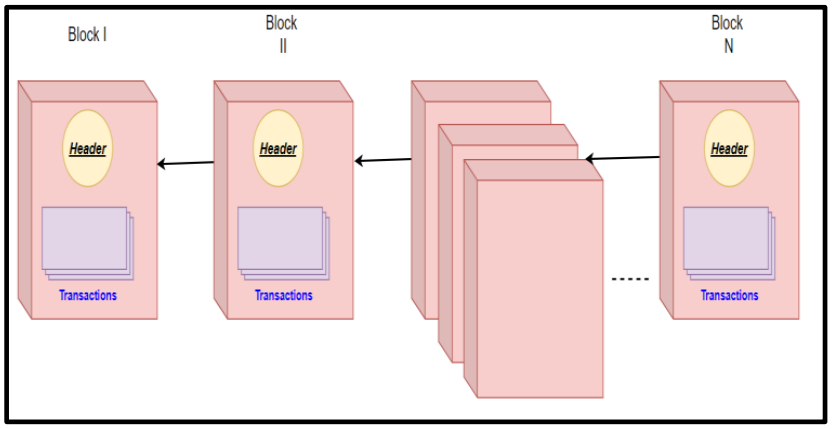

Fig. (1). Blockchain Architecture.

Public, private, and consortium are the three types of Blockchain. Each participant on the public blockchain can see and authenticate any transaction occurring on the network, as well as partake in the consensus mechanism. In the consortium blockchain, there must be an administrative node, which is initially chosen by network members based on the effective ways to accomplish their business objectives, such as in the case of a company. Except for one difference, a private blockchain is similar to the previous type where the public has no access to any of the data in such a distributed registry.

Smart Contract

A decentralized ledger can also be utilized to build a self-executing contract, also known as a smart contract. They are a type of digital service agreement stored in the blockchain as codes and execute only when a specific criterion is reached. Smart contracts can thus be implemented into a blockchain database and allow users to create computer codes based on contractual agreements. A contract hash and a contract address are present in a smart contract, which played a significant

CHAPTER 7

Making Great Strides Towards Road Detection

Vimal Gaur[1,*]

[1] *Maharaja Surajmal Institute of Technology, Computer Science and Engineering Department, Janakpuri, New Delhi 110058, India*

Abstract: A significant amount of research has been carried out in extracting land surface objects, but intelligent digital surface models for monitoring land surface objects are still an active research topic due to emerging technologies such as IoT and Blockchain. These technologies play an important role in quantifying the ecological and geographical properties of the land surface. About such technology of detecting buildings, roads, and terrain from satellite images offer a lot of potential for tracking the migration of large chunks of the population and helps in geographical analysis of the city. In this paper, we explore a Convolutional Neural Network method for extracting land surface objects from satellite imaging with the help of U-Net. As a known fact, the number of disasters occurring every year affects thousands of the population, so suitable mechanisms must be provided for rescue operations. To provide these rescue operations, predictions about the geographical location are of primary importance. Our model produces reasonable accuracy of 60.62% at a very minimal loss rate.

Keywords: U-Net, Spatial Processing, Image Segmentation, Deep Learning, Computer Vision, Down and Up Sampling, Skip Connection.

INTRODUCTION

The extensive process of mapping out the populated regions of a metropolitan city or even a remote town can be laborious and painstaking when done according to outdated methods. Population hotspots in metropolitan areas are rapidly changing the cause of bodily movement but also because of environmental alterations both induced naturally, like fluctuation in living conditions such as a change in weather, or human-induced like contamination of groundwater through drilling for oil. This indicates that mapping is difficult, especially in remote divisions where the attention of the authorities is minimum. Our paper focuses on addressing the wider aspect of image segmentation of satellite images by directing our classification at pixel level and checking whether pixels belong to road/path-

[*] **Correspondence author Vimal Gaur:** Maharaja Surajmal Institute of Technology, Computer Science and Engineering Department, Janakpuri, New Delhi, Delhi 110058, India; Tel: 9999620069; E-mail: vimalgaur@msit.in

Koyel Datta Gupta, Deepak Kumar Sharma, Rinky Dwivedi and Fadi Al-Turjman (Eds.)

way or not. We have developed a model for dealing with affected areas that are under stress and finding the most efficient routes to provide aid in those areas as early as possible. As seen in the year 2020 and its harrowing outbreak all around us, the outbreak of COVID-19 tested the readiness of governments of many nations. The impact of the virus could have been made minimal in many countries just by simple mapping out hotspots and by also calculating the appropriate way of distributing the test kits. All this could have been a straightforward task by using a deep learning algorithm altogether like ours. The impact on third-world countries like India, where masses have to depend on a government instantly in a situation of a pandemic like this, needed to be calculated beforehand amidst the lockdown [1 - 3]. We have tried to extend this concept to the physical world rather than in the medical field. This paper addresses the issue of segmentation of images obtained by satellite imaging. It dissects the image pixel by pixel and classifies each pixel as part of the road. We have trained our model on a set of high-resolution images obtained from [4]. As we learned from another study [5] downsampling could help us in simplifying the problem we face with high-resolution and small-size lesion regions. Our images were correspondingly labeled with binary masks, *i.e.* given a satellite image as input, our program was then able to output a corresponding predicted binary mask, which was then further processed into more labeled and accurate data to aid us in our mission of mapping route enhancement using image segmentation [6].

RELATED WORK

A few authors [5] extracted maximum accuracy when U-Nets are used in global and local modes.

Extracting objects namely buildings, lakes, ships etcetera from satellite images is not a recent field of examination. SVM algorithm has been used to extract buildings from high-resolution images [6]. A different approach called a full convolution network, which is very prevalent in today's image segmentation projects has been applied.

By extrapolation of and building more on FCN network, we get a specific type of neural network which is called U-Net, which has proven its worth in bio-medical research and works even on a small number of datasets. Moreover, similar work has been done on loss function and accuracy metrics [7]. In this paper, the author discusses pixel accuracy and the importance of right accuracy metrics and loss metrics [8, 9].

Some other works in the field of medical science include the implementation of a convolutional neural network in the segmentation of blood vessels in retina

fundus images. The neural network classifies each pixel in the fundus images as either a vessel or not using binary classification tasks.

DATASET

Data Selection

The dataset required for our model consists of 1113 satellite images and their masks [4]. Images in this dataset are very high resolution and their masks are black and white. The white pixel in the mask represents the road and the remaining area is represented by the black pixel. These are clearly shown in Fig. (**1**).

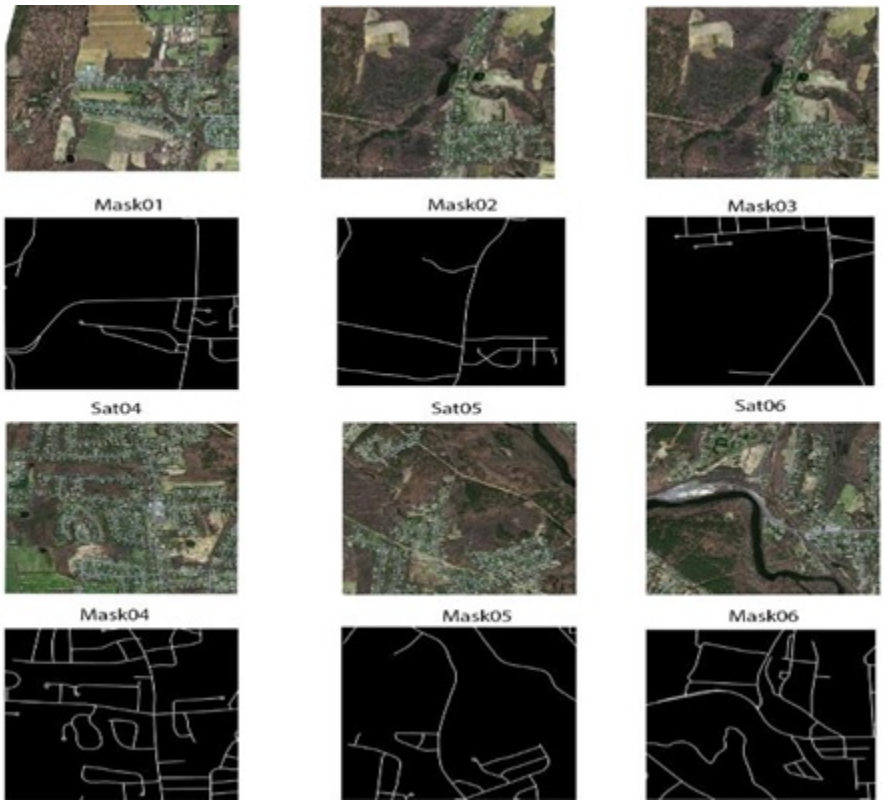

Fig. (1). Images before Pre-Processing.

Preprocessing

After completely analyzing the dataset, it has been noticed that all the images are not complete. To avoid vague data, all these images are removed and the dataset

SUBJECT INDEX

A

B

Koyel Datta Gupta, Deepak Kumar Sharma, Rinky Dwivedi and Fadi Al-Turjman (Eds.)

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

V

Koyel Datta Gupta

Dr. Koyel Datta Gupta is a professional with an experience of 17+ years in academics. She completed her B. Tech in Computer Science and Engineering from the University of Kalyani, West Bengal in 2003 and is a gold medalist in M.Tech (Computer Technology) from Jadavpur University, Kolkata (2007). She received her doctorate in 2015 from Jamia Milia Islamia, New Delhi. Her areas of research include network security, digital signal processing, pattern recognition and machine learning. Dr. Koyel Datta Gupta is currently working as an associate professor at the Maharaja Surajmal Institute of Technology (MSIT) (under the IP University), New Delhi. She is currently the head of the department of the Department of Computer Science and Engineering. She has held various other positions in MSIT for the past 12+ years. She has published more than 25 research papers in reputed journals and conference proceedings and has also authored books.

Rinky Dwivedi

Dr. Rinky Dwivedi completed her B.Tech in Computer Science and Engineering from Guru Gobind Singh Indraprastha University, Delhi in 2004 and M.E. in Computer Technology and Application from Delhi College of Engineering, Delhi in 2008. She has received her doctorate in 2016 from the Delhi Technological University, New Delhi. Dr. Rinky has over 17 years of experience in Academics, currently working as an associate professor at the Maharaja Surajmal Institute of Technology, Delhi. She has published more than 20 research papers in reputed journals and conference proceedings and has also authored books.

Deepak Kumar Sharma

Deepak Kumar Sharma is working as an associate professor at the Department of Information Technology, Indira Gandhi Delhi Technical University for Women (IGDTUW), Kashmere Gate, Delhi, India. Earlier, he worked as an assistant professor at the Netaji Subhas University of Technology (Formerly N.S.I.T.), Dwarka, Delhi. He obtained his Ph.D. in Computer Engineering from the University of Delhi, India in 2016. His research interests include opportunistic networks, wireless ad hoc and sensor networks, software defined networks and IoT networks. He has over 17 years of experience in academics. He has published various research papers in reputed international journals like ETT Wiley, IEEE Systems Journal, IEEE IoT Journal, Computer Communication Elsevier, IJCS Wiley, etc. and conferences of repute like IEEE AINA, GLOBECOM, etc. He has also authored various book chapters in edited books of IET, Wiley, Springer, Elsevier, etc. He has served as session chair in many conferences and is also a reviewer of various reputed journals like ETT Wiley, AIHC Springer, IJCS Wiley, etc.

Fadi Al-Turjman

Prof. Dr. Fadi Al-Turjman received his Ph.D. in computer science from Queen's University, Canada, in 2011. He is the associate dean for research and the founding director of the International Research Center for AI and IoT at Near East University, Nicosia. Prof. Al-Turjman is the head of the Department of Artificial Intelligence Engineering and a leading authority in the areas of smart/intelligent IoT systems, wireless, and mobile networks' architectures, protocols, deployments, and performance evaluation in Artificial Intelligence of Things (AIoT). His publication history spans over 400 SCI/E publications, in addition to numerous keynotes and plenary talks at flagship venues. He has authored and edited more than 40 books about cognition, security, and wireless sensor networks' deployments in smart IoT environments, which have been published by well-reputed publishers such as Taylor and Francis, Elsevier, IET, and Springer.