Mesopotamian journal of Computer Science
Vol.2024, **pp**. 1–14
DOI: https://doi.org/10.58496/MJCSC/2024/001; ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Research Article

An Extensive Examination of the IoT and Blockchain Technologies in Relation to their Applications in the Healthcare Industry

Karthik Kumar Vaigandla [1,*], Madhu Kumar Vanteru [1], Mounika Siluveru [1]

[1] *Assistant Professor , Electronics and Communications Engineering, Balaji Institute of Technology and Science, Telangana, India.*

ARTICLE INFO

Article History

Received 17 Oct 2023
Accepted 20 Dec 2023
Published 14 Jan 2024

Keywords

Blockchain technology
healthcare
health monitoring
industries
IoT
security
privacy

ABSTRACT

Numerous domains have been transformed by the communication technologies made possible by the Internet of Things (IoT), one of which is health monitoring systems. Patterns associated with diseases and health conditions can be identified through the utilization of machine learning and cutting-edge AI techniques. Currently, scientific endeavours are concentrated on enhancing IoT-enabled applications such as medical report administration, prescription traceability, and infectious disease surveillance through the amalgamation of blockchain technology(BCT) and machine learning(ML) models. Although recent advancements have attempted to increase the adaptability of blockchain(BC) and ML for IoT applications, there are still a number of crucial considerations that must be made for improved outcomes. This report provides a comprehensive examination of emerging technologies in the healthcare sector, encompassing the IoT, and blockchain.

1. INTRODUCTION

The concept of the IoT revolves on the idea that any device, regardless of its location, may connect to any service, at any moment, and across any network. A next-generation technology super trend, the IoT may have an impact on every market. It's essentially the same as connecting easily identifiable smart objects and devices to the current internet infrastructure, but with far-reaching benefits. One of the common benefits is that these items can talk to each other in ways that aren't limited to M2M connections. Consequently, almost every industry might benefit from some kind of automation. There are several fields that potentially benefit from the IoT, including smart cities, transportation, waste management, security, logistics, retail, industrial control, healthcare, and catastrophe services [1]. The medical and healthcare sectors emerge as particularly auspicious applications of the Internet of Things. Numerous novel medical applications may arise due to the Internet of Things, encompassing fitness programmes, remote health surveillance, care for the geriatric, and chronic illness management. A further significant potential application is to ensure medication and treatment regimen adherence among patients and healthcare professionals. Consequently, numerous medical devices, diagnostic and imaging instruments, and sensors may be regarded as intelligent objects that are fundamental components of the IoT. It is hypothesized that IoT-based healthcare services would enhance the user experience, reduce costs, and improve quality of life. The IoT presents healthcare professionals with the opportunity to reduce device downtime through the implementation of remote provisioning. Additionally, the IoT is capable of precisely determining when various devices require resupply of their components to continue operating continuously and without interruption. Additionally, the Internet of Things facilitates more efficient allocation of limited resources, enabling the provision of the same standard of care to a greater number of patients.

Recent research has been concentrated on this domain with the aim of comprehending the potential of the IoT in the healthcare sector and addressing the numerous pragmatic challenges that have emerged as a consequence [2]. As a consequence, an abundance of associated products and services, including prototypes, were created. In the realm of IoT health care research, forthcoming subjects comprise network architectures and platforms, security, interoperability, and novel services and applications. Furthermore, a number of countries and international organizations have enacted policies and guidelines governing the implementation of IoT technology within the healthcare industry. The healthcare industry, however,

*Corresponding author. Email: vkvaigandla@gmail.com

is still in its infancy with regard to IoT implementation. Stakeholders with a vested interest in further investigation should presently possess a comprehensive understanding of the extant literature concerning the IoT in healthcare environments [3]. With the intention of transforming healthcare technology through the development of the IoT, this article examines current trends in IoT-based healthcare research and identifies a number of obstacles that must be surmounted.

The potential for blockchain technology to significantly transform healthcare data exchange lies in its ability to enhance the security and efficiency of electronic medical records (EMRs). Electronic health records (EHRs) contain critical, sensitive personal information for the treatment and diagnosis of patients. By placing patients at the centre of the system and enhancing data management, information sharing, security, privacy, interoperability, and monitoring of health data, BCT has the potential to revolutionize healthcare. BCT is highly suitable for implementation in the healthcare sector due to its numerous advantageous attributes, which encompass immutability, decentralization, transparency, and traceability. A "blockchain" is a decentralized and unique distributed ledger that contains the logs of every transaction executed by every participant in the network. Blockchain, a distributed ledger system, enables peer-to-peer (P2P) networked digital data transactions that can be shared publicly or privately among all users. This enables the secure and reliable storage of data in any format. The concept of blockchain technology eliminates the requirement for a trusted third party in the implementation of transactions between multiple parties in a dependable manner. In recent years, BCT has been implemented in a variety of industries, including finance, e-healthcare, public serviceability, asset management, government policy, logistics, real estate, and supply chain management, according to Zheng et al. [4]. In the realm of safeguarding data and maintaining medical records, the healthcare industry has achieved remarkable progress through the implementation of blockchain applications. Furthermore, the utilization of blockchain technology in conventional medical practices to diagnose and treat maladies is enhancing efficacy, owing to the secure exchange of data that takes place. Undoubtedly, blockchain technology will be utilized in the future to legitimize, personalize, and protect healthcare by securely incorporating and exchanging data from medical records. IoT, ML, and BC-based applications in healthcare are shown in Figure 1.

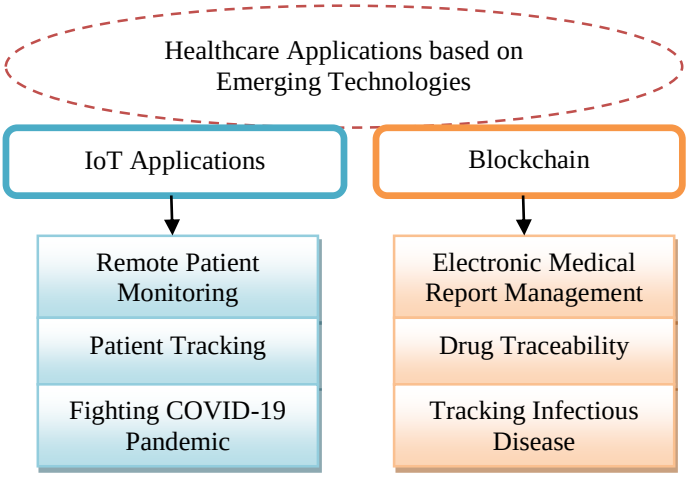

Fig.1. Applications in the healthcare sector that use IoT and BCT

Since its inception a decade ago, alternative iterations of the blockchain have been made public. Initially, blockchain technology was implemented to monitor digital assets in financial transactions. The healthcare industry is brimming with potential and enthusiasm. Blockchain technology is transforming the governance and management of healthcare data. This is primarily due to its capability of securely segmenting and modifying medical data and services in an innovative manner during transmission and adaptation [5]. Healthcare is one sector where blockchain technology is already creating ripples. Existing systems in the fields of medicine and healthcare merely exchange health resources without completely conforming to external systems. However, an increasing body of evidence suggests that these networks have the potential to significantly enhance healthcare delivery through the facilitation of communication and collaboration among academicians and organizations specializing in health informatics. Consolidating and safeguarding the vast quantities of health data generated through routine activities, commercial dealings, and the provision of services poses a formidable obstacle for the healthcare sector. The majority of health records lack standardization across systems, are difficult to comprehend, manage, and share, and are not readily accessible. Academic institutions and IT organizations collaborate in order to develop sustainable solutions by studying and enhancing IoT technologies, owing to the IoT's immense economic potential. In the past few decades, numerous free and paid plans have been introduced, but the inflexibility of IoT application development platforms means that these technologies utilize a large number of distinct data formats, exacerbating the already severe problem of heterogeneity. Consequently, an increasing demand has emerged for enhanced network administration solutions capable of

effectively handling the enormous volumes of data generated by this integrated system. Edge computing solutions are essential for data analysis in order to enhance the services provided by IoT technologies, given the inadequacy of the current paradigm of centralized processing and data storage [6]. IoT big data solutions, which represent a paradigm shift, enable the development of practical applications from the vast quantities of data generated by numerous IoT devices. The IoT introduces a multitude of challenges and opportunities, and numerous research proposals have been put forth to tackle these complexities and attributes. Regarding IoT technology, privacy and security are the most urgent concerns from a research standpoint. Integration of the IoT with the cloud, standardization of the IoT, development of a scalable architecture for the IoT, and security assurance of the IoT are additional challenges. Additionally, security concerns, QoS management, and internet applications were not exhaustively addressed in the prior IoT literature.

2. BLOCKCHAIN

Blockchain is recognized as a public ledger and a different sort of database, apart from conventional databases like relational databases. In contrast, blockchain technology securely stores information by organizing it into blocks and linking them together using cryptographic signatures inside a decentralized network. Once new data is gathered, it is then processed via a fresh block. The essential qualities of blockchain are its durability, anonymity, traceability, and decentralization. Blockchain is used in the financial industry for several purposes such as digital assets, remittance, and online payment systems. Blockchain has recently been used in developing technologies, including IoT-based public and security services. Furthermore, organizations use blockchain technology to enhance dependability and security, hence enticing consumers. In addition, blockchain has the ability to circumvent the problem of a single point of failure due to its distributed nature. Blockchain is recognized as a public ledger and a distinct sort of database, differing from conventional relational databases that store data[7]. Contrarily, blockchain technology stores information by grouping it into blocks and then connecting them using digital signatures within a decentralized network. As further data is received, it is transferred to a new block. The distributed consensus and asymmetric cryptography techniques have been used to attain comprehensive system dependability, ledger uniformity, and user protection. Furthermore, BCT has many crucial characteristics, including durability, anonymity, verifiability, and decentralization. These characteristics have the potential to greatly decrease expenses and improve effectiveness. Blockchain technology is used by many financial services, such as digital assets, remittance, and online payment systems. Furthermore, BC has the potential to be used in other domains, including IoT, public services, and security services [8]. Once transactions are recorded on the ledger, they are immutable due to the unalterable nature of the blockchain. Organizations use blockchain technology to enhance dependability and security, hence enticing clients. In addition, blockchain has the ability to disregard the problem of a single point of failure because to its distributed nature. Currently, advanced methodologies have made significant progress in exploring the compatibility of BC with ML in IoT applications. The security of IoT and network applications has been addressed by using procedures that rely on BCT. Moreover, ML algorithms use extensive data gathered from sensing devices to forecast and categories various issues [9]. ML algorithms, in conjunction with sophisticated artificial intelligence(AI) approaches, identify and analyze patterns within datasets. IoT-enabled apps combine BCT with ML models to enhance medical report management, prescription traceability, and monitoring of infectious illnesses, among other benefits.

2.1 Blockchain benefits

Figure 2 shows that blockchain technology has increased advantages for both patients and healthcare providers by making the industry more transparent and facilitating better communication. The healthcare industry is now focused on using contemporary technologies to enhance the efficacy and efficiency of healthcare systems. Here we show how blockchain technology has several uses in the healthcare industry. Decentralization : Unlike conventional databases, which are overseen by a single authority, blockchains are decentralized and built on a time-stamped record ledger that is cryptographically secured against tampering and fraud. The term "decentralization" is used in relation to blockchain technology to explain the transfer of power away from a single authority and towards a dispersed network. The decentralized storage system is the backbone of this innovation; it strengthens the system's security and authentication of stored data. In addition to the transaction data and the cryptographic hash of the preceding block, each block also contains a timestamp. To build a chain or network, it also stores details of all transactions and blocks that came before it. It just takes a change to one block's contents for the whole blockchain to become paralyzed by a domino effect. Every node in the network will lock at the same time when the blockchain has processed the data, creating a record of the transaction that cannot be changed. How and by whom blocks are added to the network is defined by each blockchain system.

Trust and transparency : Once the new block has been properly added to the blockchain, it will be dispersed to all participants. The data block is deleted instead of added to the blockchain if it is deemed invalid. In order to ensure that a data block is legitimate, participants use validation processes called consensus procedures. Through the use of consensus

procedures, participants may quickly reach a collective agreement about the data block's authenticity. It is easy to update the data captured and kept on the blockchain, and potential users may view it. The immutability of the blockchain could make it impossible to alter or steal data.

Security and privacy : Data and transaction records stored in a "block" are safeguarded by a technique known as a "blockchain" against intrusion from any source, whether deliberate or not. It is common practice to use the security and IT policies, procedures, and technologies to identify potential threats, thwart them, and respond appropriately when they do occur. A stakeholder or group's capacity to separate themselves from data and communicate in a recognizable way is what we mean when we talk about blockchain privacy [5,7]. Ability to deal without disclosing private information is what it entails. Users may also carefully self-divulgate, which helps them maintain compliance.

Availability and robustness : The BCT is very secure. The BCT holds standardized healthcare data throughout the network and does not have a central authority, eliminating the possibility of a single point of failure. By using the capabilities of all participating nodes and eliminating many-to-one traffic flows, the lack of centralized authority ensures flexibility and resilience. Moreover, this method eliminates any delays and resolves the problem of a single unsuccessful phase.

Verifiability : The data is securely kept on the blockchain with both integrity and correctness, allowing for validation without the need to access the plaintext of the records. This functionality is particularly useful in the healthcare industry, where it is necessary to authenticate documents, such as overseeing the pharmaceutical supply chain and handling insurance claims. Healthcare information components are readily verifiable and available to all network participants using digital ledger technology, enabling multiple instances of sharing across all blockchain nodes. Blockchains provide data integrity and file synchronization via automated updates at regular intervals [5].

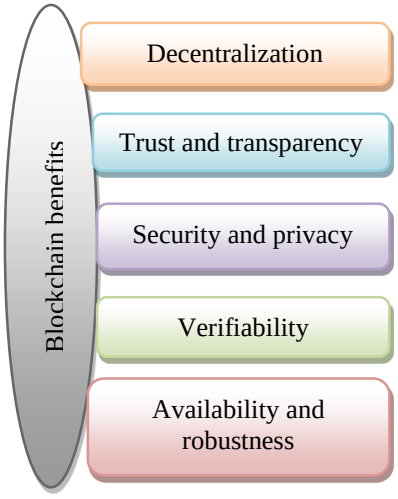

Fig.2. Blockchain benefits

2.2 Blockchain Based Applications in Healthcare

The BCT offers a wide range of applications in the healthcare industry. It helps ensure the safe transfer of patient medical data and also helps preserve the integrity of the drug supply chain. This solution uses a public blockchain that ensures both secrecy and authenticity. The suggested method effectively manages the issue of single point failure. This paper presents a groundbreaking research study on EMR management systems, specifically focusing on the challenges of scalability and data encryption. However, the suggested approach still encounters some limitations. Liang et al. [10] introduced a mobile application designed to gather patient data and facilitate its exchange across medical teams, insurance companies, and patients. A proprietary BC was used as a resolution for confidentiality and restriction of entry. The suggested solution also addressed the issues of efficiency and scalability in data processing. Several study articles have been suggested to oversee and track data related to health and medical items. For example, proposals were made to integrate medication supply chains using blockchain technology during transit. Bocek et al. [11] developed a system using the Ethereum blockchain to store data related to the drug supply chain. This method ensures that the data is publicly accessible and cannot be altered. This

system incorporates thermal sensitive sensors to distribute temperature data during the transportation of medicinal goods. A smart contract establishes a regulation for precise temperature specifications and verifies the input of temperature data for each new shipment. Huang et al. [12] proposed a blockchain-based medication ledger system designed for the purpose of tracking and regulating medicinal products. The figure 3 illustrates the sequential steps involved in the implementation of healthcare applications based on BCT. The process consists of four primary layers: healthcare raw data, BCT, healthcare application, and stakeholders. The decentralized nature of BCT allows for different stakeholders to get benefits from healthcare applications.

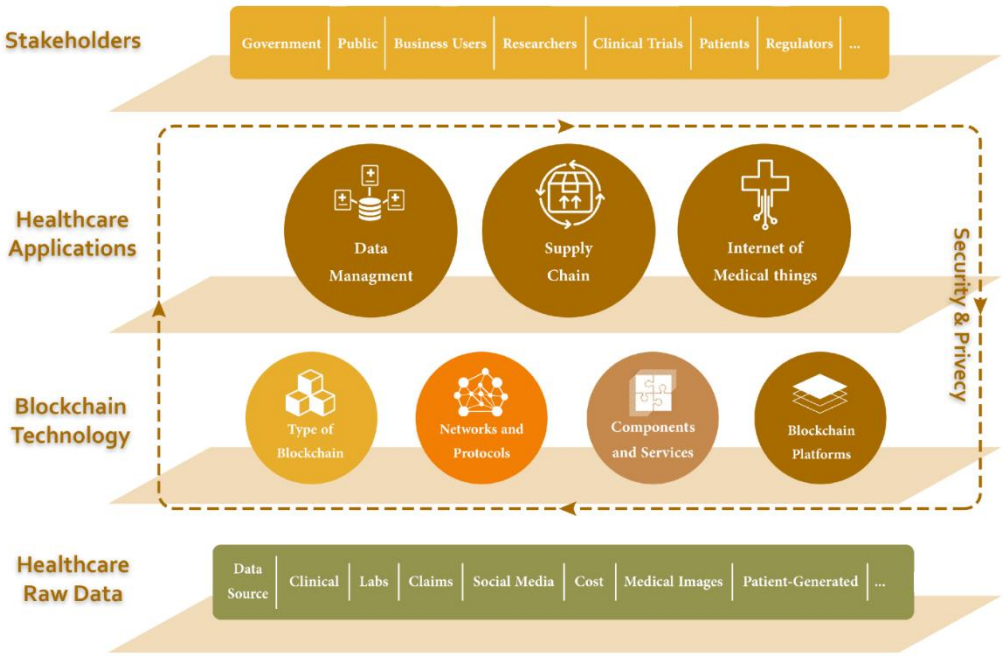

Fig.3. A visual depiction of a process for healthcare applications that use BCT

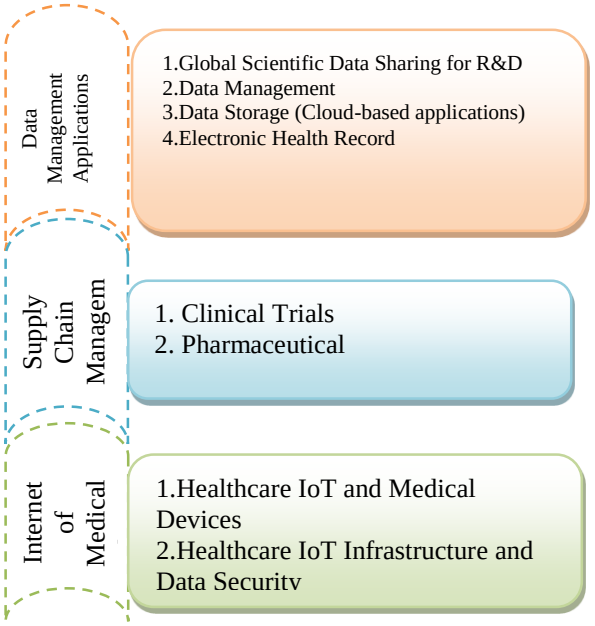

Fig.4. Blockchain-based healthcare applications.

Figure 4 depicts the use of BCT in healthcare. At the highest level of the hierarchy is the stakeholder layer, including individuals and groups who get benefits from healthcare applications based on blockchain technology, including business users, researchers, and patients. The primary considerations of users at this level are to efficiently distribute, manipulate, and oversee data while safeguarding its security and privacy. The advancements in electronic health-related data, cloud-based healthcare data storage, and legislation for protecting patient data privacy have created new possibilities for managing health data. Additionally, these advancements have made it more convenient for patients to access and share their health data. Ensuring the security and integrity of data, storage, and transactions, as well as effectively managing their seamless integration, are very useful to any organization that relies on data. This is particularly important in the healthcare industry, where BCT has the ability to address these crucial challenges in a strong and efficient manner. Sharing healthcare and medical data is a crucial step in enhancing the quality of healthcare providers and making the healthcare system more intelligent. Health records may be shared among persons. For example, a patient who want to disclose their medical history to a doctor on their first encounter. Furthermore, sharing may occur between a person and a stakeholder, such as a patient disclosing their medical information to an insurance company or a research institution. Data sharing may extend beyond international boundaries. Nevertheless, the current operating mechanism of health-related systems has some constraints. A significant constraint is the limited accessibility of patients to their health records. Consequently, people are unaware of the dissemination of their personal health information to unfamiliar entities [13]. BCT has the potential to significantly enhance the connection and cooperation with the healthcare sector by providing a secure and efficient method for exchanging electronic health data. This is regarded as one of the most essential contributions of healthcare based on BCT.

Fig. 5. Major Applications of BCT in Healthcare

3. INTERNET OF THINGS (IOT)

The IoT connects a vast number of physical items via communication technologies, leading to significant advancements in numerous scientific fields. The fundamental objective of IoT technologies is to provide information services, comprehend cognitive activities, and exert control over the physical environment via an equal number of connections between the main and edge networks. The IoT combines cloud computing, sensor networks, electronic devices, and mobile services using sophisticated frameworks and information processing technologies[14-15]. It is often believed that IoT enables the connection of personal computers, tablets, smartphones, telephones, and servers. However, IoT really links sensors and actuators that are included in digital devices. Typically, all these devices are linked to the same internet protocol (IP). IoT systems include a range of technologies such as smart home security, wireless inventory trackers, biometric scanners, and smart tennis rackets. These devices produce vast amounts of data that may be analyzed using statistical and machine learning techniques. Blockchain technology is integrated with Internet of Things (IoT) applications across many sectors, including insurance, education, healthcare, voting, and stock market. Blockchain is mostly used in smart cities, where many IoT devices are strategically deployed across various areas. Integrating BC with IoT technology enhances scalability, efficiency, resilience, time efficiency, and computational cost efficiency [16]. The IoT produces data that may be kept inside a blockchain, which is overseen by computers housed in the cloud. Authenticated users may securely get their private data from cloud databases. IoT systems use unique internet protocol (IP) addresses to identify integrated devices, using both transmission control protocol (TCP) and non-TCP protocols. Device virtualization refers to the practice of virtualizing electrical equipment, such as actuators and sensors, into virtual objects. The Internet of Things (IoT) combines virtual items and electrical devices using several communication protocols, including WiFi, ZigBee, LoRaWAN, BLE, and Z-Wave. The IoT devices possess a sufficient configuration and interfaces that may be accessed remotely. The most recent research and development in the field of IoT has introduced many new terms and ideas. These include AIoT (artificial-intelligence-enabled

IoT), IoA (Internet of Anything), IoE (Internet of Everything), IIoT (Industrial IoT), SIoT (Social IoT), WoT (Web of Things), and M2M.

BLE, or Bluetooth Low Energy, is an upgraded iteration of Bluetooth, a popular wireless technology that allows for reliable connections within a range of 10 metres. The most recent iteration of Bluetooth, version 5.2, introduces an enhanced profile for supporting IP. Studies indicate that BLE is a well-established and enhanced technique for IoT devices. WiFi is a prevalent internet protocol that facilitates communication between IoT devices and physical equipment. The effective range of communication between most electrical devices is around 50 metres, which is five times larger than the communication range of BLE [17-19]. ZigBee is a short-range wireless technology that uses a protocol to send data at a rate of 250 kbps. ZigBee is the most suitable technology for efficiently transmitting data between IoT devices because of its strong security measures, capacity to handle large amounts of data, low energy use, and long-lasting performance. Z-Wave is a wireless communication protocol designed for automation systems, such as sensors and lighting controllers, that operates on low-power frequencies. Z-wave utilizes a communication system that may operate within a range of 30-100 metres. In comparison to other protocols like WiFi, Bluetooth, and ZigBee, Z-wave is considered superior. The LoRaWAN protocol facilitates the networking of electrically powered IoT devices across vast distances, with low power consumption. It detects the amplitude of signals based on a specified threshold range [17-19]. LoRaWAN is used in applications that need the integration of a large number of devices for the safe exchange of data utilizing memory, while also requiring minimum power consumption. These applications include smart cities, smart hospitals, and smart homes.

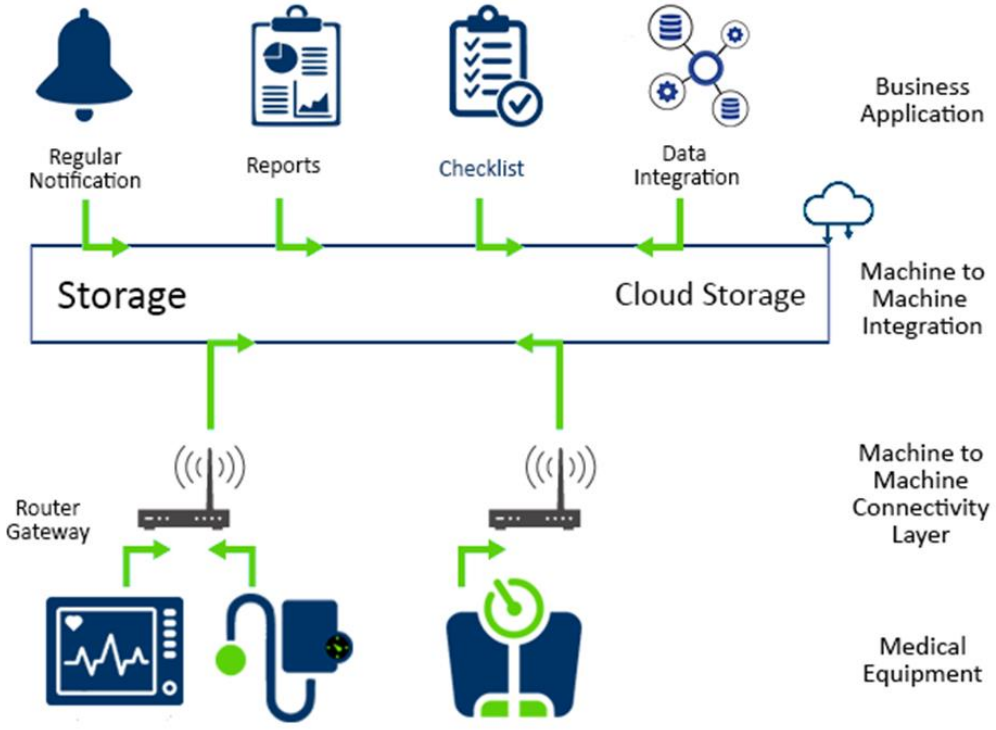

Fig.6. Architecture of Healthcare in IoT

IT organizations are making substantial investments in the development of essential IoT technologies because of their robust commercial prospects. Consequently, these organizations have implemented several IoT applications, both commercial and open source, in recent years. However, there is a need for a standardized framework to effectively adopt IoT systems and address issues related to interoperability, heterogeneity, and diversity. The use of IoT applications has been widespread across several industries, with the industrial sector being particularly significant. Industry 4.0, often known as the fourth industrial revolution with IoT, is the integration of smart technology to enhance industrial operations. Security and privacy are crucial concerns in industrial IoT applications. Cisco, IBM, GE, and AT&T established a framework for the industrial Internet of Things (IoT) to address and analyze these problems.

3.1 IoT-Based Healthcare Applications

The term "IoT" is widely discussed and has made significant advancements in several fields. In the fields of healthcare, education, gambling, banking, and several other industries. The Internet of Things has rapidly gained significance since its introduction into the field of information technology. Furthermore, there exists another colossal entity in the vicinity. AI, also known as Artificial Intelligence, has immense potential and has successfully taken over everyday life. Integrated with IoT, AI has taken over the fundamental aspect of several processes, ranging from data collection to processing and analytics. The primary function of IoT in healthcare is to provide seamless communication between physicians and patients via a sophisticated device, without any limitations. In fact, patients may exhibit improved disclosure, facilitating expedited diagnosis by physicians [20]. This leads to an enhancement of the customer, with minimal inefficiencies, and the doctor consistently makes judgments via improved connection, precision-oriented monitoring, and data collection.

Fig.7. IoT healthcare trends

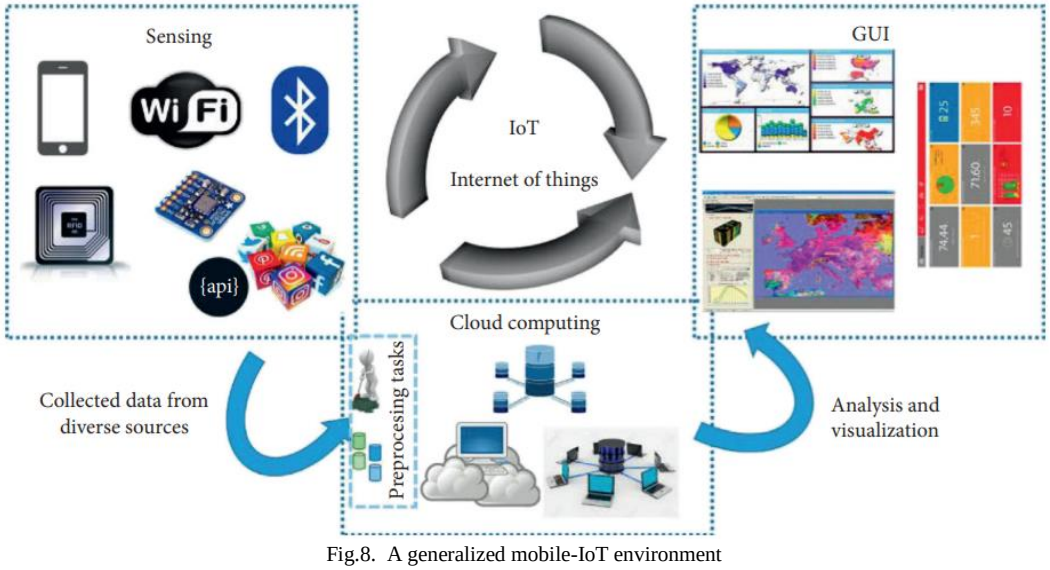

Fig.8. A generalized mobile-IoT environment

Mobile IoT refers to the integration of mobile computers, sensors, communication technologies, and cloud computing to monitor and record a patient's health information and other physiological parameters shown in Figure 8. Wearable gadgets

facilitate healthcare providers and individuals in managing diverse health concerns at a diminished expense. These devices are noninvasive and may be created by incorporating different sensors into wearable items often used by people, such as watches, wristbands, necklaces, shirts, shoes, handbags, hats, and so on. The linked sensor is used to gather environmental and patient health data. Subsequently, this data is sent to the server and stored in databases [21]. Certain wearable gadgets are further linked to mobile phones via health apps. Several studies in the literature have shown the use of these wearable devices shown in Figure 9 and mobile computing for real-time monitoring. Castillejo et al. have suggested a way for recognizing activities by combining wearable devices in a wireless sensor network. This approach is used to remotely monitor patients using a mobile application for e-health.

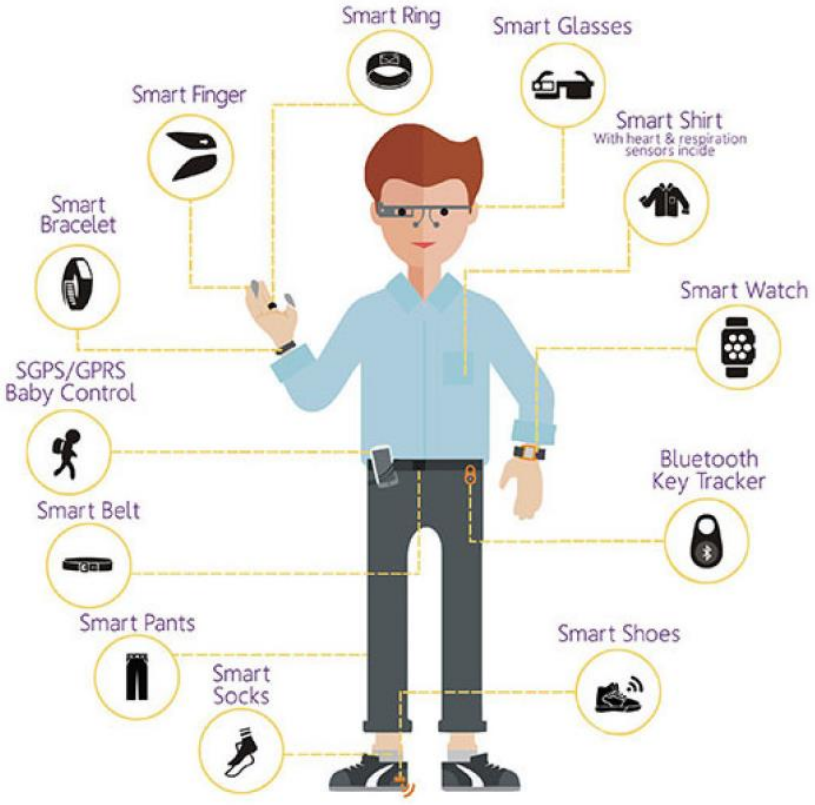

Fig.9. Advancements in wearable technology throughout the IoT era.

The IoT is transforming healthcare systems and serving as a robust platform for many healthcare applications. For example, the IoT integrates thermal cameras and embedded sensors into electrical equipment to gather data from critical locations. IoT devices gather up-to-the-minute health conditions and other patient data, which are then shared with healthcare workers. Patient health monitoring systems has the potential to monitor patients by using state-of-the-art technology. Furthermore, it enables the dissemination of patient records across healthcare teams for the purpose of data analysis. An e-Health system was developed to use sensors for hospital administration, specifically for monitoring patient health status and transmitting the analysis to healthcare workers. The researchers used electrocardiogram (ECG) sensors for the purpose of examining cardiac functions, monitoring the patient's state, assessing body temperature, and feeling acceleration. In addition, the scientists used environmental sensors to quantify the patient's room conditions. For example, [22-23] developed a health application specifically for patients with arrhythmia. The programme utilizes an ECG equipment to analyze the heartbeat and applies the k-nearest neighbour (KNN) algorithm to forecast the specific forms of arrhythmia sickness. The Alzimio mobile application is used to verify secure area hotspots and detect activity for people suffering from autism, Alzheimer's, and dementia. Additionally, it enables medical teams to choose certain interventions, and hazardous areas are alerted when any critical activities are identified. GPS is often used in several IoT devices to monitor patients and notify healthcare providers when the patient ventures outside a designated area. A soldier's health state was measured utilizing an IoT-based application that used body temperature sensors, pulse rate sensors, and an oxygen analyzer. The technology is capable of monitoring the real-time position of the soldier using GPS.

3.2 Services For IoT Healthcare

The IoT is expected to facilitate a range of healthcare services, each offering a distinct set of healthcare solutions. Within the healthcare domain, there is currently no universally accepted definition for IoT services. Nevertheless, there are instances when it is impossible to objectively distinguish a service from a specific solution or application[24]. This article posits that a service has inherent generic qualities and has the capacity to serve as a fundamental component for a range of solutions or applications. Furthermore, it is important to acknowledge that the general services and protocols needed for IoT frameworks may need minor adjustments to ensure their optimal performance in healthcare settings. These include notification services, resource-sharing services, internet services, cross-connectivity protocols for diverse devices, and connection protocols for primary connectivity [24-25]. The inclusion of effortless, rapid, reliable, and energy-efficient identification of devices and services may be appended to this inventory. Nevertheless, this study does not provide a debate on broad IoT services. For a more thorough comprehension of this subject, the reader is advised to consult the relevant literature.

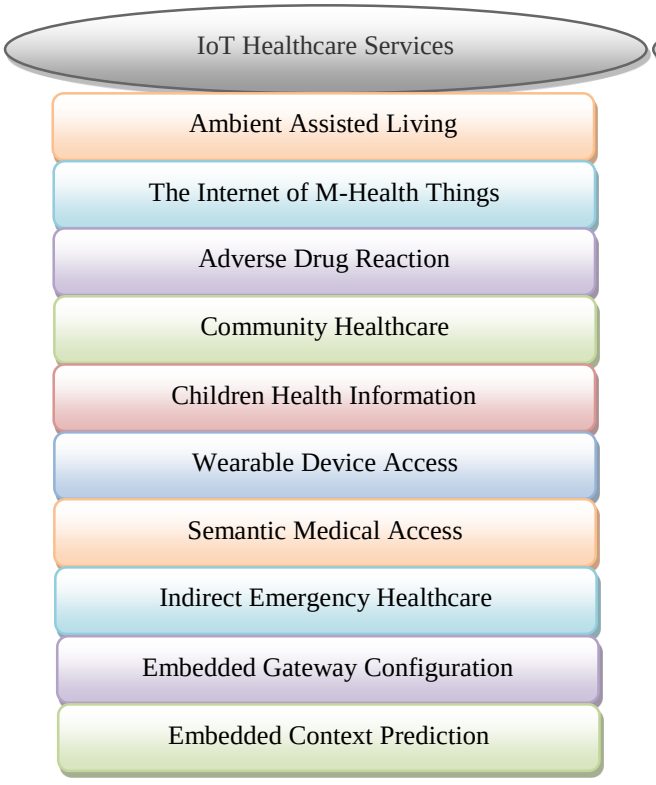

Fig.10. IoT healthcare services

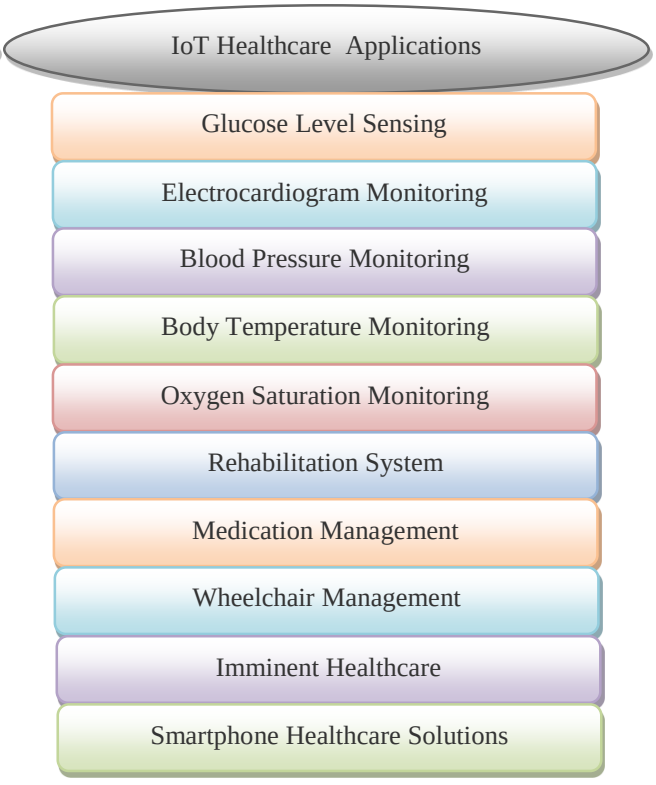

Fig.11. IoT healthcare applications

3.3 Trends and Current Status of the IoT Healthcare Industry

A Chinese company has created miPlatform, an all-in-one medical imaging and information management platform that supports cloud-based image storage and computing, web-based 3D image post-processing and visualization, and integrated telemedicine competency. Neusoft has supplied comprehensive IT solutions for China's medical sector and personal healthcare network services, as well as services for hospitals, public health facilities, and health management. Neusoft has concentrated on IoT-enabled healthcare services. LiftMaster has created solutions that facilitate house entry and provide the owner choice over how he or she enters and departs. It enables complete control and connection by being linked to cellphones at all times.

Fig. 12. Healthcare IoT devices and prototypes.

3.4 Security of IoT Healthcare

The IoT is seeing significant and fast expansion. Over the next years, the medical industry is projected to see extensive implementation of the IoT and thrive with the introduction of new eHealth IoT devices and apps. Healthcare gadgets and apps are anticipated to handle crucial sensitive information, such as personal healthcare data. Furthermore, these intelligent gadgets may be linked to worldwide information networks, allowing for access at any time and in any location [26-27]. Hence, the IoT healthcare sector is susceptible to potential attacks from malicious individuals. In order to promote the widespread use of the IoT in the healthcare industry, it is crucial to identify and examine certain aspects of IoT security and privacy. This includes analyzing security needs, vulnerabilities, threat models, and countermeasures, all from the viewpoint of healthcare. These aspects are shown in figure 13. The security requirements for IoT-based healthcare solutions are comparable to those in conventional communication contexts.

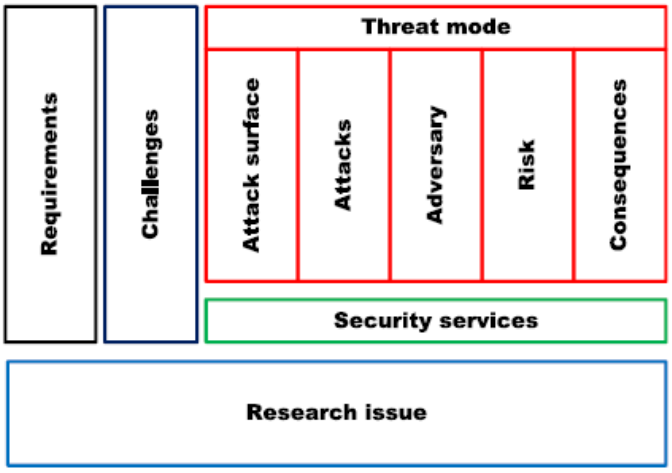

Fig. 13. Security concerns in the context of health care systems based on the IoT.

3.5 Security Challenges

Due to the inadequacy of existing security procedures, new measures are necessary to meet the security needs of IoT and tackle the emerging difficulties it presents. Obstacles for ensuring safe IoT healthcare services include. IoT health gadgets include low-speed CPUs. The speed of the central processor unit (CPU) in such gadgets is rather low. Furthermore, these devices are not specifically designed to carry out computationally demanding tasks. In other words, they function just as a sensor or actuator. Hence, the quest for a security solution that minimizes resource use and hence maximizes security performance is a formidable undertaking. The majority of IoT healthcare devices possess limited on-device memory. These devices are powered on by using an integrated operating system (OS), system software, and an application binary. Consequently, their memory may not be enough to carry out intricate security processes. An IoT healthcare network often consists of tiny health devices with low battery capacity, such as body temperature and blood pressure sensors. These devices save energy by activating the power-saving mode when there is no need to report any sensor readings. Furthermore, they function at a reduced CPU frequency when there are no significant tasks to be executed. Healthcare gadgets are often mobile rather than stationary. These devices are linked to the Internet via IoT service providers. For instance, a wearable device that measures body temperature or monitors heart activity may be linked to the Internet and provide notifications to the career on the user's health status. These wearable's are linked to the home network while the user is at home, and to the office network when the user is at the office. Various networks possess distinct security configurations and settings. Hence, the task of creating a security algorithm that is compatible with mobility poses a significant difficulty. The proliferation of IoT devices has led to a progressive growth in the number of devices that are being linked to the global information network [28-29]. Hence, creating a security system that is both highly scalable and meets all security needs is a tough undertaking.

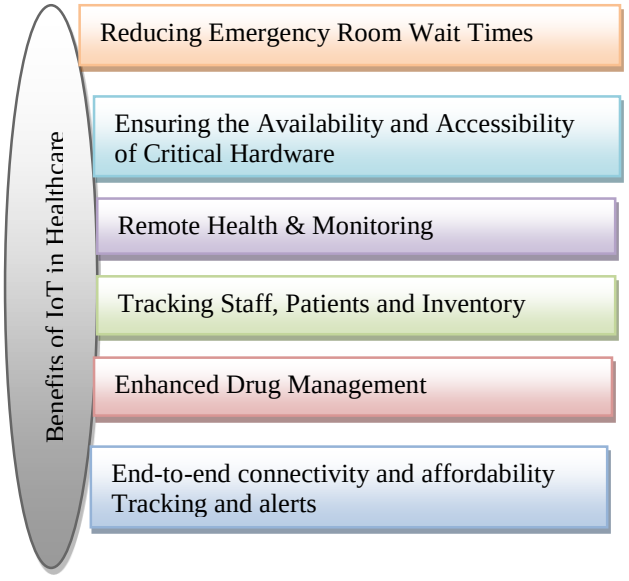

Fig. 14. Benefits of IoT in Healthcare.

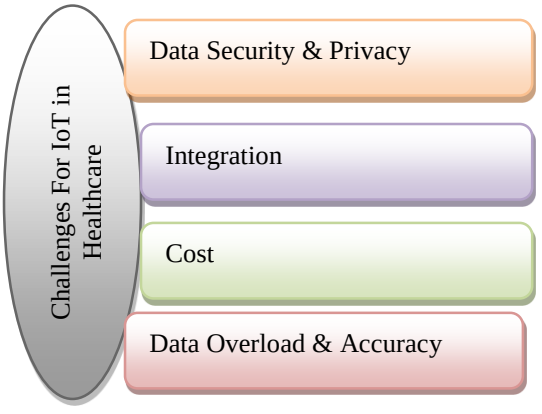

Fig. 15. Challenges For IoT in Healthcare.

4. CONCLUSION

Researchers worldwide are investigating different technology solutions to improve healthcare delivery by using the potential of the IoT while working alongside current services. This article examines several elements of healthcare technologies based on the IoT and introduces different network designs and platforms that enable access to the IoT backbone and simplify the transmission and receipt of medical data. The BCT is attracting considerable interest from people and organizations of all types and sizes. Its properties, such as decentralization, anonymity, persistency, and auditability, have the potential to revolutionize the conventional sector. The BCT is anticipated to revolutionize the healthcare environment. The approach will not only be transparent and secure, but it will also enhance the quality of healthcare while reducing costs. This article explores many uses of BCT in the healthcare sector and highlights significant research endeavours and potential areas for future study. The progress in IoT communication infrastructure and physical devices has led to significant advancements in remote health monitoring systems. ML algorithms, in conjunction with sophisticated AI methods, are capable of identifying patterns linked to illnesses and health issues. During the last ten years, health

monitoring apps that use the IoT have been created by combining blockchain technology with ML models. This integration has proven advantageous for managing medical reports, ensuring the traceability of drugs, and tracking the spread of infectious illnesses. Currently, the most advanced methods for incorporating BC into IoT applications are discussed. This research provides a thorough examination of the latest IoT technologies, and BC in relation to their applications in healthcare.

Conflicts Of Interest

The author's affiliations, financial relationships, or personal interests do not present any conflicts in the research.

Funding

The lack of a funding acknowledgment in the paper indicates that no financial support was provided by any institution or sponsor.

Acknowledgment

The author extends gratitude to the institution for fostering a collaborative atmosphere that enhanced the quality of this research.

References

[1] V. Nookala, A. ArunKumar, K. K. Vaigandla, "Investigation on Internet of Things (IoT): Technologies, Challenges and Applications in Healthcare," International Journal of Research, vol. XI, no. II, pp. 143-153, Feb. 2022.

[2] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. -S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678-708, 2015, doi: 10.1109/ACCESS.2015.2437951.

[3] P. Navya, G. S. Rama, T. P. Kumar, S. N. Pasha, and K. Mahender, "IoT technology: Architecture, stack, security risks, privacy risks and its applications," AIP Conference Proceedings, vol. 2418, no. 1, May 2022.

[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: architecture, consensus, and future trends," in 2017 IEEE International Congress on Big Data (BigData Congress), Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.

[5] K. K. Vaigandla, R. Karne, M. Siluveru, and M. Kesoju, "Review on Blockchain Technology: Architecture, Characteristics, Benefits, Algorithms, Challenges and Applications," Mesopotamian Journal of CyberSecurity, 2023, pp. 73–85, https://doi.org/10.58496/MJCS/2023/012.

[6] M. Imran, U. Zaman, J. Imtiaz, M. Fayaz, and J. Gwak, "Comprehensive Survey of IoT, Machine Learning, and Blockchain for Health Care Applications: A Topical Assessment for Pandemic Preparedness, Challenges, and Solutions," Electronics, vol. 10, 2021, 2501, https://doi.org/10.3390/electronics10202501.

[7] R. Yadav, Ritambhara, K. K. Vaigandla, G. S. P. Ghantasala, R. Singh, and D. Gangodkar, "The Block Chain Technology to protect Data Access using Intelligent Contracts Mechanism Security Framework for 5G Networks," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 108-112, doi: 10.1109/IC3I56241.2022.10072740.

[8] R. Shantha, K. Mahender, A. Jenifer, and A. Prasanth, "Security analysis of hybrid one-time password generation algorithm for IoT data," AIP Conference Proceedings, vol. 2418, no. 1, May 2022.

[9] K. K. Vaigandla, R. Karne, A. S. Rao, and Sravani, "Investigation on Machine Learning: Introduction, Algorithms, Challenges and Applications in Healthcare," International Conference On Role of Artificial Intelligence and Sustainable Engineering in Driving Smart Cities (ICRASES-2022), 2022, pp. 83-96.

[10] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, Oct. 2017, pp. 1–5.

[11] T. Bocek, B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere—A use-case of blockchains in the pharma supply-chain," in Proceedings of the 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, May 2017, pp. 772–777.

[12] Y. Huang, J. Wu, and C. Long, "Drugledger: A practical blockchain system for drug traceability and regulation," in Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, Jul.–Aug. 2018, pp. 1137–1144.

[13] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," International Journal of Intelligent Networks, vol. 2, 2021, pp. 130-139.

[14] K. K. Vaigandla and M. Siluveru, "Fog Computing with Internet of Things: An Overview of Architecture, Algorithms, Challenges and Applications," Journal of Engineering and Technology (JET), vol. 14, no. 1, 2023, pp. 187–220, https://jet.utem.edu.my/jet/article/view/6343.

[15] K. K. Vaigandla, R. K. Karne, A. S. Rao, "A Study on IoT Technologies, Standards and Protocols," IBM RD's Journal of Management & Research, vol. 10, no. 2, Sep. 2021, Print ISSN: 2277-7830, Online ISSN: 2348-5922, DOI: 10.17697/ibmrd/2021/v10i2/166798.

[16] D. R. Kumari, K. Mahender, S. Chitti, and V. Sivalenka, "IoT-based environment harmful gases detecting and controlling system," AIP Conference Proceedings, vol. 2418, no. 1, May 2022.

[17] K. K. Vaigandla and N. Venu, "A Survey on Future Generation Wireless Communications - 5G: Multiple Access Techniques, Physical Layer Security, Beamforming Approach," Journal of Information and Computational Science, vol. 11, no. 9, 2021, pp. 449-474, DOI: 10.12733.JICS.2021.V11I9.535569.36347.

[18] K. K. Vaigandla, S. Bolla, R. Karne, "A Survey on Future Generation Wireless Communications-6G: Requirements, Technologies, Challenges and Applications," International Journal of Advanced Trends in Computer Science and Engineering, vol. 10, no. 5, Sep.–Oct. 2021, pp. 3067–3076, https://doi.org/10.30534/ijatcse/2021/211052021.

[19] K. K. Vaigandla, N. Azmi, P. Ramya, R. Karne, "A Survey On Wireless Communications: 6g And 7g," International Journal Of Science, Technology & Management, vol. 2, no. 6, Nov. 2021, pp. 2018-2025, https://doi.org/10.46729/ijstm.v2i6.379.

[20] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," Internet of Things and Cyber-Physical Systems, 2024.

[21] K. R. Reddy, R. R. Arabelli, D. Rajababu, and K. Mahender, "Solar power generation system with IoT based monitoring and controlling using different sensors and protection devices to continuous power supply," IOP Conference Series: Materials Science and Engineering, vol. 981, no. 3, Dec. 2020, p. 032017.

[22] E. Moghadas, J. Rezazadeh, R. Farahbakhsh, "An IoT patient monitoring based on fog computing and data mining: Cardiac arrhythmia use case," Internet Things, vol. 11, 2020, 100251.

[23] A. Lakhan, M. A. Dootio, T. M. Groenli, A. H. Sodhro, and M. S. Khokhar, "Multi-layer latency aware workload assignment of e-transport IoT applications in mobile sensors cloudlet cloud networks," Electronics, vol. 10, 2021, 1719.

[24] C. Ramakrishna et al., "A Smart System for Future Generation Based on the Internet of Things Employing Machine Learning, Deep Learning, and Artificial Intelligence: Comprehensive Survey," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 9, Nov. 2023, pp. 1798-15, doi:10.17762/ijritcc.v11i9.9167.

[25] K. K. Vaigandla, N. Azmi, R. Karne, "Investigation on Intrusion Detection Systems (IDSs) in IoT," International Journal of Emerging Trends in Engineering Research, vol. 10, no. 3, Mar. 2022, https://doi.org/10.30534/ijeter/2022/041032022.

[26] B. Pradhan, S. Bhattacharyya, and K. Pal, "IoT-based applications in healthcare devices," Journal of Healthcare Engineering, vol. 2021, 2021, pp. 1-18.

[27] N. Venu, A. ArunKumar, K. K. Vaigandla, "Review of Internet of Things (IoT) for Future Generation Wireless Communications," International Journal for Modern Trends in Science and Technology, vol. 8, no. 03, 2022, pp. 01-08, https://doi.org/10.46501/IJMTST0803001.

[28] K. K. Vaigandla, "Communication Technologies and Challenges on 6G Networks for the Internet: Internet of Things (IoT) Based Analysis," 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), 2022, pp. 27-31, doi: 10.1109/ICIPTM54933.2022.9753990.

[29] R. Karne, S. Mounika, K. Karthikkumar V, "Applications of IoT on Intrusion Detection System With Deep Learning Analysis," International Journal For Innovative Engineering And Management Research, vol. 11, SPL ISSUE 06, 2022, pp. 203-208, DOI: 10.48047/IJIEMR/V11/SPL ISSUE 06/37.