Chapter 2
Blockchain-Based Cybersecurity in Internet of Medical Things (IoMT)-Based Assistive Systems

Amit Kumar Tyagi
https://orcid.org/0000-0003-2657-8700
National Institute of Fashion Technology, New Delhi, India

Timothy Thomas George
Vellore Institute of Technology, Chennai, India

Gulshan Soni
https://orcid.org/0000-0001-7279-2981
MSEIT, MATS University, India

ABSTRACT

Today's internet of medical things (IoMT) devices has revolutionized healthcare by enabling the development of assistive systems that enhance patient care and improve healthcare outcomes. However, the increasing connectivity and data exchange in IoMT systems raise issues about cybersecurity and patient data privacy. This chapter explains the application of blockchain-based cybersecurity in IoMT-based assistive systems. Blockchain technology offers a decentralized and immutable ledger that ensures the integrity, security, and transparency of data in IoMT systems. By adding blockchain, cybersecurity challenges in IoMT can be addressed effectively (with providing several benefits, including enhanced data protection, secure identity management, and robust access control mechanisms). Generally, in a blockchain-based cybersecurity framework for IoMT, patient health data is stored in encrypted form on the blockchain, preventing unauthorized access/tampering. Smart contracts, programmable blockchain protocols, can automate access control and consent management, etc.

DOI: 10.4018/978-1-6684-8938-3.ch002

1. INTRODUCTION

1.1 Overview of IoMT-Based Assistive Systems

Internet of Medical Things based assistive systems refer to the integration of medical devices, sensors, and healthcare systems with the internet to provide advanced monitoring, diagnostic, and assistance capabilities for individuals in need of medical support (Bai & Liu, 2020). These systems add the power of connectivity and data analysis to enhance healthcare delivery, improve patient outcomes, and enable more personalized and proactive care. Here is an overview of IoMT-based assistive systems and their key components:

- Medical Devices and Sensors: IoMT systems incorporate various medical devices and sensors to capture and monitor physiological data. These can include wearable devices like fitness trackers, smartwatches, and biosensors that measure parameters such as heart rate, blood pressure, glucose levels, and activity levels. Additionally, home monitoring devices such as blood glucose meters, blood pressure monitors, and spirometers may be connected to the IoMT network.
- Data Collection and Transmission: The collected data from medical devices and sensors is securely transmitted to a centralized platform or cloud infrastructure through wireless technologies like Bluetooth, Wi-Fi, or cellular networks. This allows healthcare providers to access and analyze the data in real-time, regardless of the location of the patient.
- Cloud Infrastructure: The cloud infrastructure serves as a centralized repository for storing and processing the collected data. It provides scalability, high availability, and security for the large amount of data generated by IoMT devices. Cloud platforms also enable advanced analytics, machine learning, and artificial intelligence algorithms to derive meaningful information from the data.
- Data Analytics and Artificial Intelligence: IoMT-based assistive systems add data analytics and AI techniques to interpret the collected data and provide important information. These systems can detect patterns, identify anomalies, and generate predictive models to assist in disease management, early detection of potential health issues, and proactive interventions. AI algorithms can also help in decision support, suggesting appropriate treatment plans or medication adjustments.
- Remote Monitoring and Telemedicine: IoMT enables remote monitoring of patients, allowing healthcare providers to track important signs and health parameters without the need for in-person visits. Telemedicine applications

integrate with IoMT systems, enabling remote consultations between patients and healthcare professionals through video conferencing, messaging platforms, or mobile apps. This enhances access to care, especially for individuals with limited mobility or living in remote areas.

- Personalized and Adaptive Care: IoMT-based assistive systems can provide personalized care by analyzing an individual's health data and tailoring interventions and treatment plans accordingly. By continuously monitoring a person's health status, these systems can adapt and provide timely alerts or recommendations for lifestyle modifications, medication adherence, and early intervention to prevent adverse health events.
- Health Data Privacy and Security: As IoMT involves the transmission and storage of sensitive health information, robust security measures are crucial. Data encryption, authentication, and access control mechanisms ensure the privacy and confidentiality of patient data. Compliance with regulatory standards such as HIPAA (Health Insurance Portability and Accountability Act) is essential to protect patient rights and maintain data integrity.

Hence, IoMT-based assistive systems hold immense potential to revolutionize healthcare by improving patient care, reducing healthcare costs, and enabling proactive interventions. However, challenges such as interoperability, data standardization, and ethical issues surrounding data privacy and security need to be addressed to realize the full benefits of these systems.

1.2 Importance of Cybersecurity in IoMT

Cybersecurity is so important in IoMTs due to the sensitive nature of healthcare data and the potential risks associated with interconnected medical devices and systems (Azaria et al., 2016; Li & Da Xu, 2018). Here are the key reasons why cybersecurity is essential in IoMT:

- Protection of Patient Data: IoMT systems collect and transmit a large amount of sensitive patient data, including personal health information, medical history, and real-time health monitoring data. This information is highly important to cybercriminals who may attempt to steal or manipulate it for various malicious purposes. Robust cybersecurity measures, such as data encryption, access controls, and secure communication protocols, are necessary to safeguard patient data from unauthorized access, breaches, or data loss.
- Prevention of Unauthorized Access and Manipulation: The interconnected nature of IoMT devices and systems introduces vulnerabilities that can be

exploited by cyber attackers. Unauthorized access to medical devices or network infrastructure can lead to tampering with critical medical equipment, altering patient data, or even causing harm to patients. Strong authentication mechanisms, network segmentation, and intrusion detection systems are important to prevent unauthorized access and ensure the integrity and authenticity of data and commands within IoMT systems.

- Mitigation of Operational Disruptions: IoMT systems rely on the continuous and reliable functioning of interconnected devices, networks, and cloud infrastructure. A cybersecurity breach can disrupt the normal operation of medical devices, leading to system failures, data corruption, or delays in patient care. Implementing robust cybersecurity measures, regular system patching, and proactive threat monitoring help prevent such disruptions and ensure the smooth operation of IoMT-based assistive systems.
- Protection against Ransomware and Malware: The healthcare industry has increasingly become a target for ransomware attacks, where cybercriminals encrypt critical data and demand a ransom for its release. IoMT systems are not immune to such attacks, and a successful ransomware infection can have severe consequences, including compromised patient safety and interruptions in healthcare services. Implementing robust endpoint protection, regular backups, and incident response plans are critical to minimizing the impact of ransomware and malware attacks.
- Safeguarding Patient Safety and Trust: A breach or compromise of IoMT systems can have severe consequences on patient safety and erode trust in healthcare providers and technology. By prioritizing cybersecurity, healthcare organizations can demonstrate their commitment to patient privacy and safety. Ensuring the security of IoMT systems helps build trust among patients, healthcare professionals, and stakeholders, facilitating the widespread adoption of these technologies for improved patient care.
- Compliance with Regulatory Requirements: Healthcare organizations must comply with various regulatory standards and privacy laws, such as HIPAA (Health Insurance Portability and Accountability Act), to protect patient data. Failure to implement adequate cybersecurity measures can result in legal and financial penalties, reputational damage, and loss of patient trust. By investing in cybersecurity, healthcare organizations can meet regulatory requirements and demonstrate their commitment to protecting patient information.

Hence, given the critical role that IoMT systems play in healthcare delivery, cybersecurity must be integrated into the design, development, and maintenance of these systems. Collaboration between healthcare providers, device manufacturers, and cybersecurity experts is essential to identifying and addressing vulnerabilities, implementing robust security controls, and staying ahead of emerging threats in the evolving landscape of healthcare technology.

1.3 Cybersecurity Challenges in IoMT-Based Assistive Systems

While IoMT-based assistive systems offer numerous benefits, they also pose significant cybersecurity challenges that need to be addressed. Here are some key challenges in securing IoMT-based assistive systems:

- Vulnerabilities in Medical Devices: Medical devices connected to the IoMT network may have inherent security vulnerabilities due to factors such as outdated operating systems, weak authentication mechanisms, or lack of encryption (Liao et al., 2018; Shih et al., 2018). These vulnerabilities can be exploited by attackers to gain unauthorized access, manipulate data, or disrupt device functionality. Ensuring the security of medical devices through regular patching, secure coding practices, and adherence to security standards is essential.
- Interoperability and Standardization: IoMT systems often consist of a variety of devices, sensors, and software from different manufacturers, each with their own protocols and interfaces. Achieving interoperability and standardization is essential for seamless communication and secure data exchange between devices. Lack of standardization can introduce vulnerabilities and increase the complexity of managing security across different components of the IoMT ecosystem.
- Data Privacy and Consent: IoMT systems collect and transmit sensitive patient data, raising issues about privacy and consent. Healthcare organizations must ensure that patient data is collected, stored, and transmitted securely, with appropriate consent obtained for data sharing and processing. Implementing privacy-enhancing technologies, strong data encryption, and transparent data handling practices can address these challenges.
- Network Security: IoMT systems rely on networks, such as Wi-Fi or cellular, for data transmission and communication between devices (Lu et al., 2018). Weak network security can expose sensitive data to eavesdropping, unauthorized access, or man-in-the-middle attacks. Implementing strong encryption protocols, network segmentation, intrusion detection systems, and regular network monitoring are essential to protect IoMT systems from network-based threats.
- Insider Threats: Insider threats, whether intentional or unintentional, pose a significant risk to IoMT systems. Healthcare professionals, employees, or third-party service providers who have authorized access to the systems

may abuse their privileges or inadvertently introduce security vulnerabilities. Implementing robust access controls, user authentication, and regular security training and awareness programs can help mitigate the risks associated with insider threats.

- Lifecycle Management and Patching: IoMT systems have a long lifecycle, and many devices may remain in use for an extended period. Ensuring the timely and consistent application of security patches and updates to all devices and software components within the IoMT ecosystem can be challenging. Organizations need to establish robust patch management processes, including monitoring vulnerability databases, coordinating with device manufacturers for updates, and applying patches promptly to minimize the risk of exploitation.
- Evolving Threat Landscape: The cybersecurity landscape is continually evolving, with new threats and attack vectors emerging regularly. Attackers may target IoMT systems with sophisticated malware, ransomware, or social engineering techniques. Staying updated with the latest security practices, conducting regular risk assessments, and implementing threat intelligence and incident response capabilities are importnat to mitigate evolving cyber threats.

Hence, these challenges require a holistic approach to cybersecurity, involving collaboration among healthcare providers, device manufacturers, regulatory bodies, and cybersecurity experts. It is essential to embed security into the design and development of IoMT systems, implement robust access controls, regularly assess vulnerabilities, and establish incident response plans to ensure the security and integrity of IoMT-based assistive systems and protect patient privacy and safety.

2. VULNERABILITIES AND THREATS IN IOMT

2.1 Risks to Data Integrity, Privacy, and Confidentiality

Data integrity, privacy, and confidentiality are critical aspects of IoMT-based assistive systems (Yue et al., 2016; Zhang et al., 2017), and several risks can compromise them. Here are the key risks to consider:

- Unauthorized Access: Unauthorized individuals gaining access to sensitive healthcare data is a significant risk. This can occur due to weak authentication mechanisms, compromised user credentials, or vulnerabilities in the system. Unauthorized access can lead to data breaches, unauthorized data modifications, or misuse of patient information.

- Data Breaches: Data breaches involve the unauthorized access, acquisition, or disclosure of sensitive data. Cybercriminals may exploit vulnerabilities in IoMT systems, network infrastructure, or cloud storage to gain access to patient data. Data breaches can result in financial losses, reputational damage, legal implications, and potential harm to individuals if their personal health information is exposed.
- Inadequate Data Encryption: Data transmitted between medical devices, sensors, and the cloud infrastructure may be intercepted if not adequately encrypted. Without proper encryption mechanisms, sensitive patient data can be exposed, compromising privacy and confidentiality. Implementing robust encryption algorithms and secure communication protocols helps protect data while in transit and at rest.
- Insider Threats: Insider threats involve individuals with authorized access to healthcare systems intentionally or unintentionally misusing or mishandling sensitive data. This could include healthcare professionals, employees, or third-party vendors. Insider threats may arise due to malicious intent, lack of awareness, or inadequate security practices. Organizations need to implement strict access controls, monitoring systems, and security awareness programs to mitigate insider threats.
- Insecure Data Storage: Inadequate security measures for data storage can expose patient information to unauthorized access. Weak access controls, lack of encryption, or insufficient safeguards in cloud storage or on-premises servers increase the risk of data breaches and unauthorized data retrieval. Implementing strong access controls, encryption at rest, regular data backups, and secure storage practices help mitigate these risks.
- Inadequate Consent Management: IoMT systems collect and process sensitive patient data, and obtaining appropriate consent for data usage is important. Inadequate consent management practices, such as unclear consent forms or improper handling of consented data, can result in privacy violations. Organizations must ensure that patients provide informed consent and that data usage adheres to applicable privacy regulations.
- Data Leakage: Data leakage refers to the unintentional exposure of sensitive information. It can occur through misconfigured devices, insecure data transfers, or human errors such as sending data to the wrong recipient. Proper security configurations, user training, and data loss prevention mechanisms can help prevent data leakage incidents.
- Insider Data Theft: Healthcare data is valuable and can be targeted for theft by insiders with authorized access. Insiders may steal patient data for

financial gain, personal reasons, or to sell it on the black market. Strict access controls, monitoring of user activities, and security audits help detect and prevent insider data theft.

- Third-Party Risks: IoMT systems often involve third-party vendors, cloud service providers, or data processors. These entities may have access to sensitive data and introduce security vulnerabilities if not properly vetted. It is essential to assess the security practices of third-party providers, establish robust contractual agreements, and conduct regular security audits to mitigate third-party risks.

Note that to mitigate these risks, healthcare organizations must implement high security measures, including strong access controls, encryption, regular security assessments, staff training, incident response plans, and adherence to privacy regulations such as HIPAA. Continuous monitoring, threat intelligence, and proactive vulnerability management are also essential to maintain the integrity, privacy, and confidentiality of data within IoMT-based assistive systems.

2.2 Potential Consequences of Cybersecurity Breaches

Cybersecurity breaches in IoMT-based assistive systems can have severe consequences on various levels, impacting individuals, healthcare organizations, and society as a whole. Here are potential consequences of cybersecurity breaches:

- Compromised Patient Safety: A cybersecurity breach can compromise patient safety by disrupting the normal functioning of medical devices or altering patient data. Attackers may manipulate medical device settings, leading to incorrect diagnoses or treatments, potentially causing harm to patients. In critical situations, patient safety can be directly jeopardized, leading to life-threatening consequences.
- Privacy Violations: Breaches can result in unauthorized access, disclosure, or theft of sensitive patient data, violating individual privacy rights. Personal health information, including medical history, diagnoses, treatments, and other identifiable data, may be leaked/ exposed (Dagher et al., 2018; Ouaddah et al., 2017). This can lead to identity theft, fraud, or exploitation of personal information for malicious purposes, impacting individuals' privacy and potentially causing emotional distress.
- Financial Losses: Cybersecurity breaches can result in significant financial losses for healthcare organizations. The costs associated with investigating and remediating breaches, notifying affected individuals, providing credit monitoring services, and potential legal settlements can be substantial.

Additionally, organizations may suffer reputational damage, leading to decreased patient trust, loss of business, and financial repercussions in the long term.

- Disruption of Healthcare Services: A cybersecurity breach can disrupt the normal operation of healthcare services. System outages, data loss, or compromised medical devices can lead to interruptions in patient care, delayed treatments, canceled appointments, or inaccurate medical records. Healthcare organizations may struggle to provide essential services, impacting patient health outcomes and overall healthcare delivery.
- Legal and Regulatory Consequences: Healthcare organizations are subject to various legal and regulatory requirements related to data protection and privacy, such as HIPAA. Failure to adequately protect patient data and address cybersecurity breaches can result in legal penalties, regulatory fines, or litigation. Organizations may also face audits, investigations, or loss of accreditation, further impacting their reputation and ability to operate effectively.
- Damage to Trust and Reputation: Cybersecurity breaches can erode patient trust in healthcare organizations and technology systems. Patients may hesitate to share sensitive information or engage in telemedicine and other digital healthcare services due to issues about data privacy and security. A loss of trust can have long-lasting effects on the reputation and viability of healthcare organizations, impeding the adoption of innovative technologies and hindering patient engagement.
- Public Health and Safety Risks: In some cases, cybersecurity breaches can have broader public health and safety implications. For example, attacks targeting critical healthcare infrastructure, such as hospitals or emergency services, can disrupt emergency response capabilities and hinder public health interventions. Attacks on connected medical devices or public health systems can lead to the spread of misinformation, undermining public health efforts and putting lives at risk.

Hence given the potential issues/ consequences, it is essential for healthcare organizations and stakeholders to prioritize cybersecurity and implement robust security measures. This includes regular risk assessments, employee training, incident response planning, encryption, access controls, and adherence to best practices and regulatory requirements. Proactive cybersecurity measures are essential to protect patient safety, maintain privacy, and safeguard the integrity of healthcare systems.

3. BLOCKCHAIN TECHNOLOGY OVERVIEW

3.1 Introduction to Blockchain

Blockchain is a decentralized and distributed digital ledger technology that enables the secure and transparent recording of transactions across multiple computers or nodes (Nair & Tyagi, 2023; et al., 2023; Sk et al., 2022). It provides a way to store and verify data in a manner that is resistant to tampering and unauthorized alterations. Initially introduced as the underlying technology for cryptocurrencies like Bitcoin, blockchain has since expanded into various industries and applications beyond digital currencies. At its core, a blockchain consists of a chain of blocks, where each block contains a list of transactions or data records. These blocks are linked together in a chronological order, forming a continuous and immutable chain of information. Here are some key components and characteristics of blockchain:

- Decentralization: Unlike traditional centralized systems, blockchain operates in a decentralized manner. The blockchain network is composed of multiple nodes, each maintaining a copy of the entire blockchain. This decentralized architecture eliminates the need for a central authority or intermediary, ensuring that no single entity has complete control over the data or transactions.
- Distributed Consensus: Blockchain relies on consensus algorithms to ensure that all nodes in the network agree on the validity of transactions and the state of the blockchain. Through consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS), nodes collectively validate and verify transactions, preventing fraudulent or malicious activities.
- Transparency and Immutability: Transparency is a basic characteristic of blockchain. Once a transaction is recorded on the blockchain, it becomes visible to all participants in the network. This transparency helps to establish trust and accountability. Moreover, the immutability of the blockchain means that once a transaction is recorded, it cannot be altered or deleted, ensuring the integrity and authenticity of the data.
- Security and Cryptography: Blockchain utilizes advanced cryptographic algorithms to secure the data and maintain the integrity of the transactions. Each block contains a cryptographic hash that uniquely identifies its contents, and any modification to the block would result in a change in the hash value, alerting the network to tampering attempts. Additionally, public-private key cryptography is used to authenticate and authorize transactions.
- Smart Contracts: Blockchain platforms often support smart contracts, which are self-executing contracts with predefined rules and conditions. Smart contracts automatically execute and enforce the terms of an agreement when

specific conditions are met. These contracts are stored on the blockchain, ensuring transparency and eliminating the need for intermediaries in contract execution.

Hence, Blockchain technology has the potential to revolutionize various industries, including finance, supply chain management, healthcare, and more. It offers benefits such as enhanced security, improved transparency, increased efficiency, and reduced reliance on intermediaries (refer figure 1). However, it also faces challenges such as scalability, energy consumption, and regulatory issues, which need to be addressed for widespread adoption.

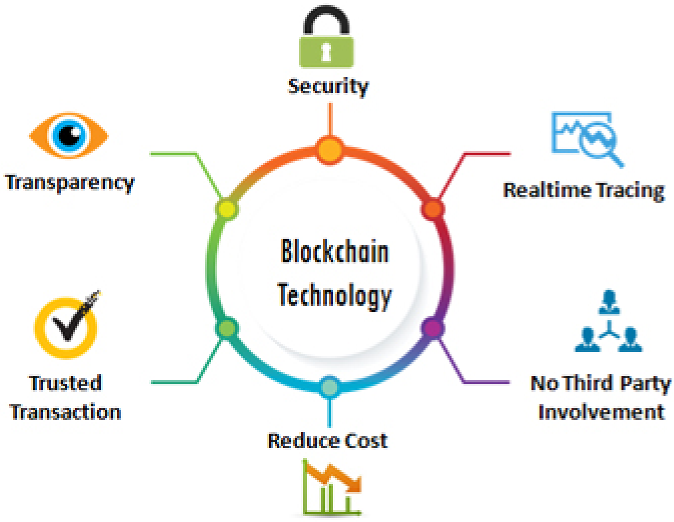
In summary, blockchain represents a significant shift in how data is stored, shared, and verified. Its decentralized and transparent nature has the potential to transform numerous industries and enable new possibilities for secure and trustless transactions.

3.2 Key Concepts: Decentralization, Transparency, Immutability

These terms can be discussed as:

- Decentralization: Decentralization refers to the distribution of authority, control, and decision-making across a network of participants instead of relying on a central authority. In the context of blockchain, decentralization means that the ledger and the validation process are distributed across multiple

Figure 1. Features of blockchain



nodes or computers. No single entity has complete control over the network, reducing the risk of a single point of failure or manipulation. Decentralization enhances transparency, security, and resilience within blockchain systems.

- Transparency: Transparency is a basic characteristic of blockchain technology. It means that all transactions recorded on the blockchain are visible to all participants in the network. Every participant can verify the validity of transactions, view the transaction history, and ensure compliance with predefined rules and protocols. Transparency in blockchain enhances trust and accountability, as it allows all network participants to independently verify and validate the data, reducing the need for trust in centralized authorities.
- Immutability: Immutability refers to the inability to change or alter data once it has been recorded on the blockchain. Once a transaction is added to a block and appended to the blockchain, it becomes permanent and cannot be modified retroactively. The immutability of blockchain ensures the integrity and authenticity of the recorded data, providing a tamper-resistant and auditable ledger. The use of cryptographic hash functions and consensus mechanisms makes it computationally infeasible to alter previous transactions without consensus from the majority of network participants.

These key concepts—decentralization, transparency, and immutability are basic principles that underpin the unique properties and value propositions of blockchain technology (Sun et al., 2018; Zeng et al., 2018). They enable trust, integrity, and security in decentralized systems, allowing for more transparent and tamper-proof record-keeping, verification, and transactions.

3.3 Blockchain Consensus Mechanisms

Blockchain consensus mechanisms are protocols or algorithms that ensure agreement and validation of transactions within a decentralized network (). These mechanisms enable nodes in the network to collectively reach a consensus on the state of the blockchain and validate the integrity of transactions. Here are some commonly used consensus mechanisms in blockchain:

- Proof of Work (PoW): PoW is the original consensus mechanism introduced by Bitcoin. In PoW, miners compete to solve complex mathematical puzzles, requiring significant computational power. The miner who successfully solves the puzzle first adds the next block to the blockchain and is rewarded with cryptocurrency. The consensus is reached based on the longest chain, assuming that the majority of participants act honestly. PoW is known for its security but is energy-intensive and can lead to scalability challenges.

- Proof of Stake (PoS): In PoS, the probability of being chosen to validate the next block is determined by the amount of cryptocurrency a participant holds and is willing to "stake" or lock up. Validators, also known as "stakers," are selected to create new blocks based on their stake, and they validate transactions accordingly. PoS consumes significantly less energy compared to PoW, but critics argue that it can lead to centralization if a few participants hold a majority of the cryptocurrency.
- Delegated Proof of Stake (DPoS): DPoS is a variation of PoS where token holders elect a limited number of representatives, known as delegates or block producers, who are responsible for validating transactions and creating new blocks. DPoS improves scalability and transaction throughput compared to PoW and PoS but introduces a certain degree of centralization as the number of delegates is limited.
- Practical Byzantine Fault Tolerance (PBFT): PBFT is a consensus mechanism commonly used in permissioned blockchains. It focuses on achieving consensus in a network where all participants are known and trusted. PBFT requires a predetermined number of validators to reach a consensus on the order and validity of transactions. It offers faster transaction confirmation times compared to PoW or PoS but is less suitable for open and public networks due to its reliance on trusted validators.
- Proof of Authority (PoA): PoA is a consensus mechanism in which a limited number of pre-approved, trusted nodes are designated as validators. These validators take turns creating new blocks and validating transactions. PoA provides fast block confirmation times and high throughput but sacrifices the decentralization aspect as trust is placed on a limited number of validators.
- Hybrid Consensus Mechanisms: Some blockchain platforms use hybrid consensus mechanisms that combine multiple approaches to consider their strengths. For example, some networks may use PoW for block validation and PoS for selecting validators or reaching secondary consensus.

In summary, the choice of consensus mechanism depends on factors such as the goals of the blockchain network, its scalability requirements, the level of decentralization desired, and the trust model established among participants. Different consensus mechanisms strike a balance between security, efficiency, scalability, and decentralization, enabling blockchain networks to cater to various use cases and requirements.

3.4 Smart Contracts and Security Benefits

Smart contracts are self-executing contracts with predefined rules and conditions written as code on a blockchain. They automatically execute actions when specific conditions are met, eliminating the need for intermediaries and enhancing the security and efficiency of transactions (Tyagi, Chandrasekaran, & Sreenath, 2022; Varsha, 2022). Smart contracts offer several security benefits:

- Tamper Resistance: Smart contracts are stored on a blockchain, which provides immutability and tamper resistance. Once a smart contract is deployed and recorded on the blockchain, it cannot be modified, deleted, or tampered with. This ensures that the agreed-upon rules and conditions of the contract remain unchanged, providing a high level of trust and eliminating the risk of fraud or manipulation.
- Transparency: Smart contracts are transparent and visible to all participants in the blockchain network. The code and logic of the contract are open and accessible, allowing all parties to verify the rules and conditions of the contract. This transparency enhances trust among participants, as there is no ambiguity regarding the execution of the contract.
- Automation and Elimination of Intermediaries: Smart contracts automate the execution of contractual obligations once predefined conditions are met. This eliminates the need for intermediaries, such as lawyers or escrow agents, to oversee and enforce the terms of the contract. By removing intermediaries, smart contracts reduce the risk of human error, bias, or intentional misconduct, enhancing the security and efficiency of transactions.
- Cryptographic Security: Smart contracts add cryptographic techniques to ensure the security of the contract and its associated transactions. Public-key cryptography is used to authenticate and authorize participants, protecting the integrity and confidentiality of the contract. Digital signatures and cryptographic hashes are employed to verify the authenticity of transactions, preventing unauthorized alterations or tampering.
- Trustless Execution: Smart contracts enable trustless execution, meaning that participants can engage in transactions without relying on trust in a central authority or counterparty. The predefined rules and conditions embedded in the smart contract are automatically enforced, ensuring that transactions are executed exactly as agreed upon. This reduces the risk of fraud, non-compliance, or disputes, as the execution of the contract is based on code and mathematics rather than subjective trust.
- Auditable and Immutable Recordkeeping: Smart contracts on a blockchain provide an auditable and immutable record of all contract-related transactions

and events. Every transaction and state change associated with the smart contract is permanently recorded on the blockchain, allowing for transparent and verifiable tracking of the contract's history. This audit trail can be beneficial for regulatory compliance, dispute resolution, and accountability purposes.

While smart contracts offer significant security benefits, it is important to note that the security of smart contracts relies on the quality of the code and proper implementation. Careful code development, thorough testing, and auditing are important to identify and mitigate potential vulnerabilities or bugs that could be exploited. Additionally, the security of the underlying blockchain infrastructure and the protection of private keys used to interact with smart contracts are essential issues to ensure overall security in smart contract applications.

4. BLOCKCHAIN-BASED CYBERSECURITY IN IOMT-BASED ASSISTIVE SYSTEMS

4.1 Role of Blockchain in Enhancing Cybersecurity in IoMT-based Assistive Systems

Blockchain technology can play an important role in enhancing cybersecurity in IoMT-based assistive systems (Varsha, 2022). Here are several ways in which blockchain can contribute to strengthening cybersecurity:

- Immutable and Tamper-Resistant Storage: Blockchain's immutable nature ensures that once data is recorded on the blockchain, it cannot be altered or tampered with. This property provides a secure and tamper-resistant storage mechanism for critical healthcare data, including patient records, treatment information, and device logs. By adding blockchain for data storage, healthcare organizations can enhance data integrity and protect against unauthorized modifications or tampering.
- Secure Data Sharing and Access Control: Blockchain enables secure and decentralized data sharing among authorized participants. Using cryptographic techniques, blockchain can facilitate granular access control, ensuring that only authorized entities can access specific data. This helps protect sensitive patient information from unauthorized access and enables secure sharing of data between different healthcare providers while maintaining patient privacy.
- Identity Management and Authentication: Blockchain can provide a secure and decentralized framework for identity management and authentication. By

adding blockchain's public-private key cryptography, individuals and devices can have unique digital identities stored on the blockchain. This enhances the security of access control and authentication processes, reducing the risk of unauthorized access to IoMT systems and sensitive healthcare data.

- Auditability and Compliance: Blockchain's transparent and auditable nature makes it well-suited for compliance and audit purposes. All transactions and changes made to the blockchain are permanently recorded and can be audited, facilitating regulatory compliance and ensuring accountability. This is particularly important in healthcare, where compliance with regulations such as HIPAA is critical. Blockchain's audit trail can help demonstrate adherence to privacy and security requirements.
- Secure Interoperability and Data Integrity: Blockchain can address interoperability challenges by providing a standardized and secure platform for exchanging data between different IoMT devices, systems, and healthcare providers. Blockchain's decentralized consensus mechanism ensures that data is verified and validated by multiple participants, enhancing data integrity and reducing the risk of compromised data due to a single point of failure or malicious manipulation.
- Cyber Threat Detection and Response: Blockchain can be used to enhance threat detection and response mechanisms in IoMT systems. By adding blockchain's distributed nature, anomaly detection algorithms can be deployed across multiple nodes to identify abnormal behaviors or potential cyber threats. Additionally, blockchain's immutability can assist in forensic investigations, providing a trustworthy historical record of events and transactions for incident response and recovery.
- Supply Chain Security: Blockchain technology can enhance the security and traceability of the supply chain for medical devices and pharmaceuticals. By recording the entire lifecycle of devices and medications on the blockchain, it becomes easier to track and verify the authenticity, origin, and integrity of these products. This reduces the risk of counterfeit or substandard products entering the healthcare system.

While blockchain brings several cybersecurity advantages, it is important to note that it is not a silver bullet and should be implemented alongside other security measures. The integration of strong access controls, encryption, secure software development practices, and regular security audits is essential to build a high cybersecurity framework for IoMT-based assistive systems.

4.2 Data Integrity and Immutable Audit Trail in IoMT-Based Assistive Systems

Data integrity and the creation of an immutable audit trail are essential aspects of IoMT-based assistive systems, and blockchain technology can contribute to addressing these requirements effectively. Here's how data integrity and an immutable audit trail can be achieved:

- Data Integrity: Maintaining data integrity ensures that the data remains accurate, complete, and unaltered throughout its lifecycle. In IoMT systems, data integrity is of utmost importance as it directly impacts the quality of patient care and treatment decisions. Blockchain technology can play a significant role in ensuring data integrity through its immutable and tamper-resistant properties.
- By storing medical data and transaction records on a blockchain, each data entry is time-stamped, digitally signed, and cryptographically linked to previous data entries. Any alteration or tampering with the data would require the consensus of the majority of nodes in the network, making it extremely difficult for malicious actors to manipulate or corrupt the data. As a result, healthcare providers can rely on the integrity of the data stored on the blockchain for accurate diagnostics, treatment plans, and monitoring.
- Immutable Audit Trail: An audit trail is a chronological record of activities and transactions, providing a historical account of actions taken within a system. In IoMT-based assistive systems, maintaining an immutable audit trail is important for transparency, accountability, and compliance with regulatory requirements. Blockchain technology inherently provides an immutable and transparent ledger that serves as an audit trail for all transactions and activities recorded on the blockchain.
- Every transaction or data entry on the blockchain is permanently recorded and cannot be modified or deleted. This creates an immutable audit trail that allows healthcare providers, regulators, and auditors to trace the entire history of data access, modifications, and transactions. The audit trail on the blockchain can be added for compliance audits, regulatory reporting, dispute resolution, and ensuring accountability among the participants in the system.
- Secure Data Hashing and Verification: Blockchain utilizes cryptographic hashing functions to generate unique, fixed-length representations of data called hashes. These hashes act as digital fingerprints of the data, providing a secure and efficient way to verify the integrity of the stored information. When new data is added to the blockchain, its hash is computed, and this hash is stored within the subsequent block, linking it to the previous data.

By comparing the computed hash of a particular data entry with the stored hash on the blockchain, data integrity can be verified. Any alteration to the data would result in a different hash value, immediately indicating tampering or data corruption. This cryptographic verification process adds another layer of security and trust to the integrity of the data in IoMT-based assistive systems. In summary, blockchain technology offers a robust solution for ensuring data integrity and creating an immutable audit trail in IoMT-based assistive systems. By adding the decentralized and transparent nature of blockchain, healthcare providers can rely on the integrity of the data, enhance trust, and streamline compliance with regulatory requirements.

4.3 Secure Identity Management, Access Control and Permissioned Blockchains in IoMT-based Assistive Systems

Secure identity management, access control, and the use of permissioned blockchains are essential components in ensuring the confidentiality, privacy, and secure operation of IoMT-based assistive systems. Here's how these aspects contribute to the overall security:

- Secure Identity Management: Secure identity management is important in IoMT systems to establish the identities of participants, devices, and entities accessing the network. It involves the secure creation, storage, and verification of digital identities associated with individuals, devices, and healthcare providers. Blockchain technology can provide a decentralized and tamper-resistant framework for secure identity management. By adding blockchain, participants can have unique digital identities stored on the blockchain, secured through public-private key cryptography. These digital identities can be used for authentication, authorization, and access control purposes, ensuring that only authorized entities can interact with the IoMT system. Blockchain-based identity management reduces the risk of identity theft, impersonation, and unauthorized access to sensitive healthcare data.
- Access Control: Access control mechanisms are essential to restrict access to sensitive data and functionalities within IoMT-based assistive systems. Access control ensures that only authorized individuals or entities have the necessary privileges to view, modify, or interact with specific data or functionalities. Blockchain can facilitate secure and decentralized access control by integrating access control rules into smart contracts. With blockchain-based access control, the rules defining who can access which data or perform specific actions are encoded in smart contracts stored on the blockchain. Smart contracts automatically enforce these access control rules, allowing only authorized entities to perform predefined operations.

Blockchain's transparency enables participants to independently verify and audit access control policies, reducing the risk of unauthorized access or data breaches.

- Permissioned Blockchains: Permissioned blockchains provide an additional layer of security and control in IoMT-based assistive systems. Unlike public blockchains, permissioned blockchains restrict access to participate in the network and validate transactions to a predefined set of trusted entities. This approach enables healthcare organizations to maintain greater control over the network and ensure compliance with privacy and regulatory requirements. With a permissioned blockchain, healthcare organizations can restrict participation to trusted entities such as healthcare providers, medical device manufacturers, and regulatory bodies. This helps establish a trusted network environment and allows for more efficient governance, privacy protection, and scalability. Permissioned blockchains also enable faster consensus and transaction validation, making them suitable for enterprise-level healthcare applications.
- Privacy-Enhancing Technologies: In IoMT-based assistive systems, privacy-enhancing technologies can be integrated with permissioned blockchains to further protect sensitive healthcare data. Techniques like zero-knowledge proofs, differential privacy, and secure multi-party computation can be employed to ensure data privacy and confidentiality. These technologies allow computations and analyses to be performed on encrypted or aggregated data, minimizing the exposure of sensitive information. By combining privacy-enhancing technologies with permissioned blockchains, healthcare organizations can strike a balance between data security and accessibility, enabling secure data sharing and analysis while protecting patient privacy.

Hence implementing secure identity management, access control, and utilizing permissioned blockchains provide healthcare organizations with greater control over their IoMT-based assistive systems, mitigating the risks associated with unauthorized access, data breaches, and privacy violations. These measures help protect patient data, ensure compliance with regulatory requirements, and enhance the overall security and trustworthiness of the system.

4.4 Encryption and Privacy Preservation in IoMT-Based Assistive Systems

Encryption and privacy preservation are important components of ensuring the confidentiality and security of sensitive data in IoMT-based assistive systems. Here's how encryption and privacy preservation techniques contribute to protecting data in such systems:

- Data Encryption: Encryption is the process of encoding data in such a way that it becomes unreadable to unauthorized individuals. In IoMT systems, encryption is used to protect data both at rest and in transit. By applying strong encryption algorithms, sensitive patient data, such as medical records, diagnostic information, and real-time health monitoring data, can be safeguarded. When data is transmitted between devices, networks, or stored in databases or cloud infrastructure, encryption ensures that even if intercepted or accessed by unauthorized parties, the data remains unintelligible without the encryption keys. Encryption helps prevent unauthorized access, data breaches, and the misuse of patient information, providing an additional layer of protection to sensitive healthcare data.
- End-to-End Encryption: End-to-end encryption (E2EE) ensures that data remains encrypted throughout its entire journey, from the source device to the intended recipient. In IoMT systems, where data may flow through multiple nodes or network segments, E2EE ensures that only authorized parties with the necessary decryption keys can access and interpret the data. E2EE prevents unauthorized interception or tampering of data by encrypting it at the source and decrypting it only at the destination, effectively protecting the data while in transit. This is particularly important for sensitive medical data transmitted between medical devices, healthcare providers, and cloud servers.
- Homomorphic Encryption: Homomorphic encryption is an advanced encryption technique that allows computation to be performed on encrypted data without decrypting it. This privacy-preserving technique enables secure data analysis and processing in IoMT systems without exposing the underlying sensitive data. With homomorphic encryption, medical data can be encrypted and stored in a cloud or shared for analysis while preserving the privacy of the data. Healthcare providers or researchers can perform computations on the encrypted data, generating results without accessing the original data. This technique enhances data privacy and confidentiality, enabling secure data sharing and analysis while maintaining control over sensitive information.
- Differential Privacy: Differential privacy is a technique used to protect the privacy of individual data while allowing aggregated analysis. It adds statistical noise or randomness to the data to prevent the identification of individuals within a dataset. Differential privacy techniques can be employed in IoMT-based assistive systems to balance the need for data analysis and privacy preservation. By applying differential privacy, healthcare organizations can

share aggregated or anonymized data for research, population health analysis, or public health initiatives without compromising the privacy of individual patients. This helps address privacy issues while enabling important information from large-scale data analysis.

- Data Minimization and Access Controls: Data minimization is the practice of collecting and storing only the minimum amount of necessary data. By implementing data minimization strategies, IoMT systems can reduce the amount of sensitive data at risk, minimizing the potential impact of a data breach or privacy violation. Access controls play an important role in IoMT systems to restrict access to sensitive data to authorized individuals or entities. Role-based access control, strong authentication mechanisms, and granular access permissions help ensure that only authorized personnel can access specific data, further enhancing data privacy and security.

By employing encryption techniques, end-to-end encryption, homomorphic encryption, differential privacy, data minimization, and access controls, IoMT-based assistive systems can protect patient privacy, mitigate the risks of unauthorized access and data breaches, and enable secure and confidential data sharing and analysis. These measures are essential to maintaining patient trust, complying with privacy regulations, and fostering the adoption of IoMT technologies.

5. IMPLEMENTATION OF BLOCKCHAIN IN IOMT-BASED ASSISTIVE SYSTEMS

5.1 Critical Challenges and Open Issues in IoMT-Based Assistive Systems

While IoMT-based assistive systems offer numerous benefits, there are several critical challenges and open issues that need to be addressed for their successful implementation and widespread adoption. Here are some key challenges and open issues in IoMT-based assistive systems:

- Privacy and Data Security: Ensuring the privacy and security of sensitive patient data is a significant challenge in IoMT systems. Protecting data from unauthorized access, breaches, and ensuring secure data transmission and storage require robust encryption, access controls, and adherence to privacy regulations. Additionally, addressing the increasing sophistication of cyber threats and staying ahead of potential vulnerabilities is a continuous challenge.

- Interoperability and Standardization: IoMT systems involve a variety of devices, sensors, and software from different manufacturers. Achieving interoperability and standardization is critical to enable seamless communication and data exchange between different components of the IoMT ecosystem. Lack of interoperability and standardized protocols can hinder data integration, collaboration, and limit the scalability of IoMT-based assistive systems.
- Scalability and Infrastructure: IoMT systems generate a large amount of data that needs to be processed, stored, and analyzed in real-time. Scalability is a significant challenge, as the infrastructure must handle the increasing volume, velocity, and variety of data generated by IoMT devices. Ensuring sufficient computing power, storage capacity, and network bandwidth to support the growth of IoMT systems is critical.
- Ethical and Legal Issues: The deployment of IoMT-based assistive systems raises ethical and legal questions regarding consent, data ownership, liability, and patient autonomy. Balancing the benefits of collecting and analyzing patient data with individual privacy rights and ethical issues requires clear policies, regulatory frameworks, and stakeholder engagement to ensure responsible and ethical use of IoMT technologies.
- Human-Machine Interaction: IoMT systems introduce new modes of interaction between humans and machines. Ensuring a seamless and user-friendly experience, appropriate training and education for healthcare professionals and patients, and addressing usability challenges are critical to foster acceptance and adoption of IoMT-based assistive systems. Human factors, user experience, and the impact on patient-provider relationships need careful consideration.
- Reliability and Resilience: The reliable operation of IoMT systems is important for patient safety and continuity of care. Dependence on network connectivity, system availability, and the potential for technical failures pose challenges to system reliability. Robust backup and recovery mechanisms, fail-safe modes, and proactive maintenance are required to ensure system resilience and minimize disruptions to patient care.
- Regulatory and Reimbursement Frameworks: IoMT technologies often outpace the development of regulatory and reimbursement frameworks. Ensuring that regulatory bodies can keep up with the rapid advancements in IoMT-based assistive systems is essential to address safety, efficacy, privacy, and ethical issues. Additionally, developing reimbursement models that recognize the value and impact of IoMT technologies on patient outcomes is essential to encourage adoption by healthcare providers.

Hence, these critical challenges and open issues require collaboration among healthcare providers, technology developers, regulatory bodies, and other stakeholders. Continuous innovation, standardization efforts, robust cybersecurity practices, ethical frameworks, and clear regulatory guidance are necessary to overcome these challenges and unlock the full potential of IoMT-based assistive systems in improving patient care and outcomes.

6. BENEFITS AND LIMITATIONS OF BLOCKCHAIN-BASED CYBERSECURITY IN IOMT-BASED ASSISTIVE SYSTEMS

Blockchain-based cybersecurity offers several benefits and limitations when applied to IoMT-based assistive systems. We explain benefits and limitation as:

Benefits:

- Data Integrity: Blockchain ensures data integrity by providing a tamper-resistant and immutable ledger. Transactions recorded on the blockchain are verified and stored in a transparent and decentralized manner, making it difficult for unauthorized parties to alter or manipulate the data. This enhances the integrity and trustworthiness of sensitive healthcare data in IoMT systems.
- Enhanced Security: Blockchain's cryptographic algorithms and consensus mechanisms provide robust security for IoMT-based assistive systems. Encryption techniques protect data privacy, while decentralized consensus ensures that transactions are validated by multiple nodes, reducing the risk of single-point failures and malicious attacks. Blockchain's transparency also facilitates the identification of suspicious activities, enhancing overall system security.
- Decentralization and Resilience: Blockchain's decentralized nature eliminates the reliance on a central authority, making IoMT systems more resilient to attacks and system failures. As the blockchain operates on a distributed network of nodes, compromising a single node does not compromise the entire system. This decentralization enhances the overall resilience and availability of IoMT-based assistive systems.
- Auditable and Transparent: Blockchain provides an auditable and transparent environment, enabling traceability and accountability in IoMT systems. All transactions recorded on the blockchain can be audited, helping with compliance, regulatory requirements, and dispute resolution. The transparency of blockchain also enhances trust among participants, as they can independently verify the integrity and accuracy of the recorded data.

Limitations:

- Scalability: Blockchain faces scalability challenges when it comes to processing a high volume of transactions and storing large amounts of data. In IoMT-based assistive systems, which generate substantial data in real-time, scaling blockchain to accommodate the transactional demands and storage requirements can be a significant limitation. Innovative solutions are needed to address scalability issues while maintaining the security and integrity of the system.
- Performance and Speed: The consensus mechanisms employed by blockchain, such as Proof of Work or Proof of Stake, require computational resources and time to validate transactions. This can introduce latency in transaction processing, which may not be suitable for real-time IoMT applications that require immediate responses and actions. Balancing security with performance is a challenge in blockchain-based cybersecurity for IoMT systems.
- Regulatory and Compliance issues: The adoption of blockchain in IoMT-based assistive systems may introduce complexities regarding regulatory compliance. Compliance with privacy regulations, such as HIPAA, can be challenging when data is stored and shared on a distributed blockchain network. Navigating regulatory frameworks and ensuring compliance while adding the benefits of blockchain technology requires careful consideration and collaboration with regulatory bodies.
- Implementation and Integration: Integrating blockchain into existing IoMT infrastructure and legacy systems can be complex and costly. It may require significant changes to existing systems, data migration, and the development of new interfaces. Seamless integration and interoperability with various devices, platforms, and stakeholders are important to realizing the full potential of blockchain-based cybersecurity in IoMT-based assistive systems.

In summary, while blockchain-based cybersecurity brings notable benefits in terms of data integrity, enhanced security, decentralization, and transparency, there are challenges related to scalability, performance, regulatory compliance, and integration. Overcoming these limitations requires continuous research, innovation, and collaboration between blockchain developers, healthcare providers, regulators, and technology vendors to optimize the implementation of blockchain in IoMT-based assistive systems. Blockchain can help us in healthcare via enhancing data security and integrity, improving privacy and confidentiality, reducing data breach risks, trust and transparency in data exchange (between users and service providers).

7. OPEN ISSUES AND CHALLENGES TOWARDS IMPLEMENTING BLOCKCHAIN-BASED CYBERSECURITY FOR IOMT-BASED ASSISTIVE SYSTEMS

Implementing blockchain-based cybersecurity for IoMT-based assistive systems comes with several open issues and challenges. Addressing these challenges is essential ensure the successful deployment and adoption of blockchain technology in securing IoMT systems. Here are some key open issues and challenges:

- Scalability: Scaling blockchain to handle the high volume of transactions and data generated by IoMT-based assistive systems is a significant challenge. Current blockchain networks, such as Bitcoin or Ethereum, may struggle to handle the throughput and latency requirements of real-time healthcare applications. Developing scalable blockchain solutions or integrating blockchain with other technologies to address scalability issues is essential.
- Interoperability: Achieving interoperability between different blockchain platforms, existing healthcare systems, and IoMT devices is essential. Seamless integration and data exchange between various systems require standardized protocols and interfaces. Developing interoperability frameworks that allow different blockchain networks and healthcare systems to interact efficiently is an ongoing challenge.
- Governance and Regulatory Frameworks: Blockchain introduces new governance models and challenges existing regulatory frameworks. The decentralized and distributed nature of blockchain systems raises questions regarding accountability, liability, and compliance with healthcare regulations. Developing appropriate governance and regulatory frameworks that address legal, privacy, security, and ethical issues is necessary to foster the adoption of blockchain-based cybersecurity in IoMT systems.
- Privacy and Confidentiality: Ensuring privacy and confidentiality while adding the transparency of blockchain is a complex task. Balancing the need for transparent transaction verification with protecting sensitive healthcare data is essential. Innovative cryptographic techniques, privacy-preserving protocols, and consensus mechanisms need to be developed to address privacy issues and comply with regulations such as HIPAA.
- Energy Efficiency: Traditional blockchain consensus mechanisms, such as Proof of Work, consume significant amounts of energy. In the context of IoMT-based assistive systems, where energy efficiency is critical, blockchain's energy consumption can be a challenge. Developing and adopting more energy-efficient consensus mechanisms, such as Proof of

Stake or improved consensus algorithms, is necessary to reduce the carbon footprint of blockchain-based solutions.

- User Experience and Adoption: User experience plays an important role in the adoption of blockchain-based cybersecurity solutions. Ensuring a seamless and user-friendly experience for healthcare professionals, patients, and other stakeholders is essential. Designing intuitive interfaces, providing user education and training, and addressing the complexity associated with blockchain technology can help improve user adoption.
- Cost and Infrastructure Requirements: Implementing blockchain-based cybersecurity solutions requires significant investment in infrastructure, including computing power, storage, and network resources. The costs associated with deploying and maintaining blockchain networks can be a barrier to adoption, particularly for small healthcare providers or resource-constrained settings. Identifying cost-effective deployment models and incentivizing participation in the blockchain ecosystem are important considerations.

Hence, these open issues and challenges require collaboration among blockchain developers, healthcare providers, regulatory bodies, and technology vendors. Continuous research and innovation, standardization efforts, regulatory support, and interdisciplinary collaboration are important to overcome these challenges and realize the full potential of blockchain-based cybersecurity in IoMT-based assistive systems.

8. FUTURE RESEARCH OPPORTUNITIES TOWARDS IMPLEMENTING BLOCKCHAIN-BASED CYBERSECURITY FOR IOMT-BASED ASSISTIVE SYSTEMS

The implementation of blockchain-based cybersecurity for IoMT-based assistive systems presents several promising research opportunities. Addressing these areas can contribute to the development and advancement of secure and resilient IoMT systems. Here are some future research opportunities in this domain:

- Scalable Blockchain Solutions: Developing scalable blockchain solutions specifically tailored for IoMT-based assistive systems is a critical research area. Exploring new consensus algorithms, sharding techniques, or sidechains to increase transaction throughput and reduce latency can enhance the scalability of blockchain in healthcare applications. Additionally, investigating the integration of emerging technologies like off-chain computation and state channels can optimize the performance of blockchain networks.

- Privacy-Preserving Techniques: Enhancing privacy-preserving mechanisms in blockchain-based cybersecurity for IoMT systems is important. Researching privacy-enhancing technologies, such as zero-knowledge proofs, differential privacy, or secure multi-party computation, can enable secure data sharing, analysis, and collaborative research while preserving patient privacy. Developing novel privacy-preserving algorithms and protocols tailored to the unique requirements of healthcare data is an important area of exploration.
- Interoperability and Standardization: Fostering interoperability and standardization among different blockchain platforms, healthcare systems, and IoMT devices is essential. Researching interoperability frameworks, developing standardized protocols for data exchange, and exploring blockchain integration with existing healthcare standards (e.g., HL7, FHIR) can enable seamless communication and data sharing. Additionally, investigating the use of interoperability layers or middleware to bridge different blockchain networks can enhance interoperability in IoMT-based assistive systems.
- Hybrid Blockchain Architectures: Researching hybrid blockchain architectures that combine the benefits of public and private blockchains can be beneficial for IoMT-based systems. Investigating the design and implementation of hybrid networks that provide a balance between data transparency and privacy, while meeting scalability and performance requirements, is an area of interest. Developing mechanisms for secure data exchange between public and private blockchains can enable secure and interoperable IoMT ecosystems.
- Machine Learning and Artificial Intelligence for Security: Exploring the integration of machine learning and artificial intelligence techniques with blockchain-based cybersecurity can strengthen IoMT systems' security. Investigating the use of AI for anomaly detection, threat intelligence, and automated response mechanisms can enhance the ability to detect and mitigate cyber threats in real-time. Developing AI-driven approaches to secure key management, access controls, and authentication can bolster the overall security posture of IoMT-based assistive systems.
- Usability and Human Factors: Investigating the usability aspects of blockchain-based cybersecurity solutions in IoMT systems is important for user acceptance and adoption. Researching intuitive user interfaces, user-centric design principles, and user experience evaluations can help overcome the complexity and usability challenges associated with blockchain technology. Additionally, exploring the impact of blockchain-based security measures on the workflow, decision-making, and patient-provider interactions

is important for understanding the human factors involved in IoMT-based assistive systems.

- Ethical and Legal issues: Researching the ethical implications and legal frameworks surrounding blockchain-based cybersecurity in IoMT systems is essential. Examining the ethical challenges related to patient consent, data ownership, and the right to be forgotten in blockchain systems can inform the development of ethical guidelines and best practices. Investigating the regulatory landscape and identifying legal frameworks that can accommodate the unique characteristics of blockchain technology in healthcare is critical for fostering its adoption.

Hence, these research opportunities can significantly contribute to the advancement and implementation of blockchain-based cybersecurity in IoMT-based assistive systems. Collaboration between academia, industry, healthcare providers, and regulatory bodies is essential for addressing these research areas and ensuring the secure and efficient utilization of blockchain technology in IoMT applications. We can use blockchain for evolving blockchain technologies and its standards, increasing interoperability and interconnected blockchain networks, using of AI and blockchain integration for advanced threat detection and blockchain-based data analytics and machine learning for threat detection/ malware analysis.

9. CONCLUSION

This chapter has started about blockchain, its uses in healthcare and later we discuss about IoMT devices. Further we discuss about Blockchain based cyber security to overcome raised issues in healthcare. We find out that the use of standardized blockchain protocols ensures secure data exchange and communication among devices, improving system compatibility and integration. Blockchain-based cybersecurity ensures the integrity and traceability of medical device data by recording transactions and events on the blockchain. Any tampering or unauthorized modifications to the data are detectable, ensuring data authenticity and preventing data manipulation. blockchain-based cybersecurity solutions can facilitate secure interoperability between different IoMT devices and systems. Hence, blockchain based cyber security for healthcare is a necessity to future/ next generation society with minimum hurdles/ issues or maximum privacy preservation and trust among user/ service providers.

REFERENCES

Agrawal, D., Bansal, R., Fernandez, T. F., & Tyagi, A. K. (2022). Blockchain Integrated Machine Learning for Training Autonomous Cars. In: Lecture Notes in Networks and Systems. Springer, Cham. doi:10.1007/978-3-030-96305-7_4

Al Omar, A., Elbouanani, F., & Boudguiga, A. (2018). Blockchain-based access control for secure health data sharing in the cloud environment. In *International Conference on e-Infrastructure and e-Services for Developing Countries* (pp. 187-200). Springer.

Aswathy, S. U. (2021). The Future of Edge Computing with Blockchain Technology: Possibility of Threats, Opportunities and Challenges. Recent Trends in Blockchain for Information Systems Security and Privacy. CRC Press.

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. In *Proceedings of the 2nd International Conference on Open and Big Data (OBD)* (pp. 25-30). IEEE. 10.1109/OBD.2016.11

Bai, Q., & Liu, L. (2020). Blockchain-based secure and efficient data sharing scheme for IoT-enabled healthcare applications. *Journal of Medical Systems*, *44*(8), 146.

Dagher, G. G., Mohler, J., Milojkovic, M., Marella, P. B., & Ouaddah, A. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297. doi:10.1016/j.scs.2018.02.014

Deshmukh, A., Patil, D., & Tyagi, A. K. (2022). Recent Trends on Blockchain for Internet of Things based Applications: Open Issues and Future Trends. In *Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing (IC3-2022)*. Association for Computing Machinery. 10.1145/3549206.3549289

Gope, P., & Jara, A. J. (2018). Blockchain-based approach to enhance privacy and scalability in the Internet of Things. *Future Generation Computer Systems*, *82*, 860–873.

Jayaprakash, V., & Tyagi, A. K. (2022). Security Optimization of Resource-Constrained Internet of Healthcare Things (IoHT) Devices Using Asymmetric Cryptography for Blockchain Network. In: Giri, D., Mandal, J.K., Sakurai, K., De, D. (eds) *Proceedings of International Conference on Network Security and Blockchain Technology*. Springer, Singapore. 10.1007/978-981-19-3182-6_18

Li, S., & Da Xu, L. (2018). Blockchain-based secure firmware update for Internet of Things devices in an industrial 4.0 environment. *IEEE Transactions on Industrial Informatics*, *14*(8), 3690–3699.

Liao, W. H., Hsu, P. F., & Lai, C. F. (2018). Secure authentication framework for Internet of Things-based medical information systems using blockchain. *Journal of Medical Systems*, *42*(8), 144. PMID:29959535

Lu, Q., Li, X., Liang, X., Huang, J., & Shen, J. (2018). A lightweight blockchain-based system for secure medical data sharing. *Journal of Medical Systems*, *42*(8), 152. PMID:29974270

Mishra, S., & Tyagi, A. K. (2019). Intrusion Detection in Internet of Things (IoTs) Based Applications using Blockchain Technology. *2019 Third International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC),* (pp. 123-128). ACM. 10.1109/I-SMAC47947.2019.9032557

Nair, M. M., & Tyagi, A. K. (2022). Preserving Privacy Using Blockchain Technology in Autonomous Vehicles. In: Giri, D., Mandal, J.K., Sakurai, K., De, D. (eds) *Proceedings of International Conference on Network Security and Blockchain Technology.* Lecture Notes in Networks and Systems. Springer, Singapore. 10.1007/978-981-19-3182-6_19

Nair, M. M., & Tyagi, A. K. (2023). AI, IoT, blockchain, and cloud computing: The necessity of the future. R. Pandey, S. Goundar, S. Fatima, (eds.) Distributed Computing to Blockchain. Academic Press. doi:10.1016/B978-0-323-96146-2.00001-2

Ng, J., Wai, A. A., & Leung, V. C. (2018). DSecure: A blockchain-based secure data sharing framework for health IoT. *IEEE Access : Practical Innovations, Open Solutions*, *6*, 14751–14763.

Ouaddah, A., Elkalam, A. A., & Ouahman, A. A. (2017). FairAccess: A new Blockchain-based access control framework for the Internet of Things. *Security and Communication Networks*, 2017.

Pandey, A. A., Fernandez, T. F., Bansal, R., & Tyagi, A. K. (2022). Maintaining Scalability in Blockchain. In A. Abraham, N. Gandhi, T. Hanne, T. P. Hong, T. Nogueira Rios, & W. Ding (Eds.), *Intelligent Systems Design and Applications. ISDA 2021. Lecture Notes in Networks and Systems* (Vol. 418). Springer. doi:10.1007/978-3-030-96308-8_4

Sawal, N., Yadav, A., Tyagi, A., Sreenath, N. & Rekha, G. (2019). Necessity of Blockchain for Building Trust in Today’s Applications: An Useful Explanation from User’s Perspective (May 15,). doi:10.2139/ssrn.3388558

Sheth, H. S. K. (2022). Deep Learning, Blockchain based Multi-layered Authentication and Security Architectures. *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, (pp. 476-485). ACM. 10.1109/ICAAIC53929.2022.9793179

Shih, F. Y., Kuo, T. T., & Lee, W. H. (2018). Blockchain-based tamper-resistant authentication for electronic health records exchange. *Journal of Medical Systems*, *42*(8), 153. PMID:29987660

Siddharth, M. (2021). Issues and Challenges (Privacy, Security, and Trust) in Blockchain-Based Applications. In: Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles. doi:10.4018/978-1-7998-3295-9.ch012

Sun, Y., Zhang, X., Wen, Q., & Yao, L. (2018). MEDshare: Trustworthy medical data sharing through blockchain. *IEEE Transactions on Dependable and Secure Computing*, *17*(5), 1063–1076.

Tibrewal, I., Srivastava, M., & Tyagi, A. K. (2022). Blockchain Technology for Securing Cyber-Infrastructure and Internet of Things Networks. In A. K. Tyagi, A. Abraham, & A. Kaklauskas (Eds.), *Intelligent Interactive Multimedia Systems for e-Healthcare Applications*. Springer. doi:10.1007/978-981-16-6542-4_17

Tyagi, A & Nair, M. (2022). Preserving Privacy using Distributed Ledger Technology in Intelligent Transportation System. In *Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing (IC3-2022).* Association for Computing Machinery. 10.1145/3549206.3549306

Tyagi, A. (2021). Analysis of Security and Privacy Aspects of Blockchain Technologies from Smart Era' Perspective: The Challenges and a Way Forward. Recent Trends in Blockchain for Information Systems Security and Privacy. CRC Press.

Tyagi, A. (2021, October). AARIN: Affordable, Accurate, Reliable and INnovative Mechanism to Protect a Medical Cyber-Physical System using Blockchain Technology. *IJIN*, *2*, 175–183.

Tyagi, A. (2023). Decentralized everything: Practical use of blockchain technology in future applications. R. Pandey, S. Goundar, S. Fatima, (eds) Distributed Computing to Blockchain. Academic Press. doi:10.1016/B978-0-323-96146-2.00010-3

Tyagi, A. (2021). Applications of Blockchain Technologies in Digital Forensic and Threat Hunting. Recent Trends in Blockchain for Information Systems Security and Privacy. CRC Press.

Tyagi, A. K. (2022). SecVT: Securing the Vehicles of Tomorrow Using Blockchain Technology. In A. A. Sk, T. Turki, T. K. Ghosh, S. Joardar, & S. Barman (Eds.), *Artificial Intelligence. ISAI 2022. Communications in Computer and Information Science* (Vol. 1695). Springer. doi:10.1109/ICCCI54379.2022.9740965

Tyagi, A. K., Chandrasekaran, S., & Sreenath, N. (2022). Blockchain Technology:– A New Technology for Creating Distributed and Trusted Computing Environment. *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC),* (pp. 1348-1354). ACM. 10.1109/ICAAIC53929.2022.9792702

Tyagi, A. K., Fernandez, T. F., & Aswathy, S. U. (2020). *Blockchain and Aadhaar based Electronic Voting System*. 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore. 10.1109/ICECA49313.2020.9297655

Varsha, R. (2022). Security Optimization of Resource-Constrained Internet of Healthcare Things. (IoHT) Devices Using Lightweight Cryptography, In: Information Security Practices for the Internet of Things, 5G, and Next-Generation Wireless Network. IGI Global. doi:10.4018/978-1-6684-3921-0.ch009

Varsha, R. (2020, January 1). 'Deep Learning Based Blockchain Solution for Preserving Privacy in Future Vehicles'. *International Journal of Hybrid Intelligent Systems*, *16*(4), 223–236.

Yue, X., Wang, H., Jin, D., Li, M., & Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *Journal of Medical Systems*, *40*(10), 218. doi:10.100710916-016-0574-6 PMID:27565509

Zeng, X., Wang, X., & Tian, H. (2018). Secure data sharing and searching at the edge of cloud-assisted Internet of Things. *IEEE Transactions on Industrial Informatics*, *14*(7), 3014–3022.

Zhang, P., Schmidt, D. C., White, J., & Lenz, G. (2017). Blockchain technology use cases in healthcare. *Advances in Computers*, *103*, 1–39.