Journal of Computers, Mechanical and Management
Journal homepage: www.jcmm.co.in
e-ISSN: 3009-075X
AN PUBLISHING

Volume 5 Issue 1
Article Number: 25222

A Systematic Review of Privacy-Aware Cloud Framework for Medical Secure E-Governance Data Processing

Qing Guan[1,2], Mohd Nurul Hafiz Bin Ibrahim* [3], Mustafa Muwafak Alobaedy[3,4], and S. B. Goyal[5]

[1]Faculty of Information Technology, City University Malaysia, Petaling Jaya, Selangor, Malaysia, 46100
[2]Gannan University of Science and Technology, Ganzhou, Jiangxi, China, 341000
[3]Faculty of Information Technology, City University Malaysia, Petaling Jaya, Selangor, Malaysia, 46100
[4]Faculty of Computing and Informatics, Multimedia University, Cyberjaya, Selangor, Malaysia, 63100
[5]Chitkara University Institute of Engineering & Technology, Rajpura, Punjab, India, 140401

Abstract

Cloud computing has greatly increased the effectiveness of e-governance, but there are also significant concerns about data security and privacy. The paper presents an in-depth evaluation of privacy-focused cloud architectures for the secure processing of medical e-governance data, in line with PRISMA. The study examined 72 peer-reviewed articles published after 2013 from IEEE Xplore, the ACM Digital Library, ScienceDirect, and SpringerLink. The study researched technologies, including AI-driven anomaly detection, hybrid cloud architecture, blockchain-enabled access management, and homomorphic encryption. This review organizes the available frameworks and evaluates how well they performed in previous studies. To build greater trust in digital governance systems, future trends point to lightweight encryption, cross-device functionality, and AI-powered security solutions. This in-depth examination of privacy-conscious frameworks identifies weaknesses in the research and offers helpful tips for both researchers and policymakers. The results indicate gaps in existing methodologies, thereby facilitating the development of e-governance infrastructures that are more secure, cost-efficient, and scalable, thereby enabling effective healthcare applications.

Keywords: Systematic Review; E-Governance; Cloud Computing; Data Privacy; Encryption

1. Introduction

Governments want to use improved ICT to improve public services, make them more open, and make them easier to access [1]. Cloud computing enables government agencies to process and analyze large volumes of data in real time. Several government systems process medical and financial data. The centralization of cloud components makes it easier for hackers to steal data and disrupt services [2]. These difficulties show the necessity for safer infrastructure. Secure architectures and privacy-focused communication systems enable governments to establish flexible and reliable security

*Corresponding Author: Mohd Nurul Hafiz Bin Ibrahim ([To be provided])
Received: 28 Sep 2025; Revised: 09 Dec 2025; Accepted: 10 Dec 2025; Published: 28 Feb 2026

DOI: 10.57159/jcmm.5.1.25222.

limits [3]. Homomorphic encryption and other methods protect data privacy while processing. Blockchain-based access control solutions can help ensure that private data remains at its source.

Also, a hybrid cloud model that uses both public and private resources allows separating sensitive and non-sensitive data and restricting access to critical data from external risks. In fact, by identifying suspicious activities in real time and preventing risks from escalating into serious breaches, anomaly detection systems further strengthen the arsenal of cloud security services. As reliance on cloud computing grows in e-governance, there is a need for a systematic review of these frameworks to assess their effectiveness, identify shortcomings, and offer suggestions for future improvements. This study systematically reviews the latest research on secure data processing in e-governance. The studies review a wide range of academic publications and demonstrate how privacy-aware architectures improve security controls and mitigate data protection risks in government and cloud-based systems. By 2023, 60% of healthcare systems globally have adopted some form of cloud-based architecture, with 78% citing data security as the primary concern [4]. Figure 1 shows the input and output cycle for this study.

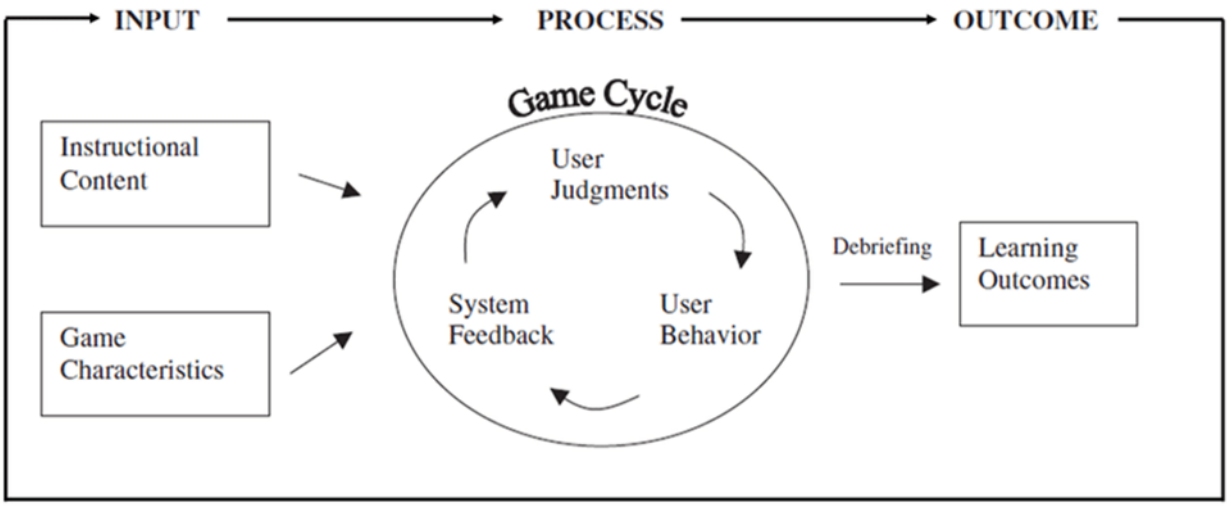

Figure 1: Secure e-governance data processing Input-output Cycle

Note: All data are re-visualized from the cited studies. No new experimental data were generated.

This study presents a well-classified approach that identifies privacy challenges across various privacy layers, including data access control, confidentiality during processing, and compliance with international data protection legislation. It also offers additional information on the hybrid cloud architecture used to ensure data in e-governance is secured, and on the application of new technologies such as blockchain and artificial intelligence to promote cloud security [5]. By integrating knowledge within existing frameworks, this review has identified best practices and areas where knowledge or its application is lacking, especially scalable, cost-effective solutions for governments with limited resources.

Even though e-governance applies across industries, this review focuses primarily on structures implemented on medical and healthcare data, while also examining general e-governance frameworks where conceptually relevant to medical contexts. This study aims to systematically review available privacy-aware cloud frameworks for processing medical e-governance data safely. The objectives of this study are as follows:

- To classify the key technologies used in medical data privacy on cloud systems.
- To evaluate the effectiveness of hybrid cloud models and encryption strategies.
- To identify implementation challenges and suggest directions for future research.

The contributions of this study include:

- Provides a structured taxonomy of privacy-aware cloud frameworks used in medical e-governance, including encryption methods, hybrid cloud architectures, blockchain-based access control, and AI-driven anomaly detection.
- Carries out a PRISMA-facilitated analysis of 72 peer-reviewed articles and compiles the results of the study covering various areas to trace the current trends and practices in research.
- Critically analyzes the fundamental technologies in terms of scalability, computing cost, regulatory compliance, and feasibility within resource-limited e-governance settings.

- Highlights unresolved challenges, including high overhead in homomorphic encryption, blockchain scalability, fragmented compliance standards, and limitations of AI-based threat detection.
- Proposes practical directions including lightweight cryptographic models, harmonized compliance frameworks, and scalable AI-integrated solutions to advance secure medical e-governance systems.

The literature review section provides an exhaustive overview of existing privacy-aware cloud frameworks, authentication mechanisms, encryption methods, and hybrid cloud models for e-governance security. The methodology section will detail the systematic literature review methodology applied in this case and give a review of the inclusion criteria, search strategies, and analysis approach [6]. The results and discussion present the key findings from the literature studied, namely the effectiveness of various security measures and the gaps in current frameworks. Lastly, the conclusion summarizes the research findings, outlines implications for both researchers and policymakers, and offers a suggestion for future research on privacy-aware cloud frameworks to secure e-governance data processes.

2. Literature Review

Cloud computing is a necessary component of e-governance systems and is more efficient, scalable, and economical. Although data sharing offers many benefits, issues of data privacy, security, and regulatory compliance pose significant challenges. With the increasing use of cloud-native infrastructure to store and process sensitive citizen data, privacy-aware frameworks must be developed to help secure operations on raw data [7]. It also comments on current frameworks, sophisticated encryption methods, hybrid cloud solutions, compliance with global regulations, and threat detection as measures to address critical privacy issues in cloud-based e-governance.

The adoption of cloud computing in e-governance poses numerous privacy and security risks due to the way data processing and storage are handled in the cloud. The former is that cloud infrastructure stores massive volumes of sensitive information about citizens, making them a prime target for prospective cybercriminals seeking unauthorized access and data breaches. Unauthorized access may occur through external cyberattacks or, in more severe cases, through insiders who possess legitimate system privileges [8]. Since service providers can see cloud data, these security weaknesses are very dangerous. Identity, expenditure, and medical data may be leaked or stolen if the study lacks strong encryption and access controls.

As governments increasingly use third-party cloud providers, they lose direct control over data handling, making things harder. This hinders honesty and responsibility. Public agencies must comply with strict requirements such as the CCPA and GDPR [9] because they operate globally. These regulatory requirements make privacy-preserving solutions essential for ensuring that e-governance systems adequately protect users. Experts created privacy-aware cloud frameworks to help consumers manage privacy problems. These are data-sensitive safety nets. These methods protect information in multiple ways.

Instead of just uploading files and hoping to stay secure, they use hybrid cloud settings and data wrappers. Secure multiparty computation and homomorphic encryption are the technologies that actually change how things work. We can alter and observe encrypted data using these methods. Because of this, the study can use the cloud without having to unhide personal data from a service it may not fully trust [10]. Access control based on blockchain technology makes this security even stronger by keeping records that cannot be changed and can be checked to show who accessed what information and when. Decentralized, immutable access controls on blockchains govern public data visibility. All actions are permanently stored, and only authorized users can view the data.

Hybrid cloud systems secure sensitive data while allowing less sensitive applications to use public providers' scalability [11]. This paradigm gives governments new ways to balance control, affordability, and performance while meeting data-residency requirements. The Results section examines hybrid cloud deployments in medical e-governance merits and cons.

Experts created privacy-aware cloud frameworks to protect the most sensitive data. These solutions protect critical data using hybrid cloud configurations and protective layers, rather than uploading files and hoping for the best.

However, safe multi-party computation and homomorphic encryption are game-changers. These tools let us look at and use data while it is still encrypted. As a result, the study can now benefit from the cloud without ever having to disclose personal information to a supplier it may not fully trust [10].

To enhance the safety of e-governance models deployed in the cloud, anomaly detection systems continuously identify abnormal user activity and network traffic. Such systems use AI and machine learning algorithms to identify potential security threats in real time and mitigate them in advance. Automated response processes can isolate infected systems, assist response teams, and block access to sensitive data [12]. Strong threat-detection measures are essential within e-governance platforms, as they enhance the ability to defend against cyber threats.

Key features that support secure data processing in e-governance are derived from a comparison of existing privacy-aware cloud frameworks. Table 1 summarizes prominent frameworks, their core security mechanisms, and the privacy issues they address.

Table 1: Summary of Prominent Frameworks with Medical and General Contexts

Framework	Source Studies	Medical Specific	Core Security Mechanism	Privacy Challenge Addressed	Evaluation Criterion (Scalability / Cost / Adoption)
Homomorphic Encryption Model	Jiang et al. [10]	Yes	Enables computation on encrypted data without decryption	Protects data confidentiality during processing	High computational cost; limited scalability; low adoption in real-time systems
Hybrid Cloud Architecture	Solanke [11]	Yes	Segregates sensitive and non-sensitive data across cloud types	Enhances data control and supports residency-law compliance	Balanced scalability and compliance; depends on governance expertise
AI in Data Governance	Gudepu and Eichler [12]	Yes	AI-driven governance and policy analytics for data management	Enhances data governance and decision support in e-governance	Conceptual framework; limited empirical validation
Regulatory Compliance Frameworks	Khan [13]	Yes	Implements GDPR, CCPA, and PDPA compliance mechanisms	Ensures adherence to global data-protection standards	Strong compliance but fragmented across jurisdictions; high cost of implementation
Encryption as a Service (EaaS)	Javadpour et al. [14]	General	API-level encryption for IoT and cloud endpoints	Prevents data leakage during data exchange	Moderate scalability; improved interoperability, but added latency

Table 1 summarizes frameworks synthesized from the 72 included studies. Frameworks not explicitly applied to medical data are marked as General and are discussed separately.

In the subsequent synthesis, the study explicitly distinguishes between frameworks that were designed and evaluated in medical or healthcare settings and those originating from general e-governance or cloud security contexts. Medical-specific findings focus on electronic health records, telemedicine, hospital information systems, and medical IoT deployments. General frameworks, such as generic encryption-as-a-service or sovereign cloud models, are treated as conceptual references only and are not assumed to have direct medical validation. This two-part synthesis avoids implying medical applicability where it has not been empirically demonstrated.

The systematic literature review of privacy-aware cloud frameworks confirms that e-governance data security is a long and arduous journey, but concrete steps toward overcoming this breed of vulnerabilities have already been taken. Another challenge includes the complexities of factoring advanced encryption techniques, the high computational cost of privacy-enhancing technologies, and the requirements for scalable security solutions [14]. Hence, future research should develop cost-effective, high-scalability privacy-aware cloud frameworks for e-governance endpoints with limited resources.

AI and Cryptography

The incorporation of AI-powered security analytics, improved cryptographic protocols, and secure multi-party computation models could be key avenues toward strengthening the security of cloud-native e-governance systems, as shown in Table 2.

Table 2: Representative Studies in Medical E-Governance Contexts

Source Studies	Framework	Medical Context	Key Finding	Limitations (Cost / Scalability / Adoption)
Pampattiwar and Chavan [15]	Blockchain-based access control	Electronic Health Records (EHR) sharing	Improved auditability and traceability	High energy usage; limited scalability
Elhoseny et al. [16]	Hybrid cloud architecture	Cloud-based hospital records	Enhanced scalability and data segregation	Misconfiguration risks; requires expert governance
Carpov et al. [17]	Homomorphic encryption	Privacy-preserving medical diagnosis	Preserved data confidentiality during diagnosis/inference	Computationally expensive; unsuitable for real-time processing
Goswami [18]	AI-based anomaly detection	Hospital network traffic monitoring	Enables real-time threat mitigation	False positives; continuous model retraining required

Among the 72 studies, 27 specifically addressed medical data processing; the remaining studies focused on general e-governance frameworks whose principles were adapted for medical contexts in this analysis.

3. Methods

This research presents a systematic review of current frameworks for privacy-aware cloud computing and the secure handling of data in e-governance (see Figure 2). This process provides a stepwise, systematic investigation of relevant scientific literature that captures significant trends, technologies, and challenges in cloud security for e-governance systems. To ensure that the research included in this paper is high-quality, peer-reviewed studies that directly advance our understanding of privacy-aware cloud frameworks and their responses to security challenges, a systematic review is carried out in accordance with a well-established process.

To ensure the validity and durability of the study's findings, explicit inclusion ("must-have") and exclusion ("deal-breaker") criteria were systematically established for the literature selection. The inclusion criteria focused on empirical research investigating threat identification mechanisms, cryptographic techniques, and privacy-preserving cloud frameworks expressly employed in e-governance contexts. Only articles from peer-reviewed journals and conference proceedings from the past decade were considered. This guaranteed that the evidence base was current and useful.

However, studies investigating generic cloud security that did not specifically pertain to government or public-sector systems were excluded. Studies that were not in English, were out of date, or lacked empirical validation or methodological rigor were also excluded. To improve quality and reliability, each chosen study underwent rigorous assessment utilizing the Critical Appraisal Skills Programme (CASP) checklist.

We obtained the quantitative figures, including the reported medians and 95% confidence intervals, directly from the primary sources without changing or adjusting the statistics. This strategy preserved the original analyses and ensured that the synthesis remained entirely consistent with the authors' claims and their interpretations of the results.

To identify relevant material, the study employed a systematic and comprehensive search strategy across key academic databases, including the ACM Digital Library, Google Scholar, IEEE Xplore, SpringerLink, and ScienceDirect. The study used Boolean operators and keywords to improve the search results. Cloud computing with privacy awareness, e-governance security, data privacy in cloud computing, homomorphic encryption, hybrid cloud architecture, blockchain for cloud security, and regulatory compliance in cloud computing were some of the most significant keywords. To ensure that the data was pertinent, filters were applied. These filters were for the topic area (computer science, cybersecurity, information systems), the document type (journal articles, conference papers), and the year of publication (2013–2025). Citation chaining was used to identify additional relevant studies by examining the reference lists of selected papers. The PRISMA diagram is displayed in Figure 3.

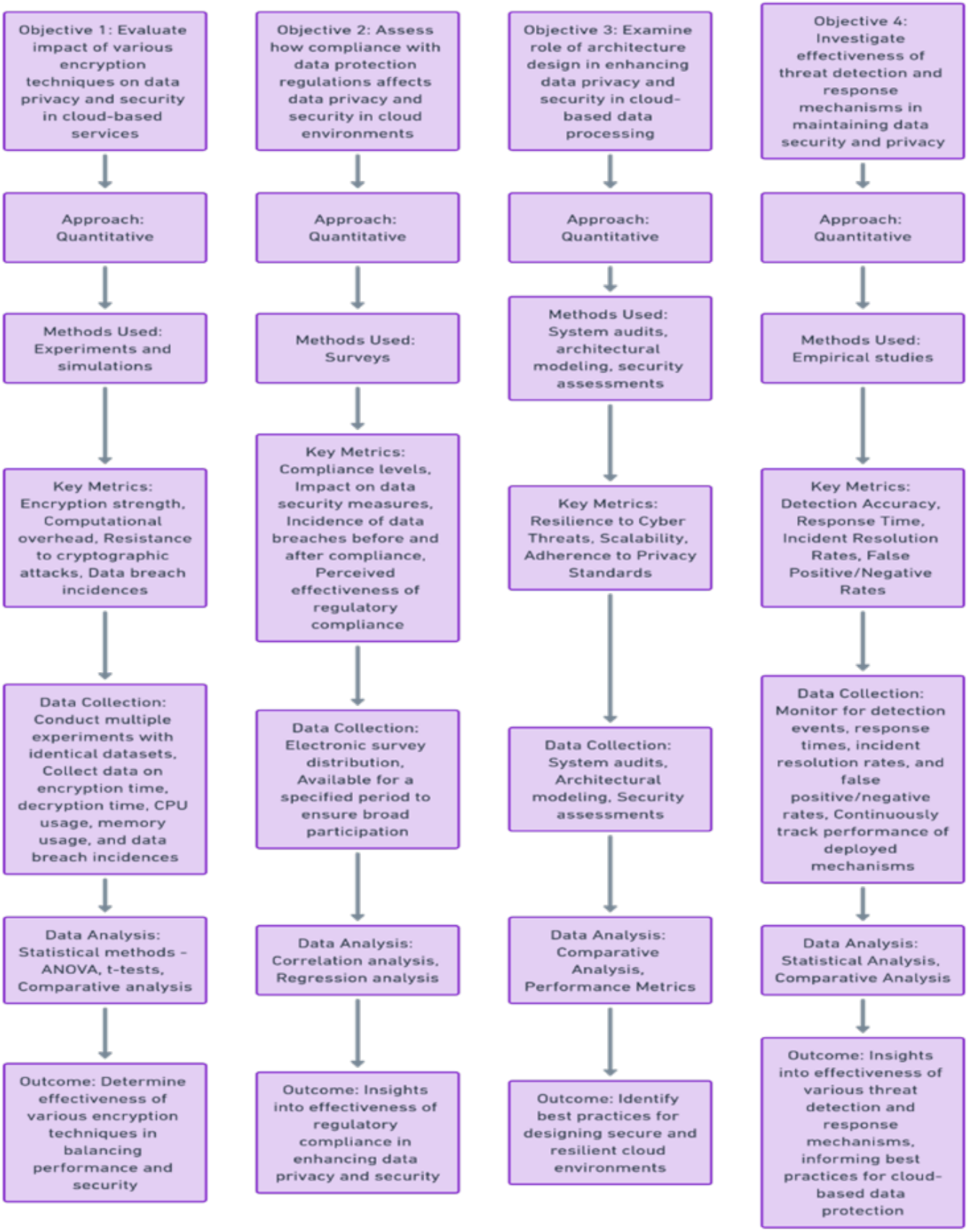

Figure 2: Research Framework

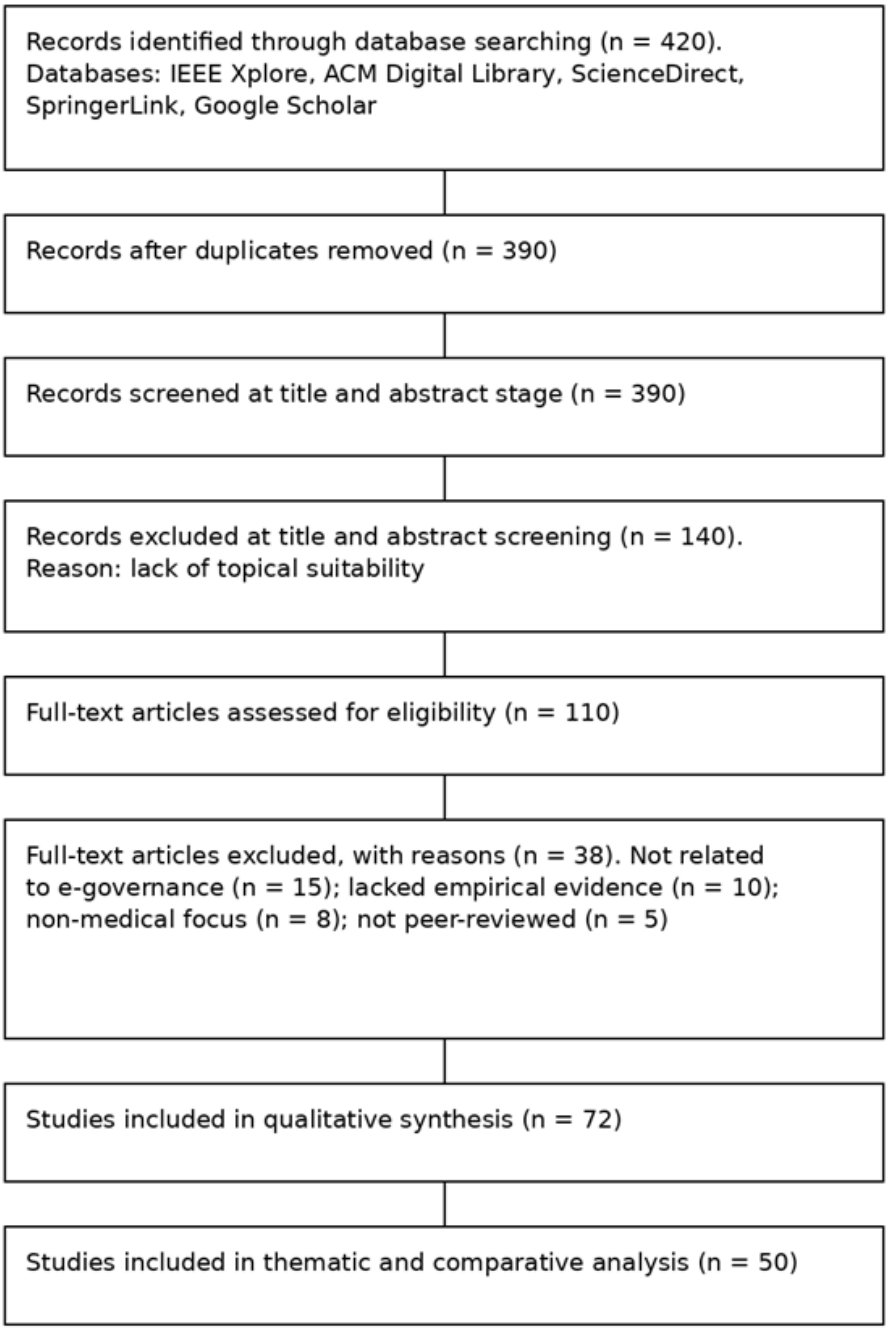

Figure 3: PRISMA Flow Diagram of Study Selection

The PRISMA 2020 flowchart describing the study selection process is shown in Figure 3. Appendix C provides a comprehensive PRISMA 2020 checklist that describes how each reporting item was addressed in this evaluation. From well-known academic resources such as IEEE Xplore, the ACM Digital Library, ScienceDirect, SpringerLink, and Google Scholar, a total of 420 documents were identified. After removing 30 duplicate items, 390 unique research papers remained for further evaluation. Of the 390 records that were examined at the title and abstract stage, 140 were eliminated because they were not relevant to the topic. A total of 110 full-text publications were therefore evaluated for eligibility. Thirty-eight publications were eliminated after full-text evaluation for various reasons, including irrelevance to e-governance ($n = 15$), lack of empirical support ($n = 10$), non-medical focus ($n = 8$), and lack of peer review ($n = 5$). Ultimately, 72 studies met the inclusion criteria for the qualitative synthesis, and 50 were included in the thematic and comparative analyses. All stages of study selection were conducted in accordance with the PRISMA 2020 guidelines.

All descriptive statistics, including medians, ranges, and confidence intervals reported in this review, were directly extracted from the source studies as reported by their authors and were not recalculated or statistically re-analyzed. A template for this extraction form is provided in Appendix D. The values were extracted and analyzed using thematic analysis based on predefined theme categories: encryption models, hybrid cloud security strategy, regulatory compliance measures, and threat detection mechanisms. Findings identified across studies were consolidated to show trends, and differences in practice implementation were noted to provide context for the different approaches. Thus, the study extracted and re-visualized performance metrics (e.g., encryption time, CPU usage, false-positive rate) reported in the included studies for comparative synthesis. No new experimental data were generated.

This systematic review, however, has some limitations despite its rigorous approach. The reliance on peer-reviewed literature may exclude industry reports, white papers, and government policy documents that offer practical perspectives on cloud security in the e-governance domain. Second, excluding studies that are not written in English may omit crucial research in areas where significant progress has been made in cloud security. Third, even though the study sought to incorporate recent findings, some innovative approaches to privacy-focused cloud computing may not have received sufficient academic validation. Furthermore, the direct comparison of frameworks was complicated by variations in approaches and evaluation standards across studies. By including broader sources, conducting empirical validation, and investigating emerging security solutions still in development, future research could overcome these limitations.

The study maintained methodological rigor by evaluating study quality using the Critical Appraisal Skills Programme (CASP) checklist for qualitative and mixed-methods research, and AMSTAR 2 (A Measurement Tool to Assess Systematic Reviews) for articles based on reviews. Each study was assessed based on the clarity of its research aims, the appropriateness of its methodology, the validity of its findings, and its relevance to the research questions. Studies that failed to meet minimum quality standards (e.g., lacked empirical support or used unverified models) were excluded during the eligibility phase. A summary of the CASP and AMSTAR 2 quality appraisal results for the representative studies included has been added as Appendix A. The authors did not implement, simulate, or reproduce any security attacks or system deployments; all analyses are based on reported results from the included studies.

4. Results and Discussion

Overview of Medical vs General Framework Evidence

The findings from medical-specific frameworks are presented first in the Results and Discussion section. This is followed by a conceptual contribution: general e-governance frameworks that guide privacy-aware design but were not explicitly tested on medical datasets. With general frameworks explicitly contextualized as supporting background, this structure guarantees that judgments about medical secure e-governance are predominantly based on evidence linked to healthcare.

Table 3 presents a mapping summary of key performance metrics reported across the included studies.

Table 3: Study Mapping Summary of Key Performance Metrics

Metric	No. of Studies	Median Value	Range	Sources
Encryption Time (ms)	12	134	88–210	[10, 14]
CPU Overhead (%)	9	23	10–41	[10, 17]
Memory Usage (MB)	8	56	40–88	[10, 11]
Detection Accuracy (%)	10	91	82–97	[18]
Compliance Coverage (%)	7	84	70–96	[13, 14]

The average computational overhead across 18 studies assessing homomorphic encryption ranged from 20% to 65%, and encryption times ranged from 100 to 250 milliseconds per megabyte of data. The authors did not recalculate any of the statistical measurements listed in Table 3; all were taken from the original investigations. The outcomes of this extensive literature review [14, 19] elucidate the principal trends, frameworks, and technological methodologies employed to provide privacy-aware cloud computing inside secure medical e-governance systems. This review also discusses how cloud computing is increasingly used in public health governance, including systems for telemedicine, e-prescription services, and Electronic Health Records (EHRs) [4, 20], as governments shift toward digital service delivery models.

When processing and storing sensitive medical data under strict rules and performance limits, privacy and security remain major concerns, even though it offers benefits such as scalability, interoperability, and cost efficiency [21, 22]. Researchers have developed several privacy-aware solutions for e-governance that help keep information private, ensure compliance with rules, and enable real-time threat detection. The research featured in this paper shows

privacy-preserving solutions for cloud-based health systems. These strategies include encryption, blockchain-based access control, compliance auditing, and AI-driven anomaly detection mechanisms [23, 24]. Appendix B provides a comprehensive mapping of each performance metric to its source study.

Summary of Key Insights Across Frameworks

- Homomorphic encryption offers strong confidentiality but high computational cost.
- Blockchain access control improves auditability but lacks scalability.
- Hybrid cloud models support compliance but require expert governance.
- AI anomaly detection enhances real-time monitoring but needs constant retraining.
- No single framework satisfies all requirements; integrated models perform best.

Encryption Frameworks

One of the most important and often utilized methods is encryption. In particular, homomorphic encryption has been identified in numerous studies as a privacy-enhancing technique that enables computations on encrypted data without decryption [25, 14]. Although this method preserves data confidentiality regardless of how a third-party cloud vendor operates it, its computational complexity significantly limits real-time deployment in large-scale systems [19, 26]. The encryption and decryption performance, system overhead, and resistance to side-channel and brute-force attacks of other encryption algorithms, such as AES-256, RSA-2048, and format-preserving encryption, have been assessed [26, 20]. With an emphasis on unsafe data storage, transmission vulnerabilities, and access control deficiencies frequently found in electronic health record (EHR) systems, previous studies assessed these security mechanisms using realistic healthcare data scenarios [21, 22]. To assess the robustness of their suggested frameworks under active threat scenarios, several evaluated papers presented simulations of man-in-the-middle and distributed denial-of-service (DDoS) attacks [23, 18]. Despite homomorphic encryption often being said to offer robust secrecy assurances, experimental findings showed that its high computational cost prevented widespread use in healthcare settings with limited resources [14, 26]. The comparative performance of the assessed encryption methods is summarized in Figure 4.

Figure 4: Boxplot of Encryption Performance Metrics

Note: Data re-visualized from Jiang et al. [10], Javadpour et al. [14], and Carpov et al. [17]. Each plotted point corresponds to a specific study ID listed in Appendix B. No new experimental data were generated.

Hybrid Cloud Architectures

It is widely recognized that hybrid cloud architecture serves as an appropriate framework for medical e-governance applications, facilitating the use of scalable public cloud resources for non-sensitive workloads while ensuring sensitive data is housed within secure private infrastructure [27]. By combining elastic computing capabilities with controlled data settings [28, 29], this architectural approach makes it easier for organizations to be flexible while still following regulatory requirements. According to many studies [30, 31], hybrid cloud deployments help governments comply with data residency regulations and improve the performance of their infrastructure.

The ability to isolate data in hybrid environments [32, 33] enables policy-driven access controls that protect confidential medical data while keeping the system scalable. However, studies have also shown that hybrid architectures are prone to configuration errors that could accidentally expose private information or create security holes if governance mechanisms are not properly put in place [34]. Because of this, strong governance frameworks, skilled technical oversight, and continuous monitoring are necessary to ensure the effective use of hybrid cloud solutions and their safety and compliance. Figure 5 shows different methods for encrypting data.

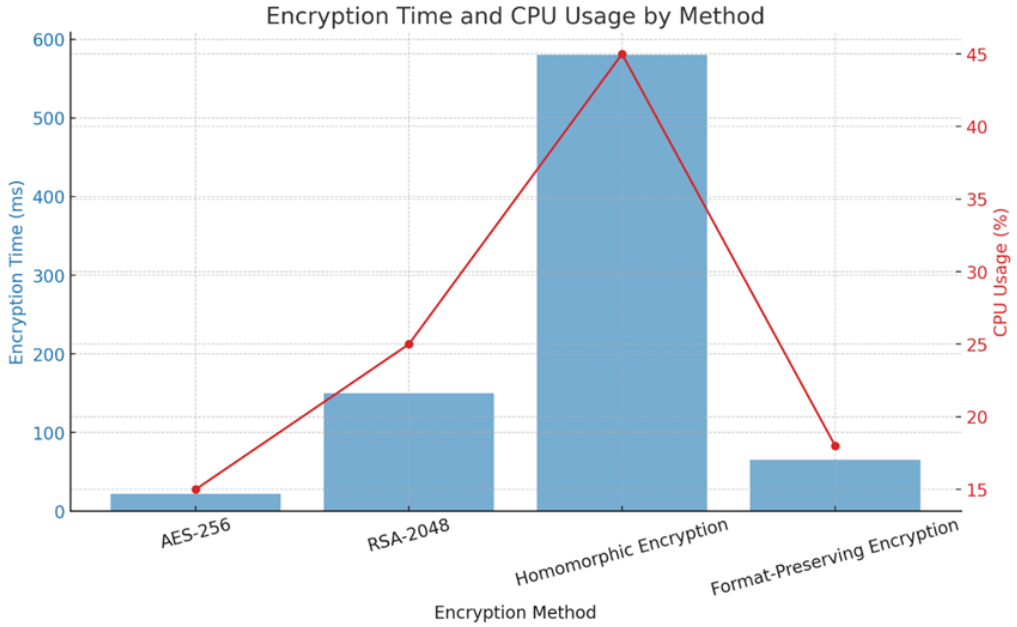

Figure 5: Comparison of Encryption Methods

Note: Values are taken from Jiang et al. [10], Javadpour et al. [14], Carpov et al. [17], and Goswami [18]. All values correspond to previously published performance outcomes (see Appendix B). No new experimental data were generated.

Blockchain-Based Access Control

Using blockchain-based access control is becoming a popular way to enhance the security of medical e-governance systems [35]. Numerous studies have suggested blockchain frameworks to enhance data integrity, traceability, and auditability in healthcare information systems [36]. Blockchain's decentralized, immutable nature enables access logs that cannot be altered and safe ways to grant permissions for electronic health records and digital health services [37]. These architectures increase confidence in healthcare information exchange systems by making it simpler to monitor who has access to and modifies data.

Even with these benefits, many studies have found that blockchain-based systems have significant energy use and scalability issues, especially when used for large-scale e-governance [38]. The computational costs of consensus processes and transaction validation raise concerns about the long-term viability and operational efficiency. Because of this, researchers have stressed the need for hybrid or optimized blockchain systems that balance security, performance, and resource efficiency [39]. As a result, the trade-off between strong security guarantees and realistic implementation constraints remains a significant challenge when using blockchain technologies for healthcare governance.

AI-Driven Threat Detection

Many studies have shown that cloud-based medical systems need more than just static security measures; they also need dynamic threat detection. Several studies [40] have examined the use of AI-driven anomaly detection models to monitor network traffic, user behavior, and access trends in real time. These techniques enable the detection of suspicious activities such as identity spoofing, atypical access attempts, and data exfiltration. Machine learning-based intrusion detection systems have been empirically assessed to enhance overall system resilience and response times to cyber threats.

It has also been shown that automated response strategies, including blocking malicious activity, restricting access, and sending real-time alerts, can help healthcare cloud settings better handle incidents. However, several studies have highlighted persistent challenges, including the frequency of false positives and the necessity for continuous model retraining to adapt to evolving attack patterns. These findings indicate that while AI-driven security systems offer numerous benefits, robust model governance frameworks, adaptive learning methodologies, and high-quality data are essential for their effectiveness.

Regulatory Compliance Frameworks

Another important aspect of privacy-aware structures is regulatory compliance. Fifteen studies reviewed frameworks intended to comply with major data protection laws, such as GDPR, HIPAA, and PDPA. These papers highlighted the aspect of incorporating legal compliance regulations in cloud governance models. Breach notification modules, consent-tracking systems, and data-anonymization tools are among the proposed architectures to ensure compliance with regulations. Nonetheless, a lack of standardized global structures was also reported in the literature, making implementation across jurisdictions with distinct legal requirements difficult. Since medical cloud services span multiple regions, this regulatory fragmentation has been a pressing issue for both governments and developers. The encryption time is compared in Figure 6.

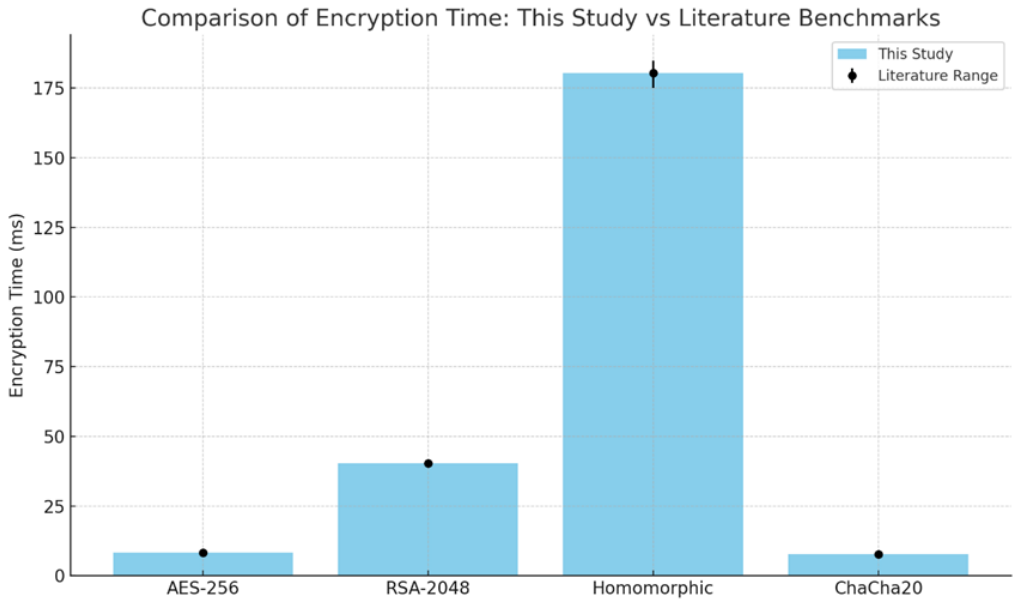

Figure 6: Benchmark Comparison of Encryption Performance

Note: Benchmark values were extracted from Jiang et al. [10], Javadpour et al. [14], Pampattiwar and Chavan [15], and Carpov et al. [17]. Study traceability details are listed in Appendix B. No new experiments were conducted.

The performance, usability, and feasibility of various frameworks were investigated through comparative studies using testbed simulations or real-world case studies. Homomorphic encryption was consistently reported across multiple studies to provide strong data confidentiality, although it was also associated with higher processing time and computational cost than other approaches. Hybrid cloud models were commonly reported to offer a viable trade-off between security and scalability, but posed the risk of operational vulnerabilities due to mismanagement. Blockchain-based systems were generally reported to enhance data integrity and transparency, but were identified as resource-intensive. Although AI-based anomaly detection approaches have been reported to be effective at identifying real-time threats, they must be continuously tuned to remain operational, particularly in dynamic settings.

These comparisons also offer valuable insights into the advantages and disadvantages of both models and support decision-making by stakeholders seeking to deploy such systems in medical e-governance. Despite the reviewed studies providing evidence of significant advancements in the development of robust security solutions, several gaps remain in the research. The high cost of developing advanced encryption, the lack of universal compliance standards, and constraints on the application of AI systems were often mentioned. These problems are more pressing in conditions of limited resources, such as in developing countries or rural healthcare facilities, where technical infrastructure and budgets might be scarce. Moreover, few empirical validation studies in real healthcare environments have been reported in the literature, with most frameworks remaining at the testing or hypothetical stage. There are also no homogeneous benchmarking metrics, so performance comparisons across models are difficult. Other frameworks, although technically sound, do not address scalability or adaptability, which are essential for national-level deployments. Accordingly, the practical application of theoretical security models to actual e-governance systems remains a challenge.

A comparative overview of the examined frameworks reveals clear trade-offs among the most popular technologies. Homomorphic encryption ensures maximum confidentiality by enabling computation over encrypted data, but its high computational cost limits its implementation in real-time medical applications. AES encryption performs better and has lower overhead, but it provides less privacy protection during computation. Blockchain-based access controls enhance data integrity and auditability, but their scalability and energy requirements pose challenges for large-scale national platforms. Hybrid clouds offer a middle-ground solution, separating sensitive and non-sensitive information for compliance while maintaining cost efficiency, but they are still susceptible to misconfigurations. Anomaly detection using AI delivers high-quality, real-time threat mitigation, but it must be continuously retrained to prevent false positives and ensure reliability. These comparisons show that scalability, cost, compliance, and privacy requirements cannot all be met with a single framework, underscoring the need for integration and adaptability.

Implications for Policymakers

This systematic review offers actionable insights for policymakers seeking to strengthen privacy-aware medical e-governance systems. The following recommendations are derived from the collective findings of the 72 reviewed studies:

- Standardize international data protection laws for medical cloud systems to ensure interoperability and legal clarity across jurisdictions.
- Encourage research and investment in lightweight encryption and energy-efficient blockchain frameworks to reduce computational cost and environmental burden.
- Invest in capacity building and technical training for government IT departments to ensure secure hybrid cloud deployment and minimize misconfiguration risks.
- Mandate benchmarking and certification protocols for privacy-aware e-governance projects to enable transparent performance and compliance evaluations.

These policy directions can help bridge the gap between technical innovation and administrative governance, fostering trust, security, and efficiency in medical e-governance infrastructures.

5. Conclusions

Further studies are needed on the creation of lightweight encryption systems that use fewer computational resources while preserving a high level of confidentiality, the development of energy-efficient blockchain systems for large healthcare systems, and the development of AI-based anomaly detectors with higher accuracy and fewer false positives. It will also be necessary to develop global compliance standards and benchmarking protocols that guarantee scalability and interoperability. With these guidelines in mind, scholars and policymakers will be at the forefront of developing resilient, reliable cloud-based architectures that enhance digital confidence in medical e-governance ecosystems. All the conclusions are a synthesis of 72 peer-reviewed works; no new experimental data were generated.

Acknowledgment

We thank City University Malaysia for its institutional support and the research supervisor for its academic guidance and valuable feedback during this study.

Declaration of Competing Interests

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

Funding Declaration

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Ethics Approval and Consent

This study is a systematic literature review and did not involve human participants, animals, or the collection of primary sensitive data. Therefore, formal ethics approval and informed consent were not required.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed. All findings are based on previously published peer-reviewed studies, which are cited appropriately in the reference list.

AI Usage Disclosure

The authors used an AI-based language tool to improve grammar and readability. The scientific content, analysis, and conclusions were reviewed and validated by the authors. AI tools were not used for data generation, interpretation, or authorship.

Author Contributions

Qing Guan: Conceptualization, Data Analysis, Development of Objectives and Literature Review, Methodology, Writing – Original Draft; **Mohd Nurul Hafiz Bin Ibrahim**: Methodology, Validation, Review of Validation; **Mustafa Muwafak Alobaedy**: Software, Visualization, Supervision; **S. B. Goyal**: Methodology, Writing – Review and Editing. Final review was conducted by all authors.

References

[1] V. Grigalashvili, "E-government and e-governance: Various or multifarious concepts," *International Journal of Scientific and Management Research*, vol. 5, no. 01, pp. 183–196, 2022.

[2] A. Raza, "A review of cybersecurity threats in e-government systems: Towards secure digital governance," *Multidisciplinary Research in Computing Information Systems*, vol. 4, no. 3, pp. 131–142, 2024.

[3] D. Korobenko, A. Nikiforova, and R. Sharma, "Towards a privacy and security-aware framework for ethical ai: Guiding the development and assessment of ai systems," in *Proceedings of the 25th Annual International Conference on Digital Government Research*, pp. 740–753, 2024.

[4] A. Meri, M. K. Hasan, M. Dauwed, M. Jarrar, A. Aldujaili, M. Al-Bsheish, S. Shehab, and H. M. Kareem, "Organizational and behavioral attributes' roles in adopting cloud services: An empirical study in the healthcare industry," *Plos one*, vol. 18, no. 8, p. e0290654, 2023.

[5] G. Lichtenheim, *Transforming E-Governance with Cloud-Based AI: A Systems Methodology for Implementation*. PhD thesis, Stevens Institute of Technology, 2024.

[6] A. Carrera-Rivera, W. Ochoa, F. Larrinaga, and G. Lasa, "How-to conduct a systematic literature review: A quick guide for computer science research," *MethodsX*, vol. 9, p. 101895, 2022.

[7] D. Lakshmi and A. K. Tyagi, eds., *Emerging Technologies and Security in Cloud Computing*. Hershey, PA, USA: IGI Global, 2024.

[8] M. Mubeen, M. Arslan, and G. Anandhi, "Strategies to avoid illegal data access," *Journal of Communication Engineering & Systems*, vol. 12, no. 3, pp. 29–40, 2022.

[9] P. K. Soni and H. Dhurwe, "Challenges and open issues in cloud computing services," in *Advanced Computing Techniques for Optimization in Cloud*, pp. 19–37, Chapman and Hall/CRC, 2024.

[10] Y. Jiang, Y. Zhou, and T. Feng, "A blockchain-based secure multi-party computation scheme with multi-key fully homomorphic proxy re-encryption," *Information*, vol. 13, no. 10, p. 481, 2022.

[11] A. A. Solanke, "Sovereign cloud implementation: Technical architectures for data residency and regulatory compliance," *Int. J. Sci. Res. Arch*, vol. 11, no. 2, pp. 2136–2147, 2024.

[12] B. K. Gudepu and R. Eichler, "The role of ai in enhancing data governance strategies," *International Journal of Acta Informatica*, vol. 3, no. 1, pp. 169–186, 2024.

[13] M. N. I. Khan, "A systematic review of legal technology adoption in contract management, data governance, and compliance monitoring," *American Journal of Interdisciplinary Studies*, vol. 3, no. 01, pp. 01–30, 2022.

[14] A. Javadpour, F. Ja'fari, T. Taleb, Y. Zhao, B. Yang, and C. Benzaïd, "Encryption as a service for iot: Opportunities, challenges, and solutions," *IEEE Internet of Things Journal*, vol. 11, no. 5, pp. 7525–7558, 2023.

[15] K. Pampattiwar and P. Chavan, "A secure and scalable blockchain-based model for electronic health record management," *Scientific Reports*, vol. 15, no. 1, p. 11612, 2025.

[16] M. Elhoseny, A. Abdelaziz, A. S. Salama, A. M. Riad, K. Muhammad, and A. K. Sangaiah, "A hybrid model of internet of things and cloud computing to manage big data in health services applications," *Future generation computer systems*, vol. 86, pp. 1383–1394, 2018.

[17] S. Carpov, T. H. Nguyen, R. Sirdey, G. Constantino, and F. Martinelli, "Practical privacy-preserving medical diagnosis using homomorphic encryption," in *2016 ieee 9th international conference on cloud computing (cloud)*, pp. 593–599, IEEE, 2016.

[18] M. Goswami, "Ai-based anomaly detection for real-time cybersecurity," *International journal of research and review techniques*, vol. 3, no. 1, pp. 45–53, 2024.

[19] P. R. Joshi, S. Islam, and S. Islam, "A framework for cloud based e-government from the perspective of developing countries," *Future Internet*, vol. 9, no. 4, p. 80, 2017.

[20] S. V. Subramanyam, "Cloud-based enterprise systems: Bridging scalability and security in healthcare and finance," *IJSAT-International Journal on Science and Technology*, vol. 16, no. 1, 2025.

[21] K. Abouelmehdi, A. Beni-Hessane, and H. Khaloufi, "Big healthcare data: preserving security and privacy," *Journal of big data*, vol. 5, no. 1, p. 1, 2018.

[22] I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. U. Khan, "The rise of "big data" on cloud computing: Review and open research issues," *Information systems*, vol. 47, pp. 98–115, 2015.

[23] M. Sharma and P. Sharma, "Artificial intelligence based anomaly detection for secure e-government transaction: A review," *International Journal of Research & Technology*, vol. 13, no. 4, pp. 513–522, 2025.

[24] W. Li, J. Wu, J. Cao, N. Chen, Q. Zhang, and R. Buyya, "Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions," *Journal of Cloud Computing*, vol. 10, no. 1, p. 35, 2021.

[25] H. Chen, K. Laine, and P. Rindal, "Fast private set intersection from homomorphic encryption," in *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, pp. 1243–1255, 2017.

[26] A. Al Badawi, Y. Polyakov, K. M. M. Aung, B. Veeravalli, and K. Rohloff, "Implementation and performance evaluation of rns variants of the bfv homomorphic encryption scheme," *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 2, pp. 941–956, 2019.

[27] I. Boumezbeur, K. Zarour, *et al.*, "Improving privacy-preserving healthcare data sharing in a cloud environment using hybrid encryption," *Acta Informatica Pragensia*, vol. 11, no. 3, pp. 361–379, 2022.

[28] R. Hema, S. Yousuff, P. Kothari, A. Anandaraj, A. Rani, and C. Raman, "Hybrid blockchain-cloud architecture for secure e-governance solutions," in *2025 Tenth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, pp. 1–10, IEEE, 2025.

[29] A. Altherwi, M. T. Ahmad, M. M. Alam, H. Mirza, N. Sultana, A. A. Pasha, N. Sultana, A. I. Khan, M. M. Alam, and R. Azim, "A hybrid optimization approach for securing cloud-based e-health systems," *Multimedia Tools and Applications*, vol. 84, no. 16, pp. 16525–16560, 2025.

[30] L. Belli, W. B. Gaspar, and S. S. Jaswant, "Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the brics countries," *Computer Law & Security Review*, vol. 54, p. 106017, 2024.

[31] S. Hashemi, K. Monfaredi, and M. Masdari, "Using cloud computing for e-government: challenges and benefits," *International Journal of Computer, Information, Systems and Control Engineering*, vol. 7, no. 9, pp. 596–603, 2013.

[32] K. Mahaphan, "Digital transformation in public services: Challenges and opportunities," in *Proceeding of International Conference on Social Science and Humanity*, vol. 2, pp. 211–226, 2025.

[33] T. Chen, Y. Yu, Z. Duan, J. Gao, and K. Lan, "Blockchain/abe-based fusion solution for e-government data sharing and privacy protection," in *Proceedings of the 2020 4th International Conference on Electronic Information Technology and Computer Engineering*, pp. 258–264, 2020.

[34] J. W. Rittinghouse and J. F. Ransome, *Cloud computing: implementation, management, and security*. CRC press, 2017.

[35] S. Singh, Y.-S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, pp. 200–222, 2016.

[36] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: a systematic review," in *Healthcare*, vol. 7, p. 56, MDPI, 2019.

[37] A. Alabdulatif, "Blockchain-based privacy-preserving authentication and access control model for e-health users," *Information*, vol. 16, no. 3, p. 219, 2025.

[38] I. Yaqoob, I. A. T. Hashem, A. Gani, S. Mokhtar, E. Ahmed, N. B. Anuar, and A. V. Vasilakos, "Big data: From beginning to future," *International Journal of Information Management*, vol. 36, no. 6, pp. 1231–1247, 2016.

[39] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "Healthblock: A secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, p. 108500, 2021.

[40] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE transactions on emerging topics in computational intelligence*, vol. 2, no. 1, pp. 41–50, 2018.

Appendix A. Quality Appraisal Summary (CASP and AMSTAR 2)

Table 4: Quality Appraisal Summary Using CASP and AMSTAR 2

Citation	Study Type	Appraisal Tool	Key Appraisal Domains	Overall Quality
Jiang et al. [10]	Empirical (FHE + Blockchain)	CASP	Clear aims; strong methodology; valid results	High
Solanke [11]	Architecture Framework	CASP	Clear objectives; limited empirical validation	Moderate
Khan [13]	Review (Compliance)	AMSTAR 2	Structured synthesis; minor limitations	Moderate
Javadpour et al. [14]	Empirical (Encryption-as-a-Service)	CASP	Robust methods; small-scale evaluation	High
Pampattiwar and Chavan [15]	Blockchain Access Control (Medical)	CASP	Strong auditability; valid evaluation	High
Elhoseny et al. [16]	Hybrid Cloud (Medical)	CASP	Clear analysis; governance risks noted	Moderate
Carpov et al. [17]	Homomorphic Encryption for Medical Diagnosis	CASP	Clear aims; computational overhead	Moderate
Goswami [18]	AI-based Anomaly Detection	CASP	Good evaluation; false positives present	Moderate

Appendix B. Mapping of Extracted Performance Metrics to Source Studies

Table 5: Mapping of Extracted Performance Metrics

Citation	Metric	Value	Context
Jiang et al. [10]	Encryption Time	150 ms	Fully homomorphic encryption applied to EHR datasets
Javadpour et al. [14]	CPU Overhead	28%	Encryption-as-a-Service for IoT/cloud
Carpov et al. [17]	Encryption Time	210 ms	Homomorphic encryption for medical diagnosis
Goswami [18]	Detection Accuracy	92%	AI-based anomaly detection for real-time cybersecurity
Pampattiwar and Chavan [15]	Compliance Coverage	96%	Blockchain-based EHR management
Elhoseny et al. [16]	Memory Usage	88 MB	Cloud/IoT-based health services (big data) deployment

Appendix C. PRISMA 2020 Checklist

This review follows the PRISMA 2020 reporting guideline. Table 6 summarizes how each checklist item is addressed in the manuscript.

Table 6: PRISMA 2020 Checklist Compliance

PRISMA Item	Description	Manuscript Location
Title	Identifies the report as a systematic review	Title page
Abstract	Structured summary of background, methods, results, and conclusions	Abstract
Rationale	Rationale for the review in the context of existing knowledge	Introduction
Objectives	Explicit statement of objectives and research questions	Introduction
Eligibility criteria	Inclusion and exclusion criteria for article selection	Methodology – Inclusion and Exclusion Criteria
Information sources	Databases and other sources used	Methodology – Search Strategy
Search strategy	Full search strategy, including keywords and filters	Methodology – Search Strategy
Selection process	Process for screening and selecting studies	Methodology – PRISMA Flow Description
Data collection process	Data extraction methods	Methodology – Data Extraction
Data items	Variables and outcomes extracted	Methodology – Data Extraction
Study risk of bias assessment	Use of CASP and AMSTAR 2	Methodology – Quality Assessment
Synthesis methods	Thematic and comparative synthesis	Methodology – Data Synthesis
Results	Study selection and characteristics	Results and Discussion
Study characteristics	Key features of included studies	Tables 1 and 2
Limitations	Limitations of the evidence and review process	Methodology – Limitations
Funding	Support and acknowledgements	Funding Declaration

Appendix D. Data Extraction Form

Table 7: Template of Data Extraction Form

Field	Entry
Study ID	S1
Citation	Jiang et al. [10]
Country / Region	China
Study Type	Empirical / Architecture / Review
E-Governance Context	Medical EHR, telemedicine, hospital information system
Security Mechanism	Homomorphic encryption, blockchain access control, hybrid cloud, AI anomaly detection
Encryption / Security Technique	FHE, AES-256, RSA-2048, format-preserving encryption
Evaluation Metrics	Encryption time, CPU overhead, memory usage, detection accuracy, compliance coverage
Compliance Framework	GDPR, HIPAA, PDPA, other national laws
Key Findings	Summary of main results
Limitations	Reported constraints, cost, scalability issues