FAIR: Intelligent Framework and Software Architecture for Healthcare Industry to ensure Information Assurance and Regulatory Compliance

Syeda Uzma Gardazi, Tahira Nazir and Naurin Farooq Khan

Lecturer, CS& IT Department
Women University, AJK, Bagh.

Abstract
The intricate reciprocity between technology and healthcare services demands robust software systems that can manage extensive amounts of data, and personal information and adhere to rigid regulatory standards set by the governing bodies. This research aims to develop a software framework for the US healthcare industry to ensure compliance with security, privacy regulations and standards using the latest techniques and technology. In this research we are going to propose a novel software architecture and framework (FAIR) by using Artificial Intelligence techniques and case study. The proposed framework and architecture help in audit of regulatory compliance, analyze impact of Compliance Attributes (CA) on Quality Attributes (QA) along with software architecture. The proposed framework and architecture will help the United States healthcare industry to track compliance and control unauthorized access to Health Information.

Keywords:
Artificial Intelligence (AI), Compliance, Compliance-driven Software Architecture, Privacy, Security, Regulatory Compliance automation, Software Architecture and Software Engineering, Risk and Legal Compliance

1. Introduction

With the boom of technology in all practical fields, healthcare has also seen a considerable share of technology transformation. As the technology becomes more sophisticated, the software supply chain becomes more complicated with each passing day. One of the most common problems of the majority healthcare organizations is managing a pool of healthcare data and its privacy. With the advent of new technology, the digital world is seeing an increase in data breaches which have become a constant threat to organizations across all sectors, particularly within the healthcare industry. Data breaches in a US healthcare facility is very dangerous as it contains and protects highly-sensitive patient information. For the sake of data privacy & security, ensuring compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) is essential. HIPAA sets robust guidelines to protect individual personal information from unauthorized access or disclosure. Office for Civil Rights (OCR) is another governing authority that mandates the healthcare organizations and other entities comply fully with HIPAA regulations to protect the security and privacy of personal health information. It is very crucial for healthcare organizations to review and improve the security measures to prevent such breaches. According to the HITECH Act, section 13402(e)(4), HHS OCR is obliged to publish a list of data breaches of unsecured PHI that impacts 500 or more individuals in any aspect whether financially, legally, personally or any other. This mandates the healthcare-covered organizations to report data breaches to the OCR. Reports must be submitted within 60 days of the data breach incident and discovery. Most data breach incidents are a result of multiple violations of the HIPAA Security Rule. In 2023, total healthcare data breaches reported to the OCR reached 548 and affected almost 122 million individuals by disclosing their health information. About 22 beaches of the 548 breaches reported to the OCR last year affected more than one million individuals. A total of 91 million individuals were affected across those 22 breaches. Fig. 1 is a representation of the healthcare data breaches reported to OCR that have happened in the year 2023 as a result of non-compliance to HIPAA Security Rule.

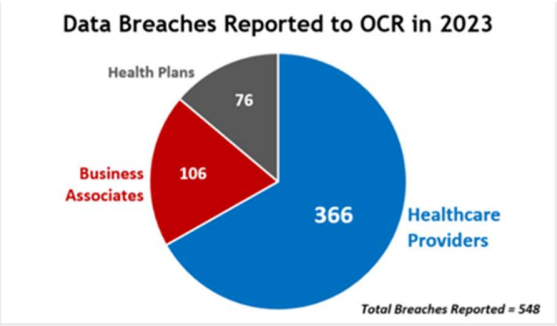

Figure 1 A complete display of data breaches reported to the OCR in 2023

Manuscript received June 5, 2025
Manuscript revised June 20, 2025
https://doi.org/10.22937/IJCSNS.2025.25.6.22

To avoid such data breach incidents, it becomes necessary to comply using emerging technologies with the data privacy regulations set by governing regulatory bodies such as HIPAA and HITECH. The Breach Notification Rule under the HIPAA mandates the covered entities and shareholders to notify immediately following the breach of unsecured Protected Health Information (PHI). As a clause of the American Recovery and Reinvestment Act of 2009, the HITECH gives guidelines for notifying individuals in the event of a breach of their unsecured PHI.

With the evolution of software systems that handle sensitive information, the need for software compliance has become increasingly essential. Software compliance not only protects against potential data breaches and cyber threats but also ensures adherence to regulatory laws and industry standards aimed specifically at protecting individuals' privacy rights. By implementing robust software compliance practices, organizations can improve their digital defenses and mitigate the risks associated with data mishandling, ultimately fostering a secure and ethically responsible digital ecosystem. In [1], it is highlighted that on May 19, 2023, the Ministry of Information Technology and Telecommunication released a Personal Data Protection Bill (PDPB). The proposed law regulates the collection, use, processing and transfer of personal data, also providing for offenses concerning the violation of data privacy rights. Similar to HIPAA and General Data Protection Regulation (GDPR), the proposed bill recommends standards for data processing (e.g., legal obligation, compliance, consent, and research). Currently, there is no approved and implemented law regulating the protection of data in Pakistan and Azad Jammu and Kashmir (AJK). Therefore, a suggestion is made to the governments of Pakistan and AJK to pass a data protection law as a proactive measure to limit the unauthorized disclosure of civilian information. The amendment would require covered entities to implement physical, administrative and technical protection. The author suggests a few improvements such that organizations should conduct periodic internal audit and monitoring. Automated log monitoring tools are suggested for use. The organizations should implement authentication requirements of Assurance Level 3 or above for remote access of confidential information and Assurance Level 1 or above for other types of access.

Author in [2] discusses the role of software architecture in regulatory compliance. He suggests that by carefully considering regulatory compliance requirements during the architectural design phase, organizations can reduce risks associated with non-compliance. He suggests during development of software architecture, there are several essential factors to keep in mind in order to make it compliant.

- *Security*: Incorporate robust security measures into the software architecture, such as access controls, encryption and secure authentication mechanisms to safeguard sensitive information.
- *Auditability*: Implement appropriate monitoring and logging features to allow organizations to capture and analyze data, enabling them to be compliant with regulations.
- *Data Governance*: Design the software architecture to align with requirements to ensure data governance practices, such as data retention and data access restrictions.
- *Scalability*: Build a scalable architecture capable of adapting to new regulatory requirements allowing organizations to stay compliant without extensive re-engineering.
- *Integration*: Design a modular architecture to support seamless integration with third-party systems by enabling secure and efficient data exchange to reach compliance.

There is a lack of work for possible technological and regulatory developments which is very concerning. The benefit of this research is that it will help highlight the need for development of an intelligent compliance-driven software using the latest AI techniques.

1.1 Basics of Software Architecture

Before diving into the discussion of software architecture, it is important to know the basics. *Standard* defines a set of recommendations, requirements, and principles that must be followed during software architecture development. A *requirement* is an indicator or barometer that must be fulfilled and that can be easily verifiable. Compliance with the standard won't be recognized if the criterion is not successfully met. A *recommendation* is a suggested choice, to take into account during the development of a project, but if not followed, compliance can still be achieved. It is not compulsory to follow a suggestion. *Principles* are mandatory guidelines that must be followed to avoid systematic faults and to achieve quality characteristics. (Source: Oxford Languages) The quality attributes of software architecture required by the standard are: i) consistency, ii) comprehensibility, iii) verifiability, iv)simplicity, v)modularity, and vi) abstraction. However, it is not always easy to interpret these guidelines into realistic solutions. So, the industry needs concrete

approaches and a strong automated to meet the criterion defined by the Standard more feasibly which evolves with time. For that purpose, the latest AI techniques seem like more suitable methods to use.

1.2 Software Architecture and Compliance from Different Aspects

In [3], the authors designed an approach such as a mobile app or a website that can be on the front-end with independent back modules and plugins. Such components could be independently installed and can evolve separately without changing the entire system software. This greatly eases healthcare access, however, the platform still needs to address challenges such as privacy/security concerns and regulatory hurdles. Authors in [4] explore the pros and cons of platform ecosystems in healthcare delivery, specifically focusing on compliance issues. Their study includes a theoretical framework focusing on electronic healthcare records, smartphones, artificial intelligence, big data, the Internet of Things, and blockchain technologies. But the researchers acknowledge possible individual biases in the selection and analysis of the study. Secondly, the study search terms were targeted at only the applications of platform ecosystems, case studies and English reports. So the data is fairly limited and does not apply globally. According to [5], during the front-end and back-end data transfer in health information exchange (HIE), a security risk exists in terms of confidentiality, authentication and access control of the data due to the limited capabilities if IoT devices are involved, as these devices do not use end-to-end encryption and decryption schemes. This poses a great threat to breach of private patient data. The healthcare industry of the United States operates according to laws containing a complex set of regulations, such as HIPAA, HITECH Act, and The Affordable Care Act (ACA), it becomes necessary to enforce rigorous pre-requisites on data privacy, security, and patient care quality which is why our work is going to contribute towards ensuring data privacy and security in compliance with international standards. In [6], the authors studied that the HITECH Act has stimulated multi-stakeholder interest in Health Information Technology (HIT). However, problems with usability and limited interoperability rose which needed to be addressed through reforms in the HITECH Act. They interviewed medical professionals from almost similar backgrounds and came up with suggestions of the need to develop a coherent national policy to promote HIE and interoperability and align policy initiatives in relation to Health Information Technology. But, with lack of diversity in the data gathered, there are concerns about the generality of findings, which is where a more general framework and policy changes are required which can be adopted in all countries over the globe. In [7], the authors highlighted the importance of data integrity to reach compliance standards in various industries. They compared two systems namely, Electronic Payment Management System (EPMS) and Order Management System (OMS) to study the data controls and how much data integrity they reached with the systems. The result of their study was that EPMS with robust coding practices focusing mainly on data security and integrity faced 90% less data breaches and malicious attacks as compared to OMS which had less secure software. Conclusion was that a proper customized framework is needed for organizations to avoid financial, legal, reputational risks along with revenue losses, penalties and bankruptcies. In order to build such a framework, certain procedures must be followed that include assessing data security risks at the beginning of the software development process. It is best to implement secure coding and testing procedures, properly navigating systems and infrastructure, and also training developers and stakeholders to assure data security and integrity. So a well-coordinated data security compliant software architecture is necessary to protect the organization from negative legal and regulatory repercussions. Comparison of the two systems namely, EPMS and OMS is shown in Fig.2.

Figure 2. Qualitative Analysis of Compliance between EPMS and OMS. Source: Scientific and Academic Publishing

In [8], the authors identify the contradiction between rate of cost-effectiveness and efficiency against the principles of confidentiality which gives rise to the ethical dilemma in the use of electronic private data. They suggest that the use of technology on one hand, reduces costs, improves clinical diagnosis and care. On the other hand, the physician is obliged to take calculated risks by trusting the machine diagnosis, this may also cause a risk of bringing harm to the patient by computer-generated clinical errors. This is where a proper framework is needed in order to navigate patients' data records and their safety while making it intelligent to reduce manual labor and time.

The US regulatory body has a rigorous set of rules and standards that must be met in relation to the transfer of electronic health information via the internet, and/or local networks. Nowadays, medical billing companies which work as backup offices in many countries such as Pakistan, face problems to maintain compliance with international standards. So, the framework suggested in this research

"FAIR", will enable the healthcare industry in sharing medical data according to compliance standards. FAIR focuses on the confidentiality, privacy, authentication and sharing of medical information. This framework is applicable for the US healthcare industry and will work as a model to follow in developing countries such as Pakistan. The implementation of the framework will be on a medical billing and transcription company namely, CareCloud. Such a framework is essential for protecting the company's corporate mission. Through thorough research, it was found that HIPAA and standards such as International Organization for Standardization (ISO)27001 and PCI Data Security Standard (version 3.0) are the most feasible components for compliance and quality assurance in order to make improvements in the software engineering processes in countries like Pakistan. By cross-mapping and identification of CA and QA between ISO 9001:2015 and ISO 27001, we can determine components that meet compliance standards. This research also suggests an improvement in the existing Pakistani Data Protection Act. This can be published as a model approach to secure data privacy within Pakistan and AJK specifically in the field of software industry, the enterprise that uses these frameworks and software architecture. This research will focus on various aspects of the FAIR framework for information assurance and regulatory compliance. This study will identify regulatory requirements and address the issues as to how the FAIR architecture will treat CA. In addition, the CA impact over QA will also be determined.

1.3 Research Area and Sub-Area for FAIR

The main research area of this study is software architecture and the sub-area is developing a software framework for Information Assurance Compliance. Fig. 3 shows the structure of the FAIR framework which uses artificial intelligence and machine learning/ deep learning along with software engineering.

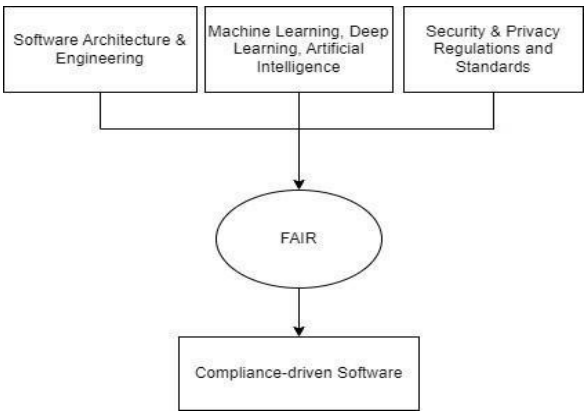

Figure 3. Research Area and Sub-area for FAIR

2. Literature Review:

Due to evolution of latest software techniques, the software architecture tends to diverge from the pre-designed models. This change makes it hard for the system to modify and maintain original goals in the long run. Still, the updates and modifications of software systems are unavoidable. Nowadays, software development happens on a global scale consuming huge amounts of software components taken from large data sets from different sources. This allows organizations to deal with challenges with the likes of traceability, manageability, auditing, adherence to policies, security vulnerabilities and usage of non-compliant features. Risks emerge when the organization fails to meet compliance with policies, industry standards and regulations, which is quite critical for not only business but also other aspects such as loss of reputation and cost of litigation. For this sake, a compliant software framework is needed with latest technological aspects to deal with the ever evolving nature of technology as well as compliance needs.

2.1 Methodology

The key elements of this framework will be Software Architecture, Machine Learning/ Deep Learning, Artificial Intelligence, Security & Privacy Regulations. By focusing on and merging these elements we will develop FAIR which is compliance-driven software for the US healthcare industry. The study will focus on a medical billing and transcription company namely Medical Transcription and Billing Company (MTBC) CareCloud. It will propose an analysis of CA & QA, and devise a framework that will help improve data confidentiality and patient rights within the healthcare industry of the United States whose backup offices are in countries like Pakistan.

The research methodology for systematic literature review for this study is based upon the works of [9]. First, research questions were formed which were then validated by the review protocol. An initial search was performed with keywords "Artificial Intelligence, Compliance-driven Software Architecture, Privacy and Compliance". The queries returned from searching these keywords were screened and identified to match relevance to the set database. After that an inclusion criteria was set and quality assessment was done. After that, the data was extracted, documented into a database, and analyzed to draw results. In the end, the results were discussed against the research questions.

2.1.1 Review Protocol:

After creating the research questions, we developed a review protocol, in which a strategy was applied for searching, selecting, including, excluding and analyzing the

literature for the study. We conducted a manual search using the terms ``Artificial Intelligence, AI in Software Architecture, Compliance-driven Software Architecture, Privacy and Compliance" to retrieve relevant studies. In order to make sure, the review includes as many relevant studies as possible within the defined search terms, we conducted a manual search in the following sources: Google Scholar, Research Gate, Public Health Records and Springer.

2.1.2 Inclusion Criteria:

To keep the literature review within the objectives created for the study, we developed a set of inclusion criteria as part of the review protocol. The final systematic literature review was based on the following criteria:

Criterion 1: Only primary studies published between 2000 and 2024 were included.

Criterion 2: Only relevant studies that relate to our research questions were included for the review.

Criterion 3: Studies, which are accessible through Google Scholar, ResearchGate, Journals, Conference Papers and the material provided by Riphah International University are considered for the review.

Criterion 4: Studies written in English are included for the review. Studies in any other language were not considered.

Criterion 5: Studies considered for the review are limited to research articles, journal publications, books, conference proceedings, and symposium proceedings. Secondary studies, presentations and reports are excluded.

2.1.3 Database:

A database was set up, to extract and record relevant literature. For this purpose, we used Microsoft Excel Sheets, to record findings. This helped in analyzing and investigating the findings easily. It also helped provide a reference for further investigations in a systematic way.

2.1.3 Exclusion Criteria

This section outlines the exclusion criteria set for systematic literature review of compliance-driven software studies employing manual frameworks or intelligent frameworks using AI techniques. These criteria are curated to ensure the selection of relevant and high-quality studies for analysis.

- Studies not published between the time frame of 2000 and 2024.
- Studies not written in English.
- Studies that are not peer-reviewed.
- Studies not focusing on compliance-driven software development or testing.
- Studies not mentioning usage of AI techniques for compliance purposes.
- Studies with unclear methodologies or findings.

2.2 Discussion

Many practical fields rely heavily on software to automate almost all operations. So, the use of software and software services becomes unavoidable in many industries. This requirement of software evolution demands robust and latest techniques to keep up with ever evolving needs. This has a negative impact on software quality as more focus is made on making the software state-of-the-art and less focus is on making it compliant according to industry requirements.

In [10], the authors performed a survey to understand the challenges in developing Software Architecture Design (SAD) in compliance with the ISO 26262. They proposed a documentation template aiming at overcoming the challenges. They suggested a correct documentation under different views such as functional and logical views, can contribute to the system comprehension and management of the software architecture design. However, the authors admit that their approach lacks the use of AI techniques for the automated verification of safety design principles. So, with our proposed framework we are going to provide the healthcare industry with a concrete and adaptable approach to meet the criterion defined by the Standard more feasible owing to the ever-evolving nature of AI and its techniques.

Authors of [11] discuss that in order to safeguard sensitive data used in healthcare systems, it is necessary to implement appropriate policies and practices. They introduced a framework which involves establishing access controls to limit access and usage of the data and implementing robust security measures to prevent unauthorized access. Their framework highlighted the need to use data anonymization procedures using latest AI techniques, whereby identities or personally identifiable information are either removed or masked to protect individuals' privacy. Encryption techniques are also highlighted to ensure the confidentiality of data during storage and transmission. However, they note that new challenges in AI security and privacy are constantly evolving. So to keep up with emerging insights, researching and developing solutions using the latest AI techniques is crucial.

To address this need for making software compliant and making data privacy the ultimate goal, authors of [12] expound upon a process called Semantic Parameterization previously used to derive rights and obligations from privacy goals. They apply the process to the Privacy Rule from HIPAA and present the methodology for extracting and prioritizing rights from regulations and show how semantic models can be used to clarify ambiguities through focused elicitation and to balance rights with obligations.

The authors of [13] present an approach that draws regulations as compliance arguments in a principled way based on architectural requirements and decisions. The approach employs "Semantic Parameterization" for modeling regulations and the "Goal Structuring Notation" for arguing compliance. This approach is applied to the architecture of a telemedicine company named Net4Care and checked against EU regulations. After applying the framework twice, the authors extracted 96 rights, 86 obligations, and 312 constraints from the database of Net4Care. Resulting in declaration of non-compliance of the company software. There are still some limitations to the framework. One is that the framework requires extensive identification and mapping for development of the compliance arguments and architectural elements. This requires time and effort. Secondly, there is a risk of bias involved if the mapping is done by the member of the company which is being analyzed. So a third-party reviewer is necessary for the unbiased mapping without errors. This is not an intelligent approach and asks for more latest techniques.

The authors of [14] propose an architecture $\phi comp$, for compliance monitoring and mitigating non-compliance in sensitive health data information systems at runtime. It is composed of a distributed architecture which closely analyzes e-health environments and enforces security rules to ensure compliance with international regulations such as HDS and HIPAA. The architecture first monitors the data and categorizes it into three security risk levels namely green, orange, and red which represent respectively, a compliant feature, a potential threat, and a non-compliant feature. ϕcomp efficiently computes security risks at runtime based on the monitoring data reported. The compliance of the system is then evaluated with respect to the computed risk. After a series of steps the data and identified risks are evaluated by an Analyser which is developed in Python. The Analyser evaluates the risk to determine whether the environment is compliant and then determines actions to minimize the in case of non-compliance. The study showed graphical representation of the working of the architecture but it has limited practical experience due to the ever-evolving nature of intelligent technology. Which is why we are proposing an AI-driven intelligence as well as a manual approach to track software compliance.

The authors in [15] discuss and compare Architecture Compliance Checking (ACC) which is a method for verifying if implemented program code adheres to high-level architectural design models. This method aims to ensure that the system's actual structure aligns with its intended design. The authors compare eight commercial and non-commercial tools that support ACC. They analyzed the tools' capabilities, limitations, and the datasets they use. Their study focused on three types of tools: a) common types of modules and their semantics; b) common types of rules; and c) inconsistency prevention within the defined architecture. They concluded the study that the tested tools provided useful support for ACC, but there is still room for improvement. Solutions need to be found to reduce the gap between documented modular architectures in software architecture documents on one side, and module and rule models in ACC-tools on the other side. Limitations of their study include limited support for complex architectural models, difficulty in handling dynamic architectures, and scalability issues for large codebases. This is where an intelligent software architecture is needed which is developed with the latest AI techniques.

Audits are an important part of compliance requirements globally. Periodic audits of firms help identify breach of potential regulations and laws. If an organization fails an audit, it means it is lacking data security. To make audits more efficient we need softwares that eases the manual labor and saves time. In [16], the authors proposed an approach for automated audits in a software system, which involved processing of log data represented as trees. Through this approach, the results showed more efficient audit through analysis of the theoretical complexity and runtime figures. But their suggested framework needs to be implemented and tested with real datasets, showing the adequacy of the pruning method in practical systems. Also there is a lack of flexible variable handling in XSLT which was used in the algorithm. So a choice of other languages are needed for better audit results, which we will propose by introducing the latest AI techniques.

The survey in [17] presents the challenges of security and privacy in big data along with its application in the healthcare industry. They evaluate the emergence of data privacy and security issues in big healthcare data. Methods like data anonymization and encryption are discussed with their pros and cons. Privacy preserving methods such as identity based anonymization are discussed as well for privacy protection concerns. However, it is difficult to combine privacy protection, big data techniques and data anonymization to analyze data while protecting personal identity. This is where we fill the gap

with AI techniques to preserve data privacy and security in the healthcare industry

IT practices have become significant due to many factors, such as management of outsourcing and acquisition of services,the selection of service providers and increasingly complex IT risks such as security issues in networks and cloud computing. By conducting comprehensive analysis of literature, case studies, and regulatory frameworks, authors in [18] provide insights into cloud adoption in healthcare and state that scalability and computational power of cloud-based infrastructure make it an ideal platform for running sophisticated analytics algorithms in the US healthcare industry. However, compliance with regulatory requirements, such as HIPAA, adds a layer of complexity to cloud adoption with issues like interoperability and data portability that may arise when integrating cloud-based systems with existing healthcare IT infrastructure. Healthcare organizations must prioritize data security and privacy measures, such as encryption, access control and audits, to mitigate risks with cloud computing by using the latest AI techniques which is the need of the hour.

Security and legislation compliance allows the regulation of IT services, which includes implementation of effective management structures and optimum practices for monitoring and improving critical IT solutions. As healthcare data is becoming interconnected and digitized, implementing sturdy cybersecurity measures and ensuring they comply with the regulations is essential. So, it is necessary that an organization follow ISMS standards such as ISO27001 to effectively counter the threat to data compliance. In case of non-compliance to this, the organization may face penalty and six-year data detention according to the HITECH Act. Authors in [19] suggested a framework designed to derive an integrated solution to overcome an organization's technical barriers and difficulties in complying with an ISMS standard (ISO 27001). This framework, called Integrated Solution Framework (ISF), helps organizations map the assessment issues and clauses of ISO 27001 and acts as a measurement tool for assessing the information security compliance level of organizations toward ISO 27001. But there are limitations that need to be addressed in this. Firstly, they only studied organizations bound with the pre determinant security cultures that may make the findings limited on a global scale. So we need a more globally adaptive framework with the latest AI techniques to automate software adherence to compliance regulations.

The effectiveness of IT services is because of the adoption of quality management standards and the adoption of tested Internet Protocol (IP) management standards i.e. ISO 17799, and ISO 9001. An organization using the framework and software architecture for provision of services is responsible for risks and control, which include security, confidentiality. Linking to this, authors of [20] created an initial framework by accelerating the translation of principles into software requirements, improving the quality of software development, and avoiding misinterpretations. Their framework focuses on the principles of Privacy-By-Design and Privacy-By-Default. However, several aspects must be further developed to provide stakeholders with a more concrete and broader methodological toolkit which can help developers to implement more user-centric software requirements, even if they lack expertise in Human Computer Interaction (HCI), as the proposed mapping guides the most effective HCI solutions for different stages of software development.

We will be using AI in the proposed intelligent framework as it has seen the latest technological advances in recent times. The basic idea behind using AI in our proposed framework is to enable computers to learn patterns from data and evolve its algorithm according to it. We will be integrating AI techniques into software architecture as it requires careful consideration and adherence to regulatory standards. Authors of [21] argue that the emergence of AI technologies such as Machine Learning, Robotic Process Automation (RPA) and Natural Language Processing (NLP) makes it feasible to conduct automated compliance assessments. They discuss RPA bots that automatically perform routine operations such as collecting information from various resources, creating a report, and sorting documents. However, without clear mandates set by policymakers, accompanied by ethical frameworks, the software development process will lead to untoward consequences implementing AI techniques. This is where we will work to develop a framework for making intelligent compliance-driven software.

The authors in [22] discuss the development of an AI-driven intelligent system in SDLC. They also identified the risk factors in light of Dervin's theory. They discuss various AI-SDLC models and propose a new model that presents the foundation of AI-SDLC. According to Dervin theory about sense making methodology (SMM), the term *sense making* defines the process of constructing meaning and understanding from complex information followed by the rise of new research fields and information science. Their approach begins with the first phase of planning. Then, the risk process starts from the requirement analysis and goes to the end of each phase. Risks are assessed by various steps: risk identification, qualitative or quantitative analysis, risk response planning and implementation, and risk monitoring. And then in the analysis phase, requirements are specified by a business analyst. This phase requires an ML technician to identify the collected features that will be considered for the end result. But this is purely

a theoretical approach and lacks practical application. The authors acknowledge that the scope of their study is limited to providing a general framework that does not delve into specific technical details or address potential risks. Also they assert that there is a lack of literature that discusses the correlation among three fields: artificial intelligence, software development life cycle and risk management.

The authors in [23] provide a comprehensive analysis of how AI is being integrated into various stages of the SDLC process. They explore the potential benefits and challenges associated with AI adoption, providing insights into areas like requirements engineering, coding, design, testing, development and maintenance. They further discuss the various AI tools used in the SDLC lately such as Machine Learning, Deep Learning with various approaches like Morphological-Rank-Linear Hybrid Intelligent Design (MRLHID), by using a Modified Genetic Algorithm (MGA) and The Least Mean Squares (LMS) algorithm. However, there is a research gap as there is no discussion on use of AI in software architecture which is the focus of our study.

In [24], authors studied the compliance challenges of using Mobile Machine Learning (MML) algorithms in Software as Medical Devices (SaMD) in the US and European industries. They authored a framework making SaMD more compliant. Their framework has categories based on (i)*the significance of the information provided by the SaMD to a health care decision(informing clinical management, to help treat, or diagnose)* and (ii) *the state of healthcare situation or condition(non-serious and critical both)*. But, such devices have a 'locked' algorithm so these are unable to 'evolve' or upgrade accordingly. This is something of a challenge for a SaMD. This is why we will be developing a framework for making intelligent compliance-driven software which can be adapted across all platforms through the latest AI techniques.

Authors of [25] created a framework called Databricks AI Security Framework (DASF) which deals with the risks associated with the integration of AI on a global scale. It is designed to work between different sectors i.e. business, IT, data, AI and security teams, involved throughout the development and integration of AI into the software. This framework provides insights into how AI impacts system security, implementing security engineering tactics, and offering a comprehensive guide for navigating the compliance of the AI into the system. As much as it is a useful framework to navigate AI algorithms, it does not explicitly address limitations of abstract data sets. Such limitations may include issues with data quality, data including diverse groups, bias etc, which can impact the effectiveness and fairness of AI models.

The authors in [26] present a literature review of tools and methods for intelligent predictive maintenance models in the Industry 4.0 by categorizing the life cycle of software maintenance projects. The latest technological advancements have led to development of connectivity, data, new sophisticated devices, customization and controlled production; this phase is called Industry 4.0. With technology like Big Data, IoT, Cloud computing and AI, there are benefits as well as risks involved. To maximize the benefits and minimize the risks, the authors introduce predictive maintenance (PdM) that are AI-driven intelligent software frameworks. The PdM is well-suited for the ever-evolving nature of technology however there are still limitations. These include the need for large amounts of data, the complexity of model development, and the potential for inaccurate predictions. Additionally, the integration of PdM into existing systems can be challenging.

In [27], authors proposed a model that uses different integration techniques with functionalities as defined in the common data interface (CDI) layer. They suggest a novel method for a unified access to health information in the healthcare ecosystem using ML/DL. They propose a unique CDI layer that fits the existing system architecture to adapt the data standards to achieve interoperability, however, the proposed framework will be completely interoperable only when laboratories collaborate fully with clinical providers to adopt and use standardized terminologies and vocabularies. The limitation of this framework is difficulty in incorporating standard vocabularies to CDI layer functionality. This is why we will provide a more proactive framework to be able to adapt and automate with AI techniques.

In [28], authors suggest a solution for analyzing, monitoring and follow-up of compliance in the cloud infrastructure. They present text classification methodologies to comply with regulatory requirements and controls against a common hierarchy. The results indicate that mapping a given security requirement to a common hierarchy with an F-score of 88% can be achieved. But there are limitations to their study as they focus only on mapping the regulatory requirements. Their study does not provide a solution for parsing the relevant regulatory documents/specifications or even identify any configurable parameters and their values to reach compliance. Also their study is limited to regulations of the National Institute of Standards and Technology (NIST) and not HIPAA which is the focus of our research.

The paper [29] explains the concept of HIPAA compliance in cloud computing. Cloud computing challenges certain parts of HIPAA Security requirements. The authors describe cyber warfare as a premise to enforce

the reasons for complying with government regulations for information systems. They propose that the NIST Computer Security Division suggest a six-step process for increasing the software security. i) Categorize Information Systems ii) Select Security Controls iii) Implement Security Controls iv) Assess Security Controls v) Authorize Information System and vi) Monitor Security State. However, this study lacks in providing solutions for latest compliance issues in cloud computing and other technology. This leaves room for our research.

In [30], authors proposed a neural network, the DigiComp system, which is tailored to specific compliance requirements based on customer needs. It focuses on incorporating vendor management, compliance management (including sanctions screening), and risk assessment using machine learning. The risk assessment framework of DigiComp utilized machine learning algorithms, particularly Artificial Neural Networks, to predict the future state of entities based on their compliance with regulations and policies. However, challenges arose in preparing the data for neural network training, such as feature selection and normalization, particularly when real data is scarce. Another challenge is the choice and design of appropriate strategies, which is why we will be using the latest AI techniques to overcome these challenges.

In [31], the authors propose a framework that regulators can use to show the performance of regulations through modeling and evaluating them against compliance requirements. The Regulator-Oriented Regulatory Intelligence Framework (RORIF) uses a regulatory intelligence approach that involves the use of data of existing Business Intelligence and analytical tools. It distinguishes between policy objectives and regulatory decisions that contribute to achieving these objectives. However there are threats that can influence the design, implementation, and evaluation of the framework. Most significant threat is construct validity, which reflects whether the constructs (performance of regulations, and the maturity level of regulators) that are proposed in the framework are actually valid or not. The internal relationships of the regulations may also pose a threat to the framework due to ever-evolving compliance requirements. Therefore, a more proactive framework is required to automate the compliance rate of software systems using the latest AI techniques in case the manual framework does not provide successful compliance results.

Authors of [32] explore the use of artificial intelligence (AI) in information security, highlighting the advantages and challenges associated with it. They argue that AI can improve security outcomes in a variety of ways, such as by automating responses to threats, detecting anomalies and providing real-time insights into security events. They discuss traditional rule-based security systems, which rely on predefined rules to identify and respond to security threats, but have several limitations that make them less effective in today's complex IT environments. One limitation is their inability to adapt to the latest evolving cyber threats. Rule-based systems are only effective at identifying threats that match the predefined rules. The study they propose mentions the advantages and disadvantages of AI but fails to provide solutions for the tackling of those disadvantages. This is where our research will play a part where we will provide a framework with the latest AI techniques to tackle limitations and make software more compliance-friendly.

Authors of [33] discuss the widespread use of AI in healthcare, which involves handling highly-sensitive health information as well as other personal data. To address privacy issues, they proposed various AI model-based privacy protection techniques:

- ***Federated learning:*** Distributing learning across multiple clients to develop a model while maintaining data confidentiality.
- ***Differential privacy:*** Adding randomness or noise to sensitive data to conceal individual contributions.
- ***Cryptographic techniques:*** Encrypting data before training and testing, using methods like Secure Multi-Party Computation (SMPC) or Homomorphic Encryption (HE).
- ***Hybrid Privacy-Preserving Techniques:*** Combining different methods to ensure data security in the biomedical domain.

These approaches aim to mitigate privacy risks associated with AI in healthcare while enabling the advancement of technology in the field. But there are still limitations in such techniques as dealing with personal data involves removing identifiers to reach compliance can be rendered redundant if such data can be re-identified through triangulation with other identifiable data sets. This marks a need for a more global approach to share private data without compromising compliance.

As in [34], authors suggest that AI-algorithms trained with biases in sample selection of data typically fail when practically used in settings different from those in which the trained data were acquired. Therefore, large datasets that are way more diverse and representative (of the heterogeneity of identifiers like gender, ethnicity and geography of the individuals or patients) are necessary to develop and refine best practices in evidence-based medicine involving the latest AI techniques.

In [35], authors present a machine learning approach to modeling compliance. Their key innovations are i) use of active learning- a semi-supervised system capable of learning interactively from the domain expert to identify regulations and ii) informing the feature representation of the active learner based on domain-specific entities and relations to effectively build a domain model of regulations. Results of their approach show that the system reduces the burden on domain experts to a large extent, enabling steps in compliance easier by the use of the proposed model. However, this paper focuses on merely identifying the rules. They do not classify the rules into various provision classes, nor provide any mechanism for transforming text of identified rules into a formal specification. Therefore we need an AI approach which we can use to identify elements of non-compliance in a system and transform them into formal specifications.

In [36], authors explored various techniques like infrastructure-as-code, continuous monitoring, AIOps, and machine learning-powered automation to reach compliance with software. By proposing an end-to-end AI-driven DevOps framework encompassing technology capabilities tailored to healthcare industry needs, they suggested solutions and identified challenges in AI-driven software adoption in healthcare such as lack of robust security and compliance adherence which may expose sensitive patient data to breaches.

Authors of [37] developed an algorithm with machine learning techniques that predict and pinpoint the activities of physicians who are most likely to not complete their documentation in the EHR database. For data analysis of their study a software called Orange was used, which is a component-based visual programming software. The machine learning algorithm alerts the health information management department at the point of a patient's admission that a particular treating physician has a probability of not completing their clinical documentation in the EHR database, which may pose an issue for the regulatory compliance of a healthcare organization. However, their study has limitations such as lack of variables for data evaluation. This provides a research opportunity for software developers to compose an approach with a wider range of variables using latest AI techniques.

Authors of [38] proposed a study to design and test a tool for predicting information security non-compliance rate. The approach provides a roadmap for converting SEM-validated theoretical models into practical ML applications. The results suggest that a short set of survey items drawn from previous queries can provide promising non-compliance prediction accuracy. However, this is not the case when dealing with large data sets containing diverse data.

A theoretical framework is designed and discussed in [39], which helps enable and monitor data supply chain through a document-based approach. The authors proposed a formal approach to verify GDPR compliance of privacy policies using natural language processing (NLP) techniques to automatically extract information from data supply chain documents. The results showed the approach outperforms local classifiers and enables the extraction of fine-grained information. But still, research is needed to implement the framework in a multi document setting, where data processing activities are explained in multiple documents. There is also a need for an approach of data protection to automate compliance checking tasks.

Another major threat to software compliance are threats of data breaches. Majority of healthcare data breaches are due to mistakes and security lapses. Recently the Change Healthcare data breach incident rocked the IT industry. In February 2024, Change Healthcare, owned by UnitedHealth Group, became a target of a cyber attack that impacted the nation's healthcare system significantly. The group ALPHV/BlackCat claimed responsibility for the cyber attack and demanded a hefty $22 billion ransom amount, which Change Healthcare reportedly paid in bitcoins. The ransomware group claimed to exfiltrate 6 TB of data from the archives of Change Healthcare, through tactics like brute-force attacks against Active Directory and gaining access by Microsoft's remote desktop protocol. This greatly impacted the financial transactions of pharmacists, hospitals, physicians and other healthcare providers. Stakeholders of the company filed class action lawsuits against Change Healthcare, alleging that the company failed to take robust security measures to protect their data.

Compliance to the privacy standards set by governing authorities help avoid cyber security risks providing protection against potential financial and legal consequences. The international standard for information security ISO/IEC 27001 provides a robust framework to organizations as a guideline to manage compliance and information security risks. Adherence to its guidelines can strengthen the defenses of organizations against cyber threats while working in developed countries like Pakistan and AJK etc.

Authors of [40] examine the data breach incidents and its implications between business partners, storage facilities, covered entities,and the affected population. They propose a theoretical concept which would help in guiding the research work on software development regarding data breaches, identity theft, entry errors and medical record exposure. However, one major limitation of the study is misreporting of covered entities by the managers to the Department of Health & Human Services (DHHS).

Misreporting of the time frame and type of stored facilities affected are a challenge which makes it difficult to track data breach incidents. So with automated logins, robust security measures, network access verifications and two-factor authentications using current AI techniques is the need of the hour.

In [41], there is a discussion about the privacy dilemma of using machine learning and its exploitation. The authors suggest a combination of a network of convolutional neural networks and a different secure privacy approach to improve the accuracy of classification of various algorithms that safeguard privacy. Experimental results showed the need to balance training data sets' privacy protection and availability by examining the original data. Although there is a risk of lack of categorization accuracy which may lead to information leakage. So other state-of-the-art AI techniques can be employed to ensure data privacy and security in the software development process.

Authors of [42] study the application of AI methods to the risk management fields of market risk, credit risk, organizational risk. An ambitious image of AI's position in risk management is presented using data mining techniques, but limitations are also defined as some restrictions in effective data management practices, and accountability. The study only discusses financial aspects of risk in an organization. There is a lack of discussion of legal, ethical and functional risk which makes room for our research.

In total, these evaluations provide useful insights to guide software architects and developers to deploy systems that can account for more empirical or technical solutions to avoid compliance risks.

2.1 Research Gap

Information security compliance at software architecture was identified after reviewing the findings from background and challenges from related research. This research will devise and review regulatory compliance systems to enhance compliance rate of US healthcare companies with backup offices in Pakistan and AJK. This research will use AI techniques in improving software systems to identify the possible benefits and challenges from previous studies and a real world case study. For the prediction of compliance and non-compliance, we will compare and implement manual software framework and intelligent software framework using AI techniques on the EHR dataset. The proposed model will be useful to adopt for the US healthcare industry and also aid in creating an impact in the software industries and US healthcare industry with backup office(s) in countries like Pakistan and AJK.

2.2 Problem statement

Global compliance is governed by appropriate information security conventions called HIPAA. Countries such as the United States (US) and the European Union (EU) have well-established supervisory and standard necessities to exchange information internally or externally. The National Assembly Standing Committee has declared a cybercrime bill on information technology which is an international perspective of data protection but this particular thesis, considering the necessity of data protection in Pakistan and AJK, will provide solutions and amendments in the existing Pakistani Data Protection Act 2005. As of now, medical billing companies with working backup offices in countries like Pakistan and AJK dealing with US healthcare data, are facing considerable issues to reach compliance with international regulations and standards. Therefore, this research attempts to provide a framework named “FAIR” that will improve the transactions of US medical information with the software industry. FAIR will predict and ensure compliance to medical billing according to US regulations and standards. This framework will have a potential to be adopted in developing countries like Pakistan and AJK which deals with US healthcare data. The framework will be validated by implementing it on the software of a medical billing and transcription company. This framework will prove to be a tool of sustainable growth and will help in protecting the company's interests while realizing its corporate mission.

This can be published as a proactive approach to secure US healthcare data within Pakistan and AJK specifically in the arena of software industry, the enterprise that uses frameworks and software architecture within Pakistan and AJK. Consequently, a new approach to embodying the compliance of software architecture to bridge the gap between Software Engineering and Compliance will be the theme of this study and thesis.

2.3 Data Set

The data set for the research will include various attributes related to healthcare facilities, patient information belonging to US healthcare data and regulatory compliance. Multiple attributes of the patient information will be considered such as Age, patient ID, gender, insurance type, diagnosis history. The dataset will be used to analyze patterns of compliance and non-compliance across regulatory areas and US healthcare facilities. It will also help identify factors associated with compliance and we will provide strategies to improve overall fulfillment of healthcare regulations and standards using the latest AI techniques.

2.4 Research questions and objectives

The aim of this study is to formulate a framework and architecture which is called FAIR. It will assist the US healthcare industry with backup office(s) in Pakistan and AJK, in tracking compliance with international security regulations and standards. Following research objectives (research questions) have been designed by following the research model:

1. What are the technical considerations involved in identifying and extracting requirements needed for the development of manual compliance-driven software architecture and intelligent compliance-driven software architecture?

2. What factors are involved in identifying CA and QA for intelligent compliance-driven software architecture and manual software architecture for regulatory compliance and information assurance?

3. What impacts does our proposed manual and intelligent FAIR have on the Software Development life cycle (SDLC) Phases and which version of the framework returns the highest compliance results?

Research Methods: Different research methods will be applied to answer above identified research questions e.g. Systematic Literature Review, Case Study, will be used as data collection tools.

2.6 Methods and challenges

The above questions are established to support the overall aim of the study which is important as it tends to contribute towards the development of a proactive framework and software architecture that reflects information assurance and regulatory compliance. In accordance with the research objectives mentioned in the above section, the researcher is proposing a framework called FAIR. The aim behind the formulation of FAIR is to assist the software house and US healthcare industry with backup office(s) in Pakistan and AJK, in maintaining their records in line with the international standards and regulations. Hence, compliance to the regulatory bodies around the world monitoring the use of software and their architectures at programming development level is targeted. The objectives are established by reviewing the prerequisites after distinguishing the prioritization of necessities. According to our proposition, QA has been obtained from the requirements that are not the administrative and compliance prerequisites. QAs determine the engineering or the formulation of a product by establishing the choices. The process will include implementing the manual framework shown in Fig. 4 first, and then implementing the intelligent FAIR after that. Results from both versions of the FAIR will be analyzed and conclude the use of either framework based on the higher compliance of the software.

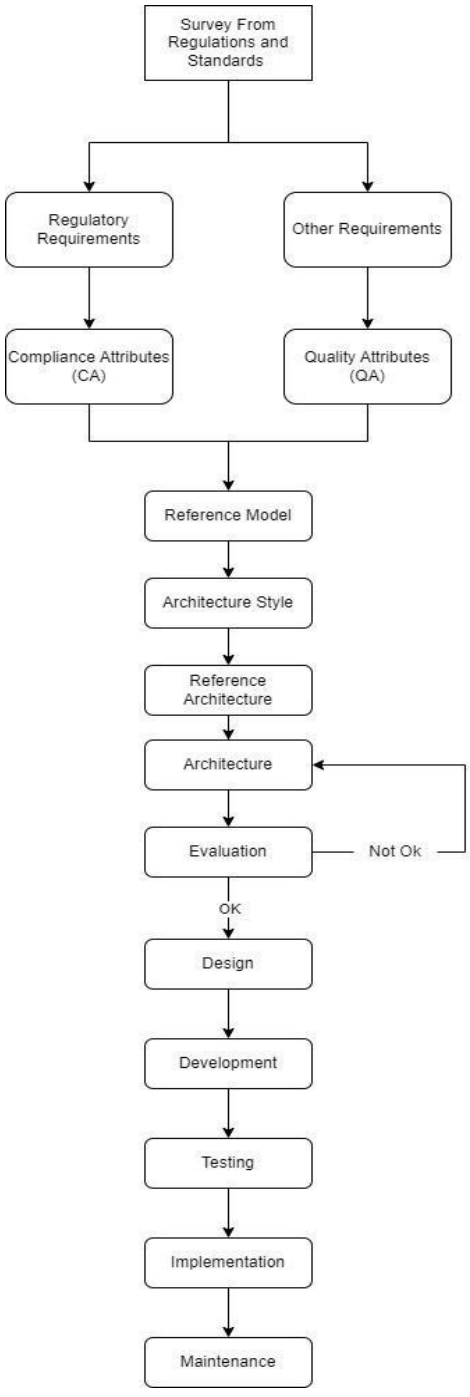

Figure 4. Manual FAIR Research Process

2.6.1 Challenges

Compliance-driven software to identify and track compliance and non-compliance through machine learning is still a big challenge and data collection of compliance and non-compliance is a major concern. In this research, we are going to develop a compliance-driven software especially focusing at software architecture level by comparing and implementing the manual approach as well as the intelligent approach using the latest AI technique(s).

3. Description of proposed research methodology

For the formulation of FAIR, the following steps will be followed:

1. A detailed systematic literature review (SLR) will be conducted to understand the previous works and get a better grasp on the topic.
2. Requirements will be curated after careful literature review and will be classified into the following categories:
    - o Functional Requirements
    - o Non-Functional Requirements
    - o Regulatory Requirements
3. Pattern styles will be formulated based upon the QA defined after step 2.
4. The combination of Functional Requirements and CA will lead to formulation of a reference model.
5. Reference Architecture will be formed after analyzing results from step 3 and 4.
6. FAIR Architecture will be designed at the next level.
7. After this, Architecture will be analyzed for compliance. In case, the evaluation of the Architecture does not return satisfactory compliance results, it will be redesigned till it reaches compliance approved benchmark.
8. The authors will collect EHR data sets and then apply the manual approach as well as intelligent approach using the latest AI techniques which is shown in Fig. 5, to predict compliance and non-compliance.

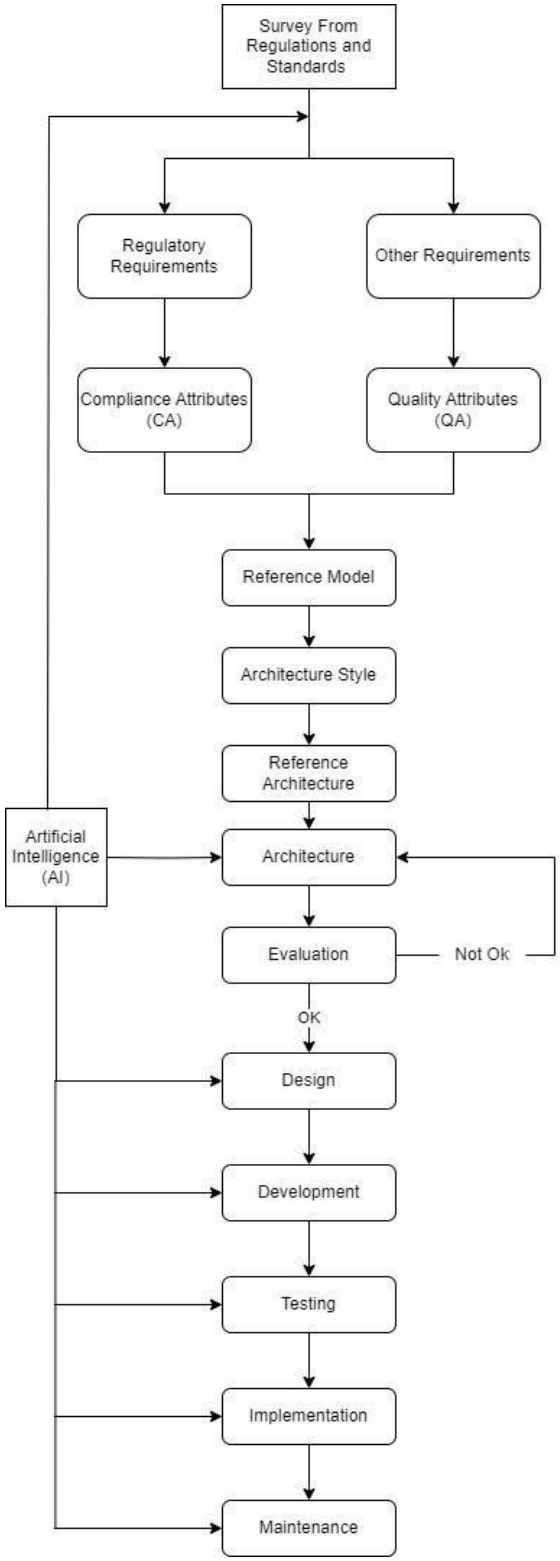

Figure 5. Intelligent FAIR Process

3.1 Limitations

This thesis will be focusing only on US security/privacy regulations and standards àccording to Health Industry e.g. HIPAA, National Institute of Standards and Technology (NIST), HITECH, Information Technology Infrastructure Library (ITIL), Office of Inspector General (OIG) and ISO 27001 and ISO 9001.

3.2 Delimitations

The security and privacy guidelines of countries other than the US will not be considered for this study, in order to maintain quality of work and results.

4 Results Achieved Till Now

4.1 A Detailed Survey of Software Architecture and Its Usage in Software Industry of Pakistan

The focus of this research is on FAIR and its usage in the Software Industry of Pakistan and AJK, so previously, a detailed survey was done and its results were discussed in a paper published in IEEE ICET 2009 as discussed in [43]. The survey described the development and usage of Software Architecture in the Pakistani software industry. The conclusion was that the Pakistani software industry needs revolutionary steps for improvement since the software projects failure rate is high due to non-compliance of software architecture. The survey is limited to Pakistan only and was done in 2009, but our paper will provide a solution and verification of the FAIR in the Software Industry of Pakistan and AJK with latest AI techniques. Further the article in [44] provides guidelines for e-court systems within Pakistan.

Suggestions are made to the judicial system considering information security-related practices to accommodate e-court requirements in Pakistan and AJK in [45].

4.2 Identification of Motivational Factors in Software Project Management and Software Architecture

A generalized survey is done in [46] which shows identification of motivational factors affecting software architects and software project managers. This will be used as a reference in the PhD dissertation research to show the research gap between 2009 and 2024. The research will provide information to the Software Industry of Pakistan and AJK to adopt FAIR during the software architecture process.

4.3 Email System Architecture for HITECH Compliance

The paper in [47] proposes a guideline for the healthcare industry following regulations set by HIPAA. Two computing models named “genetic algorithm compliance model” and “user behavior prediction model” are suggested to the Electronic Protected Health Information (E-PHI) in order to guard against unauthorized access. However, this study was done in 2010 and since then, technology and the regulatory requirements have advanced immensely. So, this research will be used as a guideline and we will provide solutions with the latest techniques for HITECH compliance which will be adopted in Pakistan and AJK.

4.4 HIPAA and QMS Based Architectural Requirements to work with the OCR audit program

By Comparing two standards, HIPAA and ISO9001, the author in [48] offers a proactive approach that can be adopted by US healthcare facilities with backup office(s) in Pakistan to achieve compliance. A case study was done on a US Healthcare IT Company (UHITC) with a backup office in Pakistan. The existing protocol of UHITC was examined and analyzed to know the level of probability of being tailored to HIPAA compliance. CA were derived from the comparison and those were classified on the basis of architectural and non-architectural nature. As this study was done in 2012, there is a significant gap of research till now which we will be addressing in our thesis.

4.5 Combining Compliance Patterns and Quality Management System (QMS) Framework to Improve Medical Billing Compliance

The research in [49] suggests that US medical companies can implement the ISO 9001 framework to reach compliance with the OIG billing regulations. This highlighted the importance of developing compliance patterns for the US healthcare industry. A case study of a third-party US Medical Billing Company (MBC) with a backup office in Pakistan was done to assess the impact of the framework. By implementing the suggested framework, the company showed an increase in customer satisfaction level from 72 percent to 84 percent. However, the study lacks the solutions to automate the mapping and identification of components for achieving compliance using latest techniques.

4.6 Billing Compliance Assurance Architecture for Healthcare Industry (BCAHI)

The paper in [50] aims at developing medical billing guidelines for software system architectures for the US healthcare industry to meet compliance with HIPAA,

HITECH and OIG. "BCAHI" aims to help the US healthcare industry to reach high levels of compliance with OIG third-party medical billing regulations by improving software architecture. This proposed architecture was evaluated through a case study from the US healthcare industry. This study was done in 2011 and we will address this gap in our research work with recommendations of the latest AI, techniques.

4.7 Compliance-driven Software Architecture (CSA) for the US Healthcare Industry

A combination of a set of US security regulations i.e. Health Insurance Portability and Accountability Act (HIPAA) and non-functional requirements were used to develop software architecture for EHR and/or Health Level Seven (HL7) in [51]. A layer of compliance was established in an existing system that helps software companies to track compliance at the software architecture level. In light of this study, we will be addressing the latest techniques to reach software compliance in the US healthcare companies working as backup office(s) in Pakistan and AJK.

4.8 Realizing Compliance Tactic to Support Authentication

The paper in [52] suggests improvements in the Pakistani Data Protection Act 2005, which should be adopted as a proactive approach to improve data security in Pakistan. Authors introduced a new approach to embodying e-Authentication architectural tactics at software architecture, in which, the first step includes cross-mapping of multiple standards and rules to identify various aspects of the e-Authentication regulatory requirement compliance. In light of this, we will focus on automated solutions to reach compliance.

5. The Expected Contributions of this research

This research is aimed at developing a framework and software architecture that will help software & medical companies working in developing countries i.e. Pakistan and AJK as a backup office, to track compliance with international security & privacy regulations by adopting FAIR. The focus will be on the national & international levels of data security and privacy laws designed to protect PHI that is shared on the internet. FAIR will act as a guideline for Pakistan and AJK software and medical industry that deals with US healthcare while working as backup office(s) in Pakistan and AJK. It will contribute to the national and international security & privacy laws in the following aspects:

5.1 Identification and Implementation of CA and its impact upon QA

1. Curation and identification of CA & QA.
2. Exploration and creation of notations to build a modeling language for FAIR.
3. Design of a suitable infrastructure and framework for FAIR that includes CA. Devising the FAIR Architecture.
4. Evaluating manual and intelligent FAIR impact to make recommendations based on evaluation results, to make compliance-driven software.

Acknowledgments

The authors, Ms. Syeda Uzma Gardazi, Tahira Nazir and Naurin Farooq Khan would like to acknowledge Riphah International University for supplying necessary resources needed to complete this research. It would have been impossible to complete this research without the continued support of our institution.

References

[1] Gardazi, S. U. (2023). Impact of compliance on Pakistan and AJK. (n.d.). Retrieved from https://bit.ly/3s23F7I

[2] The role of software architecture in regulatory compliance and risk management. (2024, January 17). Retrieved from https://moldstud.com/articles/p-the-role-of-software-architecture-in-regulatory-compliance-and-risk-management

[3] Anyanwu, A. (2024). Integrating IoT with Virtual Healthcare: A theoretical framework for enhancing accessibility and efficiency in the U.S. healthcare sector. *GSC Advanced Research and Reviews, 18,* 043-049. DOI: 10.30574/gscarr.2024.18.3.0087.

[4] Chibuike, M. C., Sara, G. S., & Adele, B. (2024). Overcoming Challenges for Improved Patient-Centric Care: A Scoping Review of Platform Ecosystems in Healthcare. *IEEE Access.*

[5] Abdullah, S., Arshad, J., Khan, M., Alazab, M., & Salah, K. (2022). PRISED tangle: a privacy-aware framework for smart healthcare data sharing using IOTA tangle. *Complex & Intelligent Systems, 9.* DOI: 10.1007/s40747-021-00610-8.

[6] Sheikh, S. A., Sood, H., & Bates, D. (2015). Leveraging Health Information Technology to Achieve the "Triple Aim" of Healthcare Reform. *Journal of the American Medical Informatics Association : JAMIA, 22.* DOI: 10.1093/jamia/ocv022.

[7] Duggineni, S. (2023). Impact of Controls on Data Integrity and Information Systems. *Journal of Software Engineering and Applications, 12*(3), 29-35. DOI: 10.5923/j.scit.20231302.04.

[8] Yeo, C. (2003). Ethical dilemmas of the practice of medicine in the Information Technology age. *Singapore Medical Journal, 44,* 141-144.

[9] Mubarkoot, M., & Altmann, J. (2021). Software Compliance in Different Industries: A Systematic Literature Review.

[10] Amalfitano, D., De Luca, M., & Rita Fasolino, A. (2023). Documenting Software Architecture Design in Compliance with the ISO 26262: a Practical Experience in Industry. In *2023 IEEE 20th International Conference on Software Architecture Companion (ICSA-C)* (pp. i-xi). L'Aquila, Italy. DOI: 10.1109/ICSA-C57050.2023.00022

[11] Villegas-Ch W, García-Ortiz J. Toward a Comprehensive Framework for Ensuring Security and Privacy in Artificial Intelligence. *Electronics*. 2023; 12(18):3786. https://doi.org/10.3390/electronics12183786

[12] Breaux, Travis & Vail, Matthew & Antón, Annie. (2006). Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations. 46-55. 10.1109/RE.2006.68.

[13] Mihaylov, B., Onea, L., & Hansen, K. M. (2016). Architecture-based regulatory compliance argumentation. *Journal of Systems and Software, 119,* 1-30.

[14] Ozeer, U. (2021). ϕcomp: An Architecture for Monitoring and Enforcing Security Compliance in Sensitive Health Data Environment. In 2021 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom) (pp. 1-6). IEEE.

[15] Pruijt, I., & Köppe, M. (2017). Architecture Compliance Checking of Semantically Rich Modular Architectures. In 2017 IEEE International Conference on Software Architecture (ICSA) (pp. 207-210). IEEE. https://doi.org/10.1109/ICSA.2017.22

[16] Accorsi, R., & Stocker, T. (2008). Automated Privacy Audits Based on Pruning of Log Data. *Proceedings of the 12th International IEEE EDOC Conference Workshops* (pp. 175-182). DOI: 10.1109/EDOCW.2008.18.

[17] Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data, 5.* DOI: 10.1186/s40537-017-0110-7.

[18] Shah, V., & Konda, S. R. (2022). Cloud Computing in Healthcare: Opportunities, Risks, and Compliance. *Revista Espanola de Documentacion Cientifica, 16*(3), 50-71.

[19] Susanto, H., Almunawar, M., N. (2018). Information Security Management Systems, A Novel Framework and Software as a Tool for Compliance with Information Security Standard. Apple Academic Press

[20] Saltarella, M., Desolda, G., Lanzilotti, R., & Barletta, V. S. (2023). Translating Privacy Design Principles Into Human-Centered Software Lifecycle: A Literature Review. *International Journal of Human–Computer Interaction, 1–19.* DOI: 10.1080/10447318.2023.2219964

[21] Devineni, S. K. (2021). Augmenting the Watchdog: AI-Driven Compliance Audits for Enhanced Efficiency and Accuracy. *International Journal of Science and Research (IJSR), 10,* 1437-1443. DOI: 10.21275/SR24127205916.

[22] Ma'ady, Mochamad Nizar Palefi & Hidayat, Alifiansyah & Anaking, Purnama & Kusumawati, Aris & Nasrullah, Muhammad & Pudji Istyanto, Noerma & Asfari, Ully. (2023). Making Sense of Developing Artificial Intelligence-Based System in Software Development Life Cycle Manner and Addressing Risk Factors. 244-249. 10.1109/IC2IE60547.2023.10331070.

[23] Jagtap, Vandana. (2015). "Use of Artificial Intelligence in Software Development Life Cycle : A state of the art review". International Journal of Advanced Engineering and Global Technology (IJAEGT), ISSN No: 2309-4893.

[24] Minssen, T., Gerke, S., Aboy, M., Price, N., & Cohen, G. (2020). Regulatory responses to medical machine learning. *Journal of Law and the Biosciences, 7,* 1-18. DOI: 10.1093/jlb/lsaa002.

[25] Khwaja, O., Pamulapati, A., & Albano, K. (2024). Introducing the Databricks AI Security Framework (DASF). *Databricks.* Retrieved from https://www.databricks.com/blog/introducing-databricks-ai-security-framework-dasf

[26] Achouch, M., Dimitrova, M., Ziane, K., Sattarpanah Karganroudi, S., Dhouib, R., Ibrahim, H., & Adda, M. (2022). On Predictive Maintenance in Industry 4.0: Overview, Models, and Challenges. Applied Sciences, 12(16), 8081.

[27] Jena, O. P., Bhushan, B., & Kose, U. (Eds.). (2022). *Machine Learning and Deep Learning in Medical Data Analytics and Healthcare Applications* (1st ed.). CRC Press. DOI: 10.1201/9781003226147

[28] Adam, C., Bulut, M. F., Hernandez, M., & Vukovic, M. (2019). Cognitive Compliance: Analyze, Monitor and Enforce Compliance in the Cloud. *Proceedings of the 12th IEEE International Conference on Cloud Computing (CLOUD)* (pp. 234-242). DOI: 10.1109/CLOUD.2019.00049.

[29] Tyagi, P., Aggarwal, N., Dubey, B. P., & Pilli, E. S. (2013). HIPAA Compliance and Cloud Computing. *International Journal of Computer Applications, 70*(24), 29-32.

[30] Rezaei, M. (2022). Machine Learning in Regulatory Compliance Software Systems: An Industrial Case Study.

[31] Akhigbe, O. (2016, September). Towards a regulator-oriented regulatory intelligence framework. In *2016 IEEE 24th International Requirements Engineering Conference (RE)* (pp. 415-420). IEEE.

[32] Mughal, A. A. (2018). Artificial Intelligence in Information Security: Exploring the Advantages, Challenges, and Future Directions. *Journal of Artificial Intelligence and Machine Learning in Management*, *2*(1), 22-34.

[33] Yadav, Neel & Pandey, Saumya & Gupta, Amit & Dudani, Pankhuri & Gupta, Somesh & Rangarajan, Krithika. (2023). Data Privacy in Healthcare: In the Era of Artificial Intelligence. Indian Dermatology Online Journal. 14. 788-792. 10.4103/idoj

[34] Chen, R. J., Lu, M. Y., Chen, T. Y., Williamson, D. F., & Mahmood, F. (2021). Synthetic data in machine learning for medicine and healthcare. *Nature Biomedical Engineering*, *5*(6), 493-497.

[35] Sunkle, S., Kholkar, D., & Kulkarni, V. (2016). Informed Active Learning to Aid Domain Experts in Modeling Compliance. *Proceedings of the 20th IEEE International Enterprise Distributed Object Computing Conference (EDOC)* (pp. 1-10). DOI: 10.1109/EDOC.2016.7579382.

[36] De Almeida, P., Santos, C., & Farias, J. (2021). Artificial Intelligence Regulation: A Framework for Governance (pp. 505-525). *Springer Link.*

[37] Al Habib, A. F., & Alharthi, H. M. (2023). Prediction of Electronic Health Record Documentation Compliance Using Machine Learning. *Perspectives in Health Information Management, 20*(3), 1e. PMCID: PMC10701635.

[38] Marshall, B., Curry, M., Crossler, R., & Correia, J. (2021). Machine Learning and Survey-based Predictors of InfoSec Non-Compliance. *ACM Transactions on Management Information Systems, 13,* 1-19. DOI: 10.1145/3466689

[39] Hamdani, R. E., Mustapha, M., Amariles, D. R., Troussel, A., Meeùs, S., & Krasnashchok, K. (2021, June). A combined rule-based and machine learning approach for automated GDPR compliance checking. In Proceedings of the Eighteenth International Conference on Artificial Intelligence and Law (pp. 40-49).
[40] Ajeali, F. E. (2019). Data Breach: Responding to the Need for an Improved Information Security Management in Hospitals. [Master's thesis, American Public University].
[41] Phan, T., & Tran, H. (2023). Consideration of Data Security and Privacy Using Machine Learning Techniques. International Journal of Data Informatics and Intelligent Computing, 2, 20-32. https://doi.org/10.59461/ijdiic.v2i4.90
[42] Bedi, P., Goyal, S. B., & Kumar, J. (2020, December). Basic structure on artificial intelligence: A revolution in risk management and compliance. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 570-576). IEEE.
[43] Gardazi, S. U., & Shahid, A. (2009). Survey of software architecture description and usage in the software industry of Pakistan. In *Proceedings of the 2009 11th International Conference on Emerging Technologies (ICET)* (pp. 395-402). DOI: 10.1109/ICET.2009.5353137
[44] Gardazi, S. U. (2017). Information Security guidelines for Pakistani E-Court. Society of Corporate Compliance and Ethics (SCCE) Compliance & Ethics Professional® (C&EP) magazine.
[45] Gardazi, S. U. (2017). Brexit Compliance and Pakistan. Society of Corporate Compliance and Ethics (SCCE) Compliance & Ethics Professional® (C&EP) magazine.
[46] Gardazi, S. U., Gardazi, S. F., Khan, H., & Shahid, A. A. (2009). Motivation in Software Architecture and Software Project Management. Paper presented at IEEE ICET 2009.
[47] Gardazi, S. U., & Shahid, A. A. (2010). Presented paper at the 2nd International Conference on Software Engineering and Data Mining (SEDM), held from June 23-25, 2010, in Chengdu, China (pp. 561-570).
[48] Gardazi, S. U., Salimbene, C., & Shahid, A. A. (2012). HIPAA and QMS based architectural requirements to cope with the OCR audit program. Paper presented at the 3rd FTRA International Conference on Mobile Ubiquitous, and Intelligent Computing (MUSIC), held from June 26-28, 2012, in Vancouver, Canada (pp. 246-253).
[49] Gardazi, S. U., & Shahid, A. A. (2013). Taking Compliance Patterns and Quality Management System (QMS) Framework Approach to Ensure Medical Billing Compliance. In 2nd International Conference on Health Information Science (HIS 2013), Lecture Notes in Computer Science (Vol. 7798, pp. 78-92). London, UK: Springer.
[50] Gardazi, S. U., & Shahid, A. A. (2011). Billing Compliance Assurance Architecture for Healthcare Industry (BCAHI). Computer Science Journal (CSJ), 1(1), 16-28.
[51] Gardazi, S. U., & Shahid, A. A. (2017). Compliance-driven Software Architecture (CSA) for Healthcare Industry. International Journal of Advanced Computer Science and Applications, 8(5), 568-577.
[52] Gardazi, S. U., & Zardari, S. (2017). Realizing Compliance Tactics to Support Authentication: Bridging the Gap Between Software Architecture and Regulatory Requirements. International Journal of Computer Science and Network Security, 17(5), 337-345.