International Journal of Computer Applications (0975 - 8887)
Volume 187 - No.130, July 2026

Data Privacy in E-Healthcare: A Systematic Review of Frameworks and Approaches

Punam Prabha, PhD
Department of Computer Science & Engineering
Bhagalpur College of Engineering, Bhagalpur
813210, Bihar, India

Kakali Chatterjee, PhD
Department of Computer Science & Engineering
National Institute of Technology Patna
800005, Bihar, India

ABSTRACT

E-Healthcare Systems (EHS) are transforming medical service delivery by enabling real-time data sharing, remote diagnostics, and integrated care via IoT and cloud infrastructures. However, the increasing volume of sensitive medical data being transmitted over distributed systems creates serious privacy and security concerns. This article reviews several papers on the EHS Data Privacy Framework, addressing critical issues such as illegal data access, identity exposure, and data integrity breaches. This review examines the existing data privacy frameworks used in EHS, focusing on four domains: traditional EHS, cloud-based EHS, IoT-based EHS and blockchain-based EHS with an emphasis on author, year, objective, and limitation. This framework provides a scalable and interoperable approach to protecting privacy for future healthcare systems.

Keywords

data privacy framework, e-healthcare system (EHS), security, survey

1. INTRODUCTION

Nowadays, the E-Healthcare System (EHS) is rapidly expanding in order to provide effective and rapid processing of medical services and patient information while keeping cost and time constraints [1]. Patient data is the foundation of EHS, enabling critical functions like patient monitoring, diagnosis, treatment, and healthcare management. Accurate and real-time data acquired from Internet of Things (IoT) devices, electronic health records, and wearable technology allows healthcare providers to provide individualized care and make informed decisions.

Data facilitates early detection of diseases, remote patient monitoring, and predictive analytics, leading to better patient outcomes and reduced healthcare costs. Furthermore, aggregated health data supports medical research, helps identify public health trends, and informs policy decisions. Ensuring the integrity, confidentiality, and availability of this data is crucial for maintaining trust in EHS and ensuring patient privacy and regulatory compliance. Data enables early disease identification, remote patient monitoring, and predictive analytics, resulting in improved patient outcomes and lower healthcare expenditures. Furthermore, aggregated health data facilitates medical research, identifies public health trends, and informs policy decisions. Ensuring the accuracy, security, and availability of these data is critical to maintaining trust in EHS while also protecting patient privacy and regulatory compliance. However, the current EHS infrastructure faces significant challenges, such as security vulnerabilities, privacy breaches, data inconsistencies, and overly accessible health records. These issues highlight the urgent need for significant restructuring in data management and patient data security. To address the above-mentioned issues, the current paper reviews a data privacy framework for EHS.

The basic history of data privacy frameworks in EHS, including its taxonomy, is covered in this article. The EHS privacy issue was resolved in a number of ways. This study provides an in-depth overview of the state-of-the-art mechanisms for data privacy frameworks by looking at different methods and frameworks to safely handle sensitive healthcare stakeholder data. A wide range of privacy-preserving techniques have been thoroughly investigated and described in the literature [1]. Some notable works are described in [2]. These privacy-preserving techniques focus on data collection, publication, data mining output, and distribution.

In an EHS, patient care in a collaborative environment improves quality of care, reduces inaccuracies in medication and misdiagnoses, and ultimately improves patient satisfaction. For example, a diabetic patient's treatment plan can involve input from a dietitian, medication prescribed by a doctor, and lifestyle recommendations from a lifestyle manager. Similarly, a patient experiencing multiple organ failures, such as kidney and heart failure, may require the intervention of specialists in multiple departments. In such scenarios, sensitive data are shared among various stakeholders, increasing the risk of data manipulation, spoofing, and other threats. This can result in clinical data breaches and falsification, with significant financial and legal implications. To address these challenges, an EHS framework is crucial for maintaining data privacy and security, motivating the development of a revised data privacy framework.

In addition, anonymous authentication plays a vital role in safeguarding sensitive patient information. It allows valid users to hide their identities, enabling authentication through pseudonymous credentials. This approach is particularly beneficial for sensitive cases, such as victims of sexual harassment or patients suffering from terminal diseases like cancer or AIDS, as identity leaks could lead to social stigma. Group authentication further supports seamless collaboration, allowing a single patient to consult multiple doctors or allowing multiple patients to receive treatment simultane-

ously through securely recorded data accessible on Internet servers. Based on the motivation above, a review paper on the data privacy framework for EHS is further classified, as illustrated in Figure 1. The authors, year, goals, and limits of each technique are examined in relation to how they affect security and privacy within EHS. This study significantly advances the creation of an EHS data privacy framework. In FIGURE 1, this data privacy architecture is divided into four domains: traditional EHS, cloud-based EHS, IoT-based EHS, and blockchain-based EHS. Thus, Table 1 to 24 conducts a thorough literature review with an emphasis on author, year, objective, and limitation.

The present paper is organized into six sections to provide a clear and structured presentation of the research work. The current section 1 introduces the work, highlighting its objectives within the context of data privacy frameworks for EHS. Furthermore, Section 2 describes significant research findings of traditional EHS. Section 3 discusses important research findings on cloud-based EHS. Section 4 highlights key study findings on IoT-based EHS. Section 5 summarizes major research findings on blockchain-based EHS. Section 6 brings the work to an end.

2. TRADITIONAL EHS

Traditional EHS is characterized by various privacy mechanisms, including additive noise based privacy, multiplicative noise based privacy, k-anonymity based privacy, l-diversity based privacy, t-closeness based privacy, and personalized privacy.

2.1 Additive noise based privacy

An in-depth literature review of the existing privacy frameworks for traditional EHS utilizing additive noise is presented in the Table 1.

Table 1. Additive noise.

Author	Year	Objective	Limitation
Kalaivani et al. [3]	2014	Using multilevel trust and additive perturbation to ensure privacy preserving data mining.	In particular scenarios, correlated noise can reduce accuracy or utility.
Abdelhameed et al. [4]	2017	Improve the utility of privacy preserving data publishing mechanism.	Accuracy of data may be compromised in particular analytical applications.
Farokhi et al. [5]	2019	Link Fisher information and utility to optimize noise for privacy.	Restricted query range and noise, utility concessions, computational cost.
Denham et al. [6]	2020	Improve privacy preserving stream mining with robust tampering techniques.	Cumulative noise may negatively impact utility of data.
Murguia et al. [7]	2020	Improve data privacy by the utilization of synchronized unpredictable cycles.	Achieving synchronization across random oscillators is challenging and prone to errors.

Techniques for protecting privacy are thoroughly investigated in order to protect sensitive information while retaining its analytical utility. For instance, Kalaivani et al. in [3] suggested an additive noise based model that incorporates random Gaussian noise and multilevel trust to safeguard against diversity attacks and ensure the secure publishing of data. In a similar way, Farokhi et al. [5] addressed database privacy by optimizing noise distributions for both static and dynamic scenarios, connecting privacy measures to the Fisher information matrix and Cramer Rao bound, and employing restricted additive noise for query replies. Additionally, for stream mining, Denham et al. [6] integrated random projection, translation, and additive noise; in this case, the cumulative noise strategy works well to prevent off recovery attempts. Furthermore, Murguia et al. [7] optimized data privacy by using random vectors produced by synchronized chaotic oscillators. This allows for secure recovery while distorting queries to minimize mutual information with private entries. In order to balance data utility and robust privacy, Abdelhameed et al. [4] improved additive noise for privacy preserving tabular data publishing, concentrating on single sensitive attributes. This makes it appropriate for cross organizational data sharing without sacrificing individual privacy. The implementation of these strategies addresses multiple challenges associated with safe data transmit and analysis, thereby progressing the area of privacy preserving data management.

2.2 Multiplicative noise based privacy

A detailed literature review of the existing privacy frameworks for traditional EHS utilizing multiplicative noise is provided in the Table 2.

Table 2. Multiplicative noise

Author	Year	Objective	Limitation
Klein et al. [8]	2014	Secure and informative data communication.	Influenced by the type of data and the distribution of noise.
Kumar et al. [9]	2014	Balancing utility with data privacy.	Balancing utility and privacy remains challenging.
Brackenbury et al. [10]	2019	Improve smart meter data privacy using sensible masking techniques.	Effectiveness is dependent on specific conditions.
Ma et al. [11]	2020	Assess and restrict disclosure risks.	Vulnerability to correlation attacks.
Nicholson et al. [12]	2020	Provide a Bayesian framework to effectively address multiplicative noise.	Required high computational complexity for large problems.
Khwaja et al. [13]	2022	Improve the efficacy and privacy of data masking in smart meters.	Applicability to real-world scenarios is uncertain.

In [11], Ma et al. defined a correlation attack estimate, wherein data intruders leverage correlations between noise multiplied and original data to re-identify critical features. The article compares the correlation attack estimate with conventional noise multiplied values and provides a metric for disclosure risk. This measure assists data providers in selecting factors for noise production, therefore enhancing the efficacy of data masking. Khwaja et al. [13] assessed lightweight techniques for confused smart meter data, contrasting additive and multiplicative algorithms across Gaussian, Rayleigh, generalized Gaussian, and chi-square distributions. Additionally, in [10], Brackenbury et al. investigated privacy vulnerabilities in smart meter electricity data by comparing two data masking techniques: the established DREAM method, which employs additive noise and encryption, and the suggested Twin Uniform multiplicative noise method, which provides a more straightforward implementation. A comparative examination with empirical data demonstrates that both strategies reach similar levels of privacy and accuracy.

Klein et al. [8] examined the application of noise multiplication as a disclosure control technique for sensitive upper tail data, including income. In contrast to top coding, noise multiplication preserves greater information and enables adjustable accuracy and protection through the modulation of the noise distribution. Kumar et al. [9] examined privacy preserving data via multiplicative perturbation, highlighting the equilibrium between utility and privacy. This

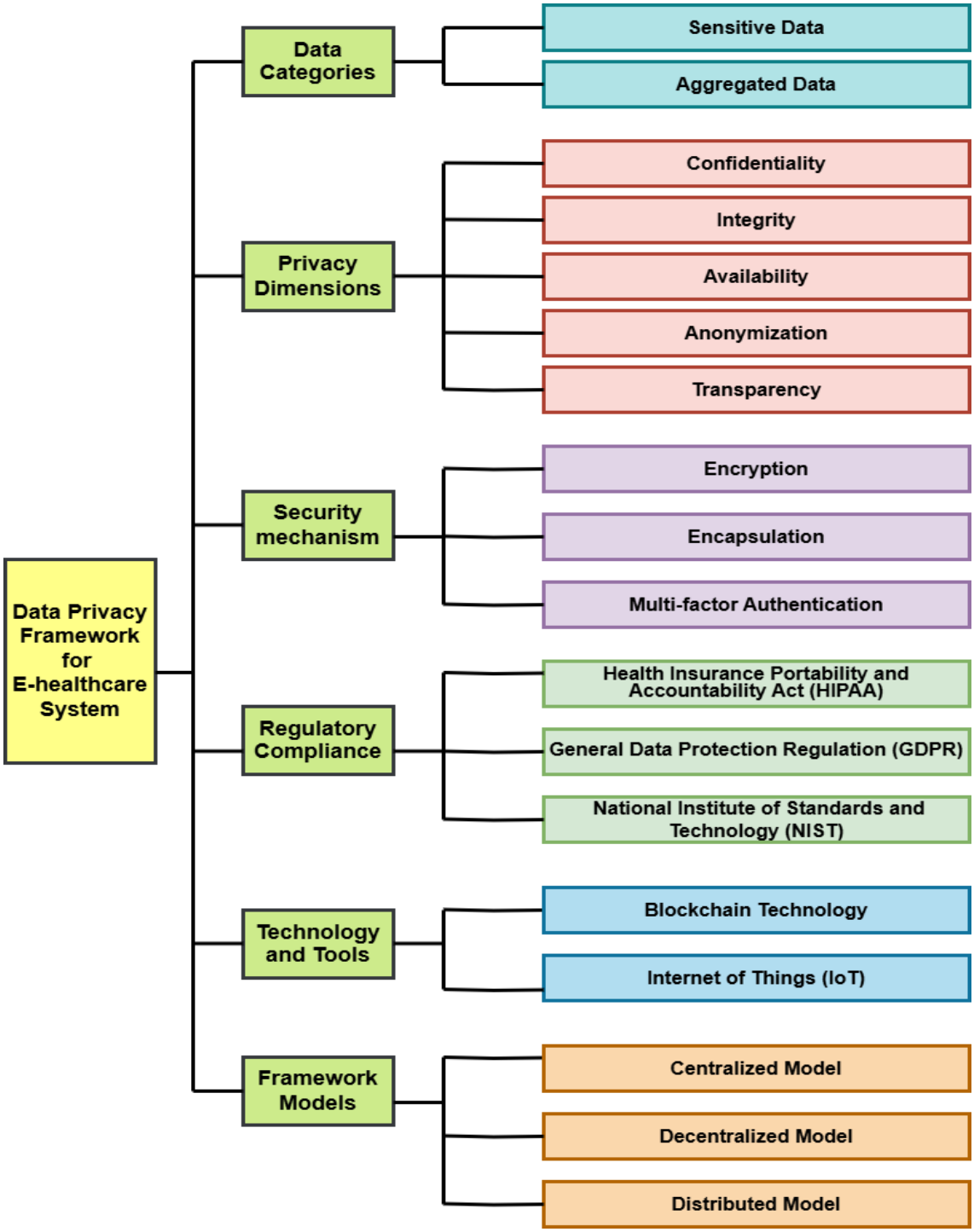

Fig. 1. Taxonomy of data privacy framework.

method aims to obscure private information while maintaining essential patterns and trends for data mining, addressing the difficulty of optimizing transformations for utility and privacy. Finally, Nicholson et al. [12] focused on mitigating the challenges posed by multiplicative noise, including positivity constraints and substantial computational expenses in complex inverse problems. This method effectively exclude noise effects by incorporating multiplicative noise statistics into an additive error term inside a Bayesian framework. The deciphering problem illustrates the incorporation of correlated noise and the provision of precise error estimates.

2.3 k-anonymity based privacy

The existing privacy frameworks for traditional EHS utilizing k-anonymity is reviewed attentively and presented in the Table 3.

Table 3. k-anonymity.

Author	Year	Objective	Limitation
Basu et al. [14]	2015	Measure the risk of re-identification.	Attribute knowledge raises re-identification risk.
Rahimi et al. [15]	2015	Improve privacy of micro-data.	Complexity of datasets.
Wei et al. [16]	2018	Improve privacy in collaborative filtering by increasing (p, l, α)-diversity.	High computational complexity.
El et al. [17]	2018	Develop a k-anonymity algorithm for quasi-identifiers.	Large datasets may struggle with scalability.
Mahanan et al. [18]	2021	Increase privacy efficiency with data and heuristic algorithms.	Restricted to the same generalization hierarchy.
Saxena et al. [19]	2022	Create a framework to ensure the robust anonymization of data.	Achieving semantic analysis accuracy is computationally intensive for huge datasets.
Karagiannis et al. [20]	2024	Promote privacy awareness.	limited applicability to complex datasets.

Mahanan et al. presented a heuristic approach for data privacy preservation utilizing identical generalization hierarchy data, wherein all quasi-identifiers possess the same data type [18]. The approach significantly improves performance by disregarding privacy constraints and minimizing node visits, resulting in up to a 21% enhancement compared to current privacy preservation techniques. Likewise, Basu et al. [14] investigated k-anonymity as a privacy preserving method for sensitive datasets utilized in data mining. K-anonymity mitigates re-identification risks by clustering records with similar quasi-identifiers; however, the work highlights its NP-hard optimization difficulties and assesses re-identification risks contingent on the knowledge of the attacker. Furthermore, it underscores weaknesses when attackers use non-quasi-identifier properties.

Building upon the discourse on privacy methodologies, [15] evaluated the compromises between data utility and privacy for statistical entities. The research highlights considerable shortcomings in current techniques such as p-sensitive k-anonymity, noting substantial distortion and inadequate safeguards against attribute disclosure. The authors suggest a technique to improve microdata preservation while reducing data distortion. Consistent with these improvements, Karagiannis et al. [20] presented a k-anonymity method tailored for educational applications. This method, supported by seven validation tests, facilitates five learning scenarios, enhancing practical understanding of privacy preservation ideas for a wider audience.

Simultaneously, El et al. [17] addressed a prevalent problem in current k-anonymity techniques by introducing an algorithm for quasi-identifier features that removes the necessity for a predetermined threshold. This technique, strictly outlined and empirically assessed, provides a versatile method for protecting privacy in large data environments. Saxena et al. [19] improved k anonymity by incorporating semantic k-anonymity with machine learning and natural language processing to conflict with sophisticated threats of deanonymization. The approach preserves data utility while accommodating diverse criteria, establishing a basis for future research in the growing difficulties of data protection.

In [16], Wei et al. introduced a diversity approach (p, l, α) to enhance privacy protection in collaborative filtering for recommended systems. The strategy enhances k-anonymity by integrating user variety and employing a Latent Factor Model to mitigate matrix sparsity. Moreover, an enhanced micro aggregation method guarantees superior data quality, while t-closeness improves privacy. The experimental findings confirm the efficacy of this method, illustrating its ability to reconcile utility and privacy in modern recommendation systems.

2.4 l-diversity based privacy

An in-depth literature review of the existing privacy frameworks for traditional EHS utilizing l-diversity is presented in the Table 4.

Table 4. l-diversity.

Author	Year	Objective	Limitation
Rajendran et al. [21]	2017	k-anonymity, l-diversity, and t-closeness in healthcare data.	Compromising data utility.
Temuujin et al. [22]	2019	l-diversity algorithm in dynamically evolving datasets.	Limited capacity for highly complicated datasets.
Mohamed et al. [23]	2020	A distributed model for k-anonymity and l-diversity in data streams.	Increased information loss, computational overhead.
Parameshwarappa et al. [24]	2021	Multi-level clustering approach for anonymizing IoT activity data.	Not suitable for complex structures.
Gehrke et al. [25]	2022	Restrict the disclosure of sensitive information.	Vulnerable to attacks.

In [24], Parameshwarappa et al. presented innovative multi-level clustering techniques for anonymizing activity data with a non-metric weighted distance metric that upholds the l-diversity model. These methods mitigate the shortcomings of traditional anonymization strategies, enhancing efficiency and usefulness preservation, especially for simple activity datasets characterized by high dimensionality and limited rows. In [25], Gehrke et al. introduced l-diversity as a data privacy method to mitigate sensitive information disclosure by guaranteeing that each equivalence class comprises a minimum of l different values for sensitive attributes. This technique efficiently mitigates re-identification risks and restricts sensitive information exposure; yet, it may remain vulnerable to attacks utilizing background knowledge.

Expanding on this, Rajendran et al. [21] investigated privacy preserving data publishing in the healthcare sector, highlighting the significance of anonymization approaches for protecting sensitive information in electronic health records. The paper examines three significant methods: l-diversity, k-anonymity, and t-closeness emphasizing their individual advantages and drawbacks in safeguarding medical data privacy. To address the dynamic character of datasets, Temuujin et al. [22] proposed an efficiency l-diversity method for safeguarding privacy in evolving datasets. This method utilizes anatomical principles for privacy preservation and incorporates Cuckoo filters, effectively tackling the issues of updates and

deletions, hence providing expedited execution times while upholding strong privacy protections.
Mohamed et al. [23] proposed a distributed privacy preserving model for streaming data that improves l-diversity and k-anonymity, hence forwarding the applicability of privacy models. This approach anonymizes data locally at spread sites, in contrast to centralized models, which subsequently combine their results to create a global clustering model. This decentralized approach minimizes information loss and communication expenses while safeguarding privacy, rendering it appropriate for challenging, real-time applications.

2.5 t-closeness based privacy

The existing privacy frameworks for traditional EHS utilizing t-closeness are discussed in detail in Table 5.

Table 5. t-closeness

Author	Year	Objective	Limitation
Sei et al. [26]	2017	Techniques for sensitive quasi-identifiers.	Restricts flexibility.
Rajendran et al. [21]	2017	l-diversity, k-anonymity, and t-closeness for protecting patients' electronic health record privacy.	Anonymization include data bias, computational complexity, and vulnerability.
Wang et al. [27]	2018	Improve privacy by developing t-closeness algorithms.	Complex datasets.
Li et al. [28]	2021	Preserve privacy for numerous sensitive attributes.	Complexity and information loss.
Gowda et al. [29]	2023	Anonymize data while maintaining t-closeness privacy concerns.	Difficult handling of attributes.

Gowda et al. [29] introduced three distinct methods for anonymizing relational datasets, employing the t-closeness technique to ensure the preservation of individual privacy. The initial approach guarantees nearly optimal equivalence classes to enhance privacy, while the second method focuses on anonymizing data that contains various sensitive attributes, permitting distinct privacy parameters. The third method enhances the management of privacy concerning multiple sensitive attributes. In the same way, Sei et al. [26] tackled the issue of privacy preserving data mining by presenting sensitive quasi-identifiers, which integrate characteristics of both sensitive attributes and quasi-identifiers. The authors introduce two innovative privacy models, (l_1, ..., l_q) diversity and (t_1, ..., t_q) closeness, along with algorithms for anonymization and reconstruction that strike a balance between simplicity and effectiveness, assessed through real world datasets. Rajendran et al. [21] analyzed anonymization techniques aimed at preserving privacy in electronic health records. Their focus includes k-anonymity, l-diversity, and t-closeness, emphasizing the advantages these methods offer for maintaining data utility. They also address the limitations associated with these techniques, such as susceptibility to attacks, challenges in managing skewed data, and the computational complexities that arise when dealing with large datasets. Wang et al. [27] introduced two algorithms aimed at enhancing t-closeness for the management of multiple sensitive attributes. This approach effectively addresses a prevalent gap in privacy models by employing clustering and principal component analysis to partition records systematically. The evaluations indicate that one algorithm provides enhanced privacy protection while minimizing information loss, even though it operates at a slower speed. Lastly, Li et al. [28] connected t-closeness as a privacy concept that builds upon l-diversity. This concept ensures that the distribution of sensitive attributes within each equivalence class closely resembles their overall distribution in the dataset. This approach effectively safeguards against privacy breaches while preserving statistical properties throughout the anonymization process.

2.6 Personalized privacy

The existing privacy frameworks for traditional EHS utilizing personalized privacy is explored in-depth and represented in the Table 6.

Table 6. Personalized privacy.

Author	Year	Objective	Limitation
Aguirre et al. [30]	2016	Examine the effects of personalized communications on people involvement and concerns regarding privacy.	Focuses only on a few sources; may not apply to other situations.
Karwatzki et al. [31]	2017	Examine how privacy, transparency, and personalization influence people's desire to contribute information.	Only works for certain types of services; may not show how people really act.
Meng et al. [32]	2018	Social recommendation framework using personalized privacy configurations.	Not very scalable.
Sun et al. [33]	2021	Federated learning system with rewards to mitigate the costs of privacy leaks.	Depends on accurate inputs.
Chang et al. [34]	2023	Personalized privacy assistant to easily manage IoT identity information.	Limited to specific properties.

Through the provision of a safe environment for users to demonstrate rankings and social interactions, while simultaneously assigning individualized noise to sensitive and non-sensitive rankings, Meng et al. proposed PrivSR [32] a framework for privacy preserving social recommendations that addresses privacy leakage in untrusted system environment. Furthermore, both theoretical and experimental analyses confirm its efficiency in reducing privacy issues while preserving system performance. Likewise, Aguirre et al. investigated elements impacting customer responses to tailored messages by means of digital media channels including display, search, social, and mobile [30]. Especially, their results show the balance between privacy issues and personalization, demonstrating that although personalizing increases participation, it also generates privacy problems across a variety of media. It consequently provide understanding for handling the personalizing privacy problem. In addition, Karwatzki et al. examined the interplay of privacy valuation, transparency features, and service personalization in data intensive digital services [31]. Interestingly, authors discovered that while personalizing appealed mostly to privacy sensitive users, transparency features did not encourage disclosure and privacy valuation discouraged information sharing. They thus propose the requirement of privacy oriented service architectures. Moreover, Sun et al. presented Pain-FL [33], a contract based incentive system for federated learning that guarantees model performance while paying workers for any privacy leaks. Analytical and experimental studies showing Pain-FL's economic viability and model convergence reveal that by adjusting privacy levels and payments

Pain-FL efficiently addresses privacy issues. Chang et al. ultimately created a customized privacy assistant that assists people in handling identification data gathered by IoT devices [34]. The assistant provides a strong answer for IoT related privacy concerns by using empirical studies and statistical models to evaluate privacy risks. Therefore, enabling users to control their data and agree with privacy protection standards.

3. CLOUD BASED EHS

Cloud based EHS refers to the use of cloud computing technologies to store, manage, and process healthcare data and applications over the internet. It is divided into several privacy preserving techniques like association rule hiding privacy, downgrading classifier effectiveness privacy, query auditing and inference control privacy, 1 out of 2 oblivious transfer privacy, secure sum based privacy, secure set union based privacy, secure size of intersection based privacy, scalar product based privacy, set intersection based privacy, homomorphic encryption privacy, and attribute based searchable encryption privacy.

3.1 Association rule hiding privacy

The existing privacy framework for cloud based EHS using association rule hiding is discussed in Table 7.

Table 7. Association rule hiding privacy.

Author	Year	Objective	Limitation
Modak et al. [35]	2016	Hiding sensitive information in distributed systems.	Hiding sensitive rules may reduce data utility.
Afzali et al. [36]	2018	Association rule hiding techniques for streaming and large scale data.	Dynamic data, scalability, and efficiency in large datasets.
Zhang et al. [37]	2019	Classify privacy preserving association rule mining techniques, metrics, and future problems.	Lacks real world application and changing threat analysis.
Silva et al. [38]	2019	Review techniques for protecting sensitive data during data mining.	Focuses on outdated inquiries, not real world applications .
Kumar et al. [39]	2023	Fuzzy logic technique for large datasets.	Problems with processing dynamic data.

Zhang et al. [37] examined privacy preserving association rule mining in the context of privacy preserving data mining. The authors provide a taxonomy of algorithms for privacy preserving association rule mining, survey relevant techniques, and assess metrics for evaluating these algorithms. The study emphasizes current methodologies, outlines limitations, and proposes future research possibilities to tackle emerging privacy challenges. Silva et al. [38] performed a bibliometric review of privacy preserving data mining, highlighting techniques for concealing sensitive information in association rule mining. The authors point out the necessity of balancing data driven retrieval with individual privacy protection, pointing out the importance of developing techniques that ensure the security of sensitive information while preserving data utility for decision making. Afzali et al. [36] examined the optimization of association rule hiding techniques for big data, specifically in the context of streaming data, by implementing data anonymization and parallelization techniques to improve scalability and processing speed. Their approach considers the rapid growth of big data and integrates participation certificates to safeguard sensitive association rules efficiently. Kumar et al. [39] examined the issue of protecting sensitive data in association rule mining through the application of fuzzy logic and innovative methodologies. The study examines techniques such as heuristic sensitive association rule hiding and genetic based sensitive association rule hiding, which seek to reduce the effects on data integrity while maintaining scalability and parallelism for big data management. Modak et al. [35] examined secure association rule mining within distributed environments, emphasizing horizontally and vertically distributed data. The authors present an idea of hierarchy technique for hiding sensitive association rules, facilitating the computation of global rules without compromising privacy, thus maintaining confidentiality while extracting valuable data patterns.

3.2 Downgrading classifier effectiveness privacy

The existing privacy framework for cloud based EHS using downgrading classifier effectiveness is discussed in Table 8.

Table 8. Downgrading classifier effectiveness privacy.

Author	Year	Objective	Limitation
Vaghashia et al. [40]	2015	Examine existing strategies and frameworks for privacy preserving data mining.	No algorithm demonstrates universal efficiency.
Mendes et al. [41]	2017	Survey techniques for privacy preserving data mining that balance utility and privacy.	Struggles to balance privacy, scalability, utility, and complexity.
Hariraman et al. [42]	2020	Increasing collaborative data mining efficiency by protecting privacy.	Problems with establishing a balance between data privacy and data utility.
Mohan et al. [43]	2021	Association rule hiding techniques to protect sensitive data.	Affect the accuracy of non-sensitive rules and data utility.
Hirschprung et al. [44]	2023	Privacy preserving data mining reduces sensitive data leakage.	Protecting privacy while optimizing data and algorithms.

Vaghashia et al. [40] examine the function of data mining in extracting interesting patterns from large datasets, noting that it frequently involves sensitive information, therefore prompting considerable privacy concerns. They point out the significance of privacy preserving data mining, which achieves data mining goals while protecting individual privacy. Nevertheless, they observe that despite progress, privacy preserving data mining approaches remain in development, lacking a single solution that excels in all parameters, therefore providing performance and utility crucial considerations. Likewise, Mendes et al. [41] examine privacy preserving data mining techniques that facilitate knowledge extraction while safeguarding privacy. Their paper examines essential techniques, evaluation metrics, and applications across diverse domains, while also emphasizing ongoing obstacles and unresolved issues, hence demonstrating the increasing significance of privacy preserving data mining in mitigating privacy concerns during data analysis and transmission.

Expanding upon these ideas, Hariraman et al. [42] investigated privacy preserving techniques in collaborative data mining, emphasizing asynchronous streaming data mining within remote environments. Their research examines privacy issues resulting from rapid technological progress and the enhanced utilization of personal data, underscoring the necessity for robust security protocols to safeguard privacy in data analysis. Mohan et al. [43] emphasized

the essential function of privacy preserving data mining in protecting sensitive data during association rule mining. They present two innovative techniques: a genetic algorithm based hiding method and a dummy item creation approach, which effectively obscure sensitive rules while preserving overall data integrity.
Hirschprung et al. [44] investigated the privacy risks linked to data mining, saying that privacy has emerged as a critical concern in this domain. They examine several privacy preserving data mining techniques, including anonymization, randomization, cryptography, and privatization, aimed at reducing information leakage. Their research emphasizes the strategies and techniques employed in privacy preserving data mining to combine data utility with privacy, effectively tackling the developing issues in privacy protection. Collectively, these works offer a thorough examination of the progress, obstacles, and methodologies in the field of privacy preserving data mining.

3.3 Query auditing and inference control privacy

A detailed literature review of the existing privacy framework for cloud based EHS using query auditing and inference control is discussed in Table 9.

Table 9. Query auditing and inference control privacy.

Author	Year	Objective	Limitation
Turkanovic et al. [45]	2015	Enhance the confidentiality and privacy of databases by addressing inference issues.	Inference control hamper the complete protection of database privacy and confidentiality.
Pasquier et al. [46]	2018	Compliance with privacy laws requires data flow audits.	Insufficient enforcement, representation of data flow, and agreement with regulations.
Zhou et al. [47]	2023	Resolve address inference challenges in databases to improve security and privacy.	Restrict full protection of database privacy and confidentiality.
Ekaputra et al. [48]	2024	Sensitive personal data governance through privacy preserving techniques.	Insufficient integrated architecture for privacy preserving data analysis.
Landis et al. [49]	2024	Improve privacy framework to mitigate inference driven risks to privacy.	Failure to address inference driven risks harms handling of personal information.

Turkanovic et al. [45] investigated inference issues in a variety of database structures, with a special focus on the privacy risks that result from indirect access to sensitive information. They claim that access control mechanisms alone are insufficient to prevent such threats, and they analyze inference control techniques while examining the obstacles presented by emerging technologies such as XML and semantic dimensions. Similarly, Pasquier et al. [46] focused on the importance of auditing data flows to ensure that systems handling personal data comply with regulatory and user requirements. They point out the importance of auditing sensitive data handling components to identify gaps in policy enforcement and to ensure that privacy policies are in compliance with data protection regulations. They point out the importance of auditing sensitive data handling components to identify gaps in policy enforcement and to ensure that privacy policies are in compliance with data protection regulations.
Building on this foundation, Zhou et al. [47] proposed a scheme that ensures both security and auditability by utilizing an indistinguishable privacy preserving model and applying an enhanced invertible bloom filter for efficient data retrieval. This scheme depends upon this foundation. Ekaputra et al. [48] introduced the WellFort approach, a semantic enabled architecture that is specifically designed for privacy preserving auditable data analysis, thereby further advancing the field. This method not only guarantees secure data storage but also integrates user consent management, as proved by a medical domain prototype that functions effectively.
Lastly, Landis et al. [49] addressed organization based privacy management, identifying significant gaps in addressing inference risks, which are the potential for sensitive information to be derived from apparently non-sensitive data. They evaluate prior incidents, identify deficiencies in existing frameworks, and suggest improved controls to increase awareness, reduce inference risks, and more effectively align technical implementations with privacy policies. Collectively, these studies offer a comprehensive perspective on the constantly changing obstacles and innovative solutions that are necessary to guarantee privacy and security in the processing and analysis of data.

Table 10. 1 out of 2 oblivious transfer privacy.

Author	Year	Objective	Limitation
Asharov et al. [50]	2017	Improve cryptography's scalability, communication, and processing.	High communication and computing cost.
Jannati et al. [51]	2017	Privacy on location based services.	Not adequately protected by the current protocol.
Wang et al. [52]	2020	User privacy in Vehicular Ad Hoc Networks.	Limited use in big Vehicular Ad Hoc Networks.
Yang et al. [53]	2021	Secure encryption and malicious user identification to ensure the privacy of data transmission.	Integration of blockchain technology and encryption may provide complexity and limit scalability.
Yadav et al. [54]	2022	Safety and effectiveness of different types of oblivious transfer protocols.	Expensive communication and computation.

3.4 1 out of 2 oblivious transfer privacy

The existing privacy framework for cloud based EHS using 1 out of 2 oblivious transfer is discussed in Table 10.
Asharov et al. [50] improved secure computation protocols by increasing communication, computation, and scalability in semi-honest and malicious adversarial scenarios. These studies show that oblivious transfer protocols are adaptable and essential for privacy and efficiency in various applications. Jannati et al. [51] criticised existing 1-out-of-l oblivious transfer protocol for location based services, claiming insufficient database security. They offer an enhanced protocol that preserves client location privacy and server database security with low performance penalties. Based on these ideas, Wang et al. [52] suggested oblivious transfer and private set intersection techniques for user privacy in Virtual Area Networks. Their method uses an effective k-out-of-n oblivious transmission protocol for private set intersection with equality tests, assuring privacy during feature matching, decreasing computational costs, and preventing quantum attacks.
Yang et al. [53] developed a privacy preserving data transfer technique for smart healthcare systems, combining secure ciphertext conversion, malicious user identification, and blockchain technology. Their method avoids tampering, identifies criminal users, and provides two way privacy using a mathematical equation protocol and a proxy re-encryption technique. Yadav et al. [54] described the

Table 11. Secure sum privacy.

Author	Year	Objective	Limitation
Fu et al. [55]	2014	Protecting sensitive data while maximizing query utility.	Limited large sum query protection.
Hartmannet al. [56]	2019	Privacy preserving distributed data combining without trust assumptions.	Subset sum difficulty.
Ranbaduge et al. [57]	2020	Enable privacy preserving computations across organizations.	Collusion and scalability issues.
Ding et al. [58]	2022	Distributed Kalman filtering and consensus to maintain user privacy.	Risk of privacy leaks.
Kjamilji et al. [59]	2024	Give quantum resistant IoT applications secure, private decision tree assessment.	Restrictions on available resources and procedures.

oblivious transfer protocol as a crucial cryptographic technique for safe multi party computation, private data retrieval, and privacy preserving tecniques. The oblivious transfer extension protocol minimizes communication and computing costs for large scale applications.

3.5 Secure sum based privacy

The existing privacy framework for cloud based EHS using secure sum is discussed in Table 11.
In order to facilitate data analytics that preserve privacy across businesses, Ranbaduge et al. [57] investigated secure multi party computation. To tackle issues of privacy and secrecy, this study presents advanced secure summing techniques that utilize homomorphic encryption. On top of that, they show that secure summation procedures are more efficient and provide better privacy than current methods while also investigating the hazards of collusion. Expanding on related concepts, Ding et al. [58] suggested a privacy protecting method for distributed Kalman filtering in multi agent systems, with an emphasis on protecting sensitive data while exchanging state information. The technique evaluates privacy threats, especially in collusive settings, and proposes effective defense strategies by including secure multihop communication and secure summing to prevent data leaking.
The work of Hartmann et al. [56] made a contribution to this area by removing the need for trustworthy servers or peer to peer connections in distributed, privacy preserving data summing. This can be applied to applications like demographic research and machine learning. They secure data protection through computational privacy via zero sum noise and shuffling, which they achieve by utilizing the multidimensional subset sum problem. At the same time, the SPLU model, which counters particular inference attacks selectively, is used by Fu et al. [55] to address privacy concerns related to sharing information. Empirical results confirm the effectiveness of the recommended sanitization algorithm, which finds a middle ground between privacy and usefulness by safeguarding sensitive information in small sum queries while preserving accuracy for large sum queries.
Moreover, Kjamilji et al. [59] centered their attention on evaluating client server classification using secure, private decision trees while meeting strict security and efficiency goals. They guarantee privacy even while dealing with malicious clients by implementing protocols that protect data during decision tree evaluations using quantum resistant cryptographic primitives.

Table 12. Secure set union privacy.

Author	Year	Objective	Limitation
Fenske et al. [60]	2017	Securely and effectively combine unique item counts in distributed systems.	Computational cost and limited scalability in large distributed networks.
Zhang et al. [61]	2023	Provide Private Set Union procedures with optimal performance and linear complexity.	Encryption techniques are used in protocols, which affects their ability to grow and work well.
Wang et al. [62]	2023	Federated submodel learning to protect user privacy.	Problems with managing multiple databases & creation of random numbers.
Lin et al.[63]	2024	Secure data aggregation protects privacy across several entities' datasets.	Persistent issues with scalability, complexity, and high computational cost.
Dumas et al. [64]	2024	Two party protocols for unbalanced private set union.	Increase receiver computational cost.

3.6 Secure set union based privacy

The existing privacy framework for cloud based EHS using secure set union is discussed in Table 12.
Fenske et al. [60] presented a cryptographic protocol for securing unique item counts across several data parties without disclosing sensitive information. Their technique protects distributed networks like Tor from attacks and provides differential privacy. It is efficient, scalable, and ideal for privacy preserving statistics. Based on privacy preserving protocols, Zhang et al. [61] offered a private set union framework using oblivious transfer and a new multi query reverse private membership test. They achieve linear computation and communication complexity, exceeding previous approaches in efficiency and real world application.
Wang et al. [62] introduced a federated submodel learning approach, allowing clients to update a central model secretly utilizing private set union and multi message symmetric information retrieval. This framework protects clients' local data and updates from the server, enabling safe and private collaborative learning.
Lin et al. [63] used Computational Diffie-Hellman problems to secure dataset aggregation from multiple parties. For privacy preserving data sharing, their private set union protocol uses encryption and randomization. It shows efficiency, security, and performance in finance, IoT, and digital libraries.
Finally, Dumas et al. [64] introduced unbalanced private set union protocols, optimizing sender computational cost and communication throughput based on set size. Their approaches balance receiver computational complexity and efficiency with homomorphic encryption. Experimental results show that their privacy preserving set operation method is cost effective and feasible. These research improve safe data aggregation and private set operations by providing scalable, efficient, and privacy-centric solutions for various applications.

3.7 Secure size of intersection based privacy

The existing privacy framework for cloud based EHS using secure size of intersection is discussed in Table 13.
Yang et al. enhanced ciphertext policy attribute based encryption by achieving full policy hiding through private set intersection approaches [65]. Both attribute names and values are hidden, allowing large domains. The research utilizes a polynomial based private set intersection and a recursive algorithm to determine authorization and mapping relationships, therefore substantially decreasing

Table 13. Secure size of intersection privacy.

Author	Year	Objective	Limitation
Yang et al. [65]	2022	Implement a ciphertext policy attribute based encryption scheme.	Computationally complicated.
Zhou et al. [66]	2022	Create location based, distributed, and secure Internet of Vehicles services.	Complex cryptography puts centralized systems at danger of failure.
Niu et al. [67]	2022	Secure multi party Computation computes private set intersections securely for privacy preserving statistics.	Expensive processing, restricted scalability, and difficulties with communication overhead.
Mohanty et al. [68]	2023	Create a ride sharing protocol that is both quantum secure and privacy preserving.	Quantum cryptography implementation complexity.
Cai et al. [69]	2024	Private set intersection mechanism for privacy preserving authorization in IoT devices.	Complex implementations.

user computation. Experimental findings indicate enhanced performance while adequately protecting critical data characteristics. In [66], Zhou et al. tackled privacy and security issues in location based services for the Internet of Vehicles by presenting a distributed privacy protection framework that combines private set intersection and blockchain technology. The approach implements two protocols: dual authentication and service recommendation, that guarantee secure communication, reliable session keys, and robust location privacy protections against risks like man-in-the-middle attacks and non-repudiation.
Niu et al. addressed privacy issues in distributed computing by utilizing secure multi party computation to create protocols for statistical analyses on private set intersections [67]. The arithmetic shared private membership test protocols effectively compute cardinality, total, average, and variance while preserving privacy. The methodology depends on secret sharing, oblivious transfer, and precomputation techniques to fulfill its objectives. Simultaneously, Mohanty et al. [68] emphasized the security vulnerabilities faced by IoT enabled ride sharing systems as a result of quantum algorithms that may compromise conventional cryptographic techniques. This work presents a quantum cryptography based threshold private set intersection technique to provide quantum resistant and long term secure ride sharing solutions.
Ultimately, in [69], Cai et al. introduced a privacy preserving authorization method for IoT systems utilizing an improved private set intersection protocol. This method reduces communication costs while improving privacy via techniques like role based access control, reduced communication complexity, and size hiding for cloud roles. The suggested approach enhances both privacy and efficiency in IoT areas, providing an acceptable option for safe authorization.

3.8 Scalar product based privacy

The existing privacy framework for cloud based EHS using scalar product is discussed in Table 14.
Zhu et al. presented a safe, efficient even dimension scalar product technique in [70], increasing privacy in distributed computations. This approach ensures fairness and privacy in calculations by avoiding homomorphic encryption costs. Distance comparisons and k-nearest neighbors analysis are possible uses. In [71], Domingo et al. solved cloud storage privacy concerns by permitting

Table 14. Scalar product privacy.

Author	Year	Objective	Limitation
Zhu et al. [70]	2015	Propose a linearly efficient mechanism for the scalar product that ensures privacy preservation.	Sometimes partial disclosure of information compromises privacy.
Domingo et al. [71]	2018	Utilize untrusted clouds to generate secure scalar products on anonymized data.	Limitations include the possibility of cloud collusion and the lack of data encryption.
Bose et al. [72]	2019	Create privacy preserving techniques for scalar product calculations with minimum overhead.	Limited to scalar product operations; may not handle complicated data.
Rahulamathavan et al. [73]	2020	Design an efficient, privacy preserving scalar product protocol based on lattice structures, ensuring security.	A lattice based approach may suffer scalability and implementation difficulties.
Van et al. [74]	2023	Provide a multi party, scalable, privacy preserving scalar product protocol.	There are still problems with scalability and privacy in multi party systems.

sensitive data scalar and matrix product computations without encryption. It examines using untrusted clouds for privacy protected data while keeping statistical features. It assumes honest but curious clouds, compares performance to local computations, and analyzes cloud collusion security.
Bose et al. presented privacy preserving procedures for computing scalar products or their signs using random data perturbation and algebraic methods in [72]. These protocols are suitable for privacy preserving database queries and distributed applications because they avoid encryption and decryption overheads. Two party computation protocols with and without third parties are proposed.
In [73], Rahulamathavan et al. introduced a lattice based privacy preserving scalar product method that improves computational efficiency and security. Compared to Paillier encryption and randomization based techniques, the scheme provides better quantum security, faster performance, and lower communication overhead for 128-bit and 256-bit security levels.
Van et al. [74] advanced privacy preserving scalar product protocols for multi party machine learning, enabling secure handling of decentralized datasets beyond typical two party setups. This approach allows secure dot product calculations for decision tree analysis without revealing data. Scalability and privacy guarantees are addressed, with comparisons showing advantages over existing methods.

3.9 Set intersection based privacy

The existing privacy framework for cloud based EHS using set intersection is discussed in Table 15.
Miyaji et al. [75] proposed privacy preserving authorization in IoT systems using private set intersection protocols, optimizing communication costs, enhancing privacy, and hiding cloud platform role set size. The system delivers efficient, scalable, and secure role based access control for IoT applications. Ruan et al. [76] updated the private set intersection protocol to enhance efficiency and secure storage of user datasets. They achieve great performance and data security in cloud environments by predicting sets with bit vectors and using additive homomorphic public key cryptosystems like Paillier and ElGamal. Shi et al. [77] progressed the field

Table 15. Set intersection privacy.

Author	Year	Objective	Limitation
Miyaji et al. [75]	2017	Develop a private set intersection protocol that protects user privacy while improving authentication for IoT devices.	Limited by the cloud platform's role set size and system scalability issues.
Ruan et al. [76]	2019	Cloud computing private set intersection protocols should be efficient and secure.	Users' datasets are not stored securely and efficiently in private set intersection.
Shi et al. [77]	2022	Propose a quantum protocol for private set intersection cardinality that guarantees privacy while maintaining linear communication.	Intersection of a quantum private set cardinality needs quantum technology, which makes it harder to scale and use.
Morales et al. [78]	2023	Look at private set intersection solutions for apps and put them into groups.	Current private set intersection protocols require important cryptographic assumptions and unreliable scenarios.
Wang et al. [79]	2024	For reliable set updates, use the forward private updatable private set intersection.	Only works in two party scenarios; bigger datasets make it more complicated.

Table 16. Homomorphic encryption privacy.

Author	Year	Objective	Limitation
Aono et al. [80]	2017	Design deep learning that is safe and protects privacy without sacrificing accuracy of data.	Encryption overhead and scalability difficulties affect system efficiency and deployment.
Lu et al. [81]	2018	Improve secure and efficient distributed optimization through homomorphic encryption and computation.	Limited function classes and high processing overhead limit its practical usefulness.
Pulido et al. [82]	2021	Analyze fully homomorphic encryption for issues in privacy preserving neural networks.	Practical homomorphic encryption suffers from high computational complexity and limited scalability.
Lee et al. [83]	2022	Enhance privacy preserving machine learning with fully homomorphic encryption for deep models that are both accurate and efficient.	Real world implementation is hampered by high processing costs and long inference times.
Yang et al. [84]	2023	Examine how to integrate homomorphic encryption with upcoming technologies for biometric security.	In biometrics, homomorphic encryption has difficulties with integration, scalability, and efficiency.

by creating a quantum private set intersection cardinality protocol using oblivious key distribution, safe summation, and counting algorithms. This protocol, with O(n) communication complexity, delivers near perfect security and addresses the privacy preserving condition query problem, as verified by IBM Qiskit simulations. In [78], Morales et al. discussed secure multi party computation protocols for private set intersection, focusing on methods for computing private input set intersections while ensuring confidentiality. Their research explores private set intersection techniques, performance trade offs, and implementation issues. Finally, Wang et al. [79] presented forward private updatable private set intersection, a protocol for dynamic environments that allows secure insertion and deletion of elements while maintaining privacy against semi-honest adversaries. Their keyword based private information retrieval methodology reduces computational and transmission overhead, ensuring efficiency and security.

3.10 Homomorphic encryption privacy

The existing privacy framework for cloud based EHS using homomorphic encryption is discussed in Table 16.

Aono et al. [80] developed a privacy preserving deep learning approach that allows participants to train neural networks without sharing their local data with a central server. This method combines asynchronous unsystematic slope descent and additively homomorphic encryption to successfully avoid data leakage while maintaining model accuracy and security with a manageable computational burden for real world applications. Similarly, Lu et al. [81] investigated the secure execution of distributed projected gradient based algorithms, ensuring participants' data privacy via homomorphic encryption. Their research established safe multiparty computation with perfect correctness, identified computable functions to ensure security, and validated the algorithms' correctness and efficiency through power system case studies on demand response and optimal power flow problems. Pulido et al. [82] investigated the use of fully homomorphic encryption for privacy preserving neural networks, examining its core concepts, applications, and problems. While pointing out fully homomorphic encryption's potential for secure encrypted data processing, the study also acknowledged its computational complexity and scalability constraints, as well as a lack of detailed evaluations in neural networks.

Lee et al. [83] used fully homomorphic encryption and bootstrapping to implement the ResNet-20 model for privacy preserving machine learning, building on prior achievements. However, large computing costs with an extended inference time restrict practical implementation. Yang et al. [84] integrated homomorphic encryption with biometric security to solve privacy and data manipulation concerns in applications including criminal justice, healthcare, and finance. Their review focused on modern homomorphic encryption approaches for securing various biometric attributes, as well as the possibility for combining homomorphic encryption with upcoming technologies like as machine learning and blockchain to improve security and functionality.

3.11 Attribute based searchable encryption privacy

The existing privacy framework for cloud based EHS using attribute based searchable encryption is discussed in Table 17.

Yin et al. [85] suggested a searchable attribute based encryption method that uses ciphertext policy attribute based encryption to make sure that only authorized users can do fine grained searches. Unlike earlier plans, it limits data users' search options based on their characteristics, which makes it safer, faster, and easier to control who can see what. Extensive tests showed that it was better than other similar methods. Following this, Han et al. [86] created a better solution that includes smart contracts within a private Ethereum network. This makes the solution more useful and faster while also allowing fine grained access control and flexible searchable encryption. Attribute based Searchable Encryption with fine grained access control was used by Zhang et al. [87] to made cloud data sharing even safer. Traditional methods show access policies in plaintext and depend upon cloud services that are easily hacked. Their blockchain based Attribute based Searchable Encryption hides access policies, prevents tampering, includes Inter Planetary File Sys-

Table 17. Attribute based searchable encryption privacy.

Author	Year	Objective	Limitation
Yin et al. [85]	2019	Enable fine grained search authorization using an attribute based searchable encryption approach.	Existing methods ignore data user search permissions.
Han et al. [86]	2022	Improve blockchain enabled searchable encryption efficiency, security, and flexibility with access control.	Actual blockchain enabled searchable encryption is inefficient and expensive.
Zhang et al. [87]	2023	Blockchain based attribute based searchable encryption makes data sharing secure, private, and efficient.	Policies written in plain text, relying on the cloud, and findings that can't be trusted all lead to a single failure.
Khan et al. [88]	2024	Use attribute based keyword searching to make cloud data search safer and more efficient, and avoid costly operations.	Using attribute based keyword search is difficult due to classical encryption and computing costs.
Yan et al. [89]	2024	Improve attribute based searchable encryption security, efficiency, and flexibility.	The efficiency and scalability of attribute based searchable encryption are poor.
Liu et al. [90]	2025	Efficient, secure, and verifiable data sharing for cloud based EHS.	Security vulnerabilities, unverifiable retrieval, integrity issues, and computational overhead.

tem for distributed storage, and makes things safer and more efficient. Yan et al. [89] looked at how Attribute based Searchable Encryption has changed over time and showed how it can fix problems with the way protected data search works for large data sets. Data sharing and cloud software can use Attribute based Searchable Encryption because it improves privacy, security, and flexibility. The study also looked at trends, current plans, and problems that might come up in the future in this area. Khan et al. [88] also come up with an improved Attribute based Keyword Search method that combines attribute based encryption with searchable encryption to make cloud computing safer and more private. Their approach eliminates costly bilinear pairing and Lagrange interpolation, improving efficiency while supporting dynamic access control policy updates without requiring re-encryption. Strong cryptographic security promises make sure that sharing data is safe, flexible, and cost effective.
In [90], efficient multi-keyword searchable and verifiable data sharing (EMKV-ABSE) enhances data integrity, security, and efficient searches but introduces computational overhead and complexity in implementation.

4. IOT BASED EHS

IoT based EHS integrate IoT devices into healthcare environments to enhance patient care, operational efficiency, and decision making. This section has covered a large amount of area in terms of the literature review on location based privacy, context aware privacy, differential privacy, and identity privacy.

4.1 Location based privacy

An extensive literature review of the existing privacy framework for IoT based EHS using location based privacy is discussed in Table 18.

Table 18. Location based privacy.

Author	Year	Objective	Limitation
Peng et al. [91]	2014	Come up with a fake location based system to make Location based Services more private.	Concerns about scalability, potential parameter compromise, and dependence on Function Generator.
Chen et al. [92]	2017	Improve the security, privacy, and robustness of IoT based locating systems.	Insufficient coverage, emerging risks, policy gaps, and limited real world application.
Asuquo et al. [93]	2018	Analyze, compare, and improve location privacy in vehicular mobile networks.	Restricted scalability, evolving threats, and deficiencies in location privacy solutions.
Jiang et al. [94]	2021	Investigate and evaluate privacy preserving methodologies in location based services.	Absence of qualitative and quantitative analysis of privacy preserving methodologies in Location based Services.
Kim et al. [95]	2021	Examine differential privacy strategies to improve the privacy of location in location based services.	Limited real world applicability, scalability issues, reduced utility, and complexity.

Peng et al. [91] introduced an improved privacy preserving framework for location based services that removes dependence on completely trusted entities. The scheme utilizes a function generator to distribute changes in space parameters, facilitating secure pseudo location exchanges between users and service providers, thereby ensuring precise service delivery and preserving user privacy. Experimental validation proved minimal computational and communication costs, illustrating its practicality. In addition, Chen et al. [92] examined privacy and security challenges in IoT based positioning systems, pointing out threats and solutions for both Global Navigation Satellite System and non-Global Navigation Satellite System technologies. The study identified cryptographic methods, legal structures, and policy regulations, offering significant recommendations for the development of secure and privacy preserving location based services in IoT environments.
Asuquo et al. [93] identified broader limitations, including restricted scalability, evolving security threats, and deficiencies in current privacy preserving mechanisms, especially within vehicular and mobile networks. The necessity for advanced privacy enhancing technologies, robust cryptographic techniques, and innovative frameworks to achieve scalable and secure location privacy solutions was observed. Jiang et al. [94] conducted a comprehensive review of privacy preserving techniques in location based services, categorizing existing methods, analyzing recent advancements, and identifying research opportunities. Their study provided knowledge about vulnerabilities, principles, and challenges, establishing a foundation for the design of effective safeguards.
Finally, Kim et al. [95] examined the relevance of differential privacy in location based services, focusing on the protection of sensitive location information. The study analyzed three variants of differential privacy: geo-indistinguishability, private spatial decomposition, and local differential privacy, focusing on their application

in data processing, collection, and publishing to improve location privacy protection. These studies provide a thorough overview of the progress, obstacles, and prospective routes in safeguarding privacy and security in location based services.

4.2 Context aware privacy

The existing privacy framework for IoT based EHS using context aware privacy is discussed in Table 19.

Table 19. Context aware privacy.

Author	Year	Objective	Limitation
Pallapa et al. [96]	2014	Develop privacy solutions that are context aware for dynamic and resource limited pervasive environments.	Limited adaptability and scalability in highly dynamic, complex, and resource intensive environments.
Huang et al. [97]	2017	Create generative adversarial privacy to achieve the best possible balance between utility and privacy.	Dependence on the representation of the dataset, computational complexity, and the stability of the generative adversarial network training.
Gheisari tet al. [98]	2019	Formulate a dynamic, context sensitive privacy preserving approach for IoT enabled smart cities.	Existing solutions are static, not context aware, and inefficient in data handling.
Jiang et al. [99]	2021	Study local information utility privacy tradeoff in data privacy.	Mechanism specific constraints, limited scalability, and dependence on prior knowledge.
Xu et al. [100]	2022	Propose a framework for maintaining context aware privacy in task offloading.	Data privacy and context aware processing are constraints that must be met at every level.

Pallapa et al. [96] suggested two adaptive strategies to augment privacy while reducing user system interactions, computing requirements, and storage demands. These technologies enhance privacy and user experience, especially in situations with limited resources. Huang et al. [97] proposed a unique context aware privacy framework, generative adversarial privacy, which use generative adversarial networks to derive privacy measures directly from datasets. The approach utilizes a minimax game between a privatizer and an adversary to enhance the privacy utility tradeoff without depending on dataset statistics, demonstrating its practical usefulness. Gheisari et al. [98] addressed the shortcomings of static approaches, the risks of data leakage, and the absence of context awareness in current strategies for addressing privacy concerns in IoT based smart cities. They suggested the integration of software defined networking with a dynamic privacy preserving technique to optimize data flow management, thereby improving accuracy and minimizing overhead.

Jiang et al. [99] proposed local information privacy, a context sensitive privacy concept that utilizes prior information to improve usefulness while mitigating local differential privacy. Their analysis examined the characteristics and utility privacy limitations, illustrating practical benefits via perturbation mechanisms such as randomized response, random sampling, and additive noise. Xu et al. [100] introduced C-fDRL, a context aware federated deep reinforcement learning framework designed for job offloading in artificial intelligence systems. By preserving privacy across the CloudAI, EdgeAI, and DeviceAI phases, it differentiates high context aware data for local computing from low context aware data for edge processing, thereby enhancing privacy and optimizing task scheduling efficiency. Collectively, these research illustrate significant advancements in context aware privacy techniques, addressing challenges in many situations.

4.3 Differential privacy

The existing privacy framework for IoT based EHS using differential privacy is discussed in Table 20.

Table 20. Differential privacy.

Author	Year	Objective	Limitation
Hassan et al. [101]	2019	Examining differential privacy techniques for safeguarding data in cyber physical systems.	Challenges include the evolution of cyber physical systems architecture and attacks, requiring modifications to existing techniques.
Arachchige et al. [102]	2019	Propose a local differential privacy technique for secure deep learning.	High processing power requirements and insufficient privacy protection with limited funds.
Zhu et al. [103]	2020	Improving AI performance with differential privacy for fairness and security.	Limited research on differential privacy solutions addressing AI specific problems.
Errounda et al. [104]	2021	Provide local differential privacy while allowing for the sharing of robust aggregate location statistics.	The trade offs between utility and privacy are difficult for current algorithms to balance.
Zhao et al. [105]	2022	Summarizing differential privacy methodologies for safeguarding the privacy of unstructured data.	Attacks aren't very successful, and there could be problems with utility loss.
Dong et al. [106]	2022	Proposes f-differential privacy to improve privacy composition analysis.	Limited handling of complicated, non-algorithmic privacy issues and assumptions.
Nanayakkara et al. [107]	2023	Create effective strategies for communicating differential privacy protections for users.	There is a lack of generalizability; it might not work in all situations or groups of user.
Yang et al. [108]	2023	To examine various approaches, uses, and difficulties associated with local differential privacy.	There are problems with implementation complexity, limited scalability, and trade offs between utility and privacy.

Arachchige et al. [102] created LATENT, a local differentially private algorithm made for IoT apps that need to protect privacy while using deep learning. LATENT protects data privacy before it gets to sites that can't be trusted by adding a randomization layer to convolutional neural networks. Hassan et al. [101] did a thorough review of different types of differential privacy methods for keeping data safe in cyber physical systems in areas such as medical, energy, transportation, and industries. The study talks about ways to protect privacy, how design problems are changing, and where future research should go to improve privacy in CPS. In an expanded study, Zhu et al. [103] looked into differential privacy uses in AI,

trying to find solutions to problems with privacy, security, and fairness. Their work shows how differential privacy can help make machine learning, distributed systems, deep learning, and multi agent systems more stable, truthful, and able to merge different models.
Focusing on location data, Errounda et al. [104] looked into how to release reliable location data while still protecting local difference privacy. They used a sliding window method to find the best way to spend the privacy budget across multiple timestamps. This gave them high usefulness and formal privacy proof on both real time and historical datasets. Comparative privacy methods were looked at by Zhao et al. [105] to protect private and sensitive data in unstructured data such as text, images, and audio. They looked at privacy models, techniques for hiding information, and problems with privacy guarantees, utility losses, and AI attacks.
f-differential privacy was suggested by Dong et al. [106] as an extension of traditional differential privacy that gets around problems with privacy composition and primitive analysis. This method provides guarantees that can be understood, allows algebraic reasoning, and makes privacy enhancement by sampling efficient. It can be used in data analysis and machine learning. Increasing users' understanding of differential privacy promises was the main goal of Nanayakkara et al. [107]. They came up with three ways to communicate: two based on odds and one on real differential privacy. This showed that odds based explanations help users understand and are more likely to share data.
Finally, Yang et al. [108] looked into local differential privacy as a way for users to change data without depending on third parties they trust. They talked about its progress, its use in specific fields, and its part in machine learning. They also talked about problems like scalability and trade offs between utility and privacy, and suggested directions for future study.
These studies overviews at the progress made in differential privacy as a whole, including IoT, AI, location privacy, and user-centered methods. They also find problems that still need to be fixed and chances for future growth.

4.4 Identity privacy

The existing privacy framework for IoT based EHS using identity privacy is discussed in Table 21.
In [113] Bouras et al. explored decentralized identity management in EHS using blockchain technology. It discusses the advantages of empowering patients with control over their identities and enhancing data security. The paper reviews existing decentralized identity solutions, models, and current projects, highlighting challenges for healthcare applications.
In [114] Saeed et al. reviewed privacy concerns in 5G networks, focusing on user identity and location privacy. It explores issues related to the use of international mobiles subscribers identifiers, temporary mobiles subscribers identifiers and cell radio networks temporary identifiers in authentication, paging, and location updates. The paper identifies challenges, discusses existing solutions, and offers future recommendations for improving patient file privacy in 5G networks.
In [109] Yang et al. proposed a global auditing scheme for cloud data sharing, ensuring both identity privacy and traceability for group members. It introduces a framework with a group manager generating authenticators and lists for identity traceability. The scheme utilizes blind signatures for data privacy and demonstrates security and performance through concrete implementations.
In [110] Ribaric et al. discussed the importance of privacy in the digital age, focusing on de-identification techniques used to protect personal identifiers in multimedia content. It reviews privacy protection methods, classifies personal identifiers into categories (non-biometric, biometric, and soft-biometric), and provides an overview of de-identification possibilities for several identifiers in multimedia.
In [111] Zhang et al. presented a conditional identity privacy preserving public auditing mechanism for cloud based wireless body area networks. It addresses security concerns by ensuring data integrity and conditional identity privacy for patients. By integrating Blockchain 2.0, it protects against malicious auditing behaviors, demonstrating practicality through security analysis and performance evaluation.
In [112] Bussone et al. explored how patient living with HIV perceive identity, privacy, trust, and security in peer data sharing platforms. Interviews with 26 participants revealed a sophisticated understanding of these concerns, emphasizing the need for robust privacy measures to enable safe and responsible sharing of personal health data.

Table 21. Identity privacy.

Author	Year	Objective	Limitation
Yang et al. [109]	2016	Propose a public auditing solution preserving identity privacy and traceability.	Limited scalability and potential performance overhead in real world implementations.
Ribaric et al. [110]	2016	Review privacy protection methods in multimedia, focusing on de-identification approaches.	De-identification may fail to address all privacy risks and challenges.
Zhang et al. [111]	2019	Conditional identity privacy preserving public auditing mechanism ensuring identity privacy and data integrity in wireless body area networks.	Limited scalability and potential blockchain overhead in large wireless body area networks systems.
Bussone et al. [112]	2020	Investigate privacy, trust, identity and security.	Limited exploration of privacy and security.
Bouras et al. [113]	2020	Decentralized identity management using blockchain for EHS.	Challenges in scalability and regulatory compliance for healthcare applications.
Saeed et al. [114]	2022	Privacy solutions for 5G user identity and location protection.	Specific privacy solutions for international & temporary mobiles subscribers identifiers.

5. BLOCKCHAIN BASED EHS

Blockchain based EHS leverage blockchain technology to enhance data security, transparency, and efficiency in EHS. A comprehensive literature survey is conducted on related domains, including access control, authentication, reputation, and identity anonymization as discussed in Table 4.

5.1 Privacy enhancing authentication system

The existing privacy frameworks for blockchain based EHS using privacy enhancing authentication system are discussed in Table 22.

The insurance claim blockchain system was created by Panda et al. [115]. It is a decentralized identification system for managing health insurance that uses Blockchain 2.0. This method makes it easy to share information safely and protects patient privacy. It also meets the need for reliable data sharing between different health-

Table 22. Privacy enhancing authentication system.

Author	Year	Objective	Limitation
Panda et al. [115]	2021	Develops a decentralized authentication method for safe health data transfer using blockchain technology.	Dependence on blockchain consensus methods, difficulties with integration, and limited scalability.
Xiang et al. [116]	2022	Design a blockchain protocol to provide secure sharing and accessing of patient file. .	Low terminal computer power and storage limit large scale medical data protection.
Rajasekaran et al. [117]	2022	Advocates for blockchain based authentication to ensure secure and anonymous transmission of patient data and reauthentication.	Limited by potential blockchain network vulnerabilities, latency issues, and scalability.
Torre et al. [118]	2023	Conduct a systematic survey of privacy preservation techniques for IoT, with a particular emphasis on security.	Limited attention is given to the interoperability, evolving technologies, and newly developed IoT threats.
Indhumathi et al. [119]	2023	Presents a medical data strategy that prioritizes privacy in EHS, utilizing blockchain technology.	Storage, processing, and centralized data control capabilities of IoT devices are limited.
Velmurugan et al. [120]	2024	Proposes a hyperledger fabric architecture that is facilitated by blockchain technology to ensure the security of electronic health record systems.	The scalability of EHS is restricted by the complexity of the infrastructure and the lengthy encryption/decryption processes.
Algarni et al. [121]	2024	Creating a four party authentication system to improve the security of EHS.	Not widely used, hard to apply in real life, expensive, and complicated cryptography.
Wang et al. [122]	2025	Secure and efficient blockchain-based identity authentication scheme for IoT devices.	High computational cost, storage overhead, scalability issues, latency, and energy consumption.

care organizations, meeting both performance and security standards. In the same way, Xiang et al. [116] suggested a decentralized protocol for EHS that is built on blockchain. This would help solve the problem of devices having limited storage and computing power. The protocol protects medical data privacy by using IoT technology and a byzantine fault tolerant negotiation method. This makes patient services more secure and reliable.
Rajasekaran et al. [117] looked at how a blockchain based authentication method could be used to keep healthcare data transmission secure. Their approach uses a transfer authentication protocol to minimize the time and effort needed for reauthentication and protects both patient and doctor privacy and anonymity. Performance tests showed that it was faster and needed less computing power and communication. Security tests proved that it was secure from attacks. To learn more about ways to protect privacy, Torre et al. [118] looked at 260 studies that came out between 2017 and 2021. Their study shows how cryptographic methods can be used to make authentication better, deal with privacy risks, and stop interference attacks. It also finds IoT privacy trends and research gaps.
It was suggested by Indhumathi et al. [119] that medical data could be sent using blockchain technology in a way that would allow for remote tracking of health data. This plan has three steps: cleaning the data, making the best keys using the Dragonfly Updated Elephant Herding Optimization model, and restoring the data. All of these steps improve security and speed. For EHS, Algarni et al. [121] created a four party authentication algorithm that uses cryptographic hash functions, concatenation, and XOR operations. The protocol addresses worries about privacy and security which is checked by BAN logic.
A study by Velmurugan et al. [120] used a blockchain enabled hyperledger fabric architecture to solve privacy and security problems in electronic health record systems. Their method is made up of three steps: authentication, secure upload, and secure transfer. Using modified key policy attribute based encryption makes the system better at both encrypting and decrypting, making it work better than other ways. An efficient blockchain-based identity authentication scheme enhances security and data integrity through blockchain integration but introduces computational overhead and scalability challenges in [122].

5.2 Privacy enhancing reputation system

The existing privacy framework for blockchain based EHS using privacy enhancing reputation system is discussed in Table 23.

Table 23. Privacy enhancing reputation system.

Author	Year	Objective	Limitation
Bag et al. [123]	2018	Keep trustworthy participants' trust scores and names safe.	Problems with scalability and high processing overhead.
Ma et al. [124]	2018	Protect sensitive information & control malicious users.	Effective management of malicious users.
Ahmad et al. [125]	2018	Mobile cloud computing trust and privacy preservation strategy.	Suspected encryption errors, and high computing costs.
Gurtler et al. [126]	2021	Tackle design conflicts and deficiencies.	Absence of integrated design ideas.
Hasan et al. [127]	2022	Blockchain based reputation systems that protect anonymity.	Lack of safeguards, and imperfect blockchain use.
Gan et al. [128]	2024	Secure and efficient medical data-sharing using blockchain with on/off-chain methods.	Storage overhead, latency issues, scalability challenges, and data synchronization complexity.
Gan et al. [129]	2025	Secure and efficient medical blockchain data sharing using asynchronous federated learning.	High computational cost, communication overhead, scalability challenges.
Wang et al. [130]	2025	Blockchain-enabled federated learning framework for accurate and secure vehicle trajectory prediction.	High computational cost, communication delays, scalability, and energy consumption.

The privacy preserving architecture for personalized reputation systems described by Bag et al. [123] allowed customers to assess companies based on trust scores obtained from a trusted participant set. The framework guarantees correctness, privacy, and security, safeguarding participant identities and trust scores. The system's linear message complexity makes it suitable for practical implementation in real world decentralized applications. Ma et al. [124] proposed two privacy preserving reputation management schemes for mobile crowd sensing, utilizing edge computing to reconcile

privacy preservation with the identification of malicious participants. The basic scheme updates reputations using variations in encrypted data, whereas the advanced scheme utilizes ranked variations to ensure enhanced productivity and security.
Ahmad et al. [125] expanded privacy preserving concepts to mobile cloud computing through the introduction of a reputation aware trust and privacy preservation scheme. This method allows mobile devices to distribute computational tasks to cloud providers, while simultaneously addressing trust management and privacy issues via advanced encryption and dynamic attribute selection for secure data management. Gurtler et al. [126] performed a thorough analysis of privacy preserving reputation systems over a 15 year period, evaluating 42 systems to tackle issues related to user privacy, standardized terminology, and design alternatives. This study organizes research, examines design possibilities, and points out underexplored areas to enhance safeguards for privacy and promote trust driven feedback mechanisms.
Hasan et al. [127] examined reputation systems that preserve privacy through blockchain technology, illustrating the principles of trustlessness, transparency, and immutability. The study examines existing frameworks, identifies their limitations, and proposes future directions, all while prioritizing user privacy and addressing concerns about punishment. Taking full advantage of blockchain's possibilities and addressing neglected security issues and attack options are important areas of research.
Medical blockchain data-sharing enhances security, transparency, and traceability but faces challenges in storage efficiency, latency, and privacy protection in [128].
Gan et al. enhances security, reliability, and strategic decision-making in the sharing of medical data, but introduces high computational complexity and potential scalability challenges in [129].
In [130] trajectory prediction accuracy and data integrity enhances but incurs high computational costs and communication overhead.

5.3 Privacy enhancing authorization system

The existing privacy framework for blockchain based EHS using privacy enhancing authorization system is discussed in Table 24.

Table 24. Privacy enhancing authorization system.

Author	Year	Objective	Limitation
Samuel et al. [131]	2015	Context aware framework for composition & enforcement of privacy policies.	Issues with policy composition accuracy, consistency, and usability.
Gholami et al. [132]	2016	Discuss cloud privacy and security issues, solutions, and innovation.	Limited scope, fluctuating threats, complicated solutions, lack consistency.
Fischer et al. [133]	2017	Summarize privacy enhancing technologies and their associated metrics.	Limited scalability, complicated integration, and increasing privacy issues.
Phillips et al. [134]	2020	Provides a privacy preserving integrated authentication and authorization system.	Possible privacy issues, dependence on biometric data, and limited scalability.
Sable et al. [135]	2023	Web3 allows for authentication solutions that prioritize user privacy and decentralized apps.	Three challenges with Web3 implementation: scalability, regulations, and complexity.
Nizam et al. [136]	2025	Secure and efficient IoT data management using Hyperledger Fabric blockchain architecture.	High resource consumption, scalability issues, latency, complexity, and integration challenges in IoT.

Samuel et al. [131] addressed privacy and security issues in multimedia big data sharing by offering a hybrid methodology for the formulation and implementation of privacy rules within access control systems. This framework incorporates a verification procedure to guarantee accuracy, security, and logical consistency while enabling users to design context-aware, conflict-free policies.
Gholami et al. [132] underlined issues in cloud security and privacy, including increasing threats, complex infrastructures, and insufficient guidelines. The author emphasizes the necessity for adaptable, scalable, and standardized security solutions to successfully mitigate these limitations.
Fischer et al. [133] examined privacy enhancing technologies, which are intended to protect personal information against innovations such as cloud services, big data, and mobile computing. It explores privacy enhancing technologies categories, privacy properties, and legal foundations, presenting criteria to assess their effectiveness in safeguarding data and preserving user rights. Phillips et al. [134] enhanced privacy preserving systems via cohesive authentication and authorization framework that combines biometric capsule based authentication with role based access control. This method utilizes deep learning techniques to provide robust, efficient, and safe access control.
Sable et al. [135] presented Web3, a framework utilizing blockchain, cryptocurrencies, and non-fungible tokens for secure and transparent applications within decentralized internet technologies. Web3 authentication solutions, such as chain authentication and authorization, address scalability and safety concerns while improving user privacy and control. These studies collectively emphasize the significance of adaptive, privacy focused solutions across several technical domains, including multimedia data sharing, cloud security, access management, and decentralized internet frameworks.
Hyperledger Fabric enhances IoT security and efficiency through smart contracts and access control, but it faces challenges related to high resource consumption, scalability, and integration complexity in [136].

6. CONCLUSION AND FUTURE WORK

This paper overviews the existing research developments of a data privacy framework for EHS by designing a taxonomy for category of EHS including traditional EHS, cloud based EHS, IoT based EHS, and blockchain based EHS. Data privacy is the principle that people should have control over how their personal information is gathered, utilized, shared, kept, and erased. It aims to ensure that enterprises manage personal data ethically and transparently. Based on the comprehensive literature discussed above, it can be affirmed that there are immense possibilities to improve the data privacy framework in relevant EHS domains in future. The future of data privacy is predicted to be shaped by breakthroughs in artificial intelligence, blockchain, quantum computing, and stricter privacy laws. As the volume of digital data increases, organizations will need to implement privacy-preserving solutions that protect personal information while allowing for secure data sharing and analytics.

Declaration

—Ethical approval: Not applicable

—Competing interests: The authors declare that they have no known competing financial interests or personal relationship that could have appeared to influence the work reported in this paper.

—Authors' contributions: The authors confirm contribution to the paper as follows: First Author: Data curation, Formal analy-

sis, Writing-original draft, Conceptualization, Writing-review & editing, Validation. Second Author: Writing-review & editing, Validation

—Funding: Not applicable

—Availability of data and materials: Not applicable

7. REFERENCES

[1] Boel Nelson and Tomas Olovsson. Security and privacy for big data: A systematic literature review. In *2016 IEEE international conference on big data (big data)*, pages 3693–3702. IEEE, 2016.

[2] Ricardo Mendes and João P Vilela. Privacy-preserving data mining: Methods, metrics, and applications. *IEEE Access*, 5:10562–10582, 2017.

[3] R Kalaivani and S Chidambaram. Additive Gaussian noise based data perturbation in multi-level trust privacy preserving data mining. *International Journal of Data Mining & Knowledge Management Process*, 4(3):21, 2014.

[4] Saad A Abdelhameed, Sherin M Moussa, and Mohamed E Khalifa. Enhanced additive noise approach for privacy-preserving tabular data publishing. In *2017 Eighth International Conference on Intelligent Computing and Information Systems (ICICIS)*, pages 284–291. IEEE, 2017.

[5] Farhad Farokhi and Henrik Sandberg. Ensuring privacy with constrained additive noise by minimizing fisher information. *Automatica*, 99:275–288, 2019.

[6] Benjamin Denham, Russel Pears, and M Asif Naeem. Enhancing random projection with independent and cumulative additive noise for privacy-preserving data stream mining. *Expert Systems with Applications*, 152:113380, 2020.

[7] Carlos Murguia, Iman Shames, Farhad Farokhi, and Dragan Nešić. Information-theoretic privacy through chaos synchronization and optimal additive noise. *Privacy in Dynamical Systems*, pages 103–129, 2020.

[8] Martin Klein, Thomas Mathew, and Bimal Sinha. Noise multiplication for statistical disclosure control of extreme values in log-normal regression samples. *Journal of Privacy and Confidentiality*, 6(1), 2014.

[9] Bhupendra Kumar Pandya, Umesh Kumar Singh, Keerti Dixit, and Kamal Bunkar. Effectiveness of multiplicative data perturbation for privacy preserving data mining. *International Journal of Advanced Research in Computer Science*, 5(6), 2014.

[10] John Brackenbury, PY O'Shaughnessy, and Yan-Xia Lin. Protecting the privacy of smart meter data: The differential privacy approach and the multiplicative noise approach. In *Working Paper 01-19, NIASRA*. University of Wollongong, 2019.

[11] Yue Ma, Yan-Xia Lin, and Rathindra Sarathy. The vulnerability of multiplicative noise protection to correlation-attacks on continuous microdata. *Sankhya B*, 82:305–327, 2020.

[12] Ruanui Nicholson and Jari P Kaipio. An additive approximation to multiplicative noise. *Journal of Mathematical Imaging and Vision*, 62(9):1227–1237, 2020.

[13] Ahmed S Khwaja, Serhat Erkucuk, Alagan Anpalagan, and Bala Venkatesh. Evaluation of noise distributions for additive and multiplicative smart meter data obfuscation. *IEEE Access*, 10:27717–27735, 2022.

[14] Anirban Basu, Toru Nakamura, Seira Hidano, and Shinsaku Kiyomoto. k-anonymity: Risks and the reality. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 983–989. IEEE, 2015.

[15] Masoud Rahimi, Mehdi Bateni, and Hosein Mohammadinejad. Extended k-anonymity model for privacy preserving on micro data. *International Journal of Computer Network and Information Security*, 7(12):42–51, 2015.

[16] Ruoxuan Wei, Hui Tian, and Hong Shen. Improving k-anonymity based privacy preservation for collaborative filtering. *Computers & Electrical Engineering*, 67:509–519, 2018.

[17] Zakariae El Ouazzani and Hanan El Bakkali. A new technique ensuring privacy in big data: k-anonymity without prior value of the threshold k. *Procedia Computer Science*, 127:52–59, 2018.

[18] Waranya Mahanan, W Art Chaovalitwongse, and Juggapong Natwichai. Data privacy preservation algorithm with k-anonymity. *World Wide Web*, 24(5):1551–1561, 2021.

[19] Ashish K Saxena. Enhancing Data Anonymization: A Semantic K-Anonymity Framework with ML and NLP Integration. *Sage Science Review of Applied Machine Learning*, 5(2):81–92, 2022.

[20] Stylianos Karagiannis, Christoforos Ntantogian, Emmanouil Magkos, Aggeliki Tsohou, and Luís Landeiro Ribeiro. Mastering data privacy: Leveraging k-anonymity for robust health data sharing. *International Journal of Information Security*, 23(3):2189–2201, 2024.

[21] Keerthana Rajendran, Manoj Jayabalan, and Muhammad Ehsan Rana. A study on k-anonymity, l-diversity, and t-closeness techniques. *IJCSNS*, 17(12):172, 2017.

[22] Odsuren Temuujin, Jinhyun Ahn, and Dong-Hyuk Im. Efficient l-diversity algorithm for preserving privacy of dynamically published datasets. *IEEE Access*, 7:122878–122888, 2019.

[23] Mona A Mohamed, Sahar Mohamed Ghanem, and Magdy H Nagi. Privacy-preserving for distributed data streams: Towards l-diversity. *Int. Arab J. Inf. Technol.*, 17(1):52–64, 2020.

[24] Pooja Parameshwarappa, Zhiyuan Chen, and Güneş Koru. Anonymization of daily activity data by using l-diversity privacy model. *ACM Transactions on Management Information Systems (TMIS)*, 12(3):1–21, 2021.

[25] Johannes Gehrke, Daniel Kifer, and Ashwin Machanavajjhala. l-diversity. In *Encyclopedia of Cryptography, Security and Privacy*, pages 1–4. Springer, 2022.

[26] Yuichi Sei, Hiroshi Okumura, Takao Takenouchi, and Akihiko Ohsuga. Anonymization of sensitive quasi-identifiers for l-diversity and t-closeness. *IEEE transactions on dependable and secure computing*, 16(4):580–593, 2017.

[27] Rong Wang, Yan Zhu, Tung-Shou Chen, and Chin-Chen Chang. Privacy-preserving algorithms for multiple sensitive attributes satisfying t-closeness. *Journal of Computer Science and Technology*, 33:1231–1242, 2018.

[28] Ninghui Li. t-closeness. In *Encyclopedia of Cryptography, Security and Privacy*, pages 1–3. Springer, 2021.

[29] Vikas Thammanna Gowda. *Methods to Achieve T-closeness for Privacy Preserving Data Publishing*. PhD thesis, Wichita State University, 2023.

[30] Elizabeth Aguirre, Anne L Roggeveen, Dhruv Grewal, and Martin Wetzels. The personalization-privacy paradox: Implications for new media. *Journal of Consumer Marketing*, 33(2):98–110, 2016.

[31] Sabrina Karwatzki, Olga Dytynko, Manuel Trenz, and Daniel Veit. Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, 34(2):369–400, 2017.

[32] Xuying Meng, Suhang Wang, Kai Shu, Jundong Li, Bo Chen, Huan Liu, and Yujun Zhang. Personalized privacy-preserving social recommendation. In *Proceedings of the AAAI Conference on Artificial Intelligence*, volume 32, 2018.

[33] Peng Sun, Haoxuan Che, Zhibo Wang, Yuwei Wang, Tao Wang, Liantao Wu, and Huajie Shao. Pain-FL: Personalized privacy-preserving incentive for federated learning. *IEEE Journal on Selected Areas in Communications*, 39(12):3805–3820, 2021.

[34] Kai-Chih Chang and Suzanne Barber. Personalized privacy assistant: Identity construction and privacy in the Internet of Things. *Entropy*, 25(5):717, 2023.

[35] Masooda Modak and Rizwana Shaikh. Privacy preserving distributed association rule hiding using concept hierarchy. *Procedia Computer Science*, 79:993–1000, 2016.

[36] Golnar Assadat Afzali and Shahriar Mohammadi. Privacy preserving big data mining: association rule hiding using fuzzy logic approach. *IET Information Security*, 12(1):15–24, 2018.

[37] Lili Zhang, Wenjie Wang, and Yuqing Zhang. Privacy preserving association rule mining: Taxonomy, techniques, and metrics. *IEEE Access*, 7:45032–45047, 2019.

[38] Jesus Silva, Jenny Cubillos, Jesus Vargas Villa, Ligia Romero, Darwin Solano, and Claudia Fernández. Preservation of confidential information privacy and association rule hiding for data mining: a bibliometric review. *Procedia Computer Science*, 151:1219–1224, 2019.

[39] M Kiran Kumar and Dr Pankaj Kawad Kar. Implementation of novel association rule hiding algorithm using fla with privacy preserving in big data mining. *Design Engineering*, pages 15852–15862, 2023.

[40] Hina Vaghashia and Amit Ganatra. A survey: Privacy preservation techniques in data mining. *International Journal of Computer Applications*, 119(4), 2015.

[41] Ricardo Mendes and João P. Vilela. Privacy-preserving data mining: Methods, metrics, and applications. *IEEE Access*, 5:10562–10582, 2017.

[42] S Hariraman and Dr S Velmurugan. An enhanced privacy preserving techniques for asynchronous streaming data mining in distributed environment. *International Journal of Engineering Research & Technology*, 8(07), 2020.

[43] S Vijayarani Mohan and Tamilarasi Angamuthu. Association rule hiding in privacy preserving data mining. In *Research Anthology on Privatizing and Securing Data*, pages 963–986. IGI Global, 2021.

[44] Ron S. Hirschprung. Privacy-preserving data mining (ppdm). In *Machine Learning for Data Science Handbook: Data Mining and Knowledge Discovery Handbook*, pages 887–911. Springer, 2023.

[45] Muhamed Turkanovic, Tatjana Welzer Druzovec, and Marko Hölbl. Inference attacks and control on database structures. *TEM Journal*, 4(1):3, 2015.

[46] Thomas Pasquier, Jatinder Singh, Julia Powles, David Eyers, Margo Seltzer, and Jean Bacon. Data provenance to audit compliance with privacy policy in the Internet of Things. *Personal and Ubiquitous Computing*, 22:333–344, 2018.

[47] Zequan Zhou, Xiling Luo, Yupeng Wang, Jian Mao, Feixiang Luo, Yi Bai, Xiaochao Wang, Gang Liu, Junjun Wang, and Feng Zeng. A practical data audit scheme with retrievability and indistinguishable privacy-preserving for vehicular cloud computing. *IEEE Transactions on Vehicular Technology*, 2023.

[48] Fajar J Ekaputra, Andreas Ekelhart, Rudolf Mayer, Tomasz Miksa, Tanja Šarčević, Sotirios Tsepelakis, and Laura Waltersdorfer. Semantic-enabled architecture for auditable privacy-preserving data analysis. *Semantic Web*, 15(3):675–708, 2024.

[49] Christopher B Landis and Joshua A Kroll. Mitigating Inference Risks with the NIST Privacy Framework. *Proceedings on Privacy Enhancing Technologies*, 2024.

[50] Gilad Asharov, Yehuda Lindell, Thomas Schneider, and Michael Zohner. More efficient oblivious transfer extensions. *Journal of Cryptology*, 30:805–858, 2017.

[51] Hoda Jannati and Behnam Bahrak. An oblivious transfer protocol based on elgamal encryption for preserving location privacy. *Wireless Personal Communications*, 97:3113–3123, 2017.

[52] Xianmin Wang, Xiaohui Kuang, Jin Li, Jing Li, Xiaofeng Chen, and Zheli Liu. Oblivious transfer for privacy-preserving in VANET's feature matching. *IEEE transactions on intelligent transportation systems*, 22(7):4359–4366, 2020.

[53] Huijie Yang, Jian Shen, Junqing Lu, Tianqi Zhou, Xueya Xia, and Sai Ji. A privacy-preserving data transmission scheme based on oblivious transfer and blockchain technology in the smart healthcare. *Security and Communication Networks*, 2021(1):5781354, 2021.

[54] Vijay Kumar Yadav, Nitish Andola, Shekhar Verma, and S Venkatesan. A survey of oblivious transfer protocol. *ACM Computing Surveys (CSUR)*, 54(10s):1–37, 2022.

[55] Ada Wai-Chee Fu, Ke Wang, Raymond Chi-Wing Wong, Jia Wang, and Minhao Jiang. Small sum privacy and large sum utility in data publishing. *Journal of biomedical informatics*, 50:20–31, 2014.

[56] Valentin Hartmann and Robert West. Secure summation via subset sums: A new primitive for privacy-preserving distributed machine learning. *arXiv preprint arXiv:1906.11993*, 2019.

[57] Thilina Ranbaduge, Dinusha Vatsalan, Peter Christen, et al. Secure multi-party summation protocols: Are they secure enough under collusion? *Trans. Data Priv.*, 13(1):25–60, 2020.

[58] Wenjie Ding, Wen Yang, Jiayu Zhou, Ling Shi, and Guanrong Chen. Privacy preserving via secure summation in distributed kalman filtering. *IEEE Transactions on Control of Network Systems*, 9(3):1481–1492, 2022.

[59] Artrim Kjamilji. Privacy-Preserving Zero-Sum-Path Evaluation of Decision Tress in Postquantum Industrial IoT. *IEEE Transactions on Industrial Informatics*, 2024.

[60] Ellis Fenske, Akshaya Mani, Aaron Johnson, and Micah Sherr. Distributed measurement with private set-union cardinality. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 2295–2312, 2017.

[61] Cong Zhang, Yu Chen, Weiran Liu, Min Zhang, and Dongdai Lin. Linear private set union from {Multi-Query} reverse private membership test. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 337–354, 2023.

[62] Zhusheng Wang and Sennur Ulukus. Private federated submodel learning via private set union. *IEEE Transactions on Information Theory*, 2023.

[63] Zihan Lin, Jingyan Wang, and Shuaiqi Xu. Advancements in private set union: Protocols, security frameworks, and applications. *Highlights in Science, Engineering and Technology*, 85:191–195, 2024.

[64] Jean-Guillaume Dumas, Alexis Galan, Bruno Grenet, Aude Maignan, and Daniel S Roche. Communication optimal unbalanced private set union. *arXiv preprint arXiv:2402.16393*, 2024.

[65] Li Yang, Cheng Li, Yuting Cheng, Shui Yu, and Jianfeng Ma. Achieving privacy-preserving sensitive attributes for large universe based on private set intersection. *Information Sciences*, 582:529–546, 2022.

[66] Quan Zhou, Zhikang Zeng, Kemeng Wang, and Menglong Chen. Privacy protection scheme for the internet of vehicles based on private set intersection. *Cryptography*, 6(4):64, 2022.

[67] Ziyu Niu, Hao Wang, Zhi Li, and Xiangfu Song. Privacy-preserving statistical computing protocols for private set intersection. *International Journal of Intelligent Systems*, 37(12):10118–10139, 2022.

[68] Tapaswini Mohanty, Vikas Srivastava, Sumit Kumar Debnath, Ashok Kumar Das, and Biplab Sikdar. Quantum secure threshold private set intersection protocol for IoT-Enabled privacy preserving ride-sharing application. *IEEE Internet of Things Journal*, 2023.

[69] Rongsheng Cai, Lanxiang Chen, and Yizhao Zhu. Using private set intersection to achieve privacy-preserving authorization for IoT systems. *Journal of Information Security and Applications*, 83:103759, 2024.

[70] Youwen Zhu and Tsuyoshi Takagi. Efficient scalar product protocol and its privacy–preserving application. *International Journal of Electronic Security and Digital Forensics*, 7(1):1–19, 2015.

[71] Josep Domingo-Ferrer, Sara Ricci, and Carles Domingo-Enrich. Outsourcing scalar products and matrix products on privacy-protected unencrypted data stored in untrusted clouds. *Information Sciences*, 436:320–342, 2018.

[72] Subrata Bose. Privacy preserving computation of scalar product and sign of scalar product. *International Journal of Internet Technology and Secured Transactions*, 9(1-2):112–135, 2019.

[73] Yogachandran Rahulamathavan, Safak Dogan, Xiyu Shi, Rongxing Lu, Muttukrishnan Rajarajan, and Ahmet Kondoz. Scalar product lattice computation for efficient privacy-preserving systems. *IEEE Internet of Things Journal*, 8(3):1417–1427, 2020.

[74] Florian Van Daalen, Lianne Ippel, Andre Dekker, and Inigo Bermejo. Privacy preserving n n-party scalar product protocol. *IEEE Transactions on Parallel and Distributed Systems*, 34(4):1060–1066, 2023.

[75] Atsuko Miyaji, Kazuhisa Nakasho, and Shohei Nishida. Privacy-preserving integration of medical data: a practical multiparty private set intersection. *Journal of Medical Systems*, 41:1–10, 2017.

[76] Ou Ruan, Zihao Wang, Jing Mi, and Mingwu Zhang. New approach to set representation and practical private set-intersection protocols. *IEEE Access*, 7:64897–64906, 2019.

[77] Run-Hua Shi and Yi-Fei Li. Quantum private set intersection cardinality protocol with application to privacy-preserving condition query. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 69(6):2399–2411, 2022.

[78] Daniel Morales, Isaac Agudo, and Javier Lopez. Private set intersection: A systematic literature review. *Computer Science Review*, 49:100567, 2023.

[79] Ruochen Wang, Jun Zhou, Zhenfu Cao, Xiaolei Dong, and Kim-Kwang Raymond Choo. Updatable private set intersection with forward privacy. *IEEE Transactions on Information Forensics and Security*, 2024.

[80] Yoshinori Aono, Takuya Hayashi, Lihua Wang, Shiho Moriai, et al. Privacy-preserving deep learning via additively homomorphic encryption. *IEEE Transactions on Information Forensics and Security*, 13(5):1333–1345, 2017.

[81] Yang Lu and Minghui Zhu. Privacy preserving distributed optimization using homomorphic encryption. *Automatica*, 96:314–325, 2018.

[82] Bernardo Pulido-Gaytan, Andrei Tchernykh, Jorge M Cortés-Mendoza, Mikhail Babenko, Gleb Radchenko, Arutyun Avetisyan, and Alexander Yu Drozdov. Privacy-preserving neural networks with homomorphic encryption: C hallenges and opportunities. *Peer-to-Peer Networking and Applications*, 14(3):1666–1691, 2021.

[83] Joon-Woo Lee, HyungChul Kang, Yongwoo Lee, Woosuk Choi, Jieun Eom, Maxim Deryabin, Eunsang Lee, Junghyun Lee, Donghoon Yoo, Young-Sik Kim, et al. Privacy-preserving machine learning with fully homomorphic encryption for deep neural network. *IEEE Access*, 10:30039–30054, 2022.

[84] Wencheng Yang, Song Wang, Hui Cui, Zhaohui Tang, and Yan Li. A review of homomorphic encryption for privacy-preserving biometrics. *Sensors*, 23(7):3566, 2023.

[85] Hui Yin, Jixin Zhang, Yinqiao Xiong, Lu Ou, Fangmin Li, Shaolin Liao, and Keqin Li. Cp-abse: A ciphertext-policy attribute-based searchable encryption scheme. *IEEE Access*, 7:5682–5694, 2019.

[86] Jiujiang Han, Ziyuan Li, Jian Liu, Huimei Wang, Ming Xian, Yuxiang Zhang, and Yu Chen. Attribute-based access control meets blockchain-enabled searchable encryption: A flexible and privacy-preserving framework for multi-user search. *Electronics*, 11(16):2536, 2022.

[87] Kai Zhang, Yan Zhang, Yanping Li, Ximeng Liu, and Laifeng Lu. A blockchain-based anonymous attribute-based searchable encryption scheme for data sharing. *IEEE Internet of Things Journal*, 2023.

[88] Shahzad Khan, Shawal Khan, Abdul Waheed, Gulzar Mehmood, Mahdi Zareei, and Faisal Alanazi. An optimized

dynamic attribute-based searchable encryption scheme. *PloS one*, 19(10):e0268803, 2024.

[89] Li Yan, Gaozhou Wang, Tian Yin, Peishun Liu, Hongxin Feng, Wenbin Zhang, Hailin Hu, and Fading Pan. Attribute-Based Searchable Encryption: A Survey. *Electronics*, 13(9):1621, 2024.

[90] Peng Liu, Qian He, Yiting Chen, and Shan Jiang. Efficient multi-keyword searchable and verifiable data sharing for cloud-edge collaboration intelligent transportation systems. *IEEE Internet of Things Journal*, 2025.

[91] Tao Peng, Qin Liu, and Guojun Wang. Enhanced location privacy preserving scheme in location-based services. *IEEE Systems Journal*, 11(1):219–230, 2014.

[92] Liang Chen, Sarang Thombre, Kimmo Järvinen, Elena Simona Lohan, Anette Alén-Savikko, Helena Leppäkoski, M Zahidul H Bhuiyan, Shakila Bu-Pasha, Giorgia Nunzia Ferrara, Salomon Honkala, et al. Robustness, security and privacy in location-based services for future IoT: A survey. *IEEE Access*, 5:8956–8977, 2017.

[93] Philip Asuquo, Haitham Cruickshank, Jeremy Morley, Chibueze P Anyigor Ogah, Ao Lei, Waleed Hathal, Shihan Bao, and Zhili Sun. Security and privacy in location-based services for vehicular and mobile communications: An overview, challenges, and countermeasures. *IEEE Internet of Things Journal*, 5(6):4778–4802, 2018.

[94] Hongbo Jiang, Jie Li, Ping Zhao, Fanzi Zeng, Zhu Xiao, and Arun Iyengar. Location privacy-preserving mechanisms in location-based services: A comprehensive survey. *ACM Computing Surveys (CSUR)*, 54(1):1–36, 2021.

[95] Jong Wook Kim, Kennedy Edemacu, Jong Seon Kim, Yon Dohn Chung, and Beakcheol Jang. A survey of differential privacy-based techniques and their applicability to location-based services. *Computers & Security*, 111:102464, 2021.

[96] Gautham Pallapa, Sajal K Das, Mario Di Francesco, and Tuomas Aura. Adaptive and context-aware privacy preservation exploiting user interactions in smart environments. *Pervasive and Mobile Computing*, 12:232–243, 2014.

[97] Chong Huang, Peter Kairouz, Xiao Chen, Lalitha Sankar, and Ram Rajagopal. Context-aware generative adversarial privacy. *Entropy*, 19(12):656, 2017.

[98] Mehdi Gheisari, Guojun Wang, Wazir Zada Khan, and Christian Fernández-Campusano. A context-aware privacy-preserving method for IoT-based smart city using software defined networking. *Computers & Security*, 87:101470, 2019.

[99] Bo Jiang, Mohamed Seif, Ravi Tandon, and Ming Li. Context-aware local information privacy. *IEEE Transactions on Information Forensics and Security*, 16:3694–3708, 2021.

[100] Yang Xu, Md Zakirul Alam Bhuiyan, Tian Wang, Xiaokang Zhou, and Amit Kumar Singh. C-fdrl: Context-aware privacy-preserving offloading through federated deep reinforcement learning in cloud-enabled IoT. *IEEE Transactions on Industrial Informatics*, 19(2):1155–1164, 2022.

[101] Muneeb Ul Hassan, Mubashir Husain Rehmani, and Jinjun Chen. Differential privacy techniques for cyber physical systems: A survey. *IEEE Communications Surveys & Tutorials*, 22(1):746–789, 2019.

[102] Pathum Chamikara Mahawaga Arachchige, Peter Bertok, Ibrahim Khalil, Dongxi Liu, Seyit Camtepe, and Mohammed Atiquzzaman. Local differential privacy for deep learning. *IEEE Internet of Things Journal*, 7(7):5827–5842, 2019.

[103] Tianqing Zhu, Dayong Ye, Wei Wang, Wanlei Zhou, and S Yu Philip. More than privacy: Applying differential privacy in key areas of artificial intelligence. *IEEE Transactions on Knowledge and Data Engineering*, 34(6):2824–2843, 2020.

[104] Fatima Zahra Errounda and Yan Liu. Collective location statistics release with local differential privacy. *Future Generation Computer Systems*, 124:174–186, 2021.

[105] Ying Zhao and Jinjun Chen. A survey on differential privacy for unstructured data content. *ACM Computing Surveys (CSUR)*, 54(10s):1–28, 2022.

[106] Jinshuo Dong, Aaron Roth, and Weijie J Su. Gaussian differential privacy. *Journal of the Royal Statistical Society: Series B (Statistical Methodology)*, 84(1):3–37, 2022.

[107] Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, Gabriel Kaptchuk, and Elissa M Redmiles. What are the chances? explaining the epsilon parameter in differential privacy. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 1613–1630, 2023.

[108] Mengmeng Yang, Taolin Guo, Tianqing Zhu, Ivan Tjuawinata, Jun Zhao, and Kwok-Yan Lam. Local differential privacy and its applications: A comprehensive survey. *Computer Standards & Interfaces*, page 103827, 2023.

[109] Guangyang Yang, Jia Yu, Wenting Shen, Qianqian Su, Zhangjie Fu, and Rong Hao. Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability. *Journal of Systems and Software*, 113:130–139, 2016.

[110] Slobodan Ribaric, Aladdin Ariyaeeinia, and Nikola Pavesic. De-identification for privacy protection in multimedia content: A survey. *Signal Processing: Image Communication*, 47:131–151, 2016.

[111] Xiaojun Zhang, Jie Zhao, Chunxiang Xu, Hongwei Li, Huaxiong Wang, and Yuan Zhang. CIPPPA: Conditional identity privacy-preserving public auditing for cloud-based WBANs against malicious auditors. *IEEE transactions on cloud Computing*, 9(4):1362–1375, 2019.

[112] Adrian Bussone, Bakita Kasadha, Simone Stumpf, Abigail C Durrant, Shema Tariq, Jo Gibbs, Karen C Lloyd, and Jon Bird. Trust, identity, privacy, and security considerations for designing a peer data sharing platform between people living with HIV. *Proceedings of the ACM on Human-Computer Interaction*, 4(CSCW2):1–27, 2020.

[113] Mohammed Amine Bouras, Qinghua Lu, Fan Zhang, Yueliang Wan, Tao Zhang, and Huansheng Ning. Distributed ledger technology for eHealth identity privacy: State of the art and future perspective. *Sensors*, 20(2):483, 2020.

[114] Mamoon M Saeed, Mohammad Kamrul Hasan, Ahmed J Obaid, Rashid A Saeed, Rania A Mokhtar, Elmustafa Sayed Ali, Md Akhtaruzzaman, Sanaz Amanlou, and AKM Zakir Hossain. A comprehensive review on the users' identity privacy for 5G networks. *IET Communications*, 16(5):384–399, 2022.

[115] Soumyashree S Panda, Debasish Jena, and Priti Das. A blockchain-based distributed authentication system for

healthcare. *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, 16(4):1–14, 2021.

[116] Xinyin Xiang, Jin Cao, and Weiguo Fan. Decentralized authentication and access control protocol for blockchain-based e-health systems. *Journal of network and computer applications*, 207:103512, 2022.

[117] Arun Sekar Rajasekaran and Maria Azees. An Anonymous Blockchain-Based Authentication Scheme for Secure Healthcare Applications. *Security and Communication Networks*, 2022(1):2793116, 2022.

[118] Damiano Torre, Anitha Chennamaneni, and Alex Rodriguez. Privacy-preservation techniques for IoT devices: a systematic mapping study. *IEEE Access*, 11:16323–16345, 2023.

[119] R Indhumathi and S Sathiya Devi. Blockchain-based medical data preservation via improved association rule hiding with optimal key generation. *International Journal of Information Technology & Decision Making*, pages 1–27, 2023.

[120] S Velmurugan, M Prakash, S Neelakandan, and Eric Ofori Martinson. An efficient secure sharing of electronic health records using IoT-based Hyperledger blockchain. *International Journal of Intelligent Systems*, 2024, 2024.

[121] Ali Delham Algarni, Fahad Algarni, Saeed Ullah Jan, and Nisreen Innab. LSP–eHS: A Lightweight and Secure Protocol for e-Healthcare System. *IEEE Access*, 2024.

[122] Wenyue Wang, Biwei Yan, Baobao Chai, Ruiyao Shen, Anming Dong, and Jiguo Yu. Ebias: Ecc-enabled blockchain-based identity authentication scheme for iot device. *High-Confidence Computing*, 5(1):100240, 2025.

[123] Samiran Bag, Muhammad Ajmal Azad, and Feng Hao. A privacy-aware decentralized and personalized reputation system. *Computers & Security*, 77:514–530, 2018.

[124] Lichuan Ma, Xuefeng Liu, Qingqi Pei, and Yong Xiang. Privacy-preserving reputation management for edge computing enhanced mobile crowdsensing. *IEEE Transactions on Services Computing*, 12(5):786–799, 2018.

[125] Waqas Ahmad, Shengling Wang, Ata Ullah, Zahid Mahmood, et al. Reputation-aware trust and privacy-preservation for mobile cloud computing. *IEEE Access*, 6:46363–46381, 2018.

[126] Stan Gurtler and Ian Goldberg. Sok: Privacy-preserving reputation systems. *Proceedings on Privacy Enhancing Technologies*, 2021.

[127] Omar Hasan, Lionel Brunie, and Elisa Bertino. Privacy-preserving reputation systems based on blockchain and other cryptographic building blocks: A survey. *ACM Computing Surveys (CSUR)*, 55(2):1–37, 2022.

[128] Chenquan Gan, Xinghai Xiao, Qingyi Zhu, Deepak Kumar Jain, and Akanksha Saini. Blockchain-assisted electronic medical data-sharing: Developments, approaches and perspectives. *Computers, Materials & Continua*, 81(3), 2024.

[129] Chenquan Gan, Xinghai Xiao, Yiye Zhang, Qingyi Zhu, Jichao Bi, Deepak Kumar Jain, and Akanksha Saini. An asynchronous federated learning-assisted data sharing method for medical blockchain. *Applied Intelligence*, 55(2):208, 2025.

[130] Bin Wang, Zhao Tian, Fengxiao Tang, Heng Pan, Wei She, and Wei Liu. Blockchain-empowered asynchronous federated reinforcement learning for iot-based traffic trajectory prediction. *IEEE Internet of Things Journal*, 2025.

[131] Arjmand Samuel, Muhammad I Sarfraz, Hammad Haseeb, Saleh Basalamah, and Arif Ghafoor. A framework for composition and enforcement of privacy-aware and context-driven authorization mechanism for multimedia big data. *IEEE Transactions on Multimedia*, 17(9):1484–1494, 2015.

[132] Ali Gholami and Erwin Laure. Security and privacy of sensitive data in cloud computing: A survey of recent developments. *arXiv preprint arXiv:1601.01498*, 2016.

[133] Simone Fischer-Hbner and Stefan Berthold. Privacy-enhancing technologies. In *Computer and information security Handbook*, pages 759–778. Elsevier, 2017.

[134] Tyler Phillips, Xiaoyuan Yu, Brandon Haakenson, Shreya Goyal, Xukai Zou, Saptarshi Purkayastha, and Huanmei Wu. Authn-authz: Integrated, user-friendly and privacy-preserving authentication and authorization. In *2020 Second IEEE international conference on trust, privacy and security in intelligent systems and applications (TPS-ISA)*, pages 189–198. IEEE, 2020.

[135] Nilesh P Sable, Rahul Sonkamble, Vijay U Rathod, Swati Shirke, Jyoti Yogesh Deshmukh, and Gurunath T Chavan. Web3 Chain Authentication and Authorization Security Standard (CAA). *International Journal on Recent and Innovation Trends in Computing and Communication*, 11(5):70–76, 2023.

[136] Muhammad Haziq Zulhazmi Hairul Nizam, Muhammad Afiq Ahmad Nizam, Muhammad Hadi Husaini Jummadi, Nik Nor Muhammad Saifudin Nik Mohd, Ahmad Anwar Zainuddin, et al. Hyperledger fabric blockchain for securing the edge internet of things: A review. *Journal of Informatics and Web Engineering*, 4(1):81–98, 2025.