Review

Application of Blockchain Technology & Integration of Differential Privacy: Issues in E-Health Domains

David Isie * and Hassan Reza *

Posted Date: 10 October 2023

doi: 10.20944/preprints202310.0553.v1

Keywords: e-Health domain; Differential Privacy; Blockchain; IoT; real-time data; health survey; electronic medical record

Review

Application of Blockchain Technology & Integration of Differential Privacy: Issues in E-Health Domains

David Isie * and Professor Hassan Reza *

School of Electrical Engineering and Computer Science University of North Dakota Grand Forks-ND 58202, U.S.A
* Correspondence: david.isie@ndus.edu; hassan.reza@und.edu

Abstract: A systematic and comprehensive review of critical applications of Blockchain Technology with Differential Privacy integration lies within the privacy and security enhancement. This paper aims to highlight the research issues in the e-health domain (e.g., Electronic Medical Records) and to review the current research directions in Differential Privacy integration with Blockchain Technology.(1) Background: The current state of the art in the e-health domain is identified as follows: (a) healthcare information poses a high level of security and privacy concerns due to its sensitivity; (b) due to vulnerabilities surrounding the healthcare system, a data breach is common and presents a risk for attacks by an adversary; and (c) the current privacy and security apparatus needs further fortification. (2) Methods: The methodology uses a systematic literature review (SLR) to identify and select relevant research papers and academic journals in DP and BT. (3) Results: The results are categorized into: e-Health Record Privacy, Real-Time Health Data, and Health Survey Data Protection to identify inherent issues with Differential Privacy integration with Blockchain and technical challenges.(4) Conclusion: This review thoroughly surveyed and summarized Differential Privacy mechanisms in EMR privacy, real-time health data, and health survey data protection while highlighting challenges.

Keywords: e-Health domain; Differential Privacy; Blockchain; IoT; real-time data; health survey; electronic medical record

1. Introduction

The evolving nature of the e-Health domain (e.g., EMR) in recent years has drawn government attention to address the issues surrounding the privacy and security of EMR. The Health Insurance Portability and Accountability Act (HIPAA) was introduced in 1996 as a federal law to regulate three significant components of healthcare data as follows [1]: (a) HIPAA Privacy Rules: This regulates the disclosure and use of Protected Health Information (PHI) health by entities such as employer-sponsored health plans, health insurers, and transactions that involve medical services; (b) Security Rules: Specifically designed to address Electronic Protected Health Information (ePHI) and to safeguard three security compliances which are administrative, physical, and technical; and (c) Breach Notification Rules: Requires organizations to report an incident of PHI breach to patients. Confidentiality, Integrity, and Availability (CIA) strongly correlate with HIPAA compliance and must be implemented. Confidentiality means the privacy of PHI is ensured. Integrity means PHI is only changed or destroyed with due process. Availability means access to PHI by keeping hardware and systems in good working condition [2].

This research focuses on privacy issues in e-Health domains (e.g., EMR) and the review of applications of Blockchain Technology and Differential Privacy to address these vulnerabilities. Although Blockchain is still evolving, particularly in the e-Health system, its adoption has multiplied recently as more Internet of Things (IoT) uses electronic gadgets to manage and provide patient services [3]. Blockchain applications also apply in other industries like finance, supply chain, insurance claim, clinical trial, and pharmaceutical counterfeit [4]. Therefore, this paper aims to review privacy issues in the e-Health domain using Blockchain Technology and integration of Differential Privacy (DP).

1.1. Research Motivations

E-Health systems' privacy and security issues have triggered the need to explore the loopholes or vulnerabilities in handling, sharing, storing, and accessing patients' ePHI. The following are the current issues cited to back up the motivation of this research:

- Surveys have shown that many people are concerned about healthcare information privacy. Close to two-thirds of clients paid attention to the privacy of personal healthcare, and 39% of respondents assume that their health data is safe [5]
- Some people are concerned that their healthcare data is not safe via the internet, and they are worried about security and privacy vulnerability [6]
- About half of the research participants believe that exchanging their medical records is not in their best interest to secure their privacy [7]
- In 2021, the Department of Health and Human Services Office for Civil Rights (OCR) implemented corrective action to settle potential violations of HIPAA, which included a privacy and security rules-related data breach that affected 9.3 million people [8]
- The existing EMR systems show that about 40% of physicians identified the design and interoperability as primary sources of dissatisfaction (sample size of 8,774 physicians) [9]

Blockchain and Differential Privacy are believed to provide solutions to mitigate these privacy issues. The benefit of Blockchain Technology spans healthcare systems to provide or reduce potential data breaches and unauthorized access or sharing of patients' PHI [10].

1.2. Problem Statements

This paper aims to evaluate the potential of using Differential Privacy as a complementary layer to enhance privacy protection in the e-Health domain, specifically in Electronic Medical Records (EMRs) management systems. Despite the decentralized nature of Blockchain technology, it has been shown to have limitations in providing adequate privacy protection for users' sensitive personal health information. This is particularly important in today's digital age, where data breaches are increasingly common, and personal health information has become a commodity. The proposed integration of Blockchain and Differential Privacy aims to address these limitations by providing a more secure and private system for managing EMRs. This study seeks to fill the current literature gap by evaluating this integration's effectiveness in terms of privacy and security and its potential for implementation in real-world e-Health systems.

1.3. Research Gaps

A comprehensive and comparative analysis of the literature review focuses on exploring different approaches, methods, theories, or operations within EMRs. The gap analysis focuses on the following:

- Lack of assessment from multiple perspectives
- Lack of a comprehensive chronological model: Lack of approach
- Highlight inherent issues
- Lack of expert assessment and qualifications
- Lack of legal framework for the EMR system
- Leveraging Differential Privacy for privacy protection
- Fundamental and applied research on Differential Privacy

1.4. Methodology Overview

The research organization and strategy consist of the following: (a) section 2 is the background study that defines Blockchain, Differential Privacy, and the integration of these two approaches in the e-Health domain. This section also gives complete information based on the research motivations, problem statements, and research questions to proposed feasible solutions; (b) section 3 is the methodology which consists of different research steps using the SLR and the selection processes of papers and publications related to the research objective and questions. Steps in this section include search items, literature sources, search process, selection, and study quality analysis. The research questions are framed according to three categories: Electronic Medical Record (EMR) Privacy, Real-Time Health Data, and Health Survey Data Protection; (c) section 4 is a presentation of the results and analysis where all the findings are listed and explained based on the three categories; (d) challenges and limitations are described in section 5; and (e) section 6 presents the conclusion where all summaries are listed.

2. Background Study

2.1. Blockchain Technology Concept

Blockchain Technology was first introduced in 2008 as a tool to manage cryptocurrency and was described as a concept of the distributed ledger by S. Nakamoto [13]. In [14], Blockchain is based on the hash that uses proof of work chain. Understanding Blockchain applications in e-Health requires Information Technology (IT). Information Technology has gradually evolved and is an integral part of e-Health systems. An e-Health system has different components, and the salient part of these systems is Privacy and Security. An example of e-Health is Electronic Medical Records (EMR). In [15], EMR is described as an electronic copy of the hard copy (paper copy) of medical information that contains the patient's treatment history. The technology and its applications, such as Blockchain, are also part and parcel of e-Health systems. In recent years, the data generated across healthcare systems have grown exponentially to account for the e-Health domain. Due to the accessibility of the Internet of Things (IoT), traditional means of communicating, transmitting, sharing, storing, and accessing healthcare information are replaced by cyberspace networking [16].

2.1.1. Types of Blockchain

There are three types of Blockchain authentication and control mechanisms: (a) public, (b) private, and (c) consortium. The public authentication is decentralized and permissionless (e.g., Bitcoin, Ethereum). For instance, Ethereum implementation is a permissionless programmable Blockchain; that is, it authorizes any user to create and execute algorithm complexity on the Ethereum platform. The consensus in Ethereum is achieved by proof of work (PoW). The "hashing" is used to validate new blocks created since PoW is based on "mining" that satisfies specific requirements [17].

On the other hand, private and consortium are restricted/controlled, and permissions are needed. Private authentication is preferred over consortium because of the Hyperledger Fabric platform. Hence, private authentication is the best fit for EMR security as it requires users to be authorized to join the platform. The ideal use cases of the Hyperledger Fabric platform for Blockchain applications are in Business-to-Business (B2B) data exchange, transaction settlement, and non-repudiation. The application of Blockchain in healthcare to secure EMRs is non-repudiation. Managing patients' EMRs is probably the area with the highest potential growth. The EMRs contain a patient's medical information, which includes the condition and clinical progress of a patient throughout treatment [18]. The benefits of a Blockchain-based network for EMRs are as follows: (a) records are stored in a distributed ledger, (b) no centralized owner or a hub for a hacker to corrupt or breach, and (c) data is updated [18]. In Hyperledger, the chain-code services are used to secure ways to execute smart contracts. The smart contract is a set of logically defined rules for transactions with the associated World State. World State, in this context, is a database that stores data in the form of arrays of keys assigned arbitrarily [19]. The significant challenges in Blockchain applications relating to EMRs are maintaining security and privacy.

2.1.2. Characteristics of Blockchain

Blockchain Technology has distinctive properties that make it suitable for EMR systems. These properties are:

- Decentralization: This is a peer-to-peer transaction without a centralized validation or authorization system. The access is granted to each participant with the full right to verify transactions within the network [20]. To decentralize the network, technology such as cryptographic hash, digital signature, and distributed consensus mechanisms are required for security fortification. The consensus protocol is to ensure data integrity. Therefore, decentralization enhances protection against vulnerability in the network at risk of security attacks [21].
- Immutability and Transparency: This concept means that after creating and adding the block, it cannot be altered or removed [22]. The structure of the Blockchain is formed and linked together in an orderly manner that contains transaction information.
- Auditability: Any transaction in the Blockchain network is traceable to its previous transaction. Therefore, the timestamp is incorporated in transaction validation and records [23].
- Smart Contract: This is based on certain conditions; when met, it is automatically filed and executed, such as control accesses and privileges [21].
- Security: By design, the Blockchain network uses a private or public key to access or make transactions. This is due to hashing that seals each block from a third party [10].

2.1.3. Blockchain Benefit in EMR

This section concerns the benefits of Blockchain as it relates to healthcare. The existing healthcare systems have evidence that requires Blockchain to overcome some inherent problems. The management and exchange of patients' data is a focal point for Blockchain applications. Other applications allow healthcare data to be distributed and immutable for greater security of patient records and data integrity. Table 2.0 below shows a significant and brief summary of the benefits of Blockchain Technology.

Table 2.0. Benefits of Blockchain.

Benefit	Description	References
Transparency	Due to Blockchain immutability, data cannot be deleted or altered. Blockchain is a more transparent system that stores EMR.	[23][21]
Data Integrity	Blockchain ensures data integrity so that no centralized authority is at risk of security attacks.	[21][24]
Security	EMR is sensitive data, and such Blockchain provides encryption capabilities that minimize attacks and protects vulnerability.	[23][21]
Interoperability	Decentralization helps to improve interoperability which facilitates the exchange of EMRs and grants patients' ownership and control of their records.	[26][23]
Patient-Centered	The right of patients to access or grant access to authorized personnel in EMR systems is restored.	[21][25]

2.1.4. Limitations of Blockchain in EMR

The major limitation of Blockchain is the difficulty in maintaining privacy and security [27]. The breach of security and privacy can come from users with false identities. Therefore, Blockchain's challenge is how to ensure anonymity. Table 2.1 summarizes the literature on Blockchain challenges and considerations in EMR Systems.

doi:10.20944/preprints202310.0553.v1

Table 2.1. Limitations of Blockchain in EMR.

Literature	Challenges/Considerations	References
Blockchain Adoption: Technological, organizational, and environmental considerations	The top factors are management support, organizational readiness, and organizational size.	[28]
Blockchain Application in EMR Systems:	Requirements that impact EMR systems as it relates to Blockchain application, such as non-standardized system, decentralized storage and privacy, key management and scalability, and IoT	[29]
Blockchain application for access control management: secure data storage	The encrypted information is stored in a third party that the hub services on the Blockchain.	[30]
A Blockchain that is based on data sharing system	Miners are provided with access to aggregate and reward the data bookkeeper.	[31]
IBM report: Technical challenges that restrict Blockchain application	The major challenge is scalability. Blockchain ecosystems within corporate legacy and systems of record are challenging operations.	[26]
IBM Institute for Business Value survey: Respondents from 200 healthcare executives in 16 nations	Studies show that over half cited Blockchain's early/immature state as an issue.	[32]
Deloitte Blockchain Technology challenges in life science and EMR System	Stakeholders engage in multiple efforts, such as healthcare organizations and health plans, standardization, cost, and regulations, to ensure commitment to Blockchain adoption.	[33]

2.2. Differential Privacy Concept

Differential Privacy is another prevalent technique capable of quantifying and anonymizing personal data within the network [34]. Differential Privacy depends on the parameter epsilon (ϵ-value), which determines the loss of privacy by adding or removing noise from a specific data account. The trade-off between adding or removing "noise" in a dataset decreases the useability of the actual data [35]. Therefore, various values of (ϵ), according to [36][37], have been experimented with to determine the proper noise for different applications. Real-time data is protected by adding a desirable amount of noise to maintain a reasonable trade-off between privacy and accuracy [38]. Differential Privacy aims to obfuscate any query's output result, thereby hiding the identity of sensitive information.

2.2.1. Mechanism of Differential Privacy

There are two branches of Differential Privacy: existing methods and noise addition mechanisms [4]. For the sake of this project, the studied method is noise addition mechanisms (that is, data perturbation mechanisms). These mechanisms are: (a) **Laplace Mechanism:** This mechanism is for numeric queries, which is a procedure of adding Laplace noise to query results. The noise is a sample from the Laplace distribution [39]. The amount of noise added is adjusted, and it is a function of sensitivity [61]; **(b) Gaussian Mechanism:** In Gaussian, numeric queries are also used to add noise to a given data. The Gaussian mechanism is calculated using a normal (Gaussian) distribution [40]; and **(c) Exponential Mechanism:** Exponential mechanism is used to implement Differential Privacy when it requires non-numerical output. In this case, query output is measured using a score function [41]. The highest scored result as output with higher probability as ε is larger [61].

2.2.2. Technical Challenges in the Application of Differential Privacy

The basic process of privacy preservation is simple, and the data only needs to be perturbated. The challenges of implementation of Differential Privacy in specific applications are highlighted as followings:

- Sensitivity: The absence or presence of individual records in the dataset is indistinguishable and maintained. Introducing Differential Privacy in practical datasets requires statistical query and low-sensitivity evaluation [42]. There is a trade-off that exists between accuracy (utility) and privacy. This challenge emerges in services and applications using different sensitivities [43][44].
- Choosing Epsilon Value (ϵ-Privacy Loss): Choosing the privacy parameter ε is a question that users of Differential Privacy cannot avoid [92]. The strength of privacy guaranteed is controlled by ε, and it is not clear how to choose an appropriate value in a given situation, as shown in [45][46]. In [61], the smaller ε is, the higher the increase in security and vice versa.
- Data Correlation: In a real-world dataset, there is a correlation in certain records that leads to the disclosure of information. Many researchers developed model-based and transformation-based approaches such that sensitivity weights, correlation degree, and correlated sensitivity overcome these challenges [47].
- Other challenges include a lack of computing environment, a system to align with users' needs, and a lack of trained personnel to verify implementation and correctness [60].

2.2.3. Other Approach to Enhance Privacy in EMR - Federated Learning (FL)

Federated Learning (FL) is another learning paradigm designed to address the problem of data sharing and privacy [48]. The FL approach was initially developed for different domains, such as mobile and edge devices, but in recent years, FL has gained traction in EMR [49]. In collaboration with the consensus model, FL enables and gains insight into data without sharing patient information beyond the firewalls of the institutions where it resides [50]. In this case, the FL process is positioned locally at each institution, and only the model characteristics, such as parameters and gradient, are transferred [51]. Therefore, in the context of EMR, for instance, FL helps in the following area:

- Find patients with similar clinical [52]
- Prediction of hospitalization due to cardiac [53]
- Medical imaging for whole brain segmentation in MRI [54]

The advantages of FL only solve some inherent challenges in EMR. Some factors, such as data quality, bias, and standardizations, depend on the successful model training [55]. Data heterogeneity is challenging in FL since collaborative learning strategies are not uniformly distributed across the institution [56]. Other considerations are privacy and security, the trade-off strategies, and risk regarding the privacy-preserving potential of FL performance and techniques [57]. Differential Privacy can also enhance privacy in an FL setting [58]. Developing counter-measures such as limiting the granularity of the updates and adding appropriate noise may be needed [59]. In effect, this is still open for further research.

2.3. Integration of Differential Privacy and Blockchain

2.3.1. Overview of Differential Privacy Integration with Healthcare Application Over Blockchain Network

Blockchain and Differential Privacy are revolutionizing and altering the concept of data storage. The decentralized property of Blockchain is considered a secure system. However, there are issues in Blockchain that require solutions before implementation in a real-world situation. One of these issues is preserving data while maintaining privacy for Blockchain applications. The integration of Differential Privacy in each layer of Blockchain Technology is classified into six different layers according to [63]. These layers are (a) data layer, (b) network layer, (c) consensus layer, (d) incentive layer, (e) contract layer, and (f) application layer. Each layer has functionality and privacy requirements. For instance, users' requirements differ from privacy requirements while creating blocks in the data or the consensus layer.

Researchers are actively investigating the effort to integrate Differential Privacy with a Blockchain-based healthcare system. In [69], the author proposed a proof of votes consensus that operates on a Blockchain-based healthcare network whereby data is mutually shared to create transaction blocks. As such, a third-party team is assigned to work and forward the blocks to companies within the network for verification through voting, thereby ensuring the decentralized characteristics of the Blockchain. Furthermore, the author discussed adding noise in their data to ensure privacy using decentralized Differential Privacy protection.

Remote connections are very crucial for doctors and patients to perform routine monitoring and fitness programs for elderly care [68]. To keep up with the modern healthcare system, traditional methods of administering services are not capable of the requirements needed because they need more transparency and trust. Adversaries can easily attack and tamper with data in a traditional healthcare system. Therefore, it is necessary to integrate Blockchain into the modern healthcare system. This trend provides tremendous benefits, but privacy concerns still exist because Blockchain stores data in a decentralized distributed ledger, whereas every node contains a copy of the ledger. A malicious node can trigger an attack on the private information of a Blockchain node.

2.3.2. Advantages of Integration of Differential Privacy in Blockchain

This section highlights the advantages of integrating Differential Privacy in Blockchain and the basic requirements of using this privacy operation. The following are the advantages:

- Various Blockchain scenarios require Differential Privacy mechanisms to protect personal data. When a transaction is carried out in a Blockchain system, the information is distributed throughout the decentralized network to update and keep records in the ledger. However, the adversary can reserve this information for a specific individual. To protect this information, Laplace and Gaussian mechanisms of Differential Privacy are efficiently perturbated to ensure identity privacy [4][63].
- Information stored in decentralized Blockchain databases can be used to conduct surveys [64]. However, personal information can be compromised if the adversary conducting the surveys is an insider in an organization. In this case, the exponential query evaluation mechanism of Differential Privacy ensures the protection of private information from such adversaries.
- Anonymization, as described in the literature, is used to address privacy concerns in Blockchain [65]. However, numerous experiments have shown that an anonymization operation is not complete data protection; for instance, in [66], any anonymized data from similar datasets can be combined to reveal personal data. These issues can be overcome by a viable solution of integration of Differential Privacy in Blockchain [4].
- In real-time data transmission in a Blockchain application, the data perturbation operation of Differential Privacy can add noise to data without compromising its accuracy [67].

There are other advantages of integration of Differential Privacy in Blockchain. In analysis, a statistical Blockchain database can be first protected using Differential Privacy. In this case, indistinguishable data is created via Differential Privacy. The query analyst on the other end of the network cannot predict a specific Blockchain node in the datasets with certainty.

3. Methodology

The methodology for this research employs a systematic mapping study (SMS). SMS is the mostly known methodology in the scientific survey which consists of different research steps and the selection processes of papers and publications to answer formulated research questions (RQs) [70]. Also, the aim of using SMS in this section is to obtain a comprehensive overview of research papers with unbiased assessment and identify research gaps while collecting evidence for future proposals

[71]. The guideline proposed by [72] implements the research method. SMS is conducted using the following steps: (a) research goal; (b) research questions (RQs); (c) searching strategy (this includes search terms, literature sources, search process, and study selection); (d) study quality assessments; and (e) result analysis.

3.1. Research Goal

Electronic Medical Records contain patients' medical history, and the issues concerning privacy and security have exponentially widened because of the era of IoT. In EMR systems, the management is ineffective without a proper system to share, store, and transmit these records in a server in a secure manner. The goals of this research are as follows:

- To identify the inherent factors that impact Blockchain applications concerning the security and privacy of EMR systems and to investigate the supporting platform that permits integration of Differential Privacy as a covering layer.
- To categorize this investigation into three areas that address (a) e-Health Record Privacy, (b) Real-Time Health Data, and (c) Health Survey Data Protection.

This research aims to facilitate the tradeoff between security and privacy during the application of Blockchain in the management of EMR systems and to formulate a proposal for future research in an area that needs more attention where inherent security and privacy challenges exist in EMR systems.

3.2. Research Questions (RQs)

The Research Questions (RQs) are formulated based on the research motivations, problem statements, and the goal of this review. Table 3.1 below summarizes the research questions (RQs).

Table 3.1. Research Questions (RQs).

ID	Research Questions
RQ1	How can DP be integrated into BC to enhance privacy and security in the e-Health domain (e.g., EMR)?
RQ2	What factors contribute to the DP mechanisms integration in Blockchain Technology and associated issues?
RQ3	What types of datasets and programming languages are being considered for implementation?
RQ4	What are the limitations and inherent challenges of the BT and DP applications, and how can they be solved?

[a.] **Note that the above questions are narrowed to only e-Health domains**

3.3. Research Strategy

The sources of the information in literature are academic publications, including conference papers, journal articles, Google scholarly books, and reports. Sources also include government agencies and reputable organizations such as IBM and AMIA. The search strategy is to find relevant works and identify applications of Blockchain and Differential Privacy and mechanisms in the e-Health domain, including the cost of privacy and challenges of the proposed solutions. According to [73] recommendation, two search strategies are primary and secondary. The primary strategy includes search terms, literature resources, and the search process, as explained below.

3.3.1. Search Terms

The search keywords used in this research are shown in Table 3.2. Online libraries, various journals, and papers are considered during the keyword search. The date filter is used to screen for current literature.

Table 3.2. Search Terms and Keywords.

Numbers	Keywords
1	Review, survey, literature review, background
2	Electronic medical records, e-Health domain*, electronic health record, health information technology, patient health information
3	Blockchain Technology, Differential Privacy*, privacy, data
4	Data perturbation, Differential Privacy mechanisms

a. *the keyword noted while searching

3.3.2. Literature Sources

The search was conducted for papers on four different electronic databases from online libraries. During the collection process, the title, the year of publication, the journal name, the number of citations, and the link are considered. The search terms with keywords for collecting conference papers and reviewing academic journals are used to formulate conceptual building blocks. The search also covers the title and abstract as keywords. The summary of the collected search is shown in Table 3.3.

Table 3.3. Numbers of Literature Review from Online Libraries.

Online Libraries	**Numbers of Retrieved Literature**
IEEE	32
ACM	8
ScienceDirect	6
AMIA	1
Others	58
Total	**105**

3.3.3. Search Process

A Systematic Literature Review (SLR) examined the resources' maturity and comprehensibility during the search. The systematic review process can be divided into two main phases.

- **Phase One**: Initial searching phase consists of the four online library databases. Each paper is searched separately with keywords, as shown in Table 3.3.
- **Phase Two**: In this phase, the search is conducted based on the references of a particular paper. By scanning the list of references for relevant papers, they are added if there is a relation to the keywords.

The search results are stored and managed in Microsoft Excel. From the phase one search, 300 papers were gathered. Ninety-eight papers were gathered from phase two of the reference search, as shown in Figure 3.1.

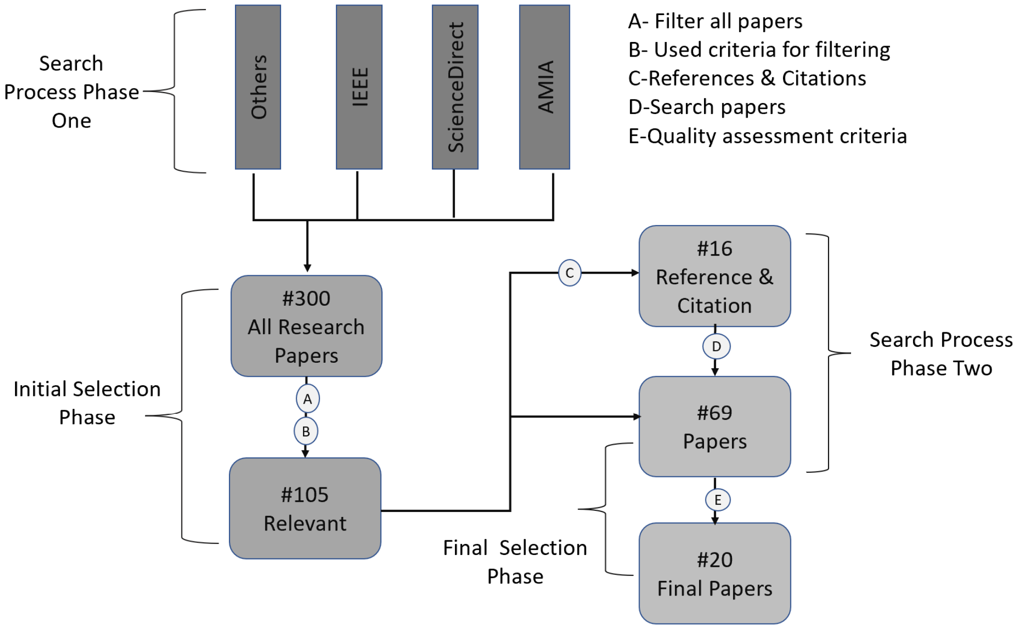

Figure 3.1. Search and Selection Process.

3.3.4. Study Selection

Research papers are selected from a different webpage. Some of the papers did not offer helpful inside knowledge concerning this research. Further filtering process was carried out. More specifically, the selection process has two phases:

- **Initial selection phase**: The aim is to obtain papers that offer sufficient background about this research. This section applies inclusion criteria (IC) and exclusion criteria (EC) to filter any related papers that answer the research questions. IC and EC are defined below.

o The inclusion criteria (IC) are as follows:
  - Papers published from 2008 (only a few papers published in 2005 and 2006)
  - Papers published until 2022
  - Papers that describe Blockchain and Differential Privacy
  - Papers that describe EMR, e-Health domain
  - Academic papers and journals
  - Review or survey papers
  - Check for duplicate publications - completed or newly released of the same study

o The exclusion criteria (EC) are presented below:
  - Papers in digital libraries that are duplicated
  - News, correspondences, summaries of presentations, posters, and workshop
  - Abstract of papers that are not written in the English language
  - **Final selection phase:** This phase selects papers with the acceptable quality needed to extract information. The selection in the final phase uses study quality assessment, as explained in section 3.4 below.

The citations and references from the above papers were also reviewed, and the last step included quality assessment criteria for data extraction.

3.4. Study Quality Assessment

This section addresses how quality assessment questions (QAQs) give credit to the reviewed paper. These questions are shown in Table 3.4. The questions are used for the quality assessment of the paper and the criteria. QAQ1 evaluates how the e-Health domain uses Blockchain and Differential Privacy to enhance protection for sensitive health information. Noticeably, the researchers have used the DP method to address the security concerns in the e-Health domain. QAQ2 attempts to discover if the papers provide a more comprehensive perspective other than EMR systems since the privacy of personal information is cut across all fields. QAQ3 explores whether the research results can be deployed to real-world applications. QAQ4 evaluates common limitations in the papers that are inherent. QAQ5 identifies similarities in research questions, while QAQ6 defines different methods to provide solutions. Finally, 20 papers have been selected, as shown in Table 3.5.

Table 3.4. Quality Assessment Questions.

ID	Quality Assessment Questions
QAQ1	Are the review papers related to e-Health domain under Blockchain and Differential Privacy?
QAQ2	Do the papers cover other Differential Privacy applications under different fields?
QAQ3	Do the papers use theoretical or practical based methods to answer research questions?
QAQ4	Are there common or inherent limitations in their studies?
QAQ5	Is the research question similar or different from other papers?
QAQ6	Do the proposed methods provide solutions that are different from the existing papers?

Table 3.5. List of Papers for Methodology.

Category	Papers Selection*
EMR Privacy	Roehrs et al. [20], ElSalamouny et al. [43], Saleheen et al. [77], Raisaro et al. [98], Lin et al. [78], Guan et al. [101], Machanavajjhala et al. [44], [98], Alnemari et al. [93], Hadian et al. [80], Mohammed et al. [97], Tang et al. [102], Raisaro et at. [99]
Real-Time Health Data	Geo et al. [83], McSherry et al. [46], Machanavajjhala et al [45], Zhang et al. [3]
Health Survey Data Protection	Luo et al. [84], Narayanan et al. [104], Valdezet al. [91], Narayanan et al. [105]

*This selection is for the research framework and methodology

4. Results

The analysis of research results is based on the research questions (RQs) in section 3. After an extensive literature review and rigorous investigation into different papers, the Differential Privacy mechanisms used to enhance Blockchain Technology in e-Health domains have been organized into three main categories. These categories are:

1. Real-Time Health Data represents papers that have been investigated based on the real-time health data releasing scheme. Most of this data comes from IoT devices such as wearables for real-time data collection and sharing. Therefore, all papers discussing Differential Privacy and Blockchain are under this category.
2. Electronic Medical Record (EMR) Privacy represents papers that EMR systems have covered. The EMR consists of all clinical data, laboratory tests, and diagnosis results in different numeric and non-numeric queries. These papers discussed protecting sensitive health data from databases using Differential Privacy mechanisms.
3. Health Survey Data Protection represents papers discussed in the statistical database regarding how health survey data is improved based on users' perspectives and the Differential Privacy mechanisms to enhance privacy-utility trade-off in e-Health (e.g., EMR).

Figure 4.1 portrays the taxonomy diagram for Differential Privacy in e-Health domain and health systems and approaches implemented in e-Health systems. The figure shows each category: real-time health data, electronic medical records (EMRs), and survey data records.

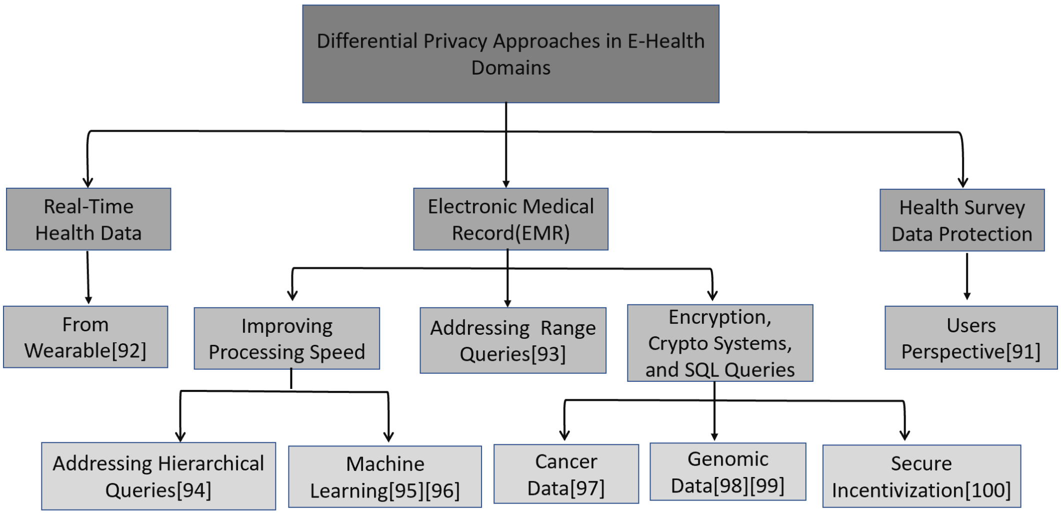
Differential Privacy Approaches in E-Health Domains
Real-Time Health Data
Electronic Medical Record(EMR)
Health Survey Data Protection
From Wearable[92]
Improving Processing Speed
Addressing Range Queries[93]
Encryption, Crypto Systems, and SQL Queries
Users Perspective[91]
Addressing Hierarchical Queries[94]
Machine Learning[95][96]
Cancer Data[97]
Genomic Data[98][99]
Secure Incentivization[100]

Figure 4.1. The Taxonomy for Differential Privacy in Approach in e-Health Domains.

4.1. *RQ1: How can DP be integrated into BC to enhance privacy and security in the e-Health domain (e.g., EMR)?*

Integrating Differential Privacy in decentralized healthcare is considered part of modern smart cities. Every patient, doctor, and hospital is connected to provide services such as remote health monitoring, fitness programmers, and elderly care [69]. The integration trend has potential benefits, although it raises privacy concerns as data over the Blockchain is stored in a decentralized ledger. Therefore, the authors in [69] proposed a healthcare system whereby a secure Blockchain-based system is used as a proof of vote (PoV) consensus mechanism. By using one of the categories to answer RQ1, real-time health data is considered. Real-time health data used in e-Health domains mostly comes from IoT devices, which is different from conventional health data [74]. The mechanisms are also called data perturbation, including the Laplace, Exponential, and Gaussian mechanisms. This research question explores which mechanisms researchers have used to protect the privacy of sensitive health data in real-time.

4.2. *RQ2: What factors contribute to the DP mechanisms integration in Blockchain Technology and associated issues?*

This research question explores the factors contributing to Blockchain Technology integration with DP based on reliability, utility-privacy trade-off, and risk minimization. The data over the Blockchain is stored in a decentralized distributed Hyperledger. Furthermore, the node contains a copy of that ledger [39]. The researchers suggest privacy preservation strategies based on e-Health systems, and one of these strategies is called Differential Privacy in decentralized healthcare [69]. A report of diagnosis of disease falls under this EMR, and the technical work is kept secure by using centralized Differential Privacy and pseudo-identity mechanisms [75]. The researchers introduced a risk minimization strategy using test errors to overcome adversaries in a public Blockchain environment. The associated issues concern the navigation between utility (accuracy) and privacy, the trade-off. For example, adding noise to the data may reduce the accuracy of the information in the e-Health domain [43]. Furthermore, this may put the safety and welfare of the patient at risk. Therefore, an adequate trade-off between privacy and utility (accuracy) must be maintained. The proposal in [76] involved a Differential Privacy-based solution and optimization of privacy parameters to obtain a helpful utility (accuracy) and privacy trade-off.

4.3. RQ3: What types of datasets and programming languages are being considered for implementation?

The implementation of any proposed solution depends on the quality of the datasets. As reviewed in section 2.2.1, data perturbation mechanisms for Laplace and Gaussian use numerical datasets, while Exponential uses a non-numerical dataset. The dataset used in data perturbation mechanisms is a structured dataset. However, further research reveals that most proposal applications grouped datasets into public and private datasets based on availability.

The EMR Privacy category, according to Saleheen et al. [77], shows a dataset with 660 hours of ECG (electrocardiogram) from participants whose private dataset was collected. Lin et al. [78] collected private datasets from wearable sensors, [79] collected heart disease datasets, and Hadian et al. [80] collected datasets from wearable devices that users attached to their bodies to monitor heart rate. A blood bank dataset containing individual information has utilized a research record dataset [81]. In addition, datasets are also obtained during activities such as walking, running, and sleeping. Kim et al. [82] obtained a dataset from daily step counts using a Gear S3 smartwatch. Table 4.1 below shows a summary of dataset utilization in the e-Health domain.

The Real-Time Health Data category utilizes the flu dataset that Geo et al. [83] harnesses. Wearables are also used to record and share real-time health datasets. In [78], the heart rate dataset was recorded to be used in research–real-time data. The summary is shown in Table 4.1 below.

Health Survey Data Protection discusses and provides inside surveys according to users' perspectives. Most of these datasets from a database are statistically queried. Luo et al. [84] surveyed two real-world case studies. One of the cases uses a health survey based on students' heart rates to find the average and distribution statistically. The second case is for collaboration to classify models based on emotions. Yang et al. [85] also use real-world public datasets with one million health datasets. The summary is shown in Table 4.1 below.

Table 4.1. Different Types of Datasets.

Data Type	EMR Privacy	Real-Time Health Data	Health Survey Data Protection
Private (Heart-related)	[78, 80]	[78]	[84]
Public	[81]	_	[85]
Private	[78]	_	_
Public (Activities, e.g., running, walking)	[81]	_	_
Private (Wearable sensors)	[82, 80]	[83]	_
A systemic literature review (SLR) on e-Health data under Differential Privacy			

4.4. RQ4: What are the limitations and inherent challenges of the BT and DP applications, and how can they be solved?

The limitations of the existing methodology are visible, and researchers have conducted several experiments to evaluate different approaches.

EMR Privacy: As discussed in [20], Blockchain Technology has scalability issues. Most of the proposed solutions for Differential Privacy are for static database information as it confines to a single dimension [86]. Another issue is that most of the privacy protection approach needs a practical roadmap for implementation, and some models suffer from degradation in performance as the number of cloud resources increases [87]. Zhang et al. [86] proposed a more complex algorithm than existing works. The methods are also vulnerable to information leakage, giving adversaries more knowledge about sensitive data.

Real-Time Health Data: Proposed solutions for real-time data in differential applications suffer data perturbation errors [88] because of relative and absolute errors [89]. The strength of privacy guaranteed is controlled by ε, and it is not clear how to choose an appropriate value in a given situation, as shown in [45][46], where algorithms have chosen ε from the range of 0.01 to 7. For example, in [90], a large budget (ε >1) shows no corresponding advantages. Similarly, in [83], there is evidence that increasing the epsilon value weakens the algorithm. Therefore, choosing an appropriate epsilon value is challenging for a threshold application.

Health Survey Data Protection: Challenges of complete privacy protection exist when individuals participate in a survey that potentially reveals their sensitive information [91].

5. Challenges and Limitations

Firstly, Blockchain has scalability and interoperability issues that create unreasonable constraints on exchanging patient data [20]. Secondly, Differential Privacy is challenging when choosing epsilon (ϵ) [37, 44, 45]. Sensitivity is another challenge: navigating the trade-off between privacy and accuracy (utility) [42, 43, 44]. Data correlation-dataset used in a real-world situation is strongly correlated, which gives an adversary a chance to combine obfuscated data to obtain sensitive health information [47, 10]. Mechanisms- implementation of Differential Privacy, such as Laplace noise, is vulnerable to being tracked or attacked [84].

6. Contributions and Recommendations

By accomplishing the review work from different research papers, the following claims summarize the contributions based on the findings:

- Integrating blockchain and differential is much more complex, and theoretically based models are primarily published on enhancing privacy in the e-Health Domain.
- This paper gives insight into why the failure of many differential privacy and blockchain proposed projects. These are indicated in the literature review and gap analysis sections, and a developed framework needs to be developed to leverage differential privacy.
- Most literature could be more intuitive, and we need to know the connection between the academic platform and the practical application of differential privacy. Furthermore, more knowledge about researchers' and developers' expectations are required.

Recommendations for implementing a privacy-preserving blockchain-based solution. One approach could be to use homomorphic encryption to encrypt the sensitive data stored on the blockchain, allowing for computations to be performed on the encrypted data without exposing it. The data can then be decrypted only by authorized parties. Additionally, differential privacy techniques can be used to add random noise to the data before it is stored on the blockchain to protect the privacy of individual patients further. By implementing these privacy-enhancing technologies, a secure and private system for EMR storage and management can be established, maintaining the confidentiality of sensitive medical information while allowing for the benefits of a decentralized, tamper-proof system.

Conclusion

The three categories, EMR privacy, real-time health data, and health survey data protection, are significant concerns in e-Health domains as they relate to privacy. Blockchain Technology and Differential Privacy have emerged as suitable mechanisms. This project aims to understand Blockchain and Differential Privacy in e-Health domains for privacy protection, as well as the limitations and the future direction to enhance integration and implementation of Blockchain and Differential Privacy in e-Health domains.

The literature review and related works show that gaps still exist, requiring additional mechanisms for more secure privacy in e-Health domains. In addition, the trade-off between privacy and utility (accuracy) in differential and the integration of Blockchain with Differential Privacy is a complex computational problem. Recently, most companies and establishments have experienced a rapid increase in cybersecurity attacks from adversaries to compromise the privacy of sensitive information. The attackers exploit weaknesses such as correlated data despite using Differential Privacy to breach the security mechanisms.

This review thoroughly surveyed and summarized Differential Privacy mechanisms in EMR privacy, real-time health data, and health survey data protection while highlighting limitations and challenges and exploring future research areas in Blockchain and Differential Privacy.

References

1. Centers for Disease Control and Prevention. (2018, September 14). Health Insurance Portability and accountability act of 1996 (HIPAA). Centers for Disease Control and Prevention. Retrieved January 31, 2022, from https://www.cdc.gov/phlp/publications/topic/hipaa.html
2. Compliancy Group. (2022, July 22). The CIA triad: Confidentiality, integrity, availability for HIPAA. Compliancy Group. Retrieved December 2, 2022, from https://compliancy-group.com/the-cia-triad-confidentiality-integrity-availability-for-hipaa/
3. J. Zhang, X. Liang, Z. Zhang, S. He, and Z. Shi, “Re-dpoctor: Real-time health data releasing with w-day differential privacy,” arXiv preprint arXiv:1711.00232, 2017.
4. M. U. Hassan, M. H. Rehmani and J. Chen, "Differential Privacy Techniques for Cyber Physical Systems: A Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 746-789, Firstquarter 2020, doi: 10.1109/COMST.2019.2944748
5. Keshta,I., & Odeh, A. Security and Privacy of Electronic Health Records: Concerns and Challenges, Egyptian Informatics Journal, Volume 22, Issue 2, 2021, Pages 177-183, ISSN 1110-8665, https://doi.org/10.1016/j.eij.2020.07.003. (https://www.sciencedirect.com/science/article/pii/S1110866520301365)
6. G. Perera, A. Holbrook, L. Thabane, G. Foster, D.J. Willison Views on Health Information Sharing and Privacy from Primary care Practices using Electronic Medical Records Int J Med Informatics, 80 (2) (2011), pp. 94-101 https://doi.org/10.1016/j.ijmedinf.2010.11.005
7. J. Ancker, M. Silver, M. Miller, R. Kaushal Consumer Experience with and Attitude Toward Health Information Technology: A Nationwide Survey Am Medical Informatics Assoc, 1 (2012), pp. 152-156 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3555333/
8. (OCR), O. for C. R. (2021, June 28). Health insurer pays $5.1 million to settle data breach affecting over 9.3 million people. HHS.gov. Retrieved February 1, 2022, from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/excellus/index.html
9. EHRIntelligence, K. M. (2018, September 18). Ehr Design, Interoperability Top List of physician pain points. EHRIntelligence. Retrieved February 1, 2022, from https://ehrintelligence.com/news/ehr-design-interoperability-top-list-of-physician-pain-points
10. H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, “Blockchain Challenges and Opportunities: A Survey,” International Journal of Web and Grid Services, vol. 14, no. 4, p. 352, 2018, https://www.inderscienceonline.com/doi/abs/10.1504/IJWGS.2018.095647
11. R. Cheng, F. Zhang, J. Kos, W. He, N. Hynes, N. Johnson, ... & Song, D. (2019, June). Ekiden: A platform for confidentiality-preserving, trustworthy, and performant smart contracts. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 185-200). IEEE. https://ieeexplore.ieee.org/abstract/document/8806762/authors
12. Y. Sun, L. Zhang, G. Feng, B. Yang, B. Cao and M. A. Imran, "Blockchain-Enabled Wireless Internet of Things: Performance Analysis and Optimal Communication Node Deployment," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 5791-5802, June 2019, https://ieeexplore.ieee.org/abstract/document/8668426
13. S. Sarmah, (2018). Understanding Blockchain Technology. *Computer Science and Engineering*, *8*(2), 23-29.
14. Y. Zou, T. Meng, P. Zhang, W. Zhang and H. Li, "Focus on Blockchain: A Comprehensive Survey on Academic and Application," in IEEE Access, vol. 8, pp. 187182-187201, 2020, https://ieeexplore.ieee.org/abstract/document/9220919
15. P. Garret, & J. Seidman. (2011, August 26). EMR vs EHR – What is the Difference? Health IT Buzz. Retrieved January 31, 2022, from https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference
16. M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang and C. Youn, "Wearable 2.0: Enabling Human-Cloud Integration in Next Generation Healthcare Systems," in IEEE Communications Magazine, vol. 55, no. 1, pp. 54-61, January 2017, https://ieeexplore.ieee.org/document/7823338
17. B. Cao, Z. Zhang, D. Feng, S. Zhang, L. Zhang, M. Peng, Y. Li, Performance analysis and comparison of PoW, PoS and DAG based blockchains, Digital Communications and Networks, Volume 6, Issue 4, 2020,

doi:10.20944/preprints202310.0553.v1

Pages 480-485, ISSN 2352-8648, https://doi.org/10.1016/j.dcan.2019.12.001. (https://www.sciencedirect.com/science/article/pii/S2352864819301476)

18. F. Casino, T. Dasaklis, C. Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and open issues, Telematics and Informatics, Volume 36, 2019, Pages 55-81, https://www.sciencedirect.com/science/article/pii/S0736585318306324
19. A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, & F. Wang (2018). Secure and Trustable Electronic Medical Records Sharing using Blockchain. AMIA ... Annual Symposium proceedings. AMIA Symposium, 2017, 650–659. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/
20. A. Roehrs, C. A. da Costa, and R. da Rosa Righi, “OmniPHR: A distributed architecture model to integrate personal health records,” Journal of Biomedical Informatics, vol. 71, pp. 70–81, Jul. 2017, https://www.sciencedirect.com/science/article/pii/S1532046417301089
21. S. Ølnes, J. Ubacht, M. Janssen, Blockchain in government: Benefits and implications of distributed ledger technology for information sharing, Government Information Quarterly, Volume 34, Issue 3, 2017, Pages 355-364, ISSN 0740-624X, https://doi.org/10.1016/j.giq.2017.09.007
22. M. Iansiti and K. R. Lakhani, “The Truth About Blockchain,” Harvard Business Review, no. January-February 2017, Jan. 01, 2017.
23. H. Wang, Z. Zheng, S. Xie, H. N. Dai, and X. Chen, “Blockchain Challenges and Opportunities: A Survey,” International Journal of Web and Grid Services, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/IJWGS.2018.10016848
24. M. C. Wong, K. C. Yee, and C. Nohr, “Socio-technical consideration for Blockchain Technology in healthcare: the technological innovation needs clinical transformation to achieve the outcome of improving quality and safety of patient care,” Studies in Health Technology and Informatics, vol. 247, pp. 636–640, 2018, doi: 10.3233/978-1-61499-852- 5-636.
25. A. W. Peters, B. M. Till, J. G. Meara, and S. Afshar, “Blockchain technology in health care: A primer for surgeons,” The Bulletin, Dec. 06, 2017
26. IBM, “Blockchain: The Chain of Trust and its Potential to Transform Healthcare – Our Point of View,” Aug. 2016. Accessed: Feb. 11, 2022. [Online]. Available: https://www.healthit.gov/sites/default/files/8-31-blockchain-ibm_ideation-challenge_aug8.pdf.
27. I. C. Lin, T. C. Liao. A Survey of Blockchain Security Issues and Challenges. Int. J. Netw. Secur. 2017, 19, 653–659
28. T. Clohessy, T. Acton, and N. Rogers. (2019). “Blockchain Adoption: Technological, Organisational and Environmental Considerations”, in Treiblmaier, H. and Beck, R. "Business Transformation through Blockchain", Volume 1, Cham, Switzerland: Palgrave Macmillan, pp.47-76. DOI: 10.1007/978-3-319-98911-2
29. T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, “Blockchain in healthcare applications: Research challenges and opportunities,” Journal of Network and Computer Applications, vol. 135, pp. 62–75, Jun. 2019, doi: 10.1016/j.jnca.2019.02.027
30. G. Zyskind, O. Nathan, and A. Pentland, Decentralizing privacy: Using blockchain to protect personal data. Proceedings of IEEE Security and Privacy Workshops:180–184, 2015. https://doi.org/ 10.1109/SPW.2015.27
31. A. Lippman, T. Vieira, A. Ekblaw, A. Azaria, et al., MedRec: Using blockchain for medical data. Presented at International Conference on Open & Big Data. 2016. Available: http:// ieeexplore.ieee.org/document/7573685/
32. S. Hogan, H. Fraser, P. Korsten, V. Pureswaran, and R. Gopinath, “Healthcare rallies for blockchains Keeping patients at the center,” IBM Institute for Business Value, Dec. 2016. https://www.ibm.com/downloads/cas/BBRQK3WY
33. Deloitte, “Blockchain to Blockchains in Life Sciences and Health Care,” Deloitte, 2018. https://www2.deloitte.com/uk/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey-2019/2019-adoption-by-industry.html
34. C. Dwork. (2008). Differential Privacy: A Survey of Results. Lecture Notes in Computer Science Theory and Applications of Models of Computation, 1-19. doi:10.1007/978-3-540-79228-4_1
35. C. Dwork, A. Roth, "The Algorithmic Foundations of Differential Privacy," in The Algorithmic Foundations of Differential Privacy , now, 2014. https://ieeexplore.ieee.org/document/8187424

36. J. Lee , C. Clifton.. (2011) How Much Is Enough? Choosing ϵ for Differential Privacy. In: Lai X., Zhou J., Li H. (eds) Information Security. ISC 2011. Lecture Notes in Computer Science, vol 7001. Springer, Berlin, Heidelberg. https://doi.org/10.1007/ 978-3-642-24861-0_22
37. J. Hsu et al., "Differential Privacy: An Economic Method for Choosing Epsilon," 2014 IEEE 27th Computer Security Foundations Symposium, Vienna, 2014, pp. 398-410, doi: 10.1109/CSF.2014.35
38. C. Dwork, "A firm foundation for private data analysis," Communications of the ACM, vol. 54, no. 1, pp. 86–95, 2011.
39. C. Dwork, A. Roth. et al.: An adaptive approach to real-time aggregate monitoring with differential privacy. Foundations and Trends®in Theoretical Computer Science 9(3–4), 211 (2014)
40. F. Liu, "Generalized Gaussian Mechanism for Differential privacy," IEEE Transactions on Knowledge and Data Engineering, vol. 31, no. 4, pp. 747 – 756, Apr. 2018. https://par.nsf.gov/servlets/purl/10066992
41. T. Zhu, G. Li, W. Zhou, & S. Y. Philip. (2017). *Differential privacy and applications*. Cham, Switzerland: Springer International Publishing.
42. J. Soria-Comas, J. Domingo-Ferrer, D. S´anchez, and D. Meg´ıas, "Individual differential privacy: A utility-preserving formulation of differential privacy guarantees," IEEE Transactions on Information Forensics and Security, vol. 12, no. 6, pp. 1418–1429, 2017.
43. E. ElSalamouny and S. Gambs, "Differential privacy models for location-based services," Transactions on Data Privacy, vol. 9, no. 1, pp. 15–48, 2016.
44. X. He, G. Cormode, A. Machanavajjhala, C. M. Procopiuc, and D. Srivastava, "Dpt: differentially private trajectory synthesis using hierarchical reference systems," Proceedings of the VLDB Endowment, vol. 8, no. 11, pp. 1154–1165, 2015
45. A. Machanavajjhala, A. Korolova, and A. D. Sarma. Personalized social recommendations - accurate or private? PVLDB, 4(7):440–450, 2011. https://arxiv.org/ftp/arxiv/papers/1105/1105.4254.pdf
46. F. McSherry and R. Mahajan. Differentially-private network trace analysis. In Proc. SIGCOMM, pages 123–134, 2010. https://ratul.org/papers/sigcomm2010-privacy.pdf
47. C. Dwork, K. Talwar, A. Thakurta, and L. Zhang, "Analyze gauss: optimal bounds for privacy-preserving principal component analysis," in Proceedings of the forty-sixth annual ACM symposium on Theory of computing, 2014, pp. 11–20.
48. T. Li, A. K. Sahu, A. Talwalkar. & V. Smith. Federated learning: Challenges, methods, and future directions. IEEE Signal Processing Magazine 37, 50–60 (IEEE, 2020).
49. Kairouz, P. et al. Advances and open problems in federated learning. arXiv preprint arXiv:1912.04977 (2019).
50. N. Rieke, J. Hancox, W. Li. et al. The future of digital health with federated learning. npj Digit. Med. 3, 119 (2020). https://doi.org/10.1038/s41746-020-00323-1
51. N. Rieke, J. Hancox, W. Li. et al. The future of digital health with federated learning. npj Digit. Med. 3, 119 (2020). https://doi.org/10.1038/s41746-020-00323-1
52. J. Lee. et al. Privacy-preserving patient similarity learning in a federated environment: development and analysis. JMIR Med. Inform. 6, e20 (2018).
53. T.S. Brisimi. et al. Federated learning of predictive models from federated electronic health records. Int. J. Med. Inform. 112, 59–67 (2018).
54. A. G. Roy, S. Siddiqui, S. Pölsterl, N. Navab, & C. Wachinger Braintorrent: a peer-to-peer environment for decentralized federated learning. arXiv preprint arXiv:1905.06731 (2019).
55. Wang, F., Casalino, L. P. & Khullar, D. Deep learning in medicine—promise, progress, and challenges. JAMA Intern. Med. 179, 293–294 (2019).
56. Sheller, M. J., Reina, G. A., Edwards, B., Martin, J. & Bakas, S. Multi-institutional deep learning modeling without sharing patient data: a feasibility study on brain tumor segmentation. In International MICCAI Brainlesion Workshop, 92–104 (Springer, 2018)
57. Kairouz, P. et al. Advances and open problems in federated learning. arXiv preprint arXiv:1912.04977 (2019)
58. Abadi, M. et al. Deep learning with differential privacy. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 308–318 (ACM, 2016
59. Li, X. et al. Multi-site fmri analysis using privacy-preserving federated learning and domain adaptation: abide results. arXiv preprint arXiv:2001.05647 (2020).

60. S. Garfinkel, J. Abowd, and S. Powazek. 2018. Issues Encountered Deploying Differential Privacy. In Proceedings of the 2018 Workshop on Privacy in the Electronic Society (WPES'18). Association for Computing Machinery, New York, NY, USA, 133–137. https://doi.org/10.1145/3267323.3268949
61. P. Jain, M. Gyanchandani, & N. Khare. Differential privacy: its technological prescriptive using big data. J Big Data 5, 15 (2018). https://link.springer.com/article/10.1186/s40537-018-0124-9
62. M. Hassan, M. H. Rehmani, J. Chen,Differential privacy in Blockchain Technology: A futuristic approach, Journal of Parallel and Distributed Computing, Volume 145,2020, Pages 50-74, ISSN 0743-7315, (https://www.sciencedirect.com/science/article/pii/S0743731520303105)
63. P. Wang, J. Huang, Z. Cui, L. Xie, J. Chen, A Gaussian error correction multi-objective positioning model with nsga-ii, Concurr. Comput.: Pract. Exper. 32 (5) (2020) e5464.
64. X. Cai, Y. Niu, S. Geng, J. Zhang, Z. Cui, J. Li, J. Chen, An under-sampled software defect prediction method based on hybrid multi-objectivecuckoo search, Concurr. Comput.: Pract. Exper. 32 (5) (2020) e5478
65. L. Axon, Privacy-Awareness in Blockchain-Based PKI, University of Oxford, 2015
66. Y.-A. De Montjoye, L. Radaelli, V.K. Singh, et al., Unique in the shopping mall: On the reidentifiability of credit card metadata, Science 347 (6221) (2015) 536–539.
67. G. Eibl, D. Engel, Differential privacy for real smart metering data, Comput. Sci.-Res. Dev. 32 (1–2) (2017) 173–182.
68. J. Xie, H. Tang, T. Huang, F.R. Yu, R. Xie, J. Liu, Y. Liu, A survey of Blockchain Technology applied to smart cities: Research issues and challenges, IEEE Commun. Surv. Tutor. (2019) i
69. J. Vora, A. Nayyar, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, J.J.Rodrigues, BHEEM: A blockchain-based framework for securing electronic health records, in: IEEE Globecom Workshops (GC Wkshps), 2018,pp. 1–6. https://ieeexplore.ieee.org/abstract/document/8644088
70. A. Dewey, & A. Drahota (2016) Introduction to systematic reviews: online learning module Cochrane Training https://training.cochrane.org/interactivelearning/module-1-introduction-conducting-systematic-reviews
71. M. Salama, R. Bahsoon, N. Bencomo, Chapter 11 - Managing Trade-offs in Self-Adaptive Software Architectures: A Systematic Mapping Study,Editor(s): Ivan Mistrik, Nour Ali, Rick Kazman, John Grundy, Bradley Schmerl,Managing Trade-Offs in Adaptable Software Architectures,Morgan Kaufmann, 2017, Pages 249-297,ISBN 9780128028551,(https://www.sciencedirect.com/science/article/pii/B9780128028551000113)
72. https://arxiv.org/ftp/arxiv/papers/1702/1702.02653.pdf
73. Fink, A.: Conducting research literature reviews: from the internet to paper. Thousand Oaks, Thousand Oaks (2019)
74. M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: A comprehensive survey, IEEE Commun. Surv. Tutor. 21 (2) (2018) 1676–1717
75. X. Wang, K. Yang, Asynchronous blockchain-based privacypreserving training framework for disease diagnosis, in: IEEE International Conference on Big Data (Big Data), 2019, pp. 5469–5473.
76. Q. Hu, R. Chen, H. Yang, and S. Kumara, ‘‘Privacy-preserving data mining for smart manufacturing,’’ Smart Sustain. Manuf. Syst., vol. 4, no. 2, Jul. 2020, Art. no. 20190043
77. N. Saleheen, S. Chakraborty, N. Ali, M. M. Rahman, S. M. Hossain, R. Bari, E. Buder, M Srivastava, S. Kumar.: In: Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing (2016), pp. 706–717
78. C. Lin, Z. Song, H. Song, Y. Zhou, Y. Wang, G. Wu.: Differential privacy preserving in big data analytics for connected health. J. Med. Syst. 40(4), 97 (2016)
79. K. Prema, A. Sriharsha: Differential privacy in big data analytics for haptic applications. Technology 8(3), 11 (2017)
80. M. Hadian, X. Liang, T. Altuwaiyan, M. M. Mahmoud: In: 2016 IEEE Global Communications Conference (GLOBECOM) (IEEE, 2016), pp. 1–6
81. Z. Guan, Z. Lv, X. Du, L. Wu, and M. Guizani, “Achieving data utilityprivacy tradeoff in internet of medical things: A machine learning approach,” Future Generation Computer Systems, in Print, 2019.
82. J. W. Kim, J. H. Lim, S. M. Moon, H. Yoo, B. Jang: In: 2019 IEEE International Conference on Consumer Electronics (ICCE) (IEEE, 2019), pp. 1–4
83. R. Gao, X. Ma: In: 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking,

Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom) (IEEE, 2018), pp. 737–743

84. C. Luo, X. Liu, W. Xue, Y. Shen, J. Li, W. Hu, Liu, A.X.: Predictable privacy-preserving mobile crowd sensing: a tale of two roles. IEEE/ACM Trans. Network. 27(1), 361 (2019)
85. M. Yang: Improving privacy preserving in modern applications. Deakin University, Tech. rep. (2019)
86. Z. Zhang, B. Han, H. C. Chao, F. Sun, L. Uden, Tang, D.: A new weight and sensitivity based variable maximum distance to average vector algorithm for wearable sensor data privacy protection. IEEE Access 7, 104045 (2019)
87. Y. Zhang, Y. Qu, L. Gao, T. H. Luan, X. Zheng, S. Chen, Y. Xiang: APDP: Attack-Proof Personalized Differential Privacy Model for a Smart Home. IEEE Access 7, 166593 (2019)
88. V. Rastogi, S. Nath: In: Proceedings of the 2010 ACM SIGMOD International Conference on Management of data (2010), pp. 735–746
89. L. Fan, L. Xiong: An adaptive approach to real-time aggregate monitoring with differential privacy. IEEE Trans. Knowl. Data Eng. 26(9), 2094 (2013)
90. Fan, L., Xiong, L.: In: Proceedings of the 21st ACM international conference on Information and knowledge management (2012), pp. 2169–2173
91. A. C. Valdez and M. Ziefle, “The users’ perspective on the privacyutility trade-offs in health recommender systems,” International Journal of Human-Computer Studies, in Print, vol. 121, pp. 108–121, Jan. 2019 https://moam.info/arxiv181202282v1-cscr-6-dec-2018_5c362c14097c478d538b456d.html
92. J. Zhang, X. Liang, Z. Zhang, S. He, and Z. Shi, “Re-dpoctor: Real-time health data releasing with w-day differential privacy,” arXiv preprint arXiv:1711.00232, 2017. https://arxiv.org/pdf/1812.02282v1.pdf
93. A. Alnemari, C. J. Romanowski, and R. K. Raj, “An adaptive differential privacy algorithm for range queries over healthcare data,” in IEEE International Conference on Healthcare Informatics (ICHI), 2017, pp. 397–402 https://ieeexplore.ieee.org/abstract/document/8031181
94. H. Li, Y. Dai, and X. Lin, “Efficient e-health data release with consistency guarantee under differential privacy,” in IEEE 17th International Conference on E-health Networking, Application & Services (HealthCom), 2015, pp. 602–608
95. Z. Guan, Z. Lv, X. Du, L. Wu, and M. Guizani, “Achieving data utilityprivacy tradeoff in internet of medical things: A machine learning approach,” Future Generation Computer Systems, in Print, 2019.
96. B. K. Beaulieu-Jones, W. Yuan, S. G. Finlayson, and Z. S. Wu, “Privacy-preserving distributed deep learning for clinical data,” arXiv preprint arXiv:1812.01484, 2018.
97. N. Mohammed, S. Barouti, D. Alhadidi, and R. Chen, “Secure and private management of healthcare databases for data mining,” in IEEE 28th International Symposium on Computer-Based Medical Systems (CBMS), 2015, pp. 191–196
98. J. L. Raisaro, J. Troncoso-Pastoriza, M. Misbach, J. S. Sousa, S. Pradervand, E. Missiaglia, O. Michielin, B. Ford, and J.-P. Hubaux, “Medco: Enabling secure and privacy-preserving exploration of distributed clinical and genomic data,” IEEE/ACM transactions on computational biology and bioinformatics, in Print, 2018
99. J. L. Raisaro, G. Choi, S. Pradervand, R. Colsenet, N. Jacquemont, N. Rosat, V. Mooser, and J.-P. Hubaux, “Protecting privacy and security of genomic data in i2b2 with homomorphic encryption and differential privacy,” IEEE/ACM transactions on computational biology and bioinformatics, vol. 15, no. 5, pp. 1413 – 1426, Sep. 2018
100. W. Tang, J. Ren, K. Deng, and Y. Zhang, “Secure Data Aggregation of Lightweight E-healthcare IoT Devices with Fair Incentives,” IEEE Internet of Things Journal, in Print, 2019
101. Z. Guan, Z. Lv, X. Du, L. Wu, and M. Guizani, “Achieving data utilityprivacy tradeoff in internet of medical things: A machine learning approach,” Future Generation Computer Systems, in Print, 2019. https://arxiv.org/ftp/arxiv/papers/1902/1902.02898.pdf
102. W. Tang, J. Ren, K. Deng, and Y. Zhang, “Secure Data Aggregation of Lightweight E-healthcare IoT Devices with Fair Incentives,” IEEE Internet of Things Journal, in Print, 2019 https://ieeexplore.ieee.org/abstract/document/8737719
103. Gao, R., Ma, X.: In: 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications
104. A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In Proc. S&P. IEEE, May 2008 https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf

105. A. Narayanan and V. Shmatikov. De-anonymizing social networks. In IEEE Symposium on Security and Privacy (S&P), Oakland, California, pages 173–187, 2009 https://ieeexplore.ieee.org/abstract/document/5207644

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.