Bridging the gap through a literature review on enhancing anonymization techniques for seamless integration within the IoMT ecosystem.

Yuvraj Singh Thakur[1], Aaditya Singh[1], Aakash Shukla[1], Akash Singh[1], Ayush Sahu[1], and Tushar Khandelwal[1]

Bhilai Institute of Technology, Bhilai House, Durg, Chhattisgarh, India

ARTICLE INFO

Keywords:
Internet of Medical Things (IoMT)
Anonymization Techniques
Data Privacy
Security
Real-Time Processing
Advanced Technologies

ABSTRACT

The Internet of Medical Things (IoMT) is a transformative shift in healthcare, allowing for interconnection of medical devices and systems to improve patient care and operational efficiency. However, integration of IoMT also presents some significant challenges related to data privacy and security, requiring the development of strong anonymization techniques to protect sensitive health information. This literature review analyzes the existing anonymization methods: k-anonymity, differential privacy, and data perturbation, indicating their advantages and disadvantages with respect to IoMT. Some of the major challenges are scalability, real-time processing of data, and the requirement of standardized methodologies. Further, advanced technologies such as Homomorphic Encryption and Federated Learning have the potential to further improve privacy protections. Recommendations for future research highlight hybrid approaches, interdisciplinary collaboration, and the establishment of frameworks that would facilitate the effective implementation of anonymization techniques across diverse IoMT applications. By addressing these critical areas, this paper will contribute to the ongoing discourse on enhancing data privacy and security in the rapidly evolving landscape of IoMT.

Introduction

The Internet of Medical Things, or IoMT, is a paradigm shift in the healthcare industry which relies on interlinked medical appliances, wearables, and health systems to revolutionize the treatment of patients while also maximizing the efficiency of health services (Akilan et al., 2023). IoMT provides focused and individualized medical treatment, seamless exchange of medical information, and coordination of different smart appliances on an integrated platform for healthcare information. According to Chenxi Huang et al. (2023), applications of IoMT include remote patient monitoring, telemedicine, smart hospitals, and infectious disease tracking.

While IoMT provides numerous benefits, including cost-effectiveness in health care and improved quality of treatment, it has issues of data security, interoperability, and ethical issues. Shashank P. Kumar et al. (2020) argues that these challenges must be addressed for the sustainable growth of IoMT. Future directions for IoMT research are artificial intelligence, personalized medicine, and addressing scalability issues, as noted by Akilan et al. (2023).

The Internet of Medical Things (IoMT) is revolutionizing healthcare by integrating medical devices and allowing for real-time data transmission and processing (Pradyumna et al., 2024). IoMT enhances the accuracy, reliability, and productivity of electronic devices in healthcare. According to Kagita et al. (2020), it allows remote patient monitoring, telemedicine, and personalized care and leads to better patient outcomes and reduced healthcare costs.

Despite all the benefits offered by IoMT, challenges in the form of data security, privacy concerns, interoperability issues, and regulatory complexities must be overcome for its mass adoption. According to Nishad & Tripathi (2020), The future trends in IoMT include the integration of machine learning, blockchain technology, and industry 5.0 concepts as more promising factors that will revolutionize healthcare delivery and management further (Mathkor et al., 2024).

Anonymization is crucial for data privacy in Internet of Medical Things (IoMT) ecosystems. It helps mitigate privacy

risks while balancing data quality and output (Colonna, 2020). According to Neves et al. (2023), various anonymization techniques, particularly k-anonymity combined with other methods, have shown promise in addressing privacy concerns in IoT environments.

For IoMT cloud systems, sensitive data privacy can be achieved through anonymization and setting different privacy levels for cloud types (Aileni et al., 2020). The IoMT ecosystem presents significant security and privacy issues due to its complexity as well as the evolving nature of cyber threats. In this context, Rajab et al. (2024) opine that frameworks and regulations notwithstanding, it is urgently required to define specific IoMT security, guidelines, and policies that are more tailored to suit the need of IoMT. Interdisciplinary collaboration involving healthcare, government, and technology players is necessary in order to develop effective regulation and best practices for maintaining cybersecurity and data privacy in the IoMT ecosystem.

The Internet of Medical Things (IoMT) faces significant security and privacy challenges due to its interconnected nature and the sensitivity of healthcare data (Smys & Raj, 2022). Such major concerns of big data are integrity data, privacy issues, and requiring more space for storage together with enhanced computing capabilities. Says Rathnayake et al. (2018), that such problems warrant strong solutions like multi-security encryption mechanisms in cloud structures.

To overcome these challenges, a combination of cryptographic and non-cryptographic approaches can be proposed. Advanced technologies in the form of Homomorphic Encryption, Differential Privacy, and Federated Learning were explored by Wani et al. (2024). In any case, this continuously evolving nature of cyber threats and the intrinsic complexity of IoMT ecosystems would continuously require the development of the specific security measures, guidelines, and policies in support. Rajab et al. (2024) emphasizes that collaboration among healthcare, government, and technology stakeholders is crucial for establishing effective regulations and best practices to ensure the security and privacy of IoMT environments.

Existing anonymization techniques for IoMT, or Internet of Medical Things, focus on privacy preservation and data utility. K-anonymity, often combined with other methods, has proven effective in IoT environments (Flávio Neves et al., 2023). Partitioning-based approaches have been proposed to anonymize IoT data streams by Ankhbayar Otgonbayar et al. (2016) that deal with missing values and variable data widths.

Researchers now focus on risk-mitigation strategies, such as anonymization and synthetic data generation, balancing privacy concerns and quality requirements in the context of the IoHT. Indeed, according to Liane Colonna (2020), pseudonymity and anonymization are key factors for ensuring security in shared medical data. Horizontal data distribution is widely used in the field of healthcare applications. While these techniques promise, no consensus has been achieved toward standardized methodologies applicable to all IoT scenarios. Thereby, further research is required toward addressing privacy issues in IoMT (Flávio Neves et al., 2023).

Existing anonymization techniques in IoMT face several limitations. While k-anonymity has shown promise when combined with other methods, there is a lack of consensus on standardized solutions applicable across all IoT scenarios (Flávio Neves et al., 2023). According to Shilan S. Hameed et al. (2021), traditional security measures struggle to adapt to IoMT systems, and machine learning approaches, while promising, often neglect crucial performance metrics like resource complexity and power usage.

Key issues are privacy protection, renewable energy sources, sensor intelligence, and data speed. Inas Al Khatib et al. (2024) argued that IoMT devices have limited processing power, thus cannot implement robust security techniques to protect patient data during transfer. The proposed solutions are edge-fog computing, blockchain, and advanced cryptographic methods; however, further research is needed to address these limitations and develop more effective anonymization techniques for IoMT systems (Akshat Gaurav et al., 2022).

Background on Anonymization Techniques

Overview of Existing Anonymization Techniques

Anonymization techniques play a significant role in protecting the privacy of individual data subjects while still providing the freedom to share and analyze data. There are two primary forms of anonymization techniques, which include k-anonymity, differential privacy, and data perturbation.

K-Anonymity ensures that each individual in a dataset cannot be distinguished from at least k-1 others, typically achieved through generalization and suppression of data attributes (Chen, 2023). Patil & Wang (2023) claim that the new development includes a novel k-anonymity algorithm with dissimilarity tree-based clustering that decreases information loss up to 20% from conventional approaches.

Differential privacy offers a mathematical model enabling data sharing while excluding and adding just a single individual's data do not meaningfully impact the results of any given analysis (Marri et al., 2024). Xu et al. (2024) argue that this technique is particularly effective in environments like new media platforms, where user data is abundant and privacy concerns are paramount.

Data perturbation is the modification of the data in a small way, in order to prevent individual identification while preserving data utility overall. Gadotti et al. (2024) define this as the injection of noise or change in values in a controlled fashion. Although these techniques offer strong privacy protections, they are not without their caveats. For example, k-anonymity becomes vulnerable to attacks if k is too small, and differential privacy may result in a trade-off between the utility of the data and the level of privacy protection provided by the guarantees.

K-anonymity and data perturbation are key techniques for privacy preservation in traditional data environments. K-anonymity protects privacy by ensuring individuals cannot be identified within a dataset (Ajmeera Kiran & N. Shirisha, 2022). Data perturbation methods add controlled noise to data, allowing analysis while preserving privacy (Safiye Turgay & Ilter, 2023). However, these techniques face challenges with dynamic, continuously growing datasets, potentially leading to poor data quality or vulnerability to inference, as highlighted by Ji-Won Byun et al. (2006).

Other latest work has considered k-anonymity in combination with differential privacy, which lays stronger

foundations for privacy guarantees. Adding a random sample to the input before conducting the k-anonymization might easily reach (ε, δ) bounds under reasonable parameters, a contribution of Ninghui Li et al. (2011). This may serve as a complement to output perturbation methods for differential privacy beyond its typical application in micro-data publication. However, proper implementation is necessary to keep the data accurate and free of bias in analysis, according to Turgay & Ilter (2023). In summary, these techniques combined offer promising solutions to privacy preservation in dynamic datasets but depend on careful balance and implementation.

Challenges with Current Techniques in IoMT

The Internet of Medical Things (IoMT) faces several challenges in real-time data processing, large-scale data management, and high data velocity, including privacy protection, sustainable power sources, sensor intelligence, human adaptation, data speed, device reliability, and storage efficiency (Al Khatib et al., 2024). These problems are solved with the help of different solutions proposed by researchers such as network control, cryptography, edge-fog computing, and blockchain. Besides, Mavrogiorgou et al. (2019) pointed out the importance of integrating 5G network slicing and data interoperability techniques in order to better manage healthcare data. The integration of machine learning and AI in IoMT devices is both an opportunity and a challenge, especially in disease prediction and remote monitoring, as reported by Pradyumna et al. (2024). A cloud-edge AI framework, which encompasses Edge Federated Learning, has been proposed to enhance medical big data analytics with secure, real-time diagnostic feedback. (Putra et al., 2024).

The Internet of Medical Things (IoMT) faces several challenges and trade-offs in implementing security techniques. Limited computational resources on IoT devices can lead to poor performance of machine learning algorithms, as noted by Anderson et al. (2023). To address this, techniques like model pruning and offloading can improve costs and performance but may compromise inference quality (Anderson et al., 2023). The IBBD framework, according to Wong et al. (2023), would look at the optimization of trade-offs in information loss versus power overhead in IoMT data streaming. Additionally, the security measures of the IoMT systems have security levels against system performance as Yaacoub et al. (2020) and Smys & Raj (2022) discussed. It suggests lightweight cryptographic algorithms and protocols that reduce computational overhead, according to Yaacoub et al. (2020). Additionally, implementing proper security measures and providing necessary training are crucial to enhance IoMT systems' resilience against cyber-attacks, according to Yaacoub et al. (2020) and Smys & Raj (2022).

Unique Characteristics of IoMT Data

Nature of Medical Data

The Internet of Medical Things (IoMT) has revolutionized healthcare by enabling remote monitoring, personalized treatment, and data-driven decision-making, as noted by Ahmed et al. (2023) and Dimitrov (2016). IoMT devices generate vast amounts of medical data, presenting unique features and challenges. These devices, such as wearables and smart medical equipment, are continuously streaming real-time health data for the constant monitoring of health indicators of patients, as seen from the discussion by Dimitrov (2016) and Putra et al. (2024). Such data are characterized as voluminous, fast-paced, and of high variety and require analytics and AI-driven approaches to be useful for meaningful interpretation, according to Putra et al. (2024). However, the sensitive nature of this data raises significant security and privacy concerns, particularly due to the limited computational capabilities of IoMT devices, as highlighted by Sun et al. (2019). To address these challenges, researchers propose cloud-edge AI frameworks and federated learning approaches to enhance data security and processing efficiency, as suggested by Putra et al. (2024). Despite these challenges, IoMT data holds immense potential for improving healthcare outcomes and enabling preventative care strategies, according to Ahmed et al. (2023) and Dimitrov (2016).

Dynamic and Diverse Data Sources

According to Zikria et al. (2020), the IoMT provides massive volumes of heterogeneous and dynamic data that pose quite different challenges from traditional IoT data. The data resulting from IoMT are typical of variety, velocity, and volume, and therefore should be processed using big data processing techniques, as defined by Kjwan & Mohammad (2024). The semantic challenges in integrating diverse, real-time data streams for reasoning are particularly important for IoMT, Bermúdez-Edo (2016). Kjwan & Mohammad (2024) discuss how privacy is a concern in the use of the internet for transmitting medical data. Researchers have been looking into innovative solutions such as federated learning for privacy-preserving data analysis (Kjwan & Mohammad, 2024) and semantic web technologies for data integration and interoperability, according to Bermúdez-Edo (2016). According to Din et al. (2020), the IoMT field encompasses various applications, including body sensor networks, patient tracking, and predictive analytics in healthcare. These applications must contend with the unique characteristics of IoMT data, which present both challenges and opportunities for improving healthcare outcomes. It would be concluded that, even though IoMT offers a high potential for healthcare applications, it also requires careful attention to privacy, data integration, and big data processing challenges, as discussed by several researchers.

Modifications to Existing Anonymization Techniques

Adapting Techniques to IoMT

Real-time data analysis requires adaptations to support privacy preservation. Freytag et al. (2014) highlight the trade-off between privacy and utility in real-time business intelligence systems. Plagemann et al. (2022) propose tools for semi-automatic integration of privacy protection in real-time data stream applications, allowing users to specify privacy requirements. Quoc et al. (2017) introduce PRIVAPPROX, a system combining sampling and randomized response techniques to achieve privacy, utility, and low-latency in

stream processing. Ny (2020) emphasizes the importance of formal privacy definitions, such as differential privacy, to provide clear guarantees against adversaries with arbitrary side information. These papers collectively stress the need for privacy-preserving algorithms in real-time data analysis, exploring various approaches like data aggregation (Plagemann et al., 2022), approximate computing (Quoc et al., 2017), and differential privacy (Ny, 2020) to balance privacy protection with analytical utility. In conclusion, the integration of privacy-preserving techniques in real-time data analysis is critical to ensuring both data security and utility, as discussed by several authors.

Supporting Real-time Data Processing

Recent studies have concentrated on building scalable anonymization methods for large data sets, mainly in the context of IoMT devices. LeFevre & DeWitt (2007) and LeFevre et al. (2008) suggested techniques that integrate external scalability into current anonymization algorithms by means of decision tree construction and sampling. The proposed approaches guarantee that the produced output data satisfies certain anonymity constraints while preserving data quality. Vimercati et al. (2021) presented a distributed anonymization process using the Spark framework, which can handle large datasets that don't fit in main memory by partitioning the data across multiple workers. Similarly, Sameesha Vs (2017) proposed a scalable two-phase top-down specialization approach using MapReduce on cloud platforms, designed to anonymize large-scale data sets efficiently. These techniques show considerable improvements in scalability and efficiency compared to the current methods, making them suitable for handling the large and diverse data generated by IoMT devices. In summary, recent advancements in scalable anonymization methods, such as those proposed by LeFevre et al. (2007), Vimercati et al. (2021), and Sameesha Vs (2017), offer promising solutions for managing the vast amounts of data produced by IoMT devices while ensuring privacy.

Ensuring Scalability and Interoperability

As mentioned by Flávio Neves et al. (2023) and Emmanouil Palavras et al. (2018), the lack of standardization and the variety of devices, protocols, and standards pose challenges to the integration of anonymization techniques across different IoMT ecosystems. To overcome these problems, researchers have proposed frameworks and approaches for secure and interoperable interactions. A secure multi-protocol integration bridge that allows seamless communication between heterogeneous nodes and IoT protocols is SeMIBIoT, as described by Emmanouil Palavras et al. (2018).

Another framework is based on enhancing trust in decentralized IoMT environments through backtracking and vendor transparency, according to Andrzej Sobecki et al. (2020). Despite these frameworks and regulations, the need for standardized approaches with effective mechanisms to ensure IoMT security and privacy is crucial, as argued by Ramadhan Mohamed Rajab et al. (2024). Collaboration among healthcare, government, and technology stakeholders is essential to establish robust security risk assessment models and address the evolving cyber threats in the IoMT ecosystem, according to Ramadhan Mohamed Rajab et al. (2024). In conclusion, while various frameworks offer solutions for improving IoMT security and interoperability, the need for standardized approaches and collaborative efforts remains critical for tackling emerging challenges in the ecosystem.

Integration with IoMT Ecosystem

Seamless Integration of Anonymization Techniques

Internet of Medical Things (IoMT) poses many opportunities and various challenges on data privacy as well as security, it was written by Ahmed et al. (2023) Many research work has been brought into being to provide diversified smooth approaches on how anonymizing methodologies are supposed to be interfaced directly with IoMT designs. In this regard, federated learning with differential privacy, and hybrid cryptography shall guarantee end-user anonymity within an IoMT system involving computing edge and hybrid encryption end, according to Nair et al. (2023). Emerging technologies such as Physically Unclonable Functions (PUF), Blockchain, Artificial Intelligence (AI), and Software-Defined Networking (SDN) are being explored to enhance security and privacy in e-healthcare, as discussed by Razdan & Sharma (2021). A novel blockchain-enabled architecture incorporating self-sovereign identity and zero-knowledge proofs has been proposed for efficient and scalable IoMT device authentication, as outlined by Fotopoulos et al. (2020). These approaches aim to improve data protection, device security, and overall system integrity in IoMT environments while maintaining functionality and performance.

Interoperability and Standardization

Interoperability standards play a crucial role in addressing challenges faced by Internet of Medical Things (IoMT) implementations. The heterogeneity of healthcare information systems and IoMT devices poses significant obstacles to seamless data exchange and integration, as noted by Yasmeen et al. (2022) and Abdelouahid et al. (2023). HL7 FHIR has emerged as a well-adapted standard for exchanging and storing health data, with the ability to convert other formats like DICOM, CDA, and JSON for improved interoperability, according to Abdelouahid et al. (2023). Mavrogiorgou et al. (2019) have discussed some innovations, such as 5G network slicing and transformation techniques for data, enhancing data acquisition and interoperability in IoMT environments. Numerous interoperability challenges have been identified by researchers, such as the heterogeneity of devices and systems, data standardization, security and regulatory compliance. Some of the solutions proposed include ontology approaches, use of semantic frameworks, more standards, middleware design, and blockchain technology, according to Pournik et al. (2023). These advances are towards efficient data exchange and enhancement in the healthcare outcomes for the ecosystem of IoMT.

Healthcare regulations like HIPAA and GDPR play a crucial role in shaping anonymization techniques for Internet of Medical Things (IoMT) systems. These regulations require user consent for data collection and processing, emphasizing the need for robust privacy protection measures, as noted by

Said et al. (2023). IoMT frameworks and architectures must incorporate effective security mechanisms and policies to comply with these regulations, according to Ramadhan Mohamed Rajab et al. (2024). Emerging technologies such as edge computing, encryption, blockchain, and AI are being explored to address security and privacy challenges in IoMT, as discussed by Said et al. (2023) and Razdan & Sharma (2021). However, the limited computational power of IoMT devices poses challenges in implementing comprehensive security schemes, as highlighted by Sun et al. (2019). There is a critical need for tailored security measures, guidelines, and policies to ensure the widespread adoption of IoMT in clinical applications. According to Ramadhan Mohamed Rajab et al. (2024), there is a need for collaboration among healthcare, government, and technology stakeholders to establish effective regulations and best practices for IoMT security and privacy. In conclusion, the intersection of healthcare regulations, emerging technologies, and collaborative efforts is crucial to overcoming security and privacy challenges in IoMT systems.

Security and Performance Considerations

Balancing Privacy and Usability

Recent research explores anonymization techniques to balance privacy and data utility in IoT and IoMT contexts. K-anonymity, combined with other methods, has shown promise in protecting privacy while maintaining data usefulness, as discussed by Flávio Neves et al. (2023). Meta-learning approaches have been proposed to adapt anonymization to varying privacy-utility trade-offs, according to Xin Yang (2021). Contract theory provides a framework for data collectors to optimize privacy protection and data utility based on the preferences of data owners, according to Lei Xu et al. (2015). The studies suggest that privacy protection should be stronger when more data utility is needed or data is less profitable, according to Lei Xu et al. (2015). In the IoHT context, data controllers must carefully evaluate re-identification risks and select appropriate privacy models to achieve Privacy by Design principles, as emphasized by Liane Colonna (2020). Synthetic data generation has also been explored as an alternative to traditional anonymization for data sharing in IoHT, as discussed by Liane Colonna (2020).

Impact on System Performance

The Internet of Medical Things (IoMT) offers improved healthcare efficiency but faces security and privacy challenges, as noted by Yaacoub et al. (2020). Implementing appropriate security measures is crucial, with a trade-off between security level and system performance, as highlighted by Yaacoub et al. (2020) and Smys & Raj (2022). Lightweight cryptographic algorithms and protocols can reduce computational overhead, according to Yaacoub et al. (2020).

Zhao et al. (2021) have designed a lightweight privacy-preserving data sharing scheme that incorporates elliptic curve cryptography, XOR operations, and hash functions to ensure patient anonymity and access control at low computational costs. Vu Khanh et al. (2023) demonstrated that fog-to-cloud computing is more effective than cloud-based computing in satisfying the requirements of real-time applications in IoMT systems. These works underline the necessity of balancing security, privacy, and performance in IoMT systems. The goal here is to develop efficient solutions that protect patient data without compromising system responsiveness.

Ensuring data security while minimizing performance degradation is a critical challenge in modern data systems. Researchers have proposed various strategies to address this trade-off. Zorkadis (1994) suggests optimizing secure communication protocols through preprocessing, message segmenting, and compression to reduce performance overhead. Athanassoulis (2017) advocates for tunable secure data systems that offer variable levels of security and performance to meet diverse application requirements. Mattsson (2005) recommends database-level encryption as the ideal method to protect sensitive data without sacrificing performance. In doing so, he emphasizes that proper architectures and techniques must be selected, such as alternative topologies to reduce overhead of encryption and methods to reduce the number of encryption operations. All authors stress the complexity of balancing security and performance, with Mattsson (2005) particularly highlighting the need for expert guidance in implementing effective database encryption solutions tailored to specific organizational environments. In conclusion, while several strategies have been proposed to balance security and performance, as discussed by Zorkadis (1994), Athanassoulis (2017), and Mattsson (2005), expert guidance and careful consideration of system-specific requirements remain critical to successfully navigating this challenge.

Emerging Trends and Future Directions

Innovations in Anonymization for IoMT

Recent studies outline the developing trends in anonymization of IoMT using AI-based methods and federated learning. AI-based anonymization methods include differential privacy, homomorphic encryption, and generative adversarial networks that enhance data protection with respect to utility, as emphasized by Mahendralal Prajapati et al. (2024). Machine learning and deep learning-based methods improve the performance, speed, and efficiency of the cybersecurity solutions for the IoMT devices, according to Sotiris Messinis et al. (2024). Dynamic anonymization using machine learning and AI-driven access control systems are notable trends in IoT-based cloud environments, as outlined by D. Dhinakaran et al. (2024). Federated learning emerges as a promising technique for IoMT, offering reduced communication overhead and enhanced security, as explained by Junaid Ahmed et al. (2022). Physical Layer Security (PLS) can be integrated with federated learning to improve privacy preservation in IoMT networks, with clustering of IoMT devices shown to enhance secrecy rates compared to non-clustered approaches, as demonstrated by Junaid Ahmed et al. (2022). In conclusion, various AI-driven techniques such as federated learning and physical layer security are at the forefront of research into anonymization and privacy preservation for IoMT, as highlighted by multiple sources. These methods promise to enhance both data security and system performance.

Potential Areas for Research

The Internet of Medical Things (IoMT) presents significant privacy and security challenges, necessitating robust anonymization techniques, as noted by Flávio Neves et al. (2023) and Ramadhan Mohamed Rajab et al. (2024). While k-anonymity has shown promise when combined with other methods, there's a lack of standardized solutions applicable across all IoT scenarios, according to Flávio Neves et al. (2023). The healthcare sector is particularly vulnerable due to legacy devices and disjointed data systems, emphasizing the need for tailored security measures and risk assessment models, as highlighted by Ramadhan Mohamed Rajab et al. (2024). Data anonymization is one of the most important strategies for privacy preservation in IoHT, balancing the risks of privacy and the quality of output data, as mentioned by Liane Colonna (2020). Several anonymization techniques have been applied in healthcare. The data are usually distributed horizontally across regions, as mentioned by Mr. Pravin et al. (2018). Future research should focus on developing specific standards, policies, and collaborative efforts among stakeholders to address the evolving cybersecurity threats in IoMT ecosystems, as emphasized by Ramadhan Mohamed Rajab et al. (2024). In conclusion, tailored security measures, standardization, and collaborative efforts hold the potential to overcome any challenges toward privacy and security in the IoMT; multiple researchers have proposed many such studies.

The promising solution involving blockchain technology offers the greatest promise for future improvement and enhancement of IoMTs toward data safety and the privacy of related healthcare systems, as noted by Nimra Dilawar et al. (2019) and S. Forrest et al. (2021). Blockchain's decentralized, transparent, and immutable nature provides a secure framework for managing sensitive medical data generated by IoMT devices, according to Fariza Sabrina et al. (2024). However, the emergence of quantum computing poses new challenges to blockchain security, necessitating the development of quantum-resistant techniques for IoMT applications, as highlighted by Fariza Sabrina et al. (2024). While blockchain technology opens opportunities for addressing the existing issues of IoT security and IoT privacy, significant research into the adaptation of computation-intense algorithms to the tight energy and processing constraints existing on IoT devices, as discussed by Francesco Restuccia et al. (2019). Despite these challenges, blockchain-enabled IoMT technologies offer benefits such as improved security, privacy, and traceability of pandemic origins, paving the way for a more interconnected and secure healthcare ecosystem, as emphasized by S. Forrest et al. (2021).

Conclusion

Summary of Key Findings

Several key findings about modifying anonymization techniques for the Internet of Medical Things (IoMT) emerged from the literature. A major emphasis has been to adapt existing techniques toward anonymity with the primary objective of preserving privacy, but meanwhile enabling real-time analysis, which may demand some compromise between these two attributes - privacy and utility. Data aggregation, approximate computing, and differential privacy are approaches explored for achieving such balance. Scalable anonymization methods applicable for big datasets typical in IoMT environments, which are developed upon current research studies, such as the methods of decision tree construction and sampling, as well as the distributed anonymization process via frameworks like Spark. Moreover, combining different anonymization techniques, such as k-anonymity with other techniques, is recommended to improve privacy protection in IoMT systems, addressing challenges like missing values and variable data widths in IoT data streams. However, the literature also indicates a lack of consensus on standardized methodologies for anonymization applicable across all IoT scenarios, underscoring the need for further research to develop universally applicable solutions. Emerging technologies, such as Homomorphic Encryption, Differential Privacy, and Federated Learning, will be explored to enhance the security in IoMT systems to achieve both robust privacy protection and handle the complexity of IoMT ecosystems as a whole. Overall, the need for continued research and communication among stakeholders is the point that literature emphasizes to create effective scalable and standardized anonymization techniques which are tailored to the specific challenges and needs of IoMTs.

Recommendations for Future Work

The literature recommends the following ways of enhancing existing anonymization methods to merge the Internet of Medical Things: First, the literature advocates the development of anonymization methods that scale effectively in order to process large data typical of an IoMT environment. This encompasses integrating external scalability in already designed algorithms and making use of distributed processing frameworks like Spark to process data with effective management and satisfaction of anonymity. Second, it is suggested that different anonymization techniques be combined together, such as k-anonymity, differential privacy, and data perturbation, to increase the protection of privacy. The multi-faceted approach may help address specific challenges such as missing values and variable data widths while maintaining data utility. Third, any modifications to existing anonymization techniques should focus on real-time data analysis capabilities, such that privacy-preserving algorithms can operate effectively in real-time environments without compromising data responsiveness and utility. The literature also underlines a critical need for standardized anonymization methodologies applicable across several different IoT scenarios. Development in such standards would allow the acceptance of best practices and consistent privacy across an array of applications within the IoMT ecosystem. Further advanced incorporation of technologies, like Homomorphic Encryption, Differential Privacy, and Federated Learning are suggested to enhance security provisions in IoMT systems. These technologies can offer robust privacy guarantees while accommodating the complexities and evolving threats in IoMT environments. Finally, effective collaboration among healthcare providers, government entities, and technology stakeholders is essential in establishing regulations and best practices for anonymization in IoMT. This collaborative approach will help address the

unique challenges posed by the interconnected nature of IoMT systems. By adopting the proposed recommendations, anonymization in IoMT will see considerable improvement in data privacy as well as utility in health applications.

There are several promising avenues that can further advance future research for robust anonymization techniques in the Internet of Medical Things (IoMT). In particular, the potential is high to explore hybrid approaches, including k-anonymity, differential privacy, and data perturbation, which will provide enhanced protection of privacy without losing the utility of data. Secondly, the focus should be on developing real-time privacy-preserving algorithms that could adjust their privacy levels dynamically with context and sensitivity. These would result in effective privacy preservation within the real-time processing scenario. This is important, given the critical role it will play in IoMT applications. Thirdly, it is necessary to standardize frameworks for anonymization in various IoMT applications. This would enable the implementation of best practices, ensuring consistent privacy protection, and making it easier to adopt effective anonymization strategies on the part of organizations. Fourth, the integration of such emerging technologies as Homomorphic Encryption, Federated Learning, and advanced cryptographic methods into anonymization techniques is likely to provide enhanced guarantees of security and privacy in complex IoMT environments. Fifth, scalability is paramount in dealing with the sheer quantities of data generated by IoMT devices. Research should focus on the development of scalable anonymization methods and exploration of distributed processing algorithms that will efficiently anonymize large datasets without compromising performance. Comprehensive evaluation of privacy risks and trade-offs of various anonymization techniques is necessary. Understanding of the privacy-data utility balance will lead to better designs of more effective anonymization methods. Finally, interdisciplinary collaboration in computer science, healthcare, and ethics is crucial to further work on more holistic approaches to anonymization. This collaborative perspective could aid in addressing the multifaceted privacy challenges in IoMT to come up with practical, effective, and ethically appropriate solutions. All these research directions can be used in the pursuit of developing robust anonymization techniques for IoMT, thereby advancing the data privacy and security of healthcare applications.

References

[1] Ahmed, J., Nguyen, T.N., Ali, B.Q., Javed, M.A., & Mirza, J. (2022). On the Physical Layer Security of Federated Learning Based IoMT Networks. *IEEE Journal of Biomedical and Health Informatics, 27*, 691-697.

[2] Ahmed, S.F., Alam, M.S., Afrin, S., Rafa, S.J., Rafa, N., & Gandomi, A.H. (2023). Insights into Internet of Medical Things (IoMT): Data fusion, security issues and potential solutions. *Inf. Fusion, 102*, 102060.

[3] Aileni, R.M., Suciu, G., Rajagopal, M., Pasca, S., & Sukuyama, C.A. (2020). Data Privacy and Security for IoMWT (Internet of Medical Wearable Things) Cloud.

[4] Ait Abdelouahid, R., Debauche, O., Mahmoudi, S., & Marzak, A. (2023). Literature Review: Clinical Data Interoperability Models. *Information*.

[5] Akilan, U, H., Prakash, I.B., & Rajkumar, K. (2023). Exploring the Impact and Potential of the Internet of Medical Things (IoMT): A Comprehensive Review. *2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, 967-972.

[6] Anderson, C., Dwyer, M., & Chan, K. (2023). Optimizing machine learning inference performance on IoT devices: trade-offs and insights from statistical learning. *Defense + Commercial Sensing*.

[7] Athanassoulis, M. (2017). Secure Data Systems and Performance: Friends or Foe? *Conference on Innovative Data Systems Research*.

[8] Bermúdez-Edo, M. (2016). Semantic Challenges for the Variety and Velocity Dimensions of Big Data.

[9] Byun, J., Sohn, Y., Bertino, E., & Li, N. (2006). Secure Anonymization for Incremental Datasets. *Secure Data Management*.

[10] Chen, S. (2023). 3. K-anonymous mathematical model based on greedy algorithm. *Applied and Computational Engineering*, 8, Article 20230080. https://doi.org/10.54254/2755-2721/8/20230080

[11] Colonna, L. (2020). Privacy, Risk, Anonymization and Data Sharing in the Internet of Health Things. *Pittsburgh Journal of Technology Law & Policy, 20*, 148-175.

[12] Dhinakaran, D., Sankar, S.M., Selvaraj, D., & Raja, S.E. (2024). Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration. *ArXiv, abs/2401.00794*.

[13] Dilawar, N., Rizwan, M., Ahmad, F., & Akram, S. (2019). Blockchain: Securing Internet of Medical Things (IoMT). *International Journal of Advanced Computer Science and Applications*.

[14] Dimitrov, D.V. (2016). Medical Internet of Things and Big Data in Healthcare. *Healthcare Informatics Research, 22*, 156 - 163.

[15] Din, S., Aslan, N., Cheung, S.K., & Hasan, K.S. (2020). Call for Special Issue Papers: Internet of Medical Things in Big Data for Pervasive Medical Care. *Big data, 8 6*, 548-549 .

[16] Forrest, S.K., Baker, K., & Ketel, M. (2021). Blockchain Enabled IoMT and Security. *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 1-6.

[17] Fotopoulos, F., Malamas, V., Dasaklis, T.K., Kotzanikolaou, P., & Douligeris, C. (2020). A Blockchain-enabled Architecture for IoMT Device Authentication. *2020 IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)*, 89-92.

[18] Freytag, J., Bergmann, R., & Dölle, L. (2014). Query Adaptation and Privacy for Real-Time Business Intelligence - Extended Abstract. *Business Intelligence for the Real-Time Enterprises*.

[19] Gadotti, A., Rocher, L., Houssiau, F., Creţu, A.-M., & de Montjoye, Y.-A. (2024). Anonymization: The imperfect science of using data while preserving

privacy. *Science Advances*. https://doi.org/10.1126/sciadv.adn7053

[20] Gaurav, A., Psannis, K.E., & Peraković, D. (2022). Security of Cloud-Based Medical Internet of Things (MIoTs): A Survey. *Int. J. Softw. Sci. Comput. Intell., 14*, 1-16.

[21] Hameed, S.S., Hassan, W.H., Latiff, L.A., & Ghabban, F.M. (2021). A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *PeerJ Computer Science, 7*.

[22] Huang, C., Wang, J., Wang, S., & Zhang, Y. (2023). Internet of medical things: A systematic review. *Neurocomputing, 557*, 126719.

[23] Kagita, M., Thilakarathne, N.N., Gadekallu, T.R., & Maddikunta, P.K. (2020). A Review on Security and Privacy of Internet of Medical Things. *ArXiv, abs/2009.05394*.

[24] Khanh, Q.V., Chehri, A., Minh, Q.N., Anh, D.V., & Nguyen, D.C. (2023). Performance Evaluation of Fog-to-Cloud Computing Schemes for IoMT Systems Using Queuing Models. *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 1096-1100.

[25] Khatib, I.A., Shamayleh, A., & Ndiaye, M. (2024). Healthcare and the Internet of Medical Things: Applications, Trends, Key Challenges, and Proposed Resolutions. *Informatics, 11*, 47.

[26] Kiran, A., & Shirisha, N. (2022). K-Anonymization approach for privacy preservation using data perturbation techniques in data mining. *Materials Today: Proceedings*.

[27] Kjwan, A.A., & Mohammad, O.H. (2024). Enhancing Medical Data Analysis with Federated Learning in the Internet of Medical Things. *April-May 2024*.

[28] Kumar, S., Arora, A., Gupta, P.S., & Saini, B.S. (2020). A Review of Applications, Security and Challenges of Internet of Medical Things.

[29] LeFevre, K., & DeWitt, D.J. (2007). Scalable Anonymization Algorithms for Large Data Sets.

[30] LeFevre, K., DeWitt, D.J., & Ramakrishnan, R. (2008). Workload-aware anonymization techniques for large-scale datasets. *ACM Trans. Database Syst., 33*, 17:1-17:47.

[31] Li, N., Qardaji, W.H., & Su, D. (2011). Provably Private Data Anonymization: Or, k-Anonymity Meets Differential Privacy. *ArXiv, abs/1101.2604*.

[32] Marri, R., Varanasi, S., Chaitanya, S. V., & Marri, S. K. (2024). Enhancing security in geographic information systems: Anonymization and differential privacy techniques for protecting sensitive geospatial data. *Deleted Journal*, 5(1), Article 240. https://doi.org/10.60087/jaigs.v5i1.240

[33] Mathkor, D.M., Mathkor, N., Bassfar, Z., Bantun, F., Sláma, P., Ahmad, F., & Haque, S. (2024). Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends. *Journal of infection and public health, 17 4*, 559-572 .

[34] Mattsson, U.T. (2005). Database Encryption - How to Balance Security with Performance. *Information Technology & Systems*.

[35] Mavrogiorgou, A., Kiourtis, A., Touloupou, M., Kapassa, E., & Kyriazis, D. (2019). Internet of Medical Things (IoMT): Acquiring and Transforming Data into HL7 FHIR through 5G Network Slicing. *Emerging Science Journal*.

[36] Messinis, S., Temenos, N., Protonotarios, N.E., Rallis, I., Kalogeras, D., & Doulamis, N.D. (2024). Enhancing Internet of Medical Things security with artificial intelligence: A comprehensive review. *Computers in biology and medicine, 170*, 108036 .

[37] Nair, A.K., Sahoo, J., & Raj, E.D. (2023). Privacy preserving Federated Learning framework for IoMT based big data analysis using edge computing. *Comput. Stand. Interfaces, 86*, 103720.

[38] Neves, F., Souza, R., Sousa, J., Bonfim, M.S., & Garcia, V. (2023). Data privacy in the Internet of Things based on anonymization: A review. *J. Comput. Secur., 31*, 261-291.

[39] Nishad, D.K., & Tripathi, D.R. (2020). Internet of Medical Things (IoMT): Applications and Challenges. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*.

[40] Ny, J.L. (2020). Defining Privacy-Preserving Data Analysis.

[41] Otgonbayar, A., Pervez, Z., & Dahal, K.P. (2016). Toward Anonymizing IoT Data Streams via Partitioning. *2016 IEEE 13th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 331-336.

[42] Palavras, E., Fysarakis, K., Papaefstathiou, I., & Askoxylakis, I.G. (2018). SeMIBIoT: Secure Multi-Protocol Integration Bridge for the IoT. *2018 IEEE International Conference on Communications (ICC)*, 1-7.

[43] Patil, A., & Wang, B. (2023). Advancing data privacy: A novel K-anonymity algorithm with dissimilarity tree-based clustering and minimal information loss. *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(8), Article 8005. https://doi.org/10.17762/ijritcc.v11i8.8005

[44] Plagemann, T., Goebel, V., Hollick, M., Oslo, B.K., Darmstadt, T.U., & Groningen, U.O. (2022). Towards Privacy Engineering for Real-Time Analytics in the Human-Centered Internet of Things. *ArXiv, abs/2210.16352*.

[45] Pournik, O., Ghalichi, L., & Arvanitis, T.N. (2023). How Interoperability Challenges Are Addressed in Healthcare IoT Projects. *Studies in health technology and informatics, 309*, 121-125 .

[46] Pradyumna, G.R., Hegde, R.B., Bommegowda, K.B., Jan, T., & Naik, G.R. (2024). Empowering Healthcare With IoMT: Evolution, Machine Learning Integration, Security, and Interoperability Challenges. *IEEE Access, 12*, 20603-20623.

[47] Prajapati, M., Kumar Upadhyay, A., Rezaie, M., & Dongradive, J. (2024). A comparative Study on AI-Driven Anonymization Techniques for Protecting

Personal Data. *International Journal For Multidisciplinary Research*.

[48] Pravin, M., Kathavate, N., & Amudhavel, D.J. (2018). Route Map of Privacy Preservation to IOT. *International journal of engineering and technology, 7*, 825.

[49] Putra, K.T., Arrayyan, A.Z., Hayati, N., Firdaus, .., Damarjati, C., Bakar, A., & Chen, H. (2024). A Review on the Application of Internet of Medical Things in Wearable Personal Health Monitoring: A Cloud-Edge Artificial Intelligence Approach. *IEEE Access, 12*, 21437-21452.

[50] Quoc, D.L., Beck, M., Bhatotia, P., Chen, R., Fetzer, C., & Strufe, T. (2017). Privacy Preserving Stream Analytics: The Marriage of Randomized Response and Approximate Computing. *ArXiv, abs/1701.05403*.

[51] Rajab, R.M., Abuhmida, M., Wilson, I.D., & Ward, R. (2024). A Review of IoMT Security and Privacy related Frameworks. *European Conference on Cyber Warfare and Security*.

[52] Rathnayake, R.M., Karunarathne, M.S., Nafi, N.S., & Gregory, M.A. (2018). Cloud Enabled Solution for Privacy Concerns in Internet of Medical Things. *2018 28th International Telecommunication Networks and Applications Conference (ITNAC)*, 1-4.

[53] Razdan, S., & Sharma, S. (2021). Internet of Medical Things (IoMT): Overview, Emerging Technologies, and Case Studies. *IETE Technical Review, 39*, 775 - 788..

[54] Restuccia, F., D'oro, S., Kanhere, S.S., Melodia, T., & Das, S.K. (2019). Blockchain for the Internet of Things: Present and Future. *ArXiv, abs/1903.07448*.

[55] Sabrina, F., Sohail, S., & Tariq, U.U. (2024). A Review of Post-Quantum Privacy Preservation for IoMT Using Blockchain. *Electronics*.

[56] Said, A.M., Yahyaoui, A., & Abdellatif, T. (2023). HIPAA and GDPR Compliance in IoT Healthcare Systems. *MEDI Workshops*.

[57] Smys, S., & S. Raj, J. (2022). Future Challenges of the Internet of Things in the Health Care Domain - An Overview. *Journal of Trends in Computer Science and Smart Technology*.

[58] Sobecki, A., Szymański, J., Gil, D., & Mora, H.M. (2020). Framework for Integration Decentralized and Untrusted Multi-Vendor IoMT Environments. *IEEE Access, 8*, 108102-108112.

[59] Sun, Y., Lo, F.P., & Lo, B.P. (2019). Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. *IEEE Access, 7*, 183339-183355.

[60] Turgay, S., & Ilter, I. (2023). Perturbation Methods for Protecting Data Privacy: A Review of Techniques and Applications. *Automation and Machine Learning*.

[61] Vimercati, S.D., Facchinetti, D., Foresti, S., Oldani, G., Paraboschi, S., Rossi, M., & Samarati, P. (2021). Scalable Distributed Data Anonymization. *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, 401-403.

[62] Vs, S. (2017). A Scalable Two Phase Top Down Specialization Approach For Data Anonymization Using Mapreduce On Cloud. *International Journal of Computer Trends and Technology, 45*, 50-53.

[63] Wani, R.U., Thabit, F., & Can, O. (2024). Security and privacy challenges, issues, and enhancing techniques for Internet of Medical Things: A systematic review. *Secur. Priv., 7*.

[64] Wong, J.H., Piuri, V., Scotti, F., & Zhang, Q. (2023). Efficient IoT Big Data Streaming With Deep-Learning-Enabled Dynamics. *IEEE Internet of Things Journal, 10*, 4770-4782.

[65] Xu, Y., Liu, Y., & Hou, M. (2024). New media user privacy protection mechanism based on differential privacy and data anonymization. *Advances in Education, Humanities and Social Science Research*, 11(1), Article 164. https://doi.org/10.56028/aehssr.11.1.164.2024

[66] Yaacoub, J.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R., & Chehab, A. (2020). Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst., 105*, 581-606.

[67] Yasmeen, G., Javed, N., & Ahmed, T.F. (2022). Interoperability: A Challenge for IoMT. *ECS Transactions*.

[68] Zhao, Z., Hsu, C., Harn, L., Yang, Q., & Ke, L. (2021). Lightweight Privacy-Preserving Data Sharing Scheme for Internet of Medical Things. *Wirel. Commun. Mob. Comput., 2021*, 8402138:1-8402138:13.

[69] Zikria, Y.B., Afzal, M.K., & Kim, S.W. (2020). Internet of Multimedia Things (IoMT): Opportunities, Challenges and Solutions. *Sensors (Basel, Switzerland), 20*.

[70] Zorkadis, V. (1994). Security Versus Performance Requirements in Data Communications Systems. *European Symposium on Research in Computer Security*.