BLOCKCHAIN AND IoT BASED SMART HEALTHCARE SYSTEMS

Editors:
L. Ashok Kumar
D. Karthika Renuka
Sonali Agarwal
Sheng-Lung Peng

Bentham Books

Blockchain and IoT based Smart Healthcare Systems

Edited by

L. Ashok Kumar
Department of EEE
PSG College of Technology
Coimbatore, Tamilnadu
India

D. Karthika Renuka
Department of IT
PSG College of Technology
Coimbatore, Tamilnadu
India

Sonali Agarwal
Department of IT
Indian Institute of Information Technology
Allahabad
India

&

Sheng-Lung Peng
College of Innovative Design and Management
National Taipei University of Business
Creative Technologies and Product Design
Taiwan

Blockchain and IoT based Smart Healthcare Systems

Editors: L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng

ISBN (Online): 978-981-5196-29-0

ISBN (Print): 978-981-5196-30-6

ISBN (Paperback): 978-981-5196-31-3

First published in 2024.

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

FOREWORD

The Electronic Health Record (EHR) of a patient is a digitized document of their health history, progression comments, symptoms, and medications. Concerns about security abound, as they do with any online digital media. In the healthcare industry, the reliance on digital devices such as IoT, generates a massive volume of patient medical data. These EHR data statistics are confidential and cannot be made public. Medical data tampering can place a person's life in danger. Because of this, EHR information is subject to severe security and privacy risks. The high prevalence of health digital platforms presents a need for a more secure EHR system enabled by blockchain. Blockchain-based technologies have been proven and approved for delivering reliable and secure decentralised solutions to address the security and privacy threats associated with EHR data. Moreover, decentralized blockchain technology is unalterable. Preserving secrecy may allow for a more effective conversation between the physician and the patient, which is crucial for providing high-quality care. It also provides doctors, patients, and insurance providers an efficient way to obtain medical information while maintaining the privacy of the patient's data. The blockchain-based architecture provides the following features: privacy, authenticity, integrity, interoperability, and accountability of electronic health records between two entities. This book covers some state-of-the-art research associated with artificial intelligence, big data, and blockchain for smart health care development. It explains the fusion between the privacy and security of a blockchain-based data analytic environment. The book provides the fundamental framework, research insights, and empirical evidence for the efficacy of these new technologies, employing practical and basic approaches to help professionals and academics reach innovative solutions and grow competitive strengths.

V. Chandrasekar
University Distinguished Professor and Associate Dean for International Programs
Fellow IEEE, AGU, AMS, URSI and US national Academy of Inventors
Colorado, State University
Colorado, United States

PREFACE

Technology is constantly changing the healthcare industry, which is a crucial aspect of daily living. The use of technologies like Internet of Things (IoT), artificial intelligence, and blockchain systems can improve the state-of-the-art in health care and general medical practise. As the Internet of Things (IoT) has grown, its applications in the field of smart health care are adapted to various real-world scenarios. An Internet of Things (IoT)-based health care is a collection of intelligent medical tools and software that communicate online with a health care information system. It has created a world of opportunities in the medical industry. Smart connected medical gadgets can gather vital health information and offer additional information about the symptoms. Smart health care IoT devices range from basic wristbands that can track blood pressure, heart rate, and sleep patterns to linked inhalers, ingestible sensors, glucose monitors, and remote patient monitoring systems. These devices must have dependable connectivity and adhere to security and privacy laws in order to meet the demands of smart health care. A patient's medical information is kept digitally in a digital health record (EHR). The electronic health record (EHR) is a piece of technology that could provide the groundwork for new patient services and functionality. They increase patient access, raise the standard of service, and cut expenses. The blockchain security architecture assures that electronic health records between two organisations are confidential, authentic, legitimate, interoperable, and accountable. A blockchain-based approach to address the issues of data management, exchange, and storage, real-time patient monitoring at remote locations, monitoring of smart IoT devices, and faster and more seamless data transfer of patient medical records are just a few benefits that will come with the adoption of blockchain-based smart healthcare. Blockchain technology is a pervasive technology utilised in many industries, including banking, finance, supply chain management, and healthcare. The IoT and blockchain appear to be the ideal combination, as there is a great demand for data security given the volume of data generated by IoT sensors. A blockchain-enabled IoT-based smart health care is also an advancement because it can lessen the burden on healthcare systems and avoidable hospital visits by connecting patients with their health care providers and enabling the safe transfer and storage of medical data through the use of the blockchain mechanism. The book employs academic and practical approaches to assist professionals and academics in coming up with novel solutions and strengthening their competitive advantages. It provides the fundamental framework, research insights, and empirical evidence regarding the efficacy of these new technologies.

L. Ashok Kumar
Department of EEE
PSG College of Technology
Coimbatore, Tamilnadu
India

D. Karthika Renuka
Department of IT
PSG College of Technology
Coimbatore, Tamilnadu
India

Sonali Agarwal
Department of IT
Indian Institute of Information Technology
Allahabad
India

&

Sheng-Lung Peng
College of Innovative Design and Management
National Taipei University of Business
Creative Technologies and Product Design
Taiwan

List of Contributors

A. Valarmathi	Department of Computer Applications Bit Campus, Anna University, Thiruchirappalli-24, India
Anand Kumar S.	Vellore Institute of Technology, Vellore, India
Akila Victor	School of Computer Science & Engineering, VIT, Vellore, India
Chaithra V.	BMS Institute of Technology and Management, Bengaluru, India
Divya Palanisamy	N.G.P. Institute of Technology (affiliated to Anna University), NGP Nagar, Kalapatti -6410648, India
D. Karthika Renuka	Department of IT, PSG College of Technology, Coimbatore, Tamilnadu, India
G. Srinivasagan	Department of Chemistry, Rajapalayam Rajus College, Rajapalayam, Tamilnadu, India
Geeta Amol Patil	BMS Institute of Technology and Management, Bengaluru, India
Geetha Narasimhan	School of Computer Science & Engineering, VIT, Vellore, India
Jaskiranjit Kaur	Panjab University, Chandigarh, India
Jayashree K.	Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai, India
Kumaresan Natesan	Anna University Regional Campus, Coimbatore, India
K. Karthigadevi	Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India
L. Ashok Kumar	Department of EEE, PSG College of Technology Coimbatore, Tamilnadu, India
M. Narayana	Electronics and Communication Engineering Department, Anurag University, Hyderabad, India
M. Shanmuganantham	Tamilnadu Government Polytechnic College, Tamilnadu, India
Manoranjan Dash	Department of Artificial Intelligence, Anurag University, Hyderabad, India
Pranshu Tripathi	School of Computer Science & Engineering, VIT, Vellore, India
Parvesh Kumar	Chandigarh University, Chandigarh, Punjab, India
Pinaki Pratim Acharjya	Department of CSE, Haldia, Institute of Technology, Haldia -721607, India
Praveena Venkatesan	NGP Institute of Technology, Coimbatore, Tamil Nadu 641048, India
Partheeban Pon	Computer Science and Engineering, Stella Mary's College of Engineering, Aauthenganvilai, Kanyakumari, India
Priya Vijay	Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, India
R. Anusuya	Department of IT, PSG College of Technology Coimbatore, Tamilnadu, India
R. Manimegalai	Department of Computer Science and Engineering, PSG Institute of Technology and Applied Research, Neelambur, Tamil Nadu 641062, India

Ramya Easwaran	SNS College of Technology, Coimbatore, India
R. Nagarajan	Gnanamani College of Technology, Tamilnadu, India
Raghu Indrakanti	Electronics and Communication Engineering Department, Anurag University, Hyderabad, India
R. Babu	Department of Computational Intelligence, School of Computing, College of Engineering and Technology, SRMIST, Chennai, India
Surekha K.B.	BMS Institute of Technology and Management, Bengaluru, India
Saranya Rajendran	Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu 641022, India
Suresh Kumar Nagarajan	Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India
Santanu Koley	Department of CSE, Haldia, Institute of Technology, Haldia -721607, India
S. Jayanthi	Department of Computer Science and Engineering, Bit Campus, Anna University, Thiruchirappalli-24, India
Sanjay Vasudevan	School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India
Sarvana Kumar Selvaraj	Department of Computer Science and Engineering, Jain University, Bangalore, India
S. Kannadhasan	Study World College of Engineering Coimbatore, Tamilnadu, India
V. Kavitha	Computer Science and Engineering, University College of Engineering, Kancheepuram, India
Vidhya E.	Padmavani Arts and Science College for Women, Salem, Tamil Nadu 636011, India
V. Vishu	Department of Computer Applications, Coimbatore Institute of Technology, Coimbatore, Tamil Nadu 641014, India
Vijay K.	Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, India
Yash Vaish	School of Computer Science & Engineering, VIT, Vellore, India

CHAPTER 1

The Role of Emerging Technologies in Smart Health Care

Jaskiranjit Kaur[1,*] and **Parvesh Kumar**[2]

[1] *Panjab University, Chandigarh, India*

[2] *Chandigarh University, Chandigarh, Punjab, India*

Abstract: Numerous technological advancements like 3-D Printing, Virtual Reality (VR), Augmented Reality (AR), Artificial Intelligence (AI), Internet of Things (IoT), Drones, Robots, and Blockchain are now being inscribed for their ability to change the health care industry and make it a more automated and effective field. Various tools related to AI, like Google, DeepMind, Atomwise, Chatbot, Enlitic, Freenome, and Buoy Health, are helpful in makingthe health industry more efficient. There is another technology which is nanomicelle that can be used for effective drug delivery to treat various cancers, including breast, colon, and lung cancer. Moreover, self-assembling peptide nanoparticles that were prepared from SARSCov-1 spike (S) protein, successfully induced neutralizing antibodies against the coronavirus, subsequently preventing infection of Vero cells. Furthermore, the application of 3D printing in medicine can provide many benefits, including the customization and personalization of medical products, drugs, and equipment; cost-effectiveness; increased productivity; democratization of design and manufacturing; and enhanced collaboration. IoT enables real-time alerting, tracking, and monitoring, which permits hands-on treatment, better accuracy, apt intervention by doctors, and improves patient care delivery results. The other most promising application isblockchain in the healthcare sector for identity management, dynamic patient consent, and management of supply chains for medical supplies and pharmaceuticals. In addition, there are several case studies that describe the benefits of emerging tools, like recently the use of Emerging Technologies for the study, diagnosis, and treatment of patients with COVID-19 by using Deep Convolutional neural networks (CNN), which is a widely used deep learning architecture, enabled distinguishing between COVID-19 and other causes of pneumonia through chest X-ray image analysis.

Keywords: AI, Blockchain, Drone, IoT, Nanotechnology, Virtual reality.

[*] **Corresponding author Jaskiranjit Kaur:** Panjab University, Chandigarh, India; E-mail: er.jaskiran@gmail.com

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

INTRODUCTION

There are many technologies that are worthwhile in the healthcare sector, such as artificial intelligence (AI), bioprinting, nanotechnology, virtual reality, blockchain, and robotics. With the use of these technologies, anyone, anywhere at any time, might perform medicine in aneasy way, which makes the health industry more automated. In addition, with the use of emerging technologies, many other advantages are possible such as enabling remote monitoring of patients and their access to healthcare, health statistics collection, fast patient identification, access to medical records, and information exchange with providers and other patients.

Artificial Intelligence (AI)

Most of the AI and healthcare technologies have strong relevance to the healthcare field. Artificial intelligence in healthcare combines computer science and robust datasets to enable problem-solving related to health, such as patient care, diagnosing patients, end-to-end drug discovery and development, improving communication between physicians and patients, transcribing medical credentials, such as prescriptions, and remotely treating patients, administrative processes and helping them improve upon existing solutions and overcome challenges faster [1]. It also encompasses sub-fields of machine learning and deep learning, speech recognition, computer vision, and natural language processing which are frequently mentioned in conjunction with artificial intelligence to create expert systems that make predictions or classifications based on input data [2]. These learning algorithms evolve and become more accurate, they are likely to significantly impact healthcare services to identify diseases through diagnostic approaches, treatments, and care processes, and help develop more efficient and precise interventions. There are various tools that are based on AI to be helpful in the diagnosis of patients such as medical imaging technologies like computed tomography (CT), ultrasonography, x-rays, mammography, computed tomography (CT scans), nuclear medicine, and Magnetic resonance imaging (MRI) scan of human body parts.

INITIATIVES ON AI

A number of AI start-up companies like Google, Microsoft, and IBM have also been steadily increased investing in the development of health care with AI. There are several UK-based companies collaborating with UK universities and hospitals for better implementation of AI techniques. There are many Assisted Self-Diagnosis Apps that are based on AI methods, such as Ada, Babylon, Buoy Health, Your.MD, Mediktor, HealthTap, Apotheka Patient, Sensely, Health Buddy, *etc*.

Such paradigms are Harvard University's teaching hospitals advancing health care systems with artificial intelligence techniques to diagnose potential blood diseases at a very early stage.

Self-Diagnosis AI Apps

BioXcel Therapeutics, a biopharmaceutical company, combines proprietary machine learning algorithms, big data, and AI techniques to find and develop novel therapeutics in the areas of immuno-oncology and the brain. Moreover, BioXcel's firm works with two drug re-innovation programs which are BXCL501 and BXCL701.

Buoy Health employs AI-based system algorithms to accurately identify, treat, and analyse signs of sickness. Chabot asks a patient about their symptoms and health concerns, then, after making a diagnosis, directs the patient to the appropriate care [3].

BERG is a biotech company in the trial stages that uses artificial intelligence and its own platform, Interrogative Biology, to change treatments for oncology, neurology, and uncommon diseases and map diseases. Critical biomarkers can be found in BERG, which speeds up the identification and development of therapies directed at the most promising therapeutic targets and pathways. The elimination of hit-to-lead optimization and screening in Berg's method, which generates virtual models of healthy and diseased cells, results in clear time-saving. Berg avoids these procedures by selecting compounds that occur naturally and using them as the foundation for medication in its virtual model [4].

XtalPi's ID4 platform combines AI technology, cloud, and quantum physics that provide small molecule candidate chemicals and pharmaceutical compounds for drug design and development in days instead of weeks or months for quick prediction and development by maintaining a petabyte-scale database consisting of pharmaceutically active molecules [5].

Deep Genomics' AI platform handles the complexity of RNA biology, identifies new targets, evaluates thousands of opportunities, increases the number of successful clinical trials, and accelerates time to market. It also identifies the best treatment candidates to increase and reduce costs. Moreover, over 69 billion dissimilar cell connections were analyzed by Deep Genomics' Project Saturn. Headquartered in New York, Kaia Health offers AI-powered digital therapy via a mobile app for exercise routines related to chronic pain, soporific events, and learning assets for the treatment of chronic low back pain, chronic bronchitis, and emphysema (COPD). We operate a digital treatment platform that we provide [6].

CHAPTER 2

An Overview of Blockchain in the Field of Smart Healthcare System

Ramya Easwaran[1,*] and **Kumaresan Natesan**[2]

[1] *SNS College of Technology, Coimbatore, India*

[2] *Anna University Regional Campus, Coimbatore, India*

Abstract: Rapid Blockchain is one of the most talked about technologies in the world at the moment. The origin of blockchain is a cryptocurrency called "bitcoin". It is a secure currency that can be used as a medium of exchange worldwide. Blockchain itself is a decentralised, peer-to-peer distributed ledger capable of storing all transactions that take place on the network. This property makes blockchain useful for any type of exchange, such as data, currency and information. Blockchain protects against potential data theft or corruption in the healthcare network. It is important to maintain the integrity and validity of patient records to ensure wellness. Artificial intelligence and blockchain will provide a smart healthcare system for people around the world by extracting useful information, protecting medical data, simplifying claims processing, using patient self-generated data and systematising procedures.

Keywords: Bitcoin, Distributed Ledger, Peer to peer, Smart Healthcare, Systematized procedures.

INTRODUCTION

The foundation of blockchain technology is bitcoin. It was first introduced by Satoshi Nakamoto in January 2009. Blockchain uses an innovation that is a mix of mathematics and software engineering called cryptography. Blockchain is a distributed database used to store an infinite number of records, called chunks. Blockchain is a distributed record. It is an open currency that anyone can buy; however, once the information is created, it cannot be corrected and does not allow for correction in the form of computerised trust [1]. Hashes or cryptographic signatures play an important role; they are used to record transactions. There are four types of blockchains. The first type is an open blockchain where anyone can participate. The second type is a reserved blockchain, where anyone can join after applying for membership. The third is a

* **Corresponding author Ramya Easwaran:** SNS College of Technology, Coimbatore, India E-mail: ramya.e.ece@snsct.org

semi-private blockchain, which combines public and private blockchains, and the fourth is a side chain, which manages the idea of running a different conveyed record off the primary chain. However, exchanges are ready to take place in a similar currency [2].

Blockchain is the use of cryptography to create an immutable, decentralised, dynamic or evolving record of bits of records, called blocks, that are linked and bound together in a sequential request. Fig. (**1**) shows the hash functions in blockchain.

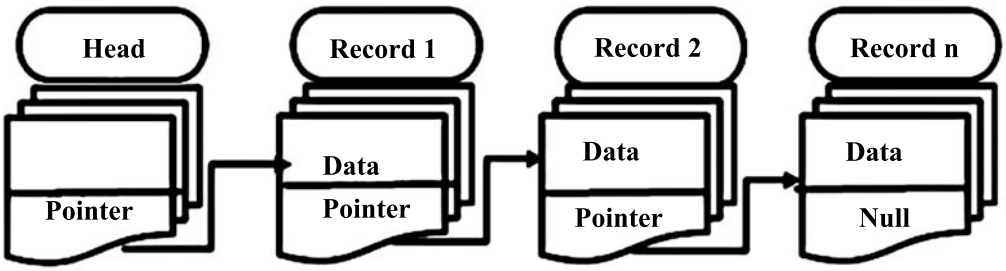

Fig. (1). Structure of records associated together, each record has the hash of an earlier record.

There are numerous blockchain platforms, such as IBM Blockchain, IOTA, Multichain, Open Chain, Quorum, R3 Corda, Ripple, Steller and Symbiont Assembly. The Ripple and Corda protocols are primarily used in the financial industry. Blockchain has many features, such as immutability of stored information, scalability, unanimity and high security. There are many efficient algorithms, such as proof of work (Pow), proof of stake (PoS), and proof of activity (PoA), which are used in blockchain [2]. In Fig. (**2**), the typical structure of a blockchain has the following elements in each block: current hash, nonce, timestamp, transaction details, and previous hash.

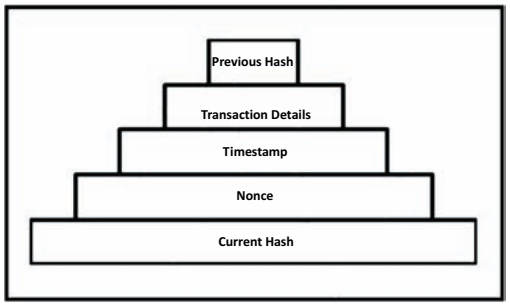

Fig. (2). Typical Structure of the block in Blockchain.

The block is a basic unit of the blockchain created by miners. The typical structure of a block is very simple, as shown in Fig. (**2**), and includes a chunk form that forms a chunk header [1].

MAJOR ISSUES AND CHALLENGES OF HEALTHCARE SYSTEMS

The healthcare system is made up of five stakeholders. For example, it shapes the framework for medical care between providers, patients, payers, the supply chain (manufacturers, distributors and pharmacies) and research organisations [3]. The issues and challenges in the healthcare system are illustrated in Fig. (**3**).

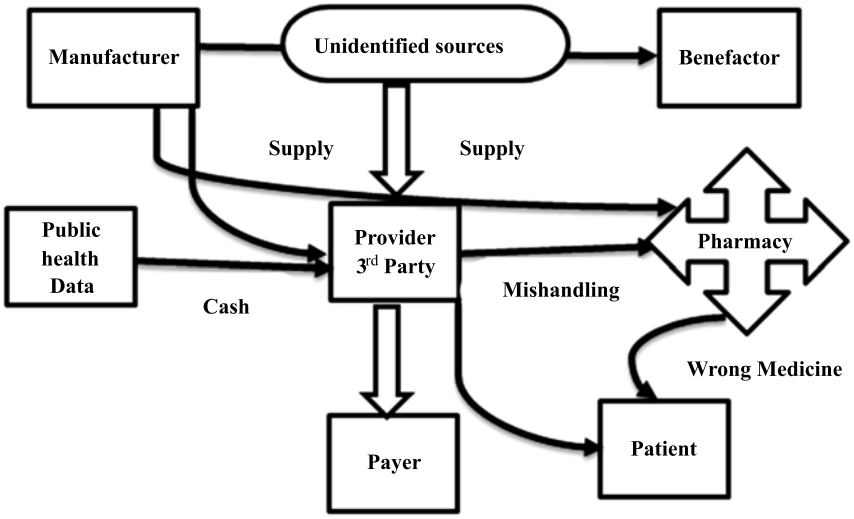

Fig. (3). Outline the links between the top five healthcare investors (providers and manufacturers and dispensers from a single unit of the pharmaceutical supply chain).

Benefactor: The provider is a key competitor in the healthcare sector. The provider is the main intermediary between patients, customers and pharmacies (Fig. **3**). The implementation of automated medication registers and health records is one of the biggest challenges for healthcare providers [4]. It is also expensive, both in terms of time and money. The lack of interoperability guidelines for the exchange of health information between research and clinical settings risks increasing the cost of time [5].

Patients: Patients are an important parameter in healthcare systems. Providers hold patients' health information. Patients are generally concerned about the security of their health information, but their privacy is exploited in many ways. Information can be used for drug promotion, research, general medical care and

CHAPTER 3

Integration of Blockchain and Internet of Things

R. Babu[1,*], Jayashree K.[2], Priya Vijay[3] and **Vijay K.[3]**

[1] *Department of Computational Intelligence, School of Computing, College of Engineering and Technology, SRMIST, Chennai, India*

[2] *Department of Artificial Intelligence and Data Science, Panimalar Engineering College, Chennai, India*

[3] *Department of Computer Science and Engineering, Rajalakshmi Engineering College, Chennai, India*

Abstract: Customers can benefit from the Internet of Things in a number of ways, and it has the potential to transform the fundamental ways that consumers interact with technology. The pervasiveness and correspondences maintained for IoT might provide various conveniences and aids for people, but also open up many security loopholes. Blockchain, a distributed digital ledger, is finding uses in industries as diverse as finance, healthcare, utilities, agriculture, real estate, and Supplier Management. The middleman acting as guardians for specific applications in these enterprises can be removed in order to provide security and those equivalent applications can be run in a distributed way with practically no centralized power. Blockchain technology makes this feasible without sacrificing efficiency or safety, which was previously impossible. Blockchain and IoT seem to be best on their own in the respective sector in which it is applied, so businesses can try and exploit this powerful combination known as Blockchain Internet of Things (BIoT) to bring immense advancements, progressions and cutting edge innovations in the area of their interest. The term "BIoT" was created by fusing blockchain with IoT applications.

Keywords: Blockchain IoT, Covid-19, Digital Ledger, Machine Learning, Quarantine Tracking.

INTRODUCTION

Many current devices can be connected to the internet using a potential new technology known as the Internet of Things (IoT). The development of IoT devices is facilitated by the seamless integration of RFID, remote connectivity, and sensors [1]. Using clever features in conjunction with IoT services gets incor-

* **Corresponding author R. Babu:** Department of Computational Intelligence, School of Computing, College of Engineering and Technology, SRMIST, Chennai, India; Tel: +91 9403615809 E-mail: babu.rajen17@gmail.com

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

porated for providing excellent types of aid, using regulators and electromechanical frameworks to lay out harmony between the internet and the real world. Clinical medical care frameworks are the newest invention that is redefining the way people live today. Blockchain technology uses an online electronic personal records system to take quality information [2]. Blockchain technology is frequently described as a sort of design that stores trade records. The public information base's “blocks” are another name for the records. An organization's chain is connected *via* distributed hubs. In order to do blockchain jobs, a variety of regulations and work methods are used. Prior to adding the entire block to the communication organisation, it is important to regularly examine the organisation framework's hubs.

With its distributed ledger, public-key authentication, and consensus procedures, blockchain technology is a perfect fit for protecting IoT networks. Due to the distributed structure of the Blockchain, the data can be shown in a straightforward and unambiguous manner. Cryptocurrency and the IoT together have become cutting-edge instruments for decentralised healthcare data sharing, patient monitoring, record integrity assurance, protection level forecasting, and supply chain management [3].

Therefore, this section analyses the fundamentals of blockchain and IoT, as well as their various applications, components, and highlights. The advantages and drawbacks of coordinating blockchain with IoT, as well as how the two ideas might be joined, will be discussed. In the next parts, you can expect to read about the various connected works and planned research courses for Integrating IoT with Blockchain.

BLOCKCHAIN

A distributed ledger known as blockchain is comparable to an electronic book that stores the past. Due to encryption, data on this system is stored decentralized across all network users and is very challenging to delete or manage [4]. The advancement of blockchain technology has a lot of advantages, including dependability, security, quickness, robustness, correctness, and usefulness [5, 6].

Components of Blockchain

A number of potential advantages of blockchain technology over existing methods have been proposed. The blockchain is made up of several simple aspects, including the records, blocks, hashes, transactions, minors, and agreements and this has been represented in the diagrammatic form in Fig. (**1**).

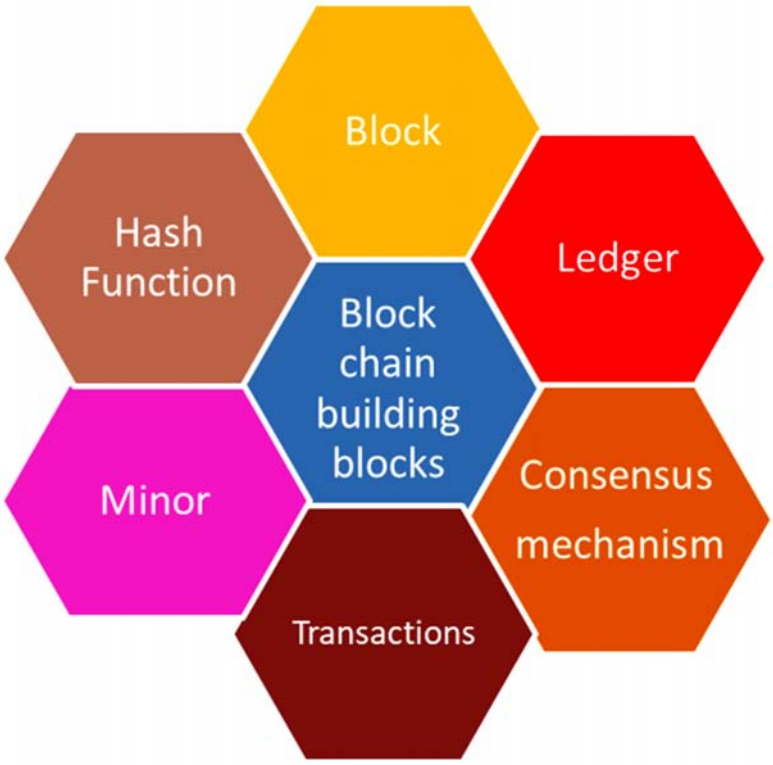

Fig. (1). Components of Blockchain.

The record is an information structure that is used to store different sorts of data. There are massive contrasts between the old-style data set and the record. A data set framework stores information as tables with segments and columns. Besides, it involves a social model for questioning and assembling information by interfacing data from a few sources [7]. Then again, the record is used to store every one of the exchanges produced using all taking part clients in the organization.

The block serves as the fundamental building block of the blockchain. Within each block, numerous exchanges take place. They were combined by including a one-of-a-kind hash of the information from the previous block in the one being processed now. Just like that chain, this union is a roadblock to development. This feature is attractive since it has no obvious effect and can be utilised without anxiety, given that it is exceedingly impossible to construct two different hashes for two separate bits of advanced data. Providing a hash reward for the block is one way to verify its identity and contents [8].

CHAPTER 4

Consequences and Deliberations in Implementation of Blockchain and Internet of Things Integration

K. Karthigadevi[1,*] and **G. Srinivasagan**[2]

[1] *Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India*

[2] *Department of Chemistry, Rajapalayam Rajus College, Rajapalayam, Tamilnadu, India*

Abstract: Blockchain technology proposes security facilities to the Internet of Things (IoT). The things or objects used in daily life are connected to the internet to form IoT. The blockchain integral safety mechanism can deliver amenities, such as authentication, accessibility, integrity, secrecy, and authorization to the IoT applications. The uses of IoT applications are the dream turning into reality. But using this IoT still faces some challenges, mainly in the areas of security such as data consistency and reliability. The objects have interacted over the internet; they can also be supervised and controlled remotely. The use of IoT reduces time, manual work, tracking and money. With the evolution of IoT, it is essential to deliver more security for enormous amounts of data. Blockchain is a circulated network with the properties of integrity and secrecy. The blockchain maintains data security in the network of IoT. Here to discover the challenges associated with the combination of IoT and blockchain, a study is taken first, then a blockchain introduction is offered, followed by the Blockchain-based IoT requirements, demand and Quality of Service (QoS) discussed. Then, tasks faced while applying this blockchain-based IoT, such as plan, progress and deployment, are discussed. Then applications of blockchain-based IoT such as throughput, efficiency, latency, privacy, fork problem, smart contracts, legal issues, security, storage and proposed solutions are deliberated. Finally, upcoming research guidelines for the combination of IoT and blockchain are designated.

Keywords: Blockchain Technology, Challenges in Blockchain IoT Applications, Internet of Things, Quality of Service, Smart Contracts.

INTRODUCTION

These days, IoT and blockchain technologies are crucial to technology. The combination of blockchain and IoT may open up new avenues as well as allow for

* **Corresponding author K. Karthigadevi:** Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India; E-mail: k.karthikrish@gmail.com

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

the development of apps that can benefit from the blockchain's distributed work. Connecting physical objects to communication networks like the internet is referred to as the Internet of Things (IoT). Currently, communication networks like the internet have connected not just computers but also devices like refrigerators, TVs, laptops, stoves, washing machines, automated doors, air conditioners, electrical appliances, vehicles, bikes, motorbikes, and cellphones, among others. According to the IoT utilization projection, the communication network may connect 50 to 60 billion devices [1]. There are many different claims made in the IoT space.

The implementation of privacy and security solutions would be done in accordance with IoT device characteristics. Equivalent degrees of security must be provided for different types of devices, and systems that can audit and regulate access are required in these environments. Data created by devices can be authorized, audited, and authenticated using blockchain technology. The trust protocol is another name for blockchain technology. It tries to reorganize security measures in order to produce a global index for every transaction that takes place in a particular network. Applications of blockchain technology include smart contracts, digital management and supply chain management [2].

Blockchain is a protocol that can be trusted, and it is called “the protocol of trust”. The fundamental idea of blockchain is to delegate the safety mechanism, and a new role has to provide an unambiguous file for all the deals or dealings and take the place of a certain link. It functions as a shared, open, and global ledger. Without the involvement of a third party, it generates agreement and assurance *via* direct communication between two diverse parties. In certain other applications, blockchain can be utilized for contracts, supply chain management and identity administration [3].

This article contains the most current requests in safety and secrecy and discusses what can impact the Internet of Things. It also intends to update some understanding of blockchain technology. The technique will be a review of cutting-edge publications that leverage the blockchain to deliver some amount of security and confidentiality and will propose a different type of egotistic mining attack [4], which we refer to as a follower. A hostile technique known as “stalker” seeks to prevent a particular miner from publishing their blocks.

We planned this article into five different sections. Section 1 is an introduction to blockchain. Section 2 represents the fundamentals of the proposed solutions that is a literature survey for understanding purposes. Section 3 represents the working mechanisms and implementation and design of the technology of blockchain. Delegates use cases, results and discussion of blockchain technology to deliver

safety cum security and confidentiality at IoT. It describes the conclusion of deliberations and open queries.

The step-by-step operation of blockchain and provides the following explanation:

(1) A block is used to indicate transactions that a node wants to execute.

(2) The P2P network is informed of the deal.

(3) The network nodes verify the transaction (PoS).

(4) The block is further to the blockchain after validation.

(5) The deal is finished.

Despite being introduced in 2008, blockchain technology wasn't actually put into use until 2009 [14]. It has the capacity to monitor and archive data from several nodes. Blockchain's decentralized architecture can handle trillions of transactions between IoT devices. It can avoid constructing and operating pricey centralized servers in this way. In contrast to the centralized Internet of Things design, it manages with all complexity in the network, providing an inducement to effective colliers (devices or nodes). IoT designs of the current nodes are taking the risk of failure that would be eliminated by the BIoT [5, 6]. Since the values are validated and confirmed by entire devices in the network and using a method before a deal is carried out, the blockchain is particularly reliable for IoT devices (users). How agreement is reached among entire devices in the verifying net to attach a new block is determined by the consensus algorithm. With the help of blockchain capabilities like secrecy and anonymity, IoT devices may help hide sensitive data [7, 8]. To enable the IoT with blockchain combination, the blockchain advocates employing smart contracts to increase the functionality and intelligence of devices [9]. The use of IoT and blockchain technology will enable bulges to buy and sell power routinely [10].

LITERATURE REVIEW

The future is defined by the IoT. The physical elements will be connected to the internet and be capable of identifying other gadgets as their own. IoT is a brand-new Internet revolution. Numerous applications, such as smart manufacturing, logistics, home appliances, lifestyles, and healthcare systems, will be impacted. The author reviews, incorporates, and summarizes hybrid approaches that can be applied to healthcare applications in an IoT setting [11, 12].

The cybersecurity of IoT has already drawn more examine of cyber security because of the Internet of Things' (IoT) steadily growing relationship. It is

CHAPTER 5

Blockchain Integrated with Internet of Things-benefits, Challenges

Geeta Amol Patil[1,*], **Surekha K.B.**[1], **Chaithra V.**[1] and **Anand Kumar S.**[2]

[1] *BMS Institute of Technology and Management, Bengaluru, India*

[2] *Vellore Institute of Technology, Vellore, India*

Abstract: All sectors are now using digital ways to facilitate humans. Be it health, finance, supply chain, communication, transport, IT, or education, all the sectors are now relying on technologies and the internet for providing facilities and also using them as sources of information. These sectors, when using traditional ways, faced a lot of challenges. For example, people earlier going to railway stations to book train tickets had to wait for long durations in queues, and if all the seats are filled by the time they reach or their turn comes to reserve seats, it goes all in vain to spend time traveling to the station and time in queues. Coming to the finance sector, people had to go to banks to create a bank account and for all the formalities. They had to spend time going to banks and then wait in queues to get their work done. Also, it took around 1-2 weeks for every task to complete in banks. So, the process was quite time-consuming, monotonous and unreliable in practice. Thus many sectors started looking for alternative methods to perform their daily tasks. Slowly, the sectors started digitizing, and started using computers to perform tasks, to store and update their data. They also started using the internet in their daily applications. Each organization of industry is now available on the internet. All of their information is present and one can apply for their services using their websites. Thus, IoT comes into the picture here. All the sectors using the internet to access and provide information, using the cloud to store their data are using IoT services. Internet of Things (IoT) technology will soon become an integral part of our daily lives to facilitate the control and monitoring of processes and objects and to change the way man interacts with the physical world. For all aspects of IoT to be fully functional, there are a few obstacles to overcome and important challenges to overcome. These include, but are not limited to, cyber security, data privacy, power consumption, and metrics. The dedicated Blockchain environment and its various processes provide a useful way to address these few IoT challenges.

Keywords: Cyber Security, Computer Vision, IoT Challenges.

[*] **Corresponding author Geeta Amol Patil:** BMS Institute of Technology and Management, Bengaluru, India; E-mail: geetapatil@bmsit.in

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

INTRODUCTION

Today, around 5 billion devices are connected to Internet of Things (IoT) systems, and this number is increasing day by day [1]. Every device on the Internet generates and exchanges data. In light of this enormous number of gadgets, significant and continuous data is created. Addressing the basic security concerns of such a large-scale information structure is challenging. The distributed architecture of the IoT presents a significant difficulty. In an IoT network, each node can be a potential failure point. A node can be a source to launch cyber-attacks such as Distributed Denial-of-Service (DDoS) [2]. A network with increasing infected nodes acting simultaneously may swiftly come to an end. Another concern is regarding its centralized configuration [3]. Nodes in the network which are vulnerable to threats have to be addressed. Maintaining confidentiality and authentication of the sensed data becomes important in the entire IoT system [4].

IoT data can be misused and exploited without data security. Data security also becomes crucial with the introduction of systems where IoT devices can exchange data resources, computational power resources and electricity resources on their own. The IoT has several important uses, including decision support systems. Timely judgments can be made using the data compiled from the fleet of sensors. Hence, it becomes important to defend the system against attacks and include safety measures to protect the nodes and the data.

Automated systems that handle real-time information, such as smart grids, manufacturing industry unit, and transportation networks, availability is essential. Losses from sensor outages can range from financial to potentially fatal. Trust building among participating organizations is a critical difficulty in the emerging economy of machines. Data-generating sensors can sell their data in data marketplaces and through end-to-end autonomous systems [5]. Instead of having a third party, a publicly verifiable audit mechanism can handle the issue of non-repudiation.

Thus integrating IoT with blockchain provides a solution to these challenges. Since blockchain uses a decentralized way of storing data in nodes and linking those nodes with hashing algorithms, thus it makes it secure to store data in IoT devices. These are also other motivations for integrating IoT with blockchain:

– Security and safety in accessing data and devices.

– Reliability of connecting devices.

– Data storage’s long-term viability.

The inherent security of the blockchain technology is typically acceptable for various IoT applications when the primary goal is to keep the user's identity confidential.

Objectives of IoT integration with Blockchain are as follows:

– The objective of integrating IoT with Blockchain is to provide a reliable way to connect devices over a network that is secure, safe and reliable with storing data.

– To provide proper power resources so that devices do not have to face the consequences of power outrage or current unavailability is one of the objectives of integrating IoT with blockchain.

– To store data in a secure way so that it is accessible within an organization but cannot be tampered with.

AN OVERVIEW OF THE INTERNET OF THINGS

The current craze of internet-connected devices is the Internet of Things with built-in computing capabilities. The term refers to a wide range of devices, including internet-connected surveillance devices, security cameras, sensors, networked industrial equipment, and consumer electronics, like refrigerators and autos [6]. Pervasive computing has increased the appeal of the IoT in the technological age of today. The usage of IoT devices has benefitted smart-cities, smart-homes and smart-transportation. In 2008, the number of IoT devices outnumbered the world's population. The IoT system's multiple features allow for the creation of new apps and services on a daily basis. According to Statista [1], by the end of 2025, the number of things connected will be crossed over 19 billion. Statista estimates that by the end of 2028, the total number of IoT objects will have surpassed 25 billion. As can be seen in Fig. (**1**), by 2030, this number will have risen to almost 29 billion devices. In addition, the Internet of Things industry is expanding at a fast pace [7].

CHAPTER 6

Blockchain Powered Medical Sector – Application, Challenges and Future Research Scope

Divya Palanisamy [1,*], **Saranya Rajendran**[2] and **Praveena Venkatesan**[3]

[1] *N.G.P. Institute of Technology (affiliated to Anna University), NGP Nagar, Kalapatti -6410648, India*

[2] *Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu 641022, India*

[3] *NGP Institute of Technology, Coimbatore, Tamil Nadu 641048, India*

Abstract: The recent research in the healthcare sector using computer technologies in the fourth industrial revolution helps to improve the quality of life by accessing the medical data to monitor, diagnose and treat the patient at the right time from anywhere in the world. Blockchain is one of the major recent innovations and trending research topics that plays a vital role in diverse applications like Smart cities, Healthcare industry, Smart grid, *etc.* Blockchain, which is fascinated with its features like secure data sharing, immutability, decentralization, and reliability in data management, has made it a prominent technology in the healthcare industry. This chapter discusses 1) The working principle of blockchain technology with its different prospectus in healthcare. 2) Advantages of blockchain technology over the Internet of Things in secured patient data management, efficient data sharing with decentralized data management accessible for authorized users using cryptography techniques. 3) Various applications of blockchain technology in healthcare, like remote patient monitoring using Internet of Things (IoT) devices for cardiac and electroencephalogram (EEG) signal monitoring to diagnose life-threatening diseases. 4) Drug traceability in the pharmaceutical drug supply chain to ensure product safety with an end-to-end tracking system and immutable transaction record. Finally, this chapter also presents the blockchain based challenges and solutions that advocate the future research scope in healthcare systems.

Keywords: Blockchain, Challenges, Drug Traceability, Healthcare, Smart Cities.

INTRODUCTION

Blockchain is the next horizontal breakthrough in healthcare, following horizontal advancements such as the Internet, Cloud computing, and image processing. Simply explained, a blockchain is a network of computers that are not owned by

* **Corresponding author Divya Palanisamy:** N.G.P. Institute of Technology (affiliated to Anna University), NGP Nagar, Kalapatti -6410648, India; E-mail: divya@drngpit.ac.in

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

one single entity that is in charge of a time-stamped repository of permanent data records. Each block of this data *(e.g.*, block) is encrypted and linked together using cryptographic principles *(e.g.*, chain). The Blockchain is greatly regarded because of the following reasons such as it is not owned by a single entity, making it distributed, the data is secured cryptographically, irreversible, and the transparency can be supervised at any time and from anywhere in the world [1].

Traditional paper-based medical records have a number of flaws, prompting medical institutions to switch to electronic health records (EHR). From transferring medical records to real-time data from multiple patient body sensors, e-Health technology has come a long way. This technology creates a new paradigm for transferring medical data, resulting in EHRs that are more efficient, accurate, and secure. As the healthcare industry grows, the quantity of electronic health records (EHRs) generated increased. Immutability, cryptography, distribution, transparency, non-repudiation, audibility, and decentralisation are all blockchain principles, as shown in Fig. (**1**), which made this technology more suitable for healthcare industry [2].

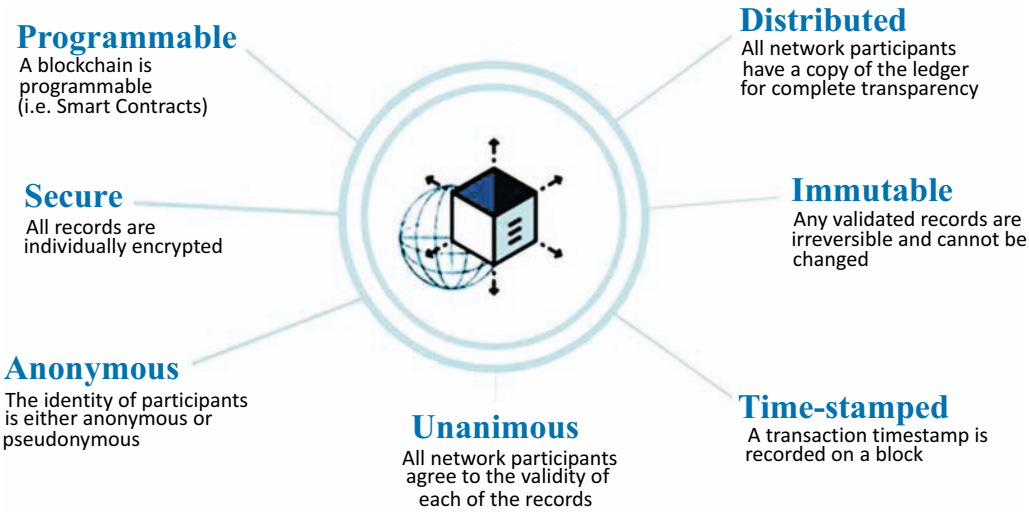

Fig. (1). Property of Blockchain Networks.

Healthcare is an important element for both developing and wealthy countries since it is closely related to people's social welfare and daily life. In the healthcare sector, research and development should be a continuous process because it will help to improve the quality of life by combating numerous health conditions and diseases. It has been simple to observe the improvement in the healthcare sector owing to recent technological advancements. The most advanced and cutting-edge

computer technology can be used to significantly improve the capabilities now available to the healthcare and medical sectors. These cutting-edge computer technologies can aid doctors and medical professionals in the early detection of a variety of ailments [3]. Nowadays, the word "Blockchain" has become one of the unavoidable terms in e-health records in the field of medical technology. As abundant data are available in the healthcare sector, the blockchain networks help to preserve, secure, exchange and provide transparency in sharing medical data [4].

The contribution of this chapter includes a discussion of the components of blockchain, application of blockchain in healthcare and challenges faced by blockchain in the healthcare industry and finally, the conclusion and future scope.

COMPONENTS OF BLOCKCHAIN

A blockchain requires four components in order to take on a life of its own. A peer-to-peer network is the primary requirement for a blockchain to function. Equally privileged nodes are a type of computer network. Anyone and everyone can attend. This network allows nodes to connect and share information from a distance. Cryptography is the second component. The technique of secure communication in a hostile environment is known as cryptography. It enables a node to communicate with other nodes. Fig. (**2**) clearly explains the design flow of the blockchain, which includes the step flow starting from the data transmission to key verification, including the transaction fee, transfer and distribution of the block [5].

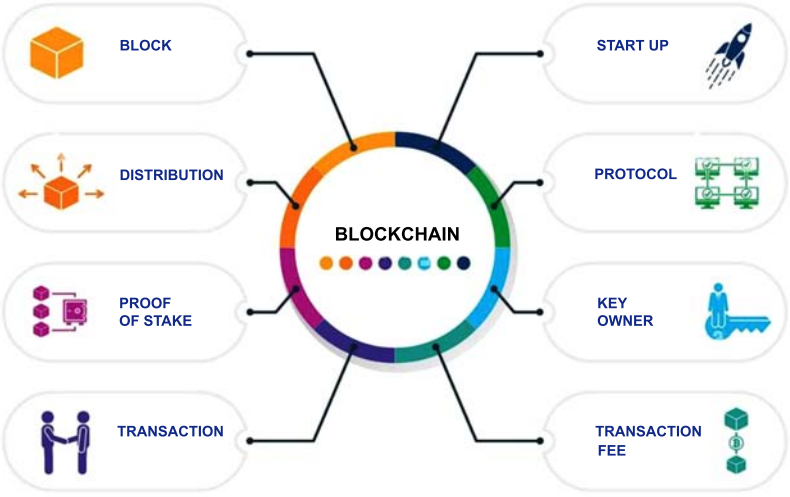

Fig. (2). Blockchain Vector Design.

CHAPTER 7

Blockchain in the Healthcare Domain and Performing Various Security Analysis

Suresh Kumar Nagarajan[1,*], **Geetha Narasimhan**[2], **Akila Victor**[2], **Yash Vaish**[2] and **Pranshu Tripathi**[2]

[1] *Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India*

[2] *School of Computer Science & Engineering, VIT, Vellore, India*

Abstract: Blockchain is a promising technology that can be used to improve the healthcare system. It can be used to store patient data securely and prevent tampering. It can also be used to improve supply chain management by increasing transparency and interoperability. This work proposes a web-based application that uses blockchain to store patient's data and retailer's information. The application will also be able to send encrypted messages securely and anonymously. The application will be deployed on the Ethereum platform. The benefits of using blockchain in healthcare are Security: Blockchain is a secure way to store data because it is decentralized and encrypted. This makes it difficult for unauthorized users to access or tamper with data. Transparency: Blockchain is transparent, which means that all transactions are recorded on the blockchain and can be viewed by anyone. This can help to increase trust and accountability in the healthcare system. Interoperability: Blockchain can be used to connect different healthcare systems together, which can improve the flow of information. This can help to improve patient care. Immutability: Blockchain is immutable, which means that data cannot be changed once it is added to the blockchain. This can help to ensure the accuracy of data. The challenges of using blockchain in healthcare are Complexity, Cost, and Regulation. Despite these challenges, blockchain is a promising technology that has the potential to improve the healthcare system. This work is a step towards realizing the potential of blockchain in healthcare.

Keywords: Blockchain, Bitcoin, Decentralization, Ethereum, HealthCare System, Security.

INTRODUCTION

Blockchain is a technology that makes data records secure and tamper- proof. It is a distributed ledger that is shared among a network of computers. This makes it

* **Corresponding author Suresh Kumar Nagarajan:** Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India; E-mail: sureshkumar@klu.ac.in

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

difficult for unauthorized users to access or modify the data. The healthcare industry is increasingly adopting blockchain technology. This is because blockchain can be used to address a number of challenges in the healthcare industry, such as:

Data security: Blockchain can be used to secure patient's data from unauthorized access or modification.

Identity management: Blockchain can be used to create a secure and reliable way to identify patients.

Supply chain management: Blockchain can be used to track the movement of drugs and other medical products through the supply chain.

Clinical trials: Blockchain can be used to record and track data from clinical trials.

Payments: Blockchain can be used to make secure and efficient payments for healthcare services [1 - 9].

The healthcare industry is still in the early stages of adopting blockchain technology. However, the potential benefits of blockchain are significant, and it is likely to play an increasingly important role in the future of healthcare. Here are some specific examples of how blockchain is being used in the healthcare industry today:

MediLedger: MediLedger is a blockchain-based platform that is used to track the movement of prescription drugs through the supply chain. This helps to ensure that patients receive genuine and safe medications.

Chronically: Chronically is a blockchain-based platform that is used to manage patient health records. This allows patients to share their health records with their healthcare providers securely and easily.

Doc.ai: Doc.ai is a blockchain-based platform that is used to make secure and efficient payments for healthcare services. This can help to reduce the administrative costs of healthcare.

These are just a few examples of how blockchain is being used in the healthcare industry. As the technology continues to develop, we can expect to see even more innovative applications of blockchain in healthcare in the future [11].

Preventing Fraud: Blockchain technology can be used to address the problem of fraud in the healthcare industry. Fraud can occur in the form of false medical rec-

ords, claims, and proof of work. Blockchain is a tamper-proof ledger of hashes that can be used to track and verify all healthcare data.

The healthcare industry is rapidly adopting digital technologies, such as electronic health records (EHRs). EHRs store a wide variety of patient data, including clinical records, statistical data, prescriptions, vaccination status, lab test reports, and other sensitive data. Blockchain can be used to secure and protect EHR data from unauthorized access and tampering [18].

In addition to securing EHR data, blockchain can also be used to improve the efficiency and transparency of the healthcare industry. For example, blockchain can be used to create a decentralized network for sharing healthcare data between different stakeholders, such as doctors, hospitals, and insurance companies. This would make it easier to access and share patient data, which could improve the quality of care.

Blockchain is a promising new technology that has the potential to revolutionize the healthcare industry. By addressing the challenges of fraud, security, and efficiency, blockchain can help to improve the quality of care and make healthcare more affordable.

Here are some specific examples of how blockchain can be used in the healthcare industry:

Secure electronic health records: Blockchain can be used to create a tamper-proof ledger of all healthcare data, making it more difficult for fraudsters to alter or steal patient records.

Manage the supply chain of drugs: Blockchain can be used to track the movement of drugs from the manufacturer to the patient, ensuring that patients receive genuine and safe medications.

Pay for healthcare services: Blockchain can be used to create a decentralized payment system for healthcare services, making it easier for patients to pay for care and for providers to get paid.

Research and development: Blockchain can be used to store and share data for medical research, making it easier to conduct clinical trials and develop new treatments.

Blockchain is still a new technology, and there are some challenges that need to be addressed before it can be widely adopted in the healthcare industry. However, the potential benefits of blockchain are significant, and it is likely to play an increasingly important role in the future of healthcare.

CHAPTER 8

IOT-Based Smart Healthcare System with Hybrid Key Generation and DNA Cryptography

Vidhya E.[1,*]

[1] *Padmavani Arts and Science College for Women, Salem, Tamil Nadu 636011, India*

Abstract: Many applications, such as smart health care, smart cities, smart homes, self-driving cars, IoT retail shops, tele-health, traffic management, and so on, will use IoT devices to generate information. In these tenders, smart health care is single of the most imperative because it generates sensitive information like disease managing, drug managing, secluded patient checking, defensive care, and so on. This large amount of information is acquired and recorded from a variety of sources (mobile phones, software, sensors, e-mail, applications and so on). These sources contain a basic encryption process, so hackers can easily hack the information and misuse it. These issues are taken by researchers, and they find solutions, but they do not fulfill the needs of encryption. Key generation is critical for encryption and decryption because a strong key increases the encryption and decryption level. In this chapter, the proposed system is designed and implemented with a strong key generation (KG) to encrypt (encr) and decrypt (decp) the information that is compatible with the limited processing capabilities of IoT devices. In this system, the mathematical key generation algorithm is created with the hybrid of prime numbers and pseudo random numbers using the Exclusive OR function. Besides, the DNA Cryptography algorithm is used to encrypt and decrypt the information. The above system makes it hard for hackers to break into. When paralleled with illustrious cryptographic schemes, the tentative outcomes of the proposed system show the best effects for every IoT scheme in terms of encryption time and key entropy. When equal to other surviving encryption schemes, the proposed system has a restored avalanche effect and key entropy value for achieving the security goals. The above security goals illustrate that such a scheme is able to protect IoT documents from present attacks.

Keywords: DNA Cryptography, IoT Devices, Pseudo Random Number, Prime Number.

INTRODUCTION

The Internet of Things is referred to as IoT, which was founded by Kevin Ashton in 1999. In the last 10 years, IoT has made any object internally connected and

[*] **Corresponding author Vidhya E.:** Padmavani Arts and Science College for Women, Salem, Tamil Nadu 636011, India; E-mail: vidhya11tamilarasi@gmail.com

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

has been considered the next technological revolution. The IoT is used by many applications such as smart health care, smart cities, smart homes, self-driving cars, IoT retail shops, tele-health, traffic management [1 - 8], and so on. In these applications, smart health care is unique and of the greatest significance because it generates sensitive information like disease management, remote patient monitoring, preventive care, drug management and so on. This large amount of information is acquired and recorded from a variety of sources (mobile phones, software, sensors, e-mail, applications and soon). IoT is really nothing more than associating processors to the internet *via* networks and sensors [9, 10]. These linked modules can be used in strength monitoring devices. The information is then conveyed to secluded locations *via* sensors such as M2M, which are machines for processors, technologies for people, handheld devices, or smartphones [11]. It is a humble, direct, much smarter, accessible, energy-efficient and interoperable method of following and enhancing care for any wellbeing issue. Currently, recent schemes provide a flexible border [12], assistant devices [13], and mental strength management [14] to help humans live a smarter lifetime. The IoT architecture is shown in the Fig. (**1**).

IoT devices generate structured and unstructured information based on their applications. This information needs a high level of security, but the IoT contains default encryption at a basic level, so it is not sufficient for this information [15]. Hackers can easily hack the information and misuse it, so the information is in a problem stage. This problem is studied by many researchers, and they find solutions, but they do not fulfill the needs of encryption because the level of encryption and decryption is based on the strength of the key generation. In this chapter, the proposed system is designed and implemented with a strong key generation to encrypt and decrypt the information that is compatible with the limited processing capabilities of IoT devices [16]. In this system, the mathematical key generation algorithm is created with the hybrid of prime numbers and pseudo random numbers using the Exclusive OR function. Besides, the DNA Cryptography algorithm is used to encrypt and decrypt the information [17]. The above system makes it hard for hackers to break into. When equaled to familiar cryptographic schemes, the tentative results of the proposed system show the best results for any IoT device in terms of encryption time, and key entropy [18]. When compared to other existing encryption systems, the proposed system has an improved avalanche effect and key entropy value for achieving the security goals. The above security goals illustrate that such a scheme is able to protect IoT documents from present attacks. The example for the Smart health care system is shown in the Fig. (**2**).

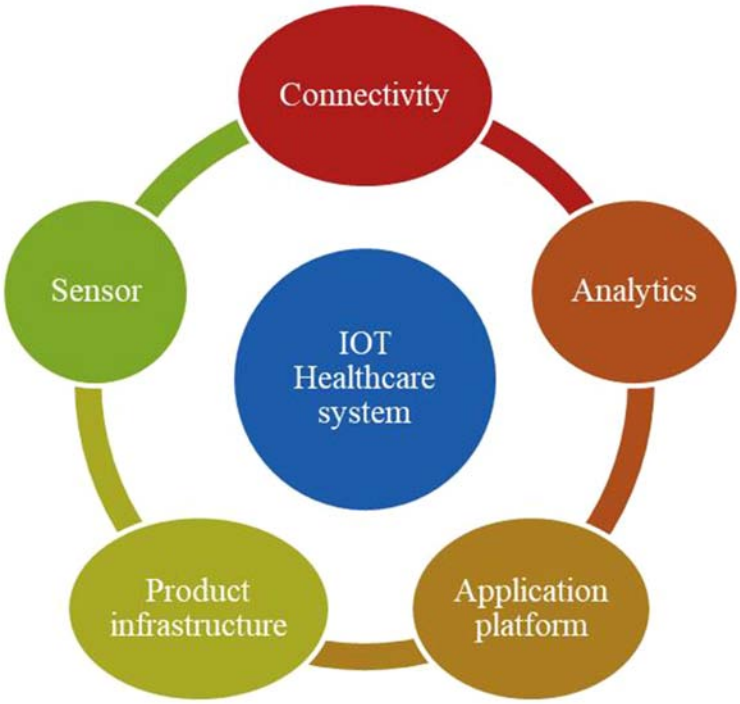

Fig. (1). IoT Health care system Architecture.

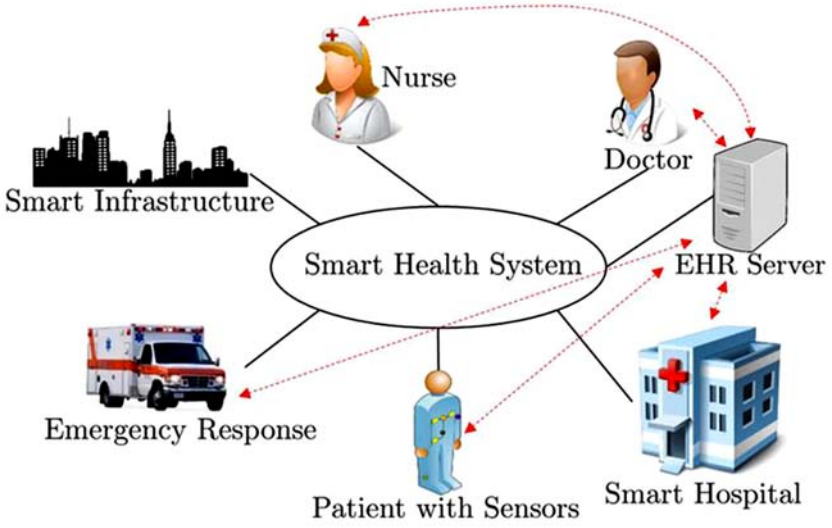

Fig. (2). Example Smart health care system.

CHAPTER 9

Security Enhancement in Cloud and Edge Computing Through Blockchain Technology

Santanu Koley[1,*] and **Pinaki Pratim Acharjya**[1]

[1] *Department of CSE, Haldia Institute of Technology, Haldia -721607, India*

Abstract: The cloud computing (CC) network is designed to tackle the security and privacy challenges of centralized cloud services by distributing computing and storage resources among networked nodes. Cloud computing, on the other hand, is restricted by the performance of linked devices, posing problems in state authorization, stats encryption, consumer privacy and more. Blockchain technology (BT) is the most popular circulated network technology right now. It is utilized in numerous fields like bitcoin, IoT, *etc*., to tackle the consistent issue of distributed data. The difficulties that CC networks present for security and privacy are covered in this chapter. Analysis and solutions brought to edge computing networks by BT in terms of data encryption, authentication and user privacy. In this chapter, the advantages of combining the cloud computing network with blockchain technology will be discussed. Finally, memory, workload, and latency problems for related future studies have been discussed.

Keywords: Blockchain, Cloud Computing, Security, Edge Computing.

INTRODUCTION

Service computing has seen an increasing number of applications in various areas recently. Topics include cloud computing, the digital economy, and the Internet of Things (IoT). The IoT is a good example. Through connected manufacturing of smart devices, healthcare, energy, and more, greater control can be achieved over the physical world, including industries. Despite its wide range of uses, there are some issues that need to be addressed to maximize its potential. Cloud computing is a service oriented architecture. In recent years, as the need for next-generation financial technology has increased, blockchain research is underway to enable the safe transaction.

Blockchain acts as a public ledger for transactions and protects against hackers when dealing with crypto currencies. It is a kind of distributed database, with an

[*] **Corresponding author Santanu Koley:** Department of CSE, Haldia Institute of Technology, Haldia -721607, India; Tel: 8944931442; E-mail: santanukoley@gmail.com

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

ever-expanding list of records, intended to prevent arbitrary manipulation by operators of distributed peers [1]. Blockchain software is installed on your computer to encrypt transaction records according to a set of rules. BT is used in electronic money, Bitcoin.

Comparing the use of blockchain with storing all data in a single database, the former can provide better security. Damage from database attacks can be avoided in terms of data storage and management. Furthermore, due to its openness attribute, blockchain [2] can provide data transparency when used in areas where data disclosure is required. These advantages allow it to be used in a variety of contexts, such as: Its potential applications could increase in the financial sector and IoT environment [3].

By consolidating transactions across the network into a single block, a digital currency lender completes a transaction record on the blockchain through a work-authentication process [4]. It is then verified and connected to the previous block to provide a hash value. This block will be updated periodically to reflect the electronic cash transaction information to convey the latest transaction details block. This procedure provides security for electronic currency exchanges while allowing the use of trustworthy mechanisms.

This chapter's sections are arranged as: Section 2 explains the fundamental ideas behind cloud computing. Section 3 explores privacy challenges in CC in more detail. The discussion on Blockchain and its benefits for security and privacy is in Section 4. Section 5 describes blockchain concepts. Section 6 elaborates on the concept of a secure solution for blockchain edge computing in cloud computing. In Section 7, it is discussed how blockchain adoption enhances edge computing security and privacy. Section 8 highlights the benefits of combining CC networks with BT. Finally, Section 9 concludes the study.

CLOUD COMPUTING

Transferring to the cloud, jogging through the clouds, these days, it seems like everything is taking place “on the cloud,” whether it is being stored or accessed from there [5 - 10]. But what precisely is this hazy idea?

On the other end of the internet connection, there is a location where users may access apps and services and keep their data securely. The cloud is essential because of three things:

It does not require any effort to manage or maintain it. It should not worry about running out of space because its size is nearly infinite. Any device with an internet connection can be used to access cloud-based applications and services.

Fig. (**1**) depicts the cloud deployment model, which is a combination of private, public and hybrid cloud (combination of private and public). The server, storage and mobile devices attached as hardware components. Applications and databases are kept in separate software modules.

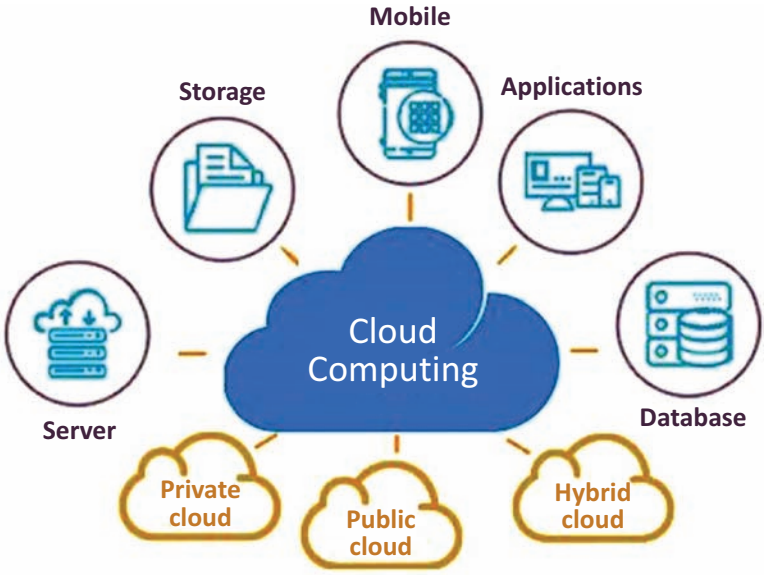

Fig. (1). Cloud Deployment Model.

Fig. (**2**) describes different parts of the cloud service model. This model is a mixture of diverse services of dissimilar software namely Software-as-a-Service (SaaS), the complete cloud platforms like H/W, S/W and infrastructure in lesser cost provided by Platform-as-a-Service (PaaS). Finally, Infrastructure-as-a-Service (IaaS) makes a variety of on-demand infrastructure services available to both enterprises and consumers *via* the cloud, including computing, storage, networking, and virtualization.

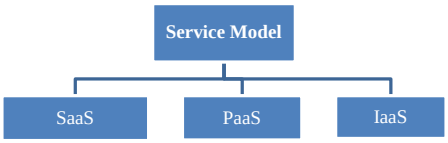

Fig. (2). Cloud Service Model.

PRIVACY CHALLENGES IN CLOUD COMPUTING

CC is an issue that is currently receiving attention from a variety of sectors, including academia, business, and research. It has become a hot topic at

CHAPTER 10

Effective Automated Medical Image Segmentation Using Hybrid Computational Intelligence Technique

Manoranjan Dash[1,*], **Raghu Indrakanti**[2] and **M. Narayana**[2]

[1] *Department of Artificial Intelligence, Anurag University, Hyderabad, India*

[2] *Electronics and Communication Engineering Department, Anurag University, Hyderabad, India*

Abstract: In biomedical domain, magnetic resonance imaging (MRI) segmentation is highly essential for the treatment or prevention of disease. The demand for fast processing and high accurate results is necessary for medical diagnosis. This can be solved by using computational intelligence (CoIn) for data processing. The CoIn can be achieved by using well-known techniques such as fuzzy logic, genetic algorithm, evolutionary algorithms and neural networks. The computational complexity of a medical image segmentation depends on the characteristics of data as well as suitable algorithms. The selection of CoIn methods is very important for better segmentation of a medical image because each algorithm outperforms a different medical image data set. The hybrid CoIn (H-CoIn) is one of the solutions to overcome the problem of individual algorithms in medical image segmentation. The H-CoIn is a combination of two or more intelligence algorithms (like fuzzy logic, evolutionary algorithms and neural networks). The drawbacks of individual intelligence algorithms can be overcome by using H-CoIn. In a medical image segmentation process, two or more variables or objectives need to be optimized for H-CoIn. This problem can be solved by using multi-objective optimization techniques, where simultaneously minimization or maximization can be performed. In this chapter, the various CoIn algorithms' performance has been discussed in detail for medical image segmentation and compared with state-of-the-art techniques. The H-Coin algorithm has been implemented in a large medical dataset and attained an accuracy of 98.89%. Further, the H-Coin algorithm is reliable and suitable to overcome the inter-observer and intra-observer variability.

Keywords: Evolutionary Algorithms, Hybrid Computational Intelligence, MRI, Segmentation.

[*] **Corresponding author Manoranjan Dash:** Department of Artificial Intelligence, Anurag University, Hyderabad, India; E-mail: manoranjanai@anurag.edu.in

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

INTRODUCTION

The eighth critical organ of the human body is the sophisticated brain, which regulates the neurological system. Uncontrolled and erratic cell proliferation within the bladder might lead to a tumor. Primary and secondary tumors are the two main categories of breast tumors. Breast cancer has the greatest fatality rate of any disease in the world and does not correspond with population growth. Auxiliary brain tumors, which develop in one more part of the body and travel to the cerebrum through the circulatory system, grow in the brain tissues. In addition, if neglected, these could lead to a critical condition [1].

Early detection and classification are the most important steps in the diagnosis and treatment of brain cancers with good prognostic accuracy with which the patient's life can be saved. However, radiologists and medical professionals find it challenging to identify and localize malignancies and normal tissues from medical imaging due to the manual examination of brain MR images [2]. Systems for computer-aided diagnosis (CADx) are essential for resolving this problem.

It must be put into practice to lighten the strain and make it easier for doctors or radiologists to analyze medical images. A number of precise and dependable ways to automate the work of identifying and classifying breast cancers have previously been put forth by numerous researchers. Customary Artificial Intelligence based strategies are applied to the analysis of brain tumors. However, ML-based systems need human feature extraction and categorization and only employ tiny amounts of data. Deep learning (DL) consolidates feature extraction and grouping in a self-learning way on a lot of named information, essentially upgrading execution.

A version of DL called convolutional neural network (CNN) was also developed exclusively for two-dimensional (2D) problems. It mechanically extracts various features from MR images and only accepts datasets that have undergone a minimal amount of preparation [3]. Profound CNN models are most often utilized for the detection of brain tumors. Nonetheless, mind growth examination is very difficult and requires a strong DL-based cerebrum cancer investigation framework to help the radiologist's judgment because of the variable morphological construction, cancer appearance in a picture, and enlightenment impacts.

This chapter presents the related works reported in the literature, the methodology employed, results followed by conclusion and future work in the subsequent sections.

RELATED WORKS

Medical image analysis research spans a wide range of topics. These encompass a variety of imaging-related medical specialties, including segmentation, classification, and detection [4 - 8]. There is a requirement for novel ways of highlighting extraction, utilizing little and class-uneven MR imaging datasets of cerebrum malignant growths and cancers from different regions of the human body as companions for mind growth order are constructed [9, 10]. In the literature, binary classifications are crudely investigated to distinguish between benign and malignant tumor occurrences. Support vector machine (SVM) and genetic algorithm (GA) features were investigated by Kharrat *et al*. [11] for the categorization of brain tumors into normal, benign, and malignant groups. The suggested method allows for two-class categorization. It has limitations because new training is needed each time the image database is altered. Abdolmaleki *et al*. [12] constructed a shallow neural network to discriminate between benign and malignant tumors using thirteen distinctive features. These qualities were picked in light of the visual impression of radiologists. Their proposed method had classification accuracy for the harmful and elucidating cancers of 91% and 94%, individually. Papageorgiou *et al*. [13] used fuzzy cognitive mapping to differentiate between low-grade and high-grade gliomas.

Their study exhibited a 90.26% accuracy rate for low-grade brain tumors and a 93.22% accuracy rate for high-grade brain tumors. The feature selection approach was suggested by Zacharaki *et al*. [14] and then used with traditional machine learning. For this, they extracted characteristics such as the tumor's form, level of intensity, and invariant texture. SVM is used for feature selection and tumor classification. Their research had the highest classification accuracy for low- and high-grade gliomas, at 88%. The difficult benchmark dataset [15] of MRI scans of brain cancers, including meningioma, gliomas, and pituitary tumors, was used by several investigations. The picture enlargement utilized as the region of interest (ROI) and the expansion of the growth district in the ring structure are both parts of the multi-phase brain tumor categorization, reported by Cheng *et al*. [16]. Its proposed model was analyzed utilizing three distinct elements, and their precision rate was 82.31%. They performed better overall because of the use of a bag of the word (characteristics, even though the intricacy of the model expanded accordingly). Sultan *et al*. [17] proposed a profound CNN-based cerebrum cancer characterization model and utilized information expansion. They scored 96.13% accuracy in multi-class classification. Ahmet and Muhammad [18] were able to analyze brain tumors with 97.2% accuracy by utilizing a range of different CNN models while employing modified ResNet50 architecture. Khwaldeh *et al*. [19]

CHAPTER 11

IoT-Botnet Detection and Mitigation for Smart Healthcare Systems using Advanced Machine Learning Techniques

S. Jayanthi[1,*] and **A. Valarmathi**[2]

[1] *Department of Computer Science and Engineering, Bit Campus, Anna University, Thiruchirappalli-24, India*

[2] *Department of Computer Applications Bit Campus, Anna University, Thiruchirappalli-24, India*

Abstract: The Internet of Things (IoT) age is quickly evolving, with millions of devices and many more intelligent systems, like healthcare. Attackers mostly aim for these IoT devices. These devices are infected with malware, which turns them into bots that are used by attackers to disrupt networks as well as steal important data. To address this issue, efficient machine learning combined with appropriate feature engineering is proposed to detect and protect the network against vulnerabilities. The proposed model will detect Distributed Denial of Service (DDOS)-based botnet attacks in the smart healthcare system. Hacktivists frequently use DDoS assaults to overwhelm networks and make them unusable. For healthcare providers who depend on network connections to enable efficient patient data access, this can be a serious problem. DDoS attacks are motivated by a social, political, ideological, or economic motive tied to a scenario that enrages cyber threat actors. Two modern Machine Learning (ML) methods, including (i) Support Vector Machine (SVM) and (ii) Light Gradient Boosting Machine (Light GBM), are used to validate the data set. From the extensive experimental analysis, feature-based algorithms are superior to other competing models in that they (i) have the highest detection rate with high accuracy, and (ii) have less computational complexity with minimal training and test time.

Keywords: Botnet, DDOS Attack, IoT, IoT Security, Light GBM, ML Algorithms, Smart Healthcare System, SVM.

INTRODUCTION

The Internet of Things (IoT) is promoting innovation and greater number of smart healthcare gadgets are getting associated with the internet. This permits more gadgets to possibly become botnet gadgets. This chapter aims to utilize the ML method to identify botnet assaults. A botnet comprises a few internet-associated

* **Corresponding author S. Jayanthi:** Department of Computer Science and Engineering, Bit Campus, Anna University, Thiruchirappalli-24, India; E-mail: dharsh02@yahoo.com

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

gadgets that might have been deliberately contaminated with malware from digital programmers. A botnet assault is a kind of malevolent assault that uses a progression of associated PCs to assault or bring down an organization, network gadget or site. It is executed with the sole purpose to upset typical working tasks or corrupt the general assistance of the objective framework [1]. Thus, the effective discovery and anticipation of botnets would have significant importance in PC security. As additional gadgets will possibly be botnet gadgets, the most common way of identifying and detecting these botnet gadgets should be possible utilizing different AI strategies. This section aims to detect botnets or pernicious traffic action on a shrewd medical care framework utilizing the arising ML strategies and give an improvement in accuracy over other related works [2].

Background Methodologies

I. Botnet

Botnet is an organization of various bots intended to bring about noxious exercises to the objective organization which are acquiring order and control conventions by the single unit called bot-herder. Bots are tainted PCs controlled from a distance by the bot-herder with no indication of being hacked and are employed to perform malignant exercises [3]. Hackers spread botnet malware and work secretly with practically no observable sign of their presence and can stay strong and work for quite a long time. The principal component in the botnet is the correspondence of the bot-herder with its related bots. Correspondence with the bots is fundamental to convey orders to the bots to carry out mean acts. Bot-herders generally remain stowed away involving low data transmission and offer secret types of assistance in the botnet network. Bot-herders generally impart orders and control servers to bots. The principal objective of bots is to stay concealed until they are expected to do the allocated undertakings. The existent pattern of a botnet comprises a few phases which includes spreading disease, secondary injection, association, order and control, update and maintenance [4].

II. DDoS attack

The most frequent cyber attack is a DDoS assault, in which many malicious packets are simultaneously sent from attacker’s computer to the target server to overload the target network. DDoS attacks aim to seriously disrupt the target server's regular operations by saturating it with large amounts of traffic, such as false requests, to overwhelm its capacity and cause a disturbance or denial of service to the legitimate traffic [5]. DDoS attacks affect the server's CPU and memory, as well as their ability to overload the network's bandwidth with traffic. As a result, genuine PCs will experience service interruptions while the server is

coping with the DDoS attack. Hackers perform DDoS attacks using a botnet. IoT devices that have been compromised by the malicious software that the attacker distributes online become targets of DDoS attacks. IoT devices that have been infected behave as bots and the attacker uses them to perform DDoS attacks [6].

III. Security vulnerabilities in IoT

Smart gadgets are used in many public and private sectors and are quickly becoming indispensable items for everyday life. So this results in high danger to data privacy. A computerized security system based on machine learning algorithms will be doomed in such a situation. Automated security systems that incorporate machine learning are necessary to stop threats like DDoS attacks, Man-in-the-Middle attacks, botnet attacks, eavesdropping and so forth [7]. Additionally, the majority of low-end IoT devices have inadequate security systems, making them targets for different security attacks or potentially serving as a botnet.

THEME OF WORK

All IoT devices are connected to the server continuously monitoring all devices. If the server has this facility installed, so, if they find any abnormalities in any connection, it immediately removes that device from the connected device. So, the malware should not spread across multiple devices.

LITERATURE REVIEW

IoT-related disciplines have produced a number of works. Researchers are still engaged in this area. IoT security research should be prioritized, according to Mahmud Hossain *et al* ., 2015, there are some unresolved issues in IoT and the IoT devices are insecure because of their limitations in mobility, usability and battery life.

Pahl *et al*., 2018, proposed an IoT service firewall and anomaly detection mechanism. Different microservices have been integrated using clustering techniques BIRCH and K-Means. The distance among various clusters was the same as the standard deviation. The clustering concept is used to update online learning techniques. The author mimics this model and achieves an overall accuracy of 96.3% [7].

By making IoT devices as intelligent as bots, Zhang *et al*., 2015, proposed an IoT defense algorithm that prevents DDoS assault while maintaining a portable and affordable solution. A node examines the consistency of the packet content to

CHAPTER 12

Smart Healthcare Classifier - Skin Lesion Detection using a Revolutionary Light Weight Deep Learning Framework

Sanjay Vasudevan[1,*], Suresh Kumar Nagarajan[2] and **Sarvana Kumar Selvaraj[3]**

[1] *School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India*

[2] *Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil, Tamilnadu, India*

[3] *Department of Computer Science and Engineering, Jain University, Bangalore, India*

Abstract: Skin lesion diagnosis has recently gotten a lot of attention. Physicians spend a lot of time analyzing these skin lesions because of their striking similarities. Clinicians can use a deep learning-based automated classification system to identify the type of skin lesion and enhance the quality of medical services. As deep learning architecture progresses, skin lesion categorization has become a popular study topic. In this work, a modern skin lesion detection system is provided using a new segmentation approach known as wide-ShuffleNet. The entropy-based weighting technique is first computed, and a first-order cumulative moment algorithm is implemented for the skin picture. These illustrations are used to differentiate the lesion from the surrounding area. The type of melanoma is then established by sending the segmentation result into the wide-ShuffleNet, a new deep-learning structure. The proposed technique was evaluated using multiple huge datasets, including ISIC2019 and HAM10000. According to the statistics, EWA and CAFO wide-ShuffleNet are more accurate than the state-of-the-art approaches. The suggested technology is incredibly light, making it ideal for flexible healthcare management.

Keywords: Big Data, Computer Vision, Portable Health Service, Second Machine Intelligence.

INTRODUCTION

Skin cancer, which develops from lesions (abnormal changes in the interstation of the skin), is one of the deadliest forms of cancer. There are two main categories of skin cancer: melanomas and non-melanomas. Death and morbidity rates from melanoma lesions, the worst form of the disease, have skyrocketed in recent years

[*] **Corresponding author Sanjay Vasudevan:** School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India; E-mail: sanjay.researcher@gmail.com

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

[1]. Recovery times can be halved if cancers are detected early [2]. The similarity between various skin lesion types also makes it hard to conduct a thorough screening for melanoma, which can lead to incorrect diagnoses. The problem of inaccurate lesion picture recognition in healthcare [3] and image analysis [4] can be solved by applying machine learning.

With about a million cases of cell carcinoma lesions per year, about 3 million cases of skin lesions that are not melanomas are recorded each year. Approximately 2.5 million people died in 2012 from sun exposure, according to the world health organization. Infections of the skin account for more than 80 percent of all cases of fatal skin cancer [5]. The concept of prostate cancer, and in particular melanoma, was already linked to a history of scorching before this study was conducted. Patients with gliomas have a better prognosis if their tumors are diagnosed at an early stage [6]. In order to account for inter-observer variations, technicians are encouraged to manually diagnose melanoma. Consequently, the accuracy and timeliness of cancer diagnoses are improved by an automated analysis procedure.

Melanoma, especially in its early stages, can have a similar appearance to benign moles (even for qualified dermatologists [7]). Artificial intelligence (AI) and human-made systems have both been offered as possible solutions to these issues.

Border, color, and visual texture were used as early low-level clues to differentiate melanoma from other tumors [8]. However, the results of Celebi *et al.* [9], who also relied on form, color, and texture cues, were subpar because of the significant infraclass similarity between the training and test sets. Segmentation, as explained [10], is another way to get rid of extraneous details and background. The images were first binary-mask partitioned, and then labelled using a support vector machine. The results of using Gabor filter masks to generate thresholding values, like in [11]'s segmentation approach, are usually unsatisfactory.

The second method is the use of artificial intelligence, which has many uses in fields including mining, ecology, and city planning. There are two main categories of artificial intelligence (AI): machine learning and deep learning [12]. [13 - 15] Algorithms capable of data recognition and prediction are the product of machine learning. The various architectures that DL can utilise to probe linked image components and extract features are constantly expanding. Large datasets are no problem for DL, which may be utilised to examine them [16 - 22]. Particularly useful in video and image processing since the advent of multiprocessor unit computers is the deep neural network DL model. A recent study [23 - 25] found that CGI is a useful technique for evaluating bioimages.

Since skin cancer is so common, early diagnosis is essential. Machine analytic approaches are still not commonly applied in therapeutic settings, despite much studies to the contrary. Machine learning and deep learning models confront various challenges, including a shortage of data for correct lesion classifications and the necessity for qualified people to operate the equipment [26]. Therefore, it is crucial to have models that are both reliable and efficient and can run on distributed nodes. Parameter-heavy, desktop-centric deep learning algorithms aren't well suited to mobile devices [27]. Consequently, setting up the infrastructure for a portable device is a challenging task. We detail a novel method for classifying skin lesions that, in contrast to previous approaches, makes use of a few variables without sacrificing accuracy [28]. An example of a system where this method would be useful is a mobile healthcare system. We used a novel wide-ShuffleNet in conjunction with an original segmentation method to detect skin lesions. The proposed method of segmentation outperforms traditional approaches and aids the infrastructure in recognizing the local feature item during classification [29].

Insights gained from this research include the following:

• Combining the entropy-based weighting technique with the first-order cumulative moment algorithm, we present a novel method for segmenting skin images.

• Before moving on to a two-dimensional wide-ShuffleNet network, the point cloud is initially identified using an entropy-based weighting technique and the first-order cumulative moment algorithm. We found that the proposed method outperformed the entropy-based weighting method, the first cumulative instant algorithm, and the full Shuffle Net when it came to accumulating Datasets.

Here is how the rest of the chapter is structured. It discusses previous work, the methodology provided, numerical results, and future directions for study.

RELATED WORKS

KNN is a guided machine learning algorithm for prediction [30]. Accuracy is high using the nearest neighbor method [31]. Another automated skin cancer diagnostic method based on K-nearest neighbors was proposed by Sajid *et al.* [32]. Their method involves applying a median filter to an image and then using other statistical and textural data to reduce noise. Statistical information was gleaned from lesion images, while sensory data was extracted using a discrete wavelet region. This proposed method could also identify potentially cancerous images.

The KNN model's computation-intensive predictions make it inappropriate for use

CHAPTER 13

Recent Trends in Telemedicine, Challenges and Opportunities

S. Kannadhasan[1,*], **R. Nagarajan**[2] and **M. Shanmugananthan**[3]

[1] *Study World College of Engineering Coimbatore, Tamilnadu, India*

[2] *Gnanamani College of Technology, Tamilnadu, India*

[3] *Tamilnadu Government Polytechnic College, Tamilnadu, India*

Abstract: Recent networking advancements in a variety of areas have encouraged the introduction of applications for the Internet of Things (IoT) and Artificial Intelligence (AI). This article analyses the implications of technologies like IoT and AI in Healthcare *via* a careful analysis of 85 peer-reviewed scientific journal publications. The study shows a previously unheard-of rise in the number of publications written in the last ten years, a wide range of publishing sources, a wide range of authors, and several technical papers in philosophy and architecture, all of which point to an evolving field with plenty of room for publication in the years to come. Medical research is currently combining the administration and analysis of telemedicine data as well as the development and use of artificial intelligence in numerous fields and enterprises (AI). Due to the difficulty of implementing telemedicine, it has been required to develop cutting-edge methods and expand its capabilities.

Keywords: Healthcare , Industry Sector, Machine Learning and Applications, Telemedicine.

INTRODUCTION

With the extension of the sharing of patient information to remote patient visits, medical evaluations and procedures, and doctor-patient relationships, the study's objective is to encourage the participation of new researchers in this field by recognizing the fundamental techniques and applications that will enable more telemedicine in their research. In an attempt to reverse the troubling tendency of categorizing raw physiological data, modern machine learning algorithms are being enhanced. In addition to responding to and adapting to the changing social needs and conditions for health, it incorporates new scientific breakthroughs. The main goals of telemedicine were to lessen the communication and coordination

[*] **Corresponding author S. Kannadhasan:** Study World College of Engineering Coimbatore, Tamilnadu, India; E-mail: kannadhasan.ece@gmail.com

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

gaps in the medical industry, as well as the escalating shortages and complicated pricing. Wireless technology has been developed for sensors and applications for case studies, including electronic health records and home monitoring, during the last 10 years. The medical community has conducted a study on the cost and use of this technology, which is included in this. One of the four fields where networks using information and communication technology (ICT) have been developed most extensively is teleradiology, which sends digital radiological images (such as X-ray images) from one site to another [1 - 6].

Clinical evaluations and/or consultations over the phone and/or through video chat are included in telepsychiatry in order to assess and interpret telepresence and video. Digital pathological observations are sent through telepath logy. Telepath logy transmits diagnostic data pertaining to skin issues. Since it has been around for such a long time, artificial intelligence technology is widely employed in a variety of fields. The software can be used in a variety of health care settings, such as creating a system for evaluating patient knowledge to pinpoint error causes and develop remedies for current clinical outcomes as well as streamlining procedures by utilizing computerized knowledge to enhance medical supplies and services [7 - 12].

TELEMEDICINE

Patient monitoring is one of telemedicine's oldest and most popular uses. It provides a simpler, more cost-effective way to carry out typical doctor-to-patient visits to ascertain the patient's current state and clinical results from a distance. This has been designed to resemble face-to-face interaction by using video conferencing and the attachment of interactive medical equipment to gather and monitor the patient's clinical information. Flexibility, convenience, quality, and cost savings over traditional physical patient monitoring is shown in Fig. (**1**). The most current telepresence robot designs are intended to be remotely controlled by a device interface that links the user to the robot through a Wi-Fi connection, enabling the robot to independently roam around hallways and rooms. This newly created method makes use of both AI and visual technologies to enable the traversing of barriers and their identification. The use of telemedicine as a flexible tool may include adding additional patients or choosing the ideal location for a treatment that will have an impact on many people's lives. Artificial intelligence has allowed telemedicine to keep up with developments, but certain problems still need to be resolved. The biggest benefit from these studies would come from their application, thus it is critical to start searching for ways to lower the cost of this technology so that it may be utilized in underdeveloped medical facilities and rural areas.

Fig. (1). Telemedicine in Biomedical Sector.

HEALTHCARE

EHRs were created by Cure because, according to an American College of Physicians survey, doctors spend 80% of their time working at their workstations and utilizing them. By substituting a chat interface for the time-consuming procedure of testing important patients, documenting the findings, and reporting them to the doctor, this device efficiently maintains medical information. It is thus easier to provide prescriptions and other paperwork to the customer, who may also submit directly for assessment images or videos.

It would be challenging to obtain and manage medical data given the large volume of health information acquired not just through manual registration in hospitals but also *via* the growing usage of self-diagnosis technologies. Given that telemedicine attempts to link patients and medical specialists from across the world, it is imperative that all involved organizations create a standardized record-keeping system using state-of-the-art techniques for accurately gathering electronic Healthcare data, such as “big data mining” and “neural networks.” AI is increasingly being used to systematize data recovery and assessment, which often tackles problems with health care systems.

Two significant new advances in robotic technology are the utilization of mechanical support components and the intelligent diagnostic use of patient knowledge and data. Both traits work to support the new Healthcare system by assisting patients-either psychologically or by evaluating the initial medical diagnostic. These methods might be used to deep learning and programmable neural networks. Continuous implementation advances using the data and results connected to the plan. Intelligent diagnostics was used for tele-health self-

CHAPTER 14

Sustainable Development for Smart Healthcare using Privacy-preserving Blockchain-based FL Framework

D. Karthika Renuka[1,*], R. Anusuya[2] and **L. Ashok Kumar[2]**

[1] *Department of IT, PSG College of Technology, Coimbatore, Tamilnadu, India*

[2] *Department of EEE, PSG College of Technology Coimbatore, Tamilnadu, India*

Abstract: Artificial Intelligence (AI) methods need to learn from an adequately large dataset to achieve clinical-grade accuracy and validation, which is vital in the healthcare field. However, sensitive medical data is usually fragmented, and not shared due to security and patient privacy policies. In this context, our work aims at classifying abdominal and chest radiographs by applying Federated Learning (FL) without exchanging patient data. FL framework has been implemented on distributed data across multiple clients. In the framework, a multilayer perceptron is used as a deep learning model for the classification task. FL is a novel approach in which machine learning models are built with the collaboration of multiple clients controlled by a central server or service provider. FL model ensures data privacy and security by retaining the training data decentralized. FL model provides security and privacy for patients by training individual models in distributed clients and sharing merely the model weights.

Keywords: Classification, Deep Learning, Federated Learning, Machine Learning, Privacy-Preserving.

INTRODUCTION

Federated learning is a method for allowing distant clients to build a shared machine-learning technique cooperatively without having to share their training data. Its primary benefit is that it enables the construction of statistical models over long distances while keeping data localized. Although this minimizes data privacy threats, privacy concerns remain because trained model weights or parameters can leak training dataset information [1 - 10]. As a result, developing federated learning algorithms that build high-accuracy models while maintaining

* **Corresponding author D. Karthika Renuka:** Department of IT, PSG College of Technology, Coimbatore, Tamilnadu, India; Tel: 9976128726; E-mail: dkr.it@psgtech.ac.in

privacy is critical. Establishing a federated learning environment, particularly one with confidentiality assurances, is a time-consuming procedure with a variety of variables and parameters. To demonstrate that collaboration is possible and for improving model accuracy, clients must use a simulation framework that preserves privacy and is secure. Giving privacy to sensitive images using deep learning [11] and federated learning algorithms is achieved in this work. To address privacy issues during data sharing, an excellent backup framework will be used to maintain data sharing. Federated learning privacy algorithms with convolutional neural networks (CNN) are used to protect privacy.

In Machine Learning, data is gathered from a variety of edge devices, such as mobile phones, laptops, and other computers and then centralized. Machine Learning systems then use this data and train themselves, eventually predicting outcomes for new data. Google, Amazon, and Microsoft, among others, dominate the AI market with cloud-based AI solutions and APIs. Sensitive user data is transferred to servers where models are trained *via* typical AI approaches. With the increased awareness of user privacy across different devices and platforms, AI developers should not ignore the fact that their model is accessing and using data that is user sensitive.

Federated Learning is the result of the convergence of on-device AI, blockchain [13], and edge computing/IoT [14] technologies. FL can be utilized in the healthcare [15] industry for collaborative analysis. Decentralized training can be done here without any privacy concerns. To tighten privacy, some privacy preservation algorithms can be federated learning. Federated learning can be implemented using several frameworks. To select the best framework for FL implementation, 2 frameworks such as Flower and Pysyft are considered and the best one is chosen. Though federated learning provides some privacy, there may be some issues when updating gradients. So, privacy generally refers to unintentional disclosure of personal information. Privacy is divided into 2 categories. Privacy on the server side and privacy on the client side. Privacy at server side is necessary because when the server broadcasts the aggregated parameters to clients for model synchronizing, this information may leak as there may exist eavesdroppers. The parameters sent from the client to the server should be secured by encrypting it so that an attacker will find it difficult to get information about the user. For privacy protection on the Client-Side, perturbation is done, which adds noise to the shared parameters of the server so that attackers cannot restore the data or at least not be able to get the identity of the user.

CNN and modified auto encoder [16] require much time to analyze information, hyperparameter tuning, and validation of the model well before developing a genuine model in an effort to keep secrecy when analyzing massive data.

Asymmetric cryptosystems make use of the need for more memory. In terms of speed, safety, and energy usage, it is not a good option. The asymmetric approach is extremely complicated and, depending on the energy consumed, more cost.

RELATED WORKS

The growing popularity of in-depth cloud-based learning raises the issue of accurate predictions and data privacy. Previous research has used it to predict privacy in simple neural networks. Since sophisticated neural networks require more than a computer, the existing privacy assumptions schemes do not work well.

A) The article titled "**Blockchain-based federated learning methodologies in smart environments**" [18] suggested the CrowdSFL crowdsourcing technology. The work integrates blockchain with FL and claims to enhance validity, security, and computational time. It does not use a reliable dataset.

B) The article titled "**Secure and Provenance Enhanced Internet of Health Things Framework: A Blockchain Managed Federated Learning Approach**" [19] suggested a cooperative training data sharing system based on games and made the updated model accessible on the blockchain. It provides model training, full dataset encryption, and inference operations. The blockchain aggregates the updated model parameters while each federated edge node executes additive encryption, however, accuracy and loss metrics are poor.

C) The article titled "**End-to-end privacy-preserving deep learning on multi-institutional medical imaging**" [20] created a PRIMIA framework incorporating differentially private federated model training with encrypted aggregation of model updates as well as encrypted remote inference. It evaluates the framework's performance and privacy guarantees and demonstrates that the protections provided prevent the reconstruction of usable data by a gradient-based model inversion attack, but the success of FL models is largely dependent on high data quality.

D) The article titled "**Blockchain-based Privacy-Preserved Federated Learning for Medical Images: A Case Study of COVID-19 CT Scans**" [21] proposed a framework that integrates privacy-preserving federated learning over the decentralized blockchain. It secures the local model through the homomorphic encryption scheme, which helps build an intelligent model without leaking the data provider's privacy and creating trust in the data training process, but it does

CHAPTER 15

Smart Ambulance for Emergency Cases to be Reported to Hospitals at the Earliest using Deep Learning Algorithms and Blockchain-based Distributed Health Record Transactions for smart Cities

V. Kavitha[1,*] and **Partheeban Pon**[2]

[1] *Computer Science and Engineering, University College of Engineering, Kancheepuram, India*

[2] *Computer Science and Engineering, Stella Mary's College of Engineering, Aauthenganvilai, Kanyakumari, India*

Abstract: The everyday eating habits and lifestyle choices that people make have a significant impact on how long they live on the planet. Ancient people ate food that had an acceptable ratio of fat, vitamins, minerals, and carbohydrates, which helped them live a long life. Nowadays, individuals live shorter lives and experience many crises like heart attacks and mental despair that cause them to drive carelessly and cause accidents. This is due to our current diets of junk food and style of life. For the people and the individuals, this results in a tremendous loss. Here, saving people's lives depends largely on the passage of time. The extent of the injury or the patient's emergency situation, the amount of traffic that makes it difficult for the ambulance to reach its destination, and the hospital's capacity to accept patients and save lives are just a few of the many factors that affect the time limitations. In the current situation, hospitals are using the available services to meet time restrictions, which correctly route the ambulance. The main disadvantage of this system is that hospitals handle all the data, making it easy to tamper with medical records and risk losing the integrity of the data. The goal of intelligent ambulances is to forecast the shortest amount of time needed to admit the patient to the local hospitals that have the resources to care for them, preventing the need to transfer patients to other hospitals, as well as to determine the most efficient route to the destination. The patient's life can be saved as a result. The aforementioned can be accomplished by using a deep learning algorithm to predict the injury and the time limit to admit the patient to the hospital, matching the injury with the treatment options available in the hospital and mapping the appropriate hospital, as well as by finding the quickest route with the least amount of traffic to get to the destination within the allotted time limit, giving first aid in the ambulance, and handling the data transfer of health records in a secure manner. Therefore, in a smart city, the smart ambulance can quickly save lives.

[*] **Corresponding author V. Kavitha:** Computer Science and Engineering, University College of Engineering, Kancheepuram, India; Tel: 9487116703; E-mail: kavinayav@gmail.com

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

Keywords: Blockchain, Emergency Systems, e-Health, m-Health, Smart Ambulance.

INTRODUCTION

Emergency calls and responses have recently highlighted characteristics of great stress in India. Millions of calls indicate an issue with emergency call protocols. This has led to a decrease in the percentage of disaster response transportations at the point of impact and lengthier response times when combined with a growing community and budget cuts at the national level. Thus, we highpoint the key problems with providing assistance in emergency and provide a summary of the aforementioned solutions. In order to improve, we create a brand-new method called the Smart Ambulance System (SAS). The main goal of SAS is to help people recover by enhancing communication between victims and first responders. Increasing the capacity of emergency communication while minimising problems with emergency call systems and causing emergency help are the two objectives of employing the most recent technologies and SAS algorithms. Using SAS's complex technologies and algorithms, the emergency response system will be made more profitable while also improving the effectiveness of emergency communication. Through computerised contacts with emergency services and the management of force data stored on a personal smartphone as well as inside tracked data, SAS aims to improve the spoken data effectively and securely, eventually reducing communication backups. SAS places a lot of focus on live communication techniques to improve first conversations between patients and emergency personnel. A predecessor to this approach has developed. A first usability, dependability, and communication performance analysis of the system has been conducted.

One of the major goals of our contemporary civilization is to increase the effectiveness of biomedical and healthcare policy. As a result, it is crucial to offer patients high-quality medical care while also lowering the expense of healthcare assistance and resolving the scarcity of nursing faculty. In fact, in the Knowledge Era of the twenty-first century, we use computational capabilities of all kinds for a variety of daily goals (such as managing household appliances and tracking endurance use), which has led to the collection and transmission of enormous amounts of personal data on a continuous basis. Sadly, reaching someone in an emergency remains a significant challenge despite the sudden surge in technology. This unresolved problem necessitates more rigorous work because it limits the patient's location to a narrow, searchable significant caller who can provide that information to the emergency call operator. We have investigated this issue in depth, digging out layouts that are being tested or that are just starting to take shape and giving them a critical analysis of their approaches.

Sonali *et al.* proposed integrating Blockchain and machine learning algorithms into healthcare in 2019. Health records are extremely sensitive data, thus, Blockchain, which operates on distributed networks and each node has a copy of the distributed ledger, provides transaction security. The transaction's integrity and authenticity are achieved by the hash code. In order to provide secure transactions across all domains, blockchain technology has been applied in the following areas: agricultural domain, funding, money transfer, lending, borrowing, stock market, educational areas, supply chain management, *etc*.

In terms of online or digital transactions, the health care industry has undergone a significant transformation. To access records on a worldwide scale, the health care industry must make billion-dollar investments. Therefore, blockchain technology has a broad application in the health sector. Dr. B. Arunkumar and others used machine learning algorithms to extract pertinent facts for generating intelligent decisions from the raw data. Many Artificial Intelligent apps that are user-friendly and easily incorporated into each person's daily life have been produced as a result of the combination of Machine Learning and Deep Learning Algorithm. To ensure the security of all such applications that conduct business with numerous end users, where the number of healthcare data breaches is significant in 2018 (3 2019 July).

AI *VS* ML *VS* DL

Artificial intelligence is the capacity of a computer to perform functions carried out by humans by adding human intelligence through the process of machine learning. AI can significantly enhance people's lives by advancing technology. Hard challenges that occur around the world can be solved with the help of meaningful interpretation of the raw data. AI is nothing more than a machine-processed emulation of the human intellect, particularly as it relates to computer systems.

Artificial intelligence is a subset that creates machine learning and aids in decision-making. With the aid of deep learning algorithms and machine learning ideas, data science helps to comprehend and analyse raw data. For businesses to succeed, data scientists and analysts need to understand algorithms and be able to evaluate forecasts.

An illustration of the significance of machine learning is shown. Ram likes music with a fast tempo and strong intensity (soaring). Therefore, when a new song is released, we can determine whether Ram likes the music based on the intensity and tempo of the song. When a song with a low speed and light intensity is released, it is obvious that Ram won't like it. But it might be very challenging to determine whether Ram loves a song when it is released because of its medium

CHAPTER 16

Authentication Techniques for Human Monitoring in Closed Environment

V. Vishu[1,*] and **R. Manimegalai**[2]

[1] *Department of Computer Applications, Coimbatore Institute of Technology, Coimbatore, Tamil Nadu 641014, India*

[2] *Department of Computer Science and Engineering, PSG Institute of Technology and Applied Research, Neelambur, Tamil Nadu 641062, India*

Abstract: Human monitoring and trailing in a blocked or closed environment such as a jail or psychological shelter is an important research concern. Industry 4.0 has enabled the monitoring of physically or mentally challenged people in asylums and criminals who are sentenced to serve their terms in jails with various tools such as sensors, wireless systems and sophisticated cameras. The hidden nature of monitoring and reporting in closed environments without any new technologies such as IoT, RFID, *etc*., may lead to ill-treatment of the inmates in the above-mentioned places. The traditional physical monitoring system can end up with wrong reports about the inmates and can hide the real scenarios. Personal opinions and characteristics of officials as well as the prisoners may vary based on their health and behavioral patterns. The automation of human monitoring involves monitoring of security, activity, fitness, and health factors of the inmates in the closed environment. The human-activity monitoring is carried out by acquiring and analyzing the body signals of the inmates. Passive tags are attached to the wristband of each person in the RFID human monitoring systems. Minimal human intervention and effort is one of the biggest advantages of the human monitoring system. Authentication, intelligent decision making and minimum use of resources are the main challenges in designing a human monitoring system. Intelligent decision making algorithms are applied to predict human behavioral patterns. This work gives a summary of different authentication protocols and methodologies used with the Internet of Things (IoT) and RFID devices in human monitoring systems. It presents the components and infrastructure of a typical human monitoring system and summarizes the sensors and IoT devices used for the same. A wide investigation is conducted on security and privacy issues while storing the private and confidential details of the inmates. A comprehensive survey on different authentication techniques and data security issues in closed human monitoring is presented in this work.

Keywords: Authentication, Closed Human Monitoring, IoT, RF-ID, Sensors.

[*] **Corresponding author V. Vishu:** Department of Computer Applications, Coimbatore Institute of Technology, Coimbatore, Tamil Nadu 641014, India; E-mail: vishu.cta.cit@gmail.com

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

INTRODUCTION

Human Monitoring system provides intelligent information and alerts to the users through the control devices such as Radio Frequency Identification (RFID), IoT and sensors. In traditional human monitoring systems, the limited access to the stored data in human monitoring systems at remote locations may lead to ill-treatment of the inmates [1]. The design of human monitoring system becomes more challenging for analyzing the data received from wearable sensors and devices. As the data handled by monitoring systems are sensitive and private, there is a need for more efficient authentication techniques. IoT and sensors play a major role in improving the security and prediction of human activities accurately. The values from sensors, RFID tags and IoT devices create the percept history and are combined to propose a key which is used in authentication and decision making, as shown in Fig. (**1**).

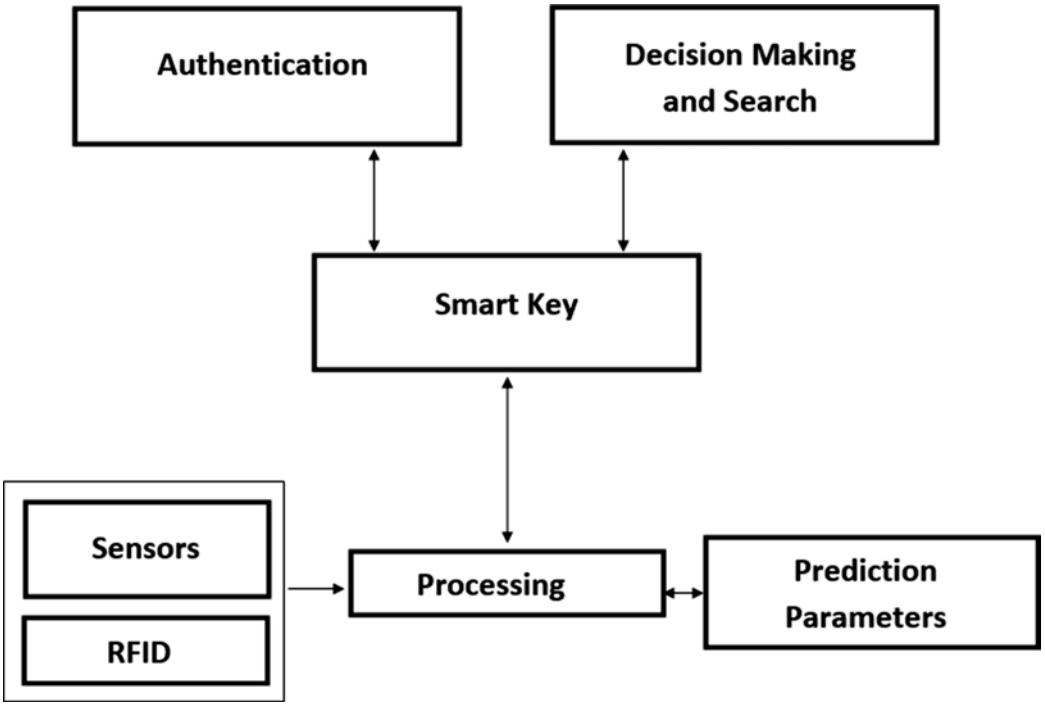

Fig. (1). Block Diagram of a Typical Human Monitoring System.

The human monitoring techniques have high computation and communication costs and are prone to a range of known attacks, which decrease their significance for applicability in real-world environments. There are various techniques for performing authentication, such as the use of text passwords or cipher texts. The combination of one or two authentication, called multi-factor authentication, is also one of the best solutions in the human monitoring environment [2]. Intelligent agents facilitate the prediction of physical and mental condition and behaviors of the inmates. Alarms are produced based on age, deceases, and unusual activities. RFID tag traces the inmate's physical and health conditions and recognizes the presence of any electronic device. When an inmate leaves a region, the nearby RFID reader beside the door scans the tags connected to the wristband and generates an alarm if the entry is limited to the particular inmate. Intelligent sensors and readers are placed in each entrance and common areas. Once the antenna identifies a passive tag, the RFID reader finds the position and reminds the officials with a message or voice through the interactive podium [3].

RADIO FREQUENCY IDENTIFICATION IN HUMAN MONITORING

Radio Frequency Identification (RFID) technology uses radio frequency signals to acquire data dynamically from tags within reading range. The data is then used for a variety of purposes, such as opening doors and gates, paying tolls, tracking equipment, materials and human beings. The RFID system consists of a reader and a transponder component called a tag, which is associated with the corresponding object. Tags are classified into passive tags and active tags [4]. The RFID systems are designed based on the transmission of radio signals. Identification of human beings is done on the basis of a unique identifier, which is stored on the tag. RFID tags are used in various environments, such as water, dust, oil *etc*. It is possible to read multiple RFID tags simultaneously through multiple objects. RFID tags are devices that contain identification and other information that is communicated to a reader from a distance [5].

An RFID tag is a microchip combined with an antenna and is packaged so that it can be attached to the human body. The reader is connected to the power source and a COM port and connected to server machines. RS 232 protocol is used to enable serial communication and Putty is used for the interface between transmitter and receiver [6]. The reader network commands such as DHCP, IP address, Net mask, Gateway, and DNS are used for interactive and autonomous mode communication. The interactive mode uses active tags, whereas the autonomous mode uses the continuous conversation style. Various triggers are incorporated in the alien RFID readers. Notifications are made whenever a new tag comes into visibility, addition and deletion of tags, and customizing the tag values. Notifications are generated from a reader in different formats, such as

ABBREVIATION

AR	Augmented Reality
AI	Artificial Intelligence
ANN	Artificial Neural Network
ABE	Attribute-Based Encryption
API	Application Programming Interface
AHS	Artificial Healthcare System
AV	Autonomous Vehicle
BIoT	Blockchain of Things
BK	Binary Key
BT	Blockchain Technology
BMI	Body Mass Index
BFT	Byzantine Fault Tolerance
BCCOT	Blockchain Technology and Cloud of Things
BCIOT	Blockchain Technology and Internet of Things
BCTFOT	Blockchain Technology and Fog of Things
BASN	Body Area Sensor Networks
CNN	Convolutional Neural Networks
CT	Computed Tomography
COPD	Chronic Bronchitis and Emphysema
CC	Cloud Computing
CoIn	Computational Intelligence
CADx	Computer-aided Diagnosis
CAT	Computed Tomography
CPS	Cyber-Physical Systems
CORE	Common Open Research Emulator
DS	Digital Signature
DLT	Distributed Ledger Technology
DDoS	Distributed Denial-of-Service
DEX	Decentralized Exchange
DAG	Directed Acyclic Graph
DPoW	Delegated Proof of Work
DP	Decryption Process

DTC Depository Trust Company
DL Deep learning
DRE Rigital Rectal Examination
DP Differential Privacy
DNN Deep Neural Networks
EHD Electronic Health Records
EHRs Electronic Health Data
EMR Electronic Medical Record
EP Encryption Process
EVM Ethereum Virtual Machine
ECDSA Elliptic Curve Digital Signature Algorithm
EPC Electronic Product Code
FL Federated Learning
FedAvg Federated Averaging
GA Genetic Algorithm
GDPR General Data Protection Regulation
G2V Grid to Vehicle
HIPAA Health Insurance Portability and Accountability Act
H-CoIn Hybrid CoIn
HLF Hyperledger Fabric
IoT Internet of Things
IoE Internet of Everything
IoMT Internet of Medical Things
ICT Information and Communication Technology
IPFS Interplanetary File System
KG Key Generation
KGP Key Generation Process
LAN Local Area Network
LightGBM Light Gradient Boosting Machine
LR Logistic Regression
LEA Lightweight Encryption Algorithm
LSTM Long Short-Term Memory
MRI Magnetic Resonance Imaging
ML Machine Learning
MLP Multi-Layer Perceptron

M2M Machine-to-Machine
MAS Multi
NC Nanocrystalline
NOS Network Operating System
NFV Network Function Virtualization
OBU On Board Unit
Pow Proof of Work
PoS Proof of Stake
PoA Proof of Authority
P2P Peer to Peer
PoET Proof of Elapsed Time
PKI Private/public Key Infrastructure
PSA Prostate-Specific Antigen
PKC Public Key Cryptograph
PoET Proof of Elapsed Time
PCA Patient Centric Agent
PoBT Proof of Block Trade
QoS Quality of Service
RFID Radio-Frequency Identification
ROI Return on Investment
RL Read Latency
RPM Remote Patient Monitoring
SQL Structured Query Language
SVM Support Vector Machine
SAS Smart Ambulance System
SAT Security Access Token
SGX Intel Software Guard Extensions
SWF Simple Workflow Services
SC Smart Contract
SDN Software Defined Network
TRT Transaction and Read Throughput
TRL Transaction and Read Latency
UHF Ultra High Frequency
VANET Vehicular Distributed Ad-hoc
VR Virtual Reality
V2G Vehicle to Grid
WSN Wireless Sensor Network

SUBJECT INDEX

A

B

L. Ashok Kumar, D. Karthika Renuka, Sonali Agarwal & Sheng-Lung Peng (Eds.)

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W

L. Ashok Kumar

Prof. L. Ashok Kumar was a postdoctoral research fellow from San Diego State University. California. He was selected among seven scientists in India for the BHAVAN Fellowship from the Indo-US Science and Technology Forum and also, he received the SYST Fellowship from DST, Govt. of India. He has 3 years of industrial experience and 22 years of academic and research experience. He has published 173 technical papers in international and national journals and presented 167 papers in national and international conferences. He has completed 26 Govt. of India funded projects worth about 15 crores and currently 9 projects are in progress worth about 12 crores. He has developed 27 products and out of that 23 products have been technology transferred to industries and for government funding agencies. His Ph.D. work on wearable electronics earned him a National Award from 1STE and he has received 26 awards in the national and international level. He has guided 92 graduate and postgraduate projects. He has produced 6 Ph.D. scholars and 12 candidates are doing Ph.D. under his supervision. He has visited many countries for institute industry collaboration and as a keynote speaker. He has been an invited speaker in 345 programs. Also, he has organized 102 events, including conferences, workshops, and seminars. He is a Certified Chartered Engineer and BSI Certified ISO 50001 2008 lead auditor. He has authored 19 books in his areas of interest published by Springer, CRC Press, Elsevier, Nova Publishers, Cambridge University Press, Wiley, Lambert Publishing and IGI Global. He has 11 patents, one Design patent and two copyrights to his credit and also contributed 18 chapters in various books. He is also the chairman of Indian Association of Energy Management Professionals and Executive Member in institution of Engineers, Coimbatore Executive Council Member at the Institute of Smart Structure and Systems. Bangalore, Associate Member in CODISSIA. He is also holding prestigious positions at various national and international forums and he is a fellow member in IET (UK), fellow member at IETE, fellow member IE and senior member at IEEE.

D. Karthika Renuka

Prof. D. Karthika Renuka is a professor in the Department of Information Technology at PSG College of Technology. Her professional career of 20 years has been with PSG College of Technology since 2004. She is an associate dean (Students Welfare) and convener for the Students Welfare Committee in PSG College of Technology. She is a recipient of Indo-U.S. Fellowship for Women in STEMM (WISTEMM)-supported by the DST, Govt. of India and implemented by the IUSSTF. She was a Postdoctoral Research Fellow from Wright State University, Ohio, USA. Her area of specialization includes data mining, evolutionary algorithms, soft computing, machine learning and deep learning, affective computing, computer visions". She is currently guiding 8 research scholars for their Ph.D. under Anna University. She has published several papers in reputed national and international journals and conferences.

Sonali Agarwal

Prof. Sonali Agarwal is working as an associate professor in the Information Technology Department of Indian Institute of Information Technology (IIIT), Allahabad, India. She received her Ph. D. Degree at IIIT Allahabad and joined as faculty at IIIT Allahabad, where she has been teaching since October 2009. She holds a bachelor of engineering (B.E.) degree in Electrical Engineering from Bhilai Institute of Technology, Bhilai, (C.G.) India and masters of engineering (M.E.) degree in computer science from Motilal Nehru National Institute of Technology (MNNIT), Allahabad, India. She has attended many national and international conferences/workshops and she has more than 70 research papers in the national / international journals and conferences. She has completed her masters thesis work at Liverpool John Moores University (LJMU), Liverpool, U.K. during November 1999 to February 2000 under Indo-UK REC Project, a collaboration in between School of Computing & Mathematical Science, LJMU Liverpool UK and Motilal Nehru National Institute of Technology, Allahabad. She has also visited Thailand and Sri-Lanka for attending/organizing international level conferences/workshops. She has also been a member of IEEE, ACM, CSI and supervised three Ph.D. scholars and several graduate and undergraduate students in big data mining and stream analytics domain.

Sheng-Lung Peng

Prof. Sheng-Lung Peng is a Professor in the Department of Creative Technologies and Product Design, and the dean of the College of Innovative Design and Management, National Taipei University of Business, Taiwan. He received PhD in computer science from the National Tsing Hua University, Taiwan. He is an honorary professor of Beijing Information Science and Technology University, China, and a visiting professor of Ningxia Institute of Science and Technology, China. He is also an adjunct professor of Mandsaur University and Kazi Nazrul University, India. He has edited several special issues of journals, such as, Frontiers in Public Health, Journal of Internet Technology, IEEE Internet of Things Magazine, Computers and Electrical Engineering, Sensors, and so on. His research interests are in the design and analysis of algorithms in the fields of bioinformatics, combinatorics, data mining and networking.