

**A Cryptographic and Threat Modeling
Approach for Privacy-Compliant Digital
Forensics in Healthcare Systems.**

Name: Jyothi Avulareddyagri

Student Id: 2436065

Module: Research Methods and Professional Development

Module code: ACFA7004

Context and Background.....	4
Problem Statement.....	4
Aim.....	5
Objectives.....	5
Research Significance.....	5
Literature Review.....	6
Introduction to Healthcare Data Privacy and Security.....	6
Digital Forensics in Healthcare: Challenges and Limitations.....	6
Cryptographic Techniques for Privacy Preservation.....	7
Threat Modeling and Privacy Frameworks.....	8
Synthesis and Research Gap.....	8
Research Methods and Materials.....	10
Research Methods.....	10
Materials.....	13
Expected Outcome.....	15
Anticipated Results.....	15
Implications.....	15
Limitations.....	15
Timeline.....	16
Conclusion.....	17
References.....	18

Context and Background

The fast digitization of the healthcare sector and the adoption of Electronic Health Records (EHRs) and interconnected medical devices has resulted in a massive and highly sensitive data environment. This digitization has both enhanced the quality of care to patients and efficiency in operations; however, it has also transformed healthcare organizations into one of the easiest targets of cyberattacks, ranging all the way to ransomware and complex data breaches. As a result, the aspect of digital forensics has turned out to be critical in the investigation of such security breaches, evidence of ill practice, and regulation. Nevertheless, inherent to the crossroads of forensics and medical care, the standard practices of digital forensics cannot be effective without total access to data storage systems, which directly conflicts with the high level of privacy requirements, stipulated by such regulations as HIPAA and GDPR. This procedure tends to reveal the confidential health data of the entire patient population within a system rather than the sensitive data of a patient pertinent to an inquiry, which results in a secondary breach of privacy in the process of carrying out a primary breach of privacy.

This conflict also poses a major operational and ethical challenge, where there is a need to choose between the integrity of the investigative process and the confidentiality of the patients. Even the currently used forensic methods, including generation of full-disk images and general keyword-based search, are by definition privacy-invasive. The case being investigated should not require the revelation of medical histories of thousands of unrelated patients to investigate a particular case of data leakage or actions taken by a single clinician. This is not only unethical but also legally hazardous and is likely to result in healthcare organizations violating the same privacy laws that they are also trying to protect. Hence, there is an acute and unfulfilled demand of a new forensic paradigm, one with data protection in mind. Such a paradigm has to use high-tech solutions to allow the investigators to complete their tasks efficiently and technically implement the principles of data minimization and access control, so that patient privacy is not the victim of a required investigation.

Problem Statement

In the healthcare industry, where patient information is not only highly sensitive to any kind of attack but also a main target of cybercrime, a fundamental dilemma emerges between the need to conduct digital forensic investigations after a security incident and the ethical-legal requirement to respect the privacy of all patient records who are not A direct part of the case, which frequently leads to a secondary privacy violation in the process of the investigation itself and does not meet the requirements of regulations such as the HIPAA and GDPR, making it essential to change the paradigm of forensic practice towards methods that effectively retrieve evidence of

Aim

To design and theoretically validate a Privacy-Preserving Healthcare Forensics (PPHF) framework that integrates advanced cryptographic techniques to enable effective digital forensic analysis in healthcare environments while rigorously protecting patient data privacy and ensuring regulatory compliance.

Objectives

- To develop a multi-stage forensic framework of healthcare incidents which incorporates privacy-saving cryptographic methods to regulate access to Electronic Health Records (EHRs) and system-logs in the process of gathering evidence and analyzing it.
- In order to formally stipulate the basic cryptographic functions of the framework, it is necessary to devise algorithms that enable investigators to detect and examine evidence pertaining to a particular security event or malpractice case without providing access to the plaintextual state of the whole patient database.
- In order to determine the security and privacy resilience of the suggested framework through the thorough analysis of the threats, both external and internal, the possible threats should be identified through such methodologies as STRIDE and LINDDUN.
- To confirm that the framework complies with the healthcare privacy regulations and best practices by aligning its controls and processes to the NIST Privacy Framework, showing that it can address the following patient privacy risk during the lifecycle of the digital forensics.
- In order to integrate the results of the threat modeling and NIST analysis into a list of evidenced-based recommendations regarding the application of privacy-preserving forensics in healthcare, it would be important to outline the trade-offs between the efficacy of investigations and patient protection against privacy invasion.

Research Significance

The study is of great practical, theoretical, and regulatory value in that it fills a critical gap in the secure healthcare operations. In practice, it offers a methodological approach to enable healthcare organizations to make the necessary digital forensic inquiries, e.g., in cases of internal breaches or malpractices, without causing secondary privacy violations to their patient base, so that their patients do not lose their trust and continue to operate. Theoretically, it helps the emerging discipline of privacy-compliant digital forensics by illustrating how cryptographic controls can be implemented and combined to a designed threat model to promote the idea that forensic investigations can be both a posteriori and privacy-compliant. More so, this work

provides a proven roadmap that healthcare entities can follow to prove and comply with highly protective data protection rules like HIPAA and GDPR by harmonizing its frameworks with other standardized systems such as the NIST Privacy Framework, which will eventually guide the whole healthcare ecosystem to ensure its resilience to the changing cyber threats and legal issues.

Literature Review

Introduction to Healthcare Data Privacy and Security

Digitization of the healthcare sector has brought new challenges in finding a balance between the utility of the data and patient privacy. There has been an explosion of Electronic Health Records (EHRs), Internet of Medical Things (IoMT) devices, and telehealth platforms that have become a complicated digital ecosystem, where the extraordinarily vulnerable information about patients is stored and processed [1]. This digitalization has dramatically broadened the scope of attack on the cybercriminals and healthcare organizations have registered a rise of 45 per cent data breaches between 2018 and 2020 as per the Data Breach Investigations Report established by Verizon [2]. The secured health information (PHI) held by the healthcare systems is one of the most expensive datasets on the dark web, and records fetch up to 1,000 dollars because of their all-encompassing nature and irreversibility [3].

Regulations regulating the privacy of healthcare data have significantly changed in the last few years with the introduction of new regulations, including the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union [4]. These laws create very rigid rules regarding manipulation, processing, and storage of PHI, financial repercussions of which are hefty. The Privacy and Security Rules of HIPAA require certain administrative, physical, and technical measures to safeguard the information of patients whereas GDPR presents the concept of minimization of data, limitation of its use, and its privacy design [5]. The combination of the growing cyber threats and the strict regulatory standards has generated a serious demand for sophisticated security systems oriented specifically on the healthcare setting.

Digital Forensics in Healthcare: Challenges and Limitations

Digital forensics within a healthcare setting has its own peculiarities, which make the process different from the common digital forensics investigations. The healthcare digital ecosystem consists of various systems such as EHR systems, medical imaging systems, clinical decision support systems, and IoMT systems all of which produce huge volumes of potentially evidentiary data [6]. Conventional digital forensic practices where full forensic images are generally generated and a thorough analysis performed simply do not comply with healthcare privacy laws, as they reveal irrelevant data of patients under investigation [7]. This brings about

an ethical and legal quandary of which the investigation process itself can be disparaging the same privacy laws it seeks to uphold.

The size and richness of healthcare data also make the forensic investigation more complicated. A hospital with a medium size is able to produce more than 5 terabytes of data in a month, which comprises clinical notes, laboratory outcomes, medication records, and system logs [8]. In such enormous data, data that pertains to a particular investigation, e.g., a breach of patient records or medication order manipulation, might captivate only a drop of the ocean of the entire data. The existing methods in forensics compel the investigators to excavate massive amounts of irrelevant PHI before they find relevant evidence, a process that contributes to the massive privacy violations on patients who have no role in the investigation [9]. This is the privacy price of digital forensics, which is a basic limitation of current approaches and the necessity of privacy-saving alternatives.

Cryptographic Techniques for Privacy Preservation

Cryptographic solutions provide high potential solutions to the dilemma regarding the necessity to reconcile the conflict between the requirements of the forensic investigation and the necessity to preserve privacy. Searchable Encryption (SE) allows the searcher to query the encrypted databases with encrypted search tokens, which will only give results of the relevant records but will not decrypt the whole dataset [10]. It is a method that preserves data confidentiality and enables them to retrieve the evidentiary information in a targeted manner. There have been various SE schemes designed such as single-writer symmetric searchable encryption and multi-user with public-key encryption and keyword search (PEKS) [11]. Such methods can be modified to fit into healthcare forensics so that the investigator is able to query specific patient records, access logs, or clinical events without revealing any unrelated PHI.

Homomorphic Encryption (HE) is one more revolutionary cryptographic method of privacy-preserving digital forensics. Fully Homomorphic Encryption (FHE) is used to make computations on encrypted data and the result is also encrypted, but on decryption, it returns results that are identical to the results of the computation done to the plaintext [12]. This allows the forensic analysts to conduct necessary investigation actions, e.g. pattern recognition, statistical analysis, and timeline reconstruction, without having to touch plaintext PHI at all [13]. Although computational overhead is an issue with FHE, partial homomorphic schemes with particular operations (e.g., addition or multiplication) are a viable alternative in most forensic procedures [14]. SE/HE combination provides an excellent platform to realize a complete digital forensics and ensure the end-to-end encryption of sensitive healthcare data.

More cryptographic building blocks to privacy-preserving investigations are offered by Secure Multi-Party Computation (MPC) and Zero-Knowledge Proofs (ZKPs). MPC can be used to have a shared calculation of a function between multiple parties on their inputs without revealing these inputs [15], thus, healthcare organizations can collaborate in forensic investigations without

sharing any sensitive patient information. ZKPs have the potential to make a statement concerning behavior of one party demonstrable by another without disclosing anything except the validity of the statement itself [16], which would give investigators the ability to confirm adherence or identify abnormal behavior without access to the underlying PHI.

Threat Modeling and Privacy Frameworks

Threat modeling offers a methodical system of detecting and alleviating security and privacy hazards in digital systems. Microsoft created the STRIDE methodology that classifies threats into six categories, namely, Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [17]. Although the coverage of the security issues in STRIDE is effective, it has low coverage of threats that are privacy-based. LINDDUN framework is a threat modeling framework that introduces a privacy-related concern, which is the concept of Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance [18]. Using both the STRIDE and LINDDUN in the process of applying it to the healthcare forensic framework is bound to cover all security threats as well as privacy threats.

The NIST Privacy Framework offers a systematic method of addressing the privacy risk by five fundamental functions, namely: identify, Govern, Control, Communicate, and Protect [19]. This model can assist organizations to focus on privacy protection whilst allowing legitimate business goals, which is of specific importance to digital forensics in the healthcare field. Identify The Identify function is concerned with the awareness of the existing practices of risk management of privacy; Govern, with setting privacy cross-organizational policies; Control, with specific privacy-enhancing practices; Communicate, with establishing and practicing relevant safeguards [20]. Comparing forensic frameworks to NIST Privacy Framework will guarantee that they are in line with the best practices and regulatory standards.

The use of privacy-enhancing technologies in healthcare has been studied in a number of studies. Acar et al. [21] conducted a survey of cryptographic solutions to healthcare data protection, demonstrating that homomorphic encryption may be used in privacy-preserving analytics. Butin et al. [22] suggested a model of cryptographic systems privacy evaluation in healthcare settings. Nevertheless, research has mainly been done on general data analytics as opposed to the needs of digital forensics. Combining sophisticated cryptography with organized privacy models is an important research gap that exists today.

Synthesis and Research Gap

The literature indicates significant individual advances in cryptography tools, digital forensics approaches, and privacy models, but minimal combination of the abilities in the specified healthcare forensic studies. Current cryptographic solutions are skewed towards data analytics, a secure storage with limited consideration of the special nature of the forensic investigation needs,

including evidence storage, chain of custody, and legal admissibility. In the same way, existing digital forensic systems place more emphasis on investigative thoroughness and less emphasis on privacy protection, which poses a regulatory compliance issue in the medical setting.

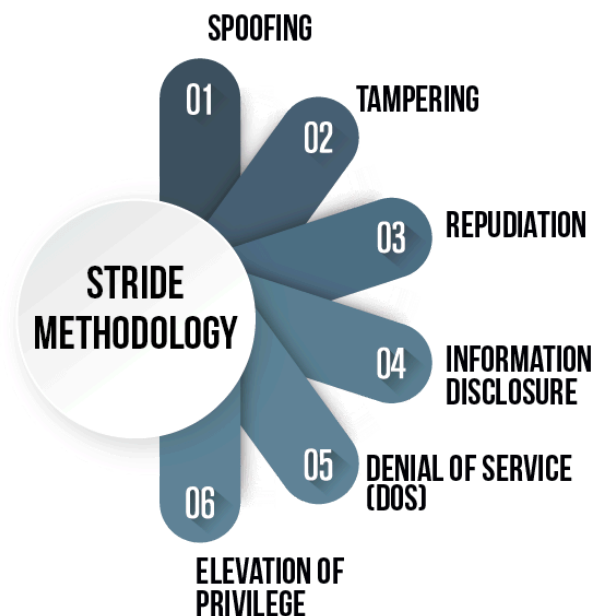
The gap in the research is in the following intersection of these areas: the creation of a holistic system that allows the successful application of digital forensics due to the use of new cryptographic tools that provide high safety in the context of patient privacy and regulatory compliance. A framework of this kind has to cover the entire forensic lifecycle, including identification and preservation of evidence, analysis and presentation of the same, and privacy by design as well. It should also offer realistic ways of striking a balance between the effectiveness of the investigations and the protection of privacy, with the understanding that utmost privacy may make forensics impossible, whereas the total openness will infringe on the regulation needs. The proposed research will fill this gap by proposing, defining, and theoretically justifying a Privacy-Preserving Healthcare Forensics (PPHF) framework combining cryptography with the known privacy frameworks to support necessary and viable digital investigation in healthcare settings.

Research Methods and Materials

Research Methods

Overview of Research Methods

The type of the research will be mixed-method (the combination of qualitative and quantitative approaches) to offer a detailed analysis of the proposed PPHF framework. The qualitative aspect will predominate and entail systematic utilization of the threat modeling principles (STRIDE, LINDDUN) and the intensified mapping of the framework on the basis of the criteria of the NIST Privacy Framework. This is critical in achieving a profound, situational comprehension of the security, privacy attributes, and compliance with regulatory qualities of the framework. This will be backed by its quantitative aspect through the power of metrics on the performance of the cryptographic operations like computational overhead, and scalability, which will give objective information on the feasibility of the cryptographic operations in the framework.



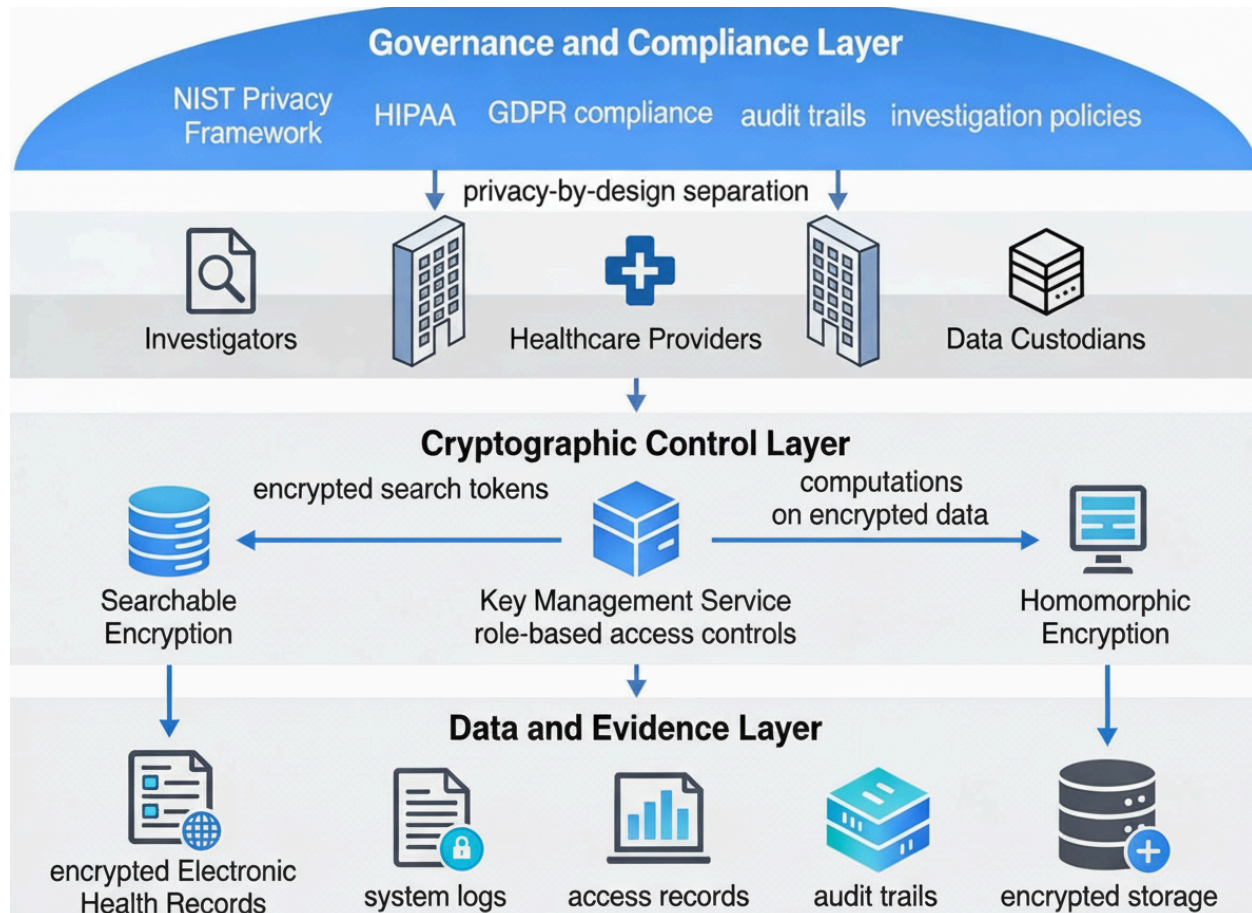
This is a mixed-methods design since the questions of the research require more than a performance benchmark; it should be a nuanced, rich insight regarding the capacity of the framework to reduce the complex threats to privacy and meet the requirements of governance. A quantitative approach would not be able to reflect the qualitative advantages and disadvantages of the security and privacy design, whereas a qualitative approach would not provide the empirical data to evaluate the computational practicability. The combination makes sure of a holistic analysis.

Research Strategy

The major research method is Conceptual Framework Development and Evaluation with a Case Study scenario in mind. The essence of the plan is the systemic development, specificity, and the theoretical support of PPHF framework. This is not a software development project as we know it where the result is a blueprint and a specification, rather than a working deployed software system. The review will be performed in the form of a detailed, hypothetical case-study, which will be placed in a realistic healthcare setting, e.g. a set of investigating a possible internal data leak of a Hospital EHR system.

This plan is suitable because it enables the strict testing of the logic and procedures of the framework in one of the controlled yet realistic settings without the ethical and logistical issues associated with gaining access to live healthcare data. It allows one to pay attention to the conceptual integrity and architectural strength of the solution prior to possible implementation. The case study gives a real-life story to follow the threat modeling and a NIST assessment to make the evaluation based on a realistic use case.

Architecture or System Design



The Privacy-Preserving Healthcare Forensics framework proposes a multi-layered architecture to end the inherent conflict between the requirements of investigation and the confidentiality of patients. The interaction between the key entities (Investigators, Healthcare Providers, and Data Custodians) is organized in this conceptual model to provide privacy by design by putting the architectural tiers between the key entities. Instead of using procedural controls, the framework integrates cryptographic enforcement rules into the forensic process to establish a systematic process in which protection of privacy is enforced technically but not just policy-driven. Such stratification guarantees that every element has certain duties to perform and that everyone is aimed at achieving the twofold goals of evidentiary integrity and regulatory compliance.

The base is the Data and Evidence Layer, which is the safe place of all possible digital evidence in the healthcare systems. This layer holds encrypted Electronic Health Records, system logs, access records and audit trails, which are kept in an encrypted state which is persistently encrypted. This layer prevents passive privacy violations that would otherwise be caused by storing all sensitive data unsecured and also retains evidence that can be used in authorized investigations. The encryption-first strategy makes it possible to guarantee that the mere existence of the forensic data cannot pose an ongoing threat to privacy, which forms a vital minimum safety of patient information, not related to a particular investigation.

The privacy-enabling layer of the core is Cryptographic Control Layer which deploys sophisticated cryptographic methods to allow investigation without the need to reveal sensitive data. This privacy layer adds Searchable Encryption, which enables investigators to upload encrypted search tokens that can be compared to records that are encrypted in place of being decrypted. At the same time, Homomorphic Encryption has made it possible to conduct computational analysis directly on the encrypted data supporting such operations as pattern recognition and statistical analysis and preserving confidentiality. These operations are coordinated by a special Key Management Service that safely manages cryptographic keys, and imposes role-based access controls that deny the ability to decrypt messages.

The framework concludes by the integrated Forensic Analysis and Governance layers that respectively facilitate the investigative work and the respect of regulatory compliance. The Forensic Analysis Layer gives investigators a mechanism to communicate with encrypted evidence, and still offers protection via cryptography during the examination process until final and relevant results are obtained. The Governance and Compliance Layer manages this whole ecosystem and incorporates principles of the existing standards, such as the NIST Privacy Framework, maintains detailed audit trails, implements investigation policies, and makes all operations legally defensible and in accordance with the healthcare laws, including HIPAA and GDPR, and thus, establishes a fully privacy-conserving forensic environment.

Data Analysis and Evaluation Methods

The assessment of the suggested framework will be conducted with the help of a multi-faceted approach, and it will start with a qualitative threat modelling analysis. The latter will entail the systematic deployment of two well-known frameworks: STRIDE and Linkability, Identifiability, and Non-compliance, LINDDUN is specifically created to detect threats to the privacy concept. The main measure of success in this measurement will be the mitigation rate- the percentage of threat types that the framework has viable and practical countermeasures. The high level of mitigation with the critical LINDDUN types of Information Disclosure and Identifiability will indicate a successful result and will demonstrate the strength of the framework to ensure patient privacy protection against a broad range of possible attacks.

The second qualitative assessment will be done by mapping the components and processes of the framework against the NIST Privacy Framework. This encompasses an examination of the alignment of the architecture to the five fundamental functions of the framework namely: Identify, Govern, Control, Communicate and Protect. The assessment will not result in a numerical value but rather, be a qualitative measure of the coverage and rationality to the NIST subcategories. Clearly and coherent mapping through all functions will be a success indicator as it will be quite visible to prove that the proposed system is essentially engineered to handle proactive privacy risk management and regulatory compliance at the ground level.

Lastly, to cover the aspect of practical feasibility, the quantitative part of the evaluation will be based on theoretical analysis of performances. Because the full software implementation is outside the scope of the project, in this analysis the computational complexity of the main cryptographic operations, including searchable encryption query and homomorphic computation overhead based on Big-O notation, will be considered. Computational complexity and asymptotic scalability are the most important measurements in this case. The findings will be critically compared with the performance characteristics of the traditional non-privacy preserving forensic operations. This comparison will explain the privacy-utility trade-off present in nature, which is the computational cost of the increased privacy, and the theoretical feasibility of using the strategy in practice in a real healthcare setting.

Materials

Details of Research Data

The proposed research will develop a Privacy-Preserving Healthcare Forensics (PPHF) model that will be theoretically justified and based on the latest cryptography methods to perform a successful digital forensic investigation in the healthcare industry and guarantee the privacy of patient data and regulatory compliance. The methodology uses a conceptual approach, which is characterized by design-science framework architecture design, formal cryptographic specification, and thorough theoretical analysis with threat modeling (STRIDE/LINDDUN) and alignment analysis with the NIST Privacy Framework. The results will be placed to be published in high-impact peer-reviewed journals, which will include the publication in IEEE Transactions on Information Forensics and Security due to its focus on security methods, the Journal of the American Medical Informatics Association (JAMIA) due to its focus on healthcare informatics, and Digital Investigation due to its focus on forensic science readers, respectively.

Software

Since this study is conceptual in nature and does not require the construction of a production system, the project will make use of a compilation of dedicated software with regard to design, modeling, and documentation. To develop the key architectural diagrams and Data Flow Diagrams (DFDs) needed in the next stage of threat modeling, the Microsoft Visio or the online

application draw.io will be used. To stringently document, organize and examine the recognized security and privacy threats, specific threat modeling tools such as the OWASP Threat Dragon or the Microsoft Threat Modeling Tool will be used. Lastly, I will attempt to write the dissertation, format and manage the citation with standard academic software, specifically, Microsoft Word or LaTeX to typeset and a reference manager such as Zotero or Mendeley to maintain consistent and accurate citation guidelines across the entire text.

Hardware Requirements

Since this is a theoretical and design-based research, no specialized equipment is necessary. Everything can be handled through the standard modern laptop or desktop computer in terms of design, documentation, and theoretical analysis. The scope of this dissertation does not require any high-performance computing resources, GPUs, or even cloud computing credits.

Expected Outcome

Anticipated Results

The major expected outcome of the study is the formulation and theoretical confirmation of an all-inclusive Privacy-Preserving Healthcare Forensics (PPHF) structure. Such a structure is likely to offer a systematic approach to carrying out digital investigations in healthcare systems as well as impose data privacy in a technical manner. In particular, it is expected that the results will be tripled. To begin with, the study will produce a specific orchestrating architectural plan, which will encompass the cryptographic controls, such as searchable and homomorphic encryption, woven into the process of digital forensics. Second, the threat modelling exercise is expected to officially show that the PPHF framework is capable of addressing a high percentage of privacy-specific threats (especially those involving information disclosure and identifiability) in comparison to the conventional methods of forensic investigations. Third, the mapping to the NIST Privacy Framework should reflect a high degree of alignment, which will serve as an excellent rationale of how the framework influences the healthcare organizations in fulfilling their ultimate privacy governance, control, and protection requirements.

Implications

The implications of this study are far-reaching both theoretically, practically, and also in policy. Theoretically, the work will enter into the growing amount of knowledge on privacy-preserving digital forensics because it offers a new model of application of advanced cryptography in the highly sensitive healthcare setting. It suggests that the paradigm needs to change to consider privacy not as a procedural challenge but as a technical limitation to the forensic process per se.

In practice, the framework provides a practical solution to healthcare organizations and practitioners in digital forensics. It may be used as a reference to create tools and procedures that allow responding to incidents and conducting internal investigations efficiently without breaking patient confidence and regulatory requirements. Its ability to offer a transparent and organized solution has the possibility of minimizing legal and reputational risks that are involved in the traditional handling of forensic data. To the broader research community, this research paper demonstrates the paramount interplay of cybersecurity, digital forensics and the law of data protection that may influence other privacy-enhancing technologies in other regulated sectors such as finance and government.

Limitations

A number of significant limitations can be applied to this research. The greatest weakness is that it is conceptual in nature. The PPHF framework will exist in theory form and will not be translated to a functional software application and implemented on a live healthcare network. As a result, the performance metrics (e.g., computational overhead, scalability with large datasets) will have an analytical complexity approach, as opposed to empirically determined benchmarks, which are unlikely to reflect all the real-world performance bottlenecks.

Moreover, the threat modelling and the NIST evaluation though systematic are subjective and useful in their nature and rely on the analysis of the author. The strength of the evaluation will be based on the completeness of the hypothetical case study and the threat scenarios that are outlined. Lastly, the suggested structure presents complexity, and it might demand specialized skills to act out, and this could be a hindrance to its uptake by smaller healthcare organizations with minimal IT capabilities. The properly applied complex cryptographic primitives and key management success of the framework in practice also depends on the proper implementation of complex cryptographic primitives and key management, which is also subject to operational challenges.

Timeline

The 12 weeks project is divided into four consecutive phases to guarantee the rational flow of the preliminary research to the end of the dissertation presentation. The schedule is realistic and allows having time to engage in analytical research and design development and documentation..

Week	Phase	Key Tasks & Milestones
1-3	Phase 1: Foundation & Problem Definition	- Conduct intensive literature review on healthcare privacy, digital forensics, and cryptographic techniques. - Finalize the problem statement, aim, and objectives. - Milestone 1: Completion of Chapters 1 & 2 (Introduction & Literature Review).
4-6	Phase 2: Framework Design & Specification	- Develop the detailed architecture of the PPHF framework. - Specify the cryptographic protocols and data flows. - Draft the Research Design and Methods chapter. - Milestone 2: Completed PPHF Framework Design & Chapter 3 Draft.
7-9	Phase 3: Evaluation & Analysis	- Perform the STRIDE and LINDDUN threat modeling analysis. - Map the framework against the NIST Privacy Framework. - Conduct the theoretical performance analysis. - Milestone 3: Comprehensive Evaluation Completed (Basis for Chapter 4).

10-12	Phase 4: Writing, Synthesis & Finalization	- Synthesize findings into the Expected Outcomes and Implications sections. - Write the Conclusion and finalize all chapters. - Perform proofreading, formatting, and compilation. - Milestone 4: Full Dissertation Draft Submission. - Final Submission.
-------	--	---

Conclusion

This research proposal aims to find the essential solution to the critical challenge of digitally forensic balance with patient privacy in healthcare creating and theoretically justifying a new Privacy-Preserving Healthcare Forensics framework in a Design Science Research approach. The sound methodology combines qualitative threat modelling and NIST Privacy Framework evaluation with quantitative theoretical analysis to determine the security, compliance, and practicability of the framework. Although restricted to conceptual validation, the study holds immense academic and practical implications by providing a well-organized avenue of performing the necessary digital investigations and, at the same time, preserving patient confidentiality in a strictly organized manner, thus offering an indispensable blueprint of securing and ensuring privacy in the healthcare sector.

References

- [1] A. Fernandez-Aleman, I. C. Senor, P. A. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541-562, 2013.
- [2] Verizon, "2020 Data Breach Investigations Report," Verizon Business, 2020.
- [3] L. J. Ponemon, "Cost of a Data Breach Report 2020," IBM Security, 2020.
- [4] I. A. Junger, "The General Data Protection Regulation and the Health Sector," *European Journal of Health Law*, vol. 25, no. 3, pp. 223-245, 2018.
- [5] D. J. Solove, "HIPAA Turns 10: Analyzing the Past, Present, and Future Impact," *Journal of American Health Information Management Association*, vol. 84, no. 4, pp. 22-28, 2013.
- [6] I. A. T. Hashem et al., "The role of big data in medical informatics: A review," *Journal of Infection and Public Health*, vol. 8, no. 3, pp. 210-220, 2015.
- [7] M. K. Rogers, J. Goldman, R. Mislán, T. Wedge, and S. Debroya, "Computer forensics field triage process model," *Journal of Digital Forensics, Security and Law*, vol. 1, no. 2, pp. 19-38, 2006.
- [8] R. Hillestad et al., "Health information technology: Can HIT lower costs and improve quality?," *RAND Health Quarterly*, vol. 5, no. 1, 2015.
- [9] K. R. B. Butler and A. D. M. Al-Sadoon, "Privacy-preserving digital forensics," *Digital Investigation*, vol. 28, pp. S114-S123, 2019.
- [10] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proceedings of IEEE Symposium on Security and Privacy*, 2000, pp. 44-55.
- [11] P. Xu, S. Tang, P. Cheng, and S. Q. Zhu, "Practical multi-keyword ranked search with access control over encrypted cloud data," *IEEE Transactions on Cloud Computing*, vol. 9, no. 2, pp. 556-568, 2021.
- [12] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the 41st annual ACM symposium on Theory of computing*, 2009, pp. 169-178.
- [13] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1-35, 2018.

- [14] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of Secure Computation*, vol. 4, no. 11, pp. 169-180, 1978.
- [15] A. C. Yao, "How to generate and exchange secrets," in *27th Annual Symposium on Foundations of Computer Science*, 1986, pp. 162-167.
- [16] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186-208, 1989.
- [17] A. Shostack, *Threat Modeling: Designing for Security*. Indianapolis, IN: John Wiley & Sons, 2014.
- [18] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering*, vol. 16, no. 1, pp. 3-32, 2011.
- [19] National Institute of Standards and Technology, "NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management," U.S. Department of Commerce, 2020.
- [20] N. A. G. Arachchilage and S. H. H. Madanayake, "A framework for privacy risk assessment in the context of big data," *IEEE Access*, vol. 9, pp. 107393-107411, 2021.
- [21] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, "A survey on homomorphic encryption schemes: Theory and implementation," *ACM Computing Surveys*, vol. 51, no. 4, pp. 1-35, 2018.
- [22] D. Butin and D. Le Metayer, "Privacy-by-design: A formal framework for the analysis of architectural choices," in *Proceedings of the 2013 ACM workshop on Privacy in the electronic society*, 2013, pp. 95-106.