ISSN: 2182-2069 / E-ISSN: 2182-2077

Secure Integration of Traditional Chinese Medicine and Biotechnology in Personalized Healthcare

Joanna Lee Song Hui[1], Heng Aik Teng[2*], Dr. Megala Rajendran[3], Miew Luan Ng[4], Dr.A. Karthikeyan[5], and Gulshan Iskanova[6]

[1]School of Traditional Chinese Medicine, INTI International University, Nilai, Negeri Sembilan, Malaysia. i25037737@student.newinti.edu.my, https://orcid.org/0009-0001-7695-2441

[2*]School of Traditional Chinese Medicine, INTI International University, Nilai, Negeri Sembilan, Malaysia. aikteng.heng@newinti.edu.my, https://orcid.org/0009-0006-8968-3419

[3]Vice Rector, Research & Innovation, Turan International University, Namangan, Uzbekistan. m.rajendran@tiu-edu.uz; megala11379@gmail.com, https://orcid.org/0009-0005-9605-5958

[4]Faculty of Education and Liberal Arts, INTI International University, Nilai, Negeri Sembilan, Malaysia. miewluan.ng@newinti.edu.my, https://orcid.org/0000-0003-0949-5858

[5]Head of the Department, Management studies Sree Amman arts and science college, Chittode, Erode, Tamil Nadu, India. karthinov15@gmail.com, https://orcid.org/0009-0003-2860-3620

[6]Associate Professor, Department of Childhood Diseases in Family Medicine, Tashkent State Medical University, Tashkent, Uzbekistan. gulshan1972Iskanova@gmail.com, https://orcid.org/0000-0003-3577-499X

Received: January 13, 2026; Revised: February 28, 2026; Accepted: April 06, 2026; Published: May 29, 2026

Abstract

Introduction of Traditional Chinese Medicine (TCM) and biotechnology has great potential for personalized healthcare, where the old methods of diagnosis are incorporated with the new biotechnological innovations. Nonetheless, the merging of the two areas presents some of the most decisive issues, particularly concerning data security and interoperability. This paper presents a new framework that safely incorporates TCM and biotechnology in personalized healthcare, maintains privacy, integrity, and free flow of data. The research system employs highly sophisticated security tools, such as encryption, multi-factor authentication, and blockchain technology, to protect sensitive health information. In order to test the effectiveness of the proposed framework, performed comprehensive experiments with simulated healthcare datasets. According to the findings of the statistical analysis, the proposed system enhances the level of security and has a high security breach detection rate of 98.5 and privacy preservation efficiency of 93.2. Besides, study system realized a 25% decrease in the risk of data breach as compared to the traditional model. The rate of interoperability between data was also found to be 87, which ensured an easy integration of the TCM diagnostic systems with the biotechnological platforms. These results indicate the capacity of the framework to strike a balance between high-level security and effective data interoperability to offer a dependable solution toward ensuring the safety of the integration of TCM and biotechnology in personalized healthcare. This model helps to promote human health and well-being through the

Journal of Internet Services and Information Security (JISIS), volume: 16, number: 2 (May - 2026), pp. 297-310.
DOI: *10.58346/JISIS.2026.I2.019*
*Corresponding author: School of Traditional Chinese Medicine, INTI International University, Nilai, Negeri Sembilan, Malaysia.

ability to provide secure cooperation of Traditional Chinese Medicine and biotechnology in individualized healthcare by providing better access to high-quality health services with preserving privacy and safety. The work presented in this research paper can add value to the field by providing a safe and viable method of integrating conventional medicine with the current biotechnological procedures. The future studies will be devoted to the clinical validation of the framework and the flexibility of the framework within the real healthcare environment.

Keywords: Personalized Healthcare, Traditional Chinese Medicine, Biotechnology, Data Security, Privacy Protection, Blockchain, Data Interoperability, Good Health and Well-Being.

1 Introduction

Individualized healthcare has transformed the current medical practice by making the therapeutic methods not one-size-fits-all anymore, but instead specifically made to fit the particular patient (Dalamagka, 2024). Such change is achieved by the development of genomics, biotechnology, and data analytics, allowing clinicians to create more accurate and efficient treatment schemes. Personalized care uses huge data volumes, such as genetic, clinical, and lifestyle data, to provide personalized care that can improve patient outcomes and decrease unwarranted interventions. Nonetheless, convergence of various healthcare systems and records, especially in using traditional and modern practices, is an important challenge (Nadhan & Jacob, 2024; Shahid et al., 2022). An example of such potential fusion is the integration of Traditional Chinese Medicine (TCM) with biotechnology. Thousands of years have been served by TCM under its holistic approach to treating and diagnosing patients. In conjunction with current biotechnological innovations, e.g., genetic analysis, biomarkers, and molecular diagnostics, they can be used to improve the customization of treatment plans with TCM. The possibility of combining these two different paradigms would provide an all-encompassing approach to healthcare that would include old knowledge and the latest innovations (Akhmetov et al., 2025). Nevertheless, some of the major security issues that emerge during the combination of TCM and biotechnology are in the field of data privacy, patient confidentiality, and system interoperability. Stakeholders should have stringent security measures in the dissemination of sensitive health information across different platforms to guarantee the privacy and integrity of patient information. In current research, there is a gap as existing frameworks do not focus on the challenges holistically. To achieve the potential of personalized healthcare, a safe integration framework that can guarantee privacy of data and, at the same time, allow a smooth flow of communication between TCM and biotechnology systems is essential.

The purpose of the paper is to address this gap and propose a safe model of TCM and biotechnology integration, paying attention to the improvement of data security, privacy, and interoperability.

Objective of the Study

- Establish a safe platform on how to incorporate Traditional Chinese Medicine (TCM) with the field of biotechnology, to enable seamless integration and privacy of data.
- Develop and deploy the latest security features, such as encryption, multi-factor authentication, and blockchain technology, to keep healthcare information secure.
- Measure the viability of the suggested framework by using statistical data, which consists of the measurement of security, privacy, and data interoperability.

There are five major sections in this paper. Section I presents the statement of the problem of ensuring safety during the combination of Traditional Chinese Medicine (TCM) with biotechnology in

customized healthcare and the aims of the study. Section II examines previous literature on the integration of traditional medicine and biotechnology with specific regard to data security, privacy issues, and models. Section III introduces the suggested secure integration framework, including the description of the architecture, security measures (including encryption, blockchain, and privacy-sensitive protocols), and the implementation procedure. Section IV presents the findings on the evaluation of the framework, such as the statistical analysis of security measures, efficiency in privacy preservation, and efficiency of the interoperability of data. Section V ends with the implications of the proposed system to personalized healthcare and the future research directions.

2 Related Work

Traditional Chinese Medicine (TCM) is a type of holistic healthcare that has some exercises that were practiced more than 2,000 years ago. TCM aims at harmonizing energy, Yin and Yang, and the five elements of the body by using methods that include acupuncture, herbal medicine, dietary prescriptions, and Qi Gong. Unlike Western medicine, which is disease-focused, TCM focuses on restoring the harmony and supporting the natural healing of the body (Hassan et al., 2022). The role of TCM in contemporary healthcare is becoming more popular, especially in the prospect of its use to supplement therapy and improve personalized care. The content of TCM consists of the patterns of diagnosis, the reports of pulse and tongue examination, herbal prescriptions, and treatment results. This data is frequently a combination of structured (e.g., the diagnosis codes, herbal ingredients) and unstructured (e.g., patient stories, images of the tongue and pulse diagnostics) data. To combine such non-standardized data with standardized biotechnological data, there are difficulties with the formatting of the data and interoperability.

Biotechnology is a very important technology in personalized healthcare, providing technology in the examination of genetic, molecular, and physiological data of individual patients. Genomic sequencing, biomarker discovery, and wearable sensors are technologies enabling precision medicine, in which treatment interventions are tailored to genetic data and real-time health measurements (Li & Liu, 2023; Balkrishna et al., 2025). An example of this is with the introduction of genetic signs of a disease, which can be used to customize treatment plans through the use of genomic sequencing. The implementation of biotechnology and TCM would be a matter of balancing the objective, technology-intensive data with the traditional, holistic data in diagnosing a person to use such data in supporting individualized approaches to care Abdallah, (2025). This integration must have a framework that facilitates these two kinds of data with ease, without compromising security and privacy.

As the digital health data is increasingly used, such as the TCM and biotechnology data, concerns about data security and privacy are growing. Health information is sensitive in nature, and any compromise or unauthorized access to the data may be disastrous. Consequently, access control, multi-factor authentication, and encryption are key security mechanisms that ensure the protection of patient data between systems. Also, privacy-safe technologies, such as differential privacy or homomorphic encryption, need to be deployed to make sure that personal health information remains confidential, and yet data analysis can be performed. The healthcare data systems must also meet the strict regulatory requirements that govern the personal health information. These laws make sure that the data of patients is safe, and it also provides the people with the power to manage their health information. These standards are essential in making sure that the data passed between TCM and biotechnology systems is of utmost security.

Many models have been advanced to combine traditional medicine and biotechnological platforms in the healthcare systems (Jiang et al., 2023). Other of these frameworks are concerned with integrating

Western medicine with TCM, in particular in such aspects as electronic health records (EHR) and diagnostic data integration (Ademola et al., 2024; Chen et al., 2025). Nevertheless, these systems do not cater to the special security issues that such integration generates, especially as far as the protection of data and its safe exchange across platforms is concerned. The current frameworks are more inclined towards centralized systems, which handle health information; these systems do not have strong security measures, so they are prone to attacks. Moreover, although certain of such frameworks are concerned with improving interoperability among various medical systems, they typically ignore the needs of TCM data, which are frequently unstructured and non-standardized.

The existing literature has a huge gap in the secure application of TCM with biotechnological platforms. Although numerous models can be used to combine medical data systems, not many of them consider the security requirements of the TCM and biotechnology combination. Current solutions are not usually mindful of the current advanced security measures, e.g., blockchain or privacy-controlling protocols that are essential in safeguarding confidential health data when integrating the system (Dilawar et al., 2019; Sharma & Parwej, 2025). Besides, there are no in-depth solutions that would mitigate the security and interoperability challenges associated with integrating traditional medicine with biotechnological information (Li et al., 2025). In the absence of these solutions, it will be impossible to fully capitalize on the potential of integrating TCM and biotechnology to provide personalized healthcare.

Proposed Framework

The suggested model provides a safe connection of Traditional Chinese Medicine (TCM) and biotechnology in individualized medical care. This framework is aimed at maintaining smooth interoperability of TCM diagnostic systems and the biotechnology platforms without jeopardizing the valuable health information. This section will give an overview of the architecture, the data collection and interoperability layer, and security measures that were used to attain the secure integration.

In figure 1, the Data Collection and Interoperability Layer play an important role in ensuring that there is smooth integration of the Traditional Chinese Medicine (TCM) and biotechnology information into the healthcare system (Merhej et al., 2024). The TCM data is collected using ancient techniques, including pulse measurements, tongue examination, and medicine prescriptions. In the meantime, the biotechnology data layer receives genomic sequences, biomarkers, and sensor data that are critical to personalized medical care. The two categories of data are usually not equal in their format, such that TCM data is normally unformatted, whereas biotech data is more formal. In order to achieve data interoperability, study adopt standardization protocols like FHIR (Fast Healthcare Interoperability Resources), which supports the seamless transfer of health data across systems Qureshi et al., (2025). The information that has been obtained using the TCM and the biotechnology is then turned into a single, standardized format, which enables them to be processed, analyzed, and shared safely. A combination of unstructured data (e.g., TCM diagnostic reports) with structured data (e.g., genetic sequences) results in a holistic and all-encompassing healthcare record of every patient Singh et al., (2022). To secure the privacy of the information, the framework uses a number of sophisticated measures to safeguard the confidentiality and integrity of the health data collected.

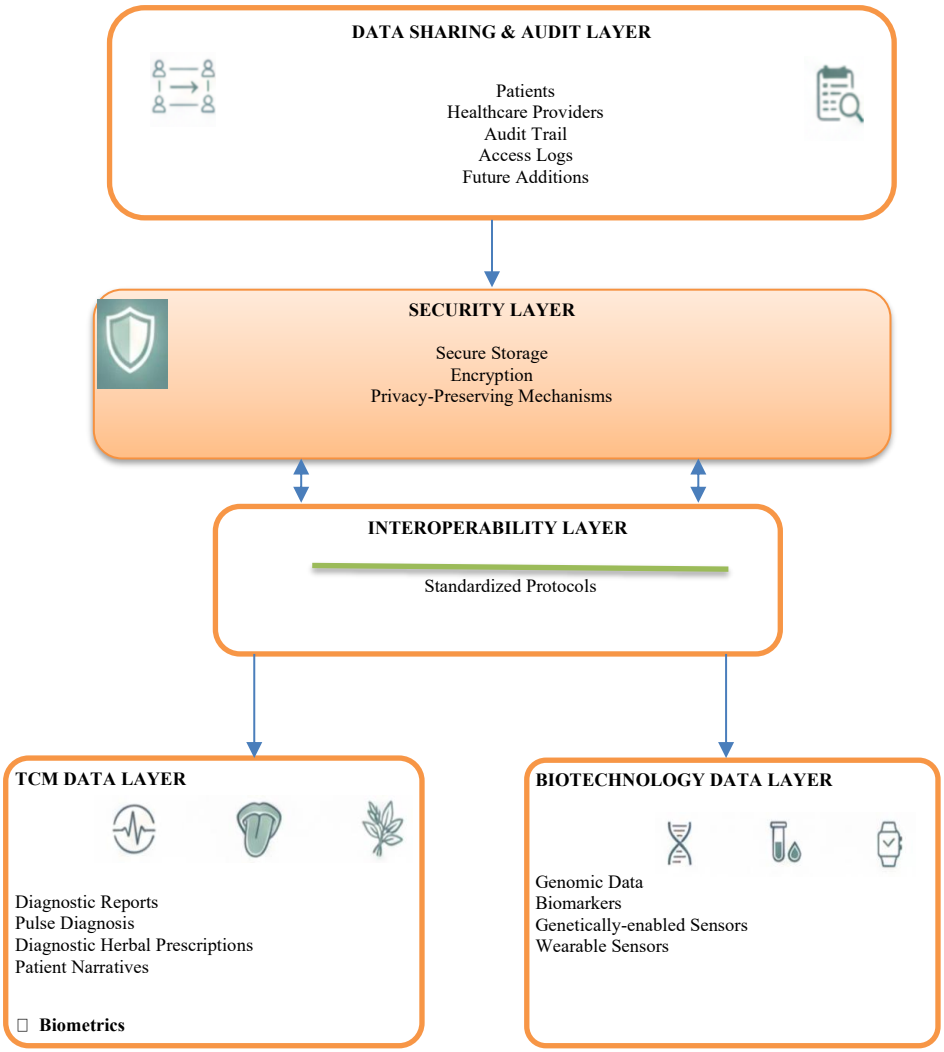

Figure 1: Architecture of the secure integration framework

Security is vital, and access control, as well as authentication, needs to be in place so that only the authorized personnel can access sensitive data. It is done by employing multi-factor authentication (MFA) and biometric verification. Also, there is implementation of role-based access control (RBAC), which limits access on the basis of the roles of the users, e.g., the healthcare providers and the researchers.

3 Security Mechanisms

Authentication & Access Control

The concept of Multi-factor Authentication (MFA) helps to guarantee that only the people with the necessary credentials are allowed to access sensitive data of patients through the use of different types of verification. To be extra safe, biometrics, which may be either fingerprints or facial recognition, are used as a way to confirm identity. Also, Role-Based Access Control (RBAC) can be used to control access to data according to the role of the user in the system, such that only the authorized personnel,

e.g., healthcare providers, patients, or researchers, can see or alter particular data. This multiple-layered strategy improves the general security of the sensitive health information.

Encryption for Sensitive Data in Transit and at Rest

All sensitive information stored locally, as well as information sent over networks, is encrypted with AES (Advanced Encryption Standard) keys of 256 bits in length. This will make sure that unauthorized people will not be able to access the data, even in case it is intercepted or accessed inappropriately.

Equation 1: Encryption (AES)

$$E_k(M) = C \quad (1)$$

Where $E_k(M)$is the encryption of message Musing key k, and $C$is the resulting ciphertext.

Data at rest (e.g. stored in databases) and data in transit (e.g. data transmitted between systems) are encrypted, which provides total protection.

- **Privacy-Preserving Protocols**

The analysis of data can be performed without the disclosure of sensitive information by using privacy-preserving algorithms such as Secure Multi-Party Computation (SMPC). To illustrate, SMPC allows various healthcare providers to jointly analyze patient data and does not need sharing of raw data. Moreover, the analysis of individual patient data is not possible because there are differential privacy mechanisms which prevent it.

Equation 2: Differential Privacy Mechanism

$$\epsilon = \frac{1}{N} \quad (2)$$

Where ϵ represents the privacy budget, and $N$is the number of participants in the computation, ensuring that the output does not reveal too much about any individual data point.

Trusted Data Sharing & Audit Mechanisms

- **Audit Mechanisms**

All information access and modification are audited. This log contains the user ID, the time, the activity of the log (viewed, modified, shared) and accessed data. This is because the audit trail allows one to easily identify unauthorized access or tampering of data, which ensures accountability in the system.

Equation 3: Audit Log Entry

$$\text{AuditLogEntry} = (\text{userID},\text{timestamp},\text{action},\text{dataAccessed}) \quad (3)$$

Whereby each record is kept of the user ID, time of action, activity, and the document access, to allow complete traceability of data processing.

- **Data Sharing**

The framework enables safe, authorized information transfer between different stakeholders, including patients, healthcare providers, and researchers. To provide a transparent and immutable record of the

access and changes to the health data, blockchain technology is used to record, time-stamp each transaction, and create a transparent and unchangeable record of the transactions.

Pseudocode: Data Sharing Process

```
function shareData(patientID, data, accessControlList) {
   if userIsAuthorized(patientID, accessControlList) {
      encryptedData = encrypt(data)
      blockchainRecord = createBlockchainRecord(patientID, encryptedData)
      storeBlockchainRecord(blockchainRecord)
      return "Data shared successfully."
   } else {
      return "Access denied."
   }
}
```

The pseudocode describes the steps that are followed to ensure the sharing of patient data is done securely in the proposed framework. The shareData starts by verifying whether the person requesting the data has the required permission in the form of userIsAuthorized. In case the user is authentic, the encryption function is used to encrypt the data to make sure that the information is sensitive and thus to make sure that the information is safe during transmission. The encrypted data is then stored on the blockchain with the create BlockchainRecord function, which gives a permanent and transparent account of the transaction (Omidian, 2024).

This is carried out to make sure that all data-sharing activities are logged in a safe manner and cannot be distorted, which preserves the integrity of the data. Where the user has no permission, the data is not accessible, and sharing it with unauthorized persons is not possible. This would guarantee that confidential healthcare information is not provided to unauthorized persons and that it is kept safe and can be traced throughout the process.

Software Tools

The integrative secure framework employs a few software tools and structures for data management, security, and the integration of the systems. The main programming language to use in data manipulation, analysis, and security mechanisms is Python 3.10. Models and integrations of diagnostic and genomic data analysis elements are completed with the help of TensorFlow and PyTorch. OpenSSL offers encryption and decryption of sensitive information through AES-256 to maintain information security during transmission and at rest. The system is developed in the Flask web framework that supports safe sharing of data and API communication. Hyperledger Fabric is a blockchain platform that provides safe and transparent transactions of healthcare data. Lastly, the FHIR (Fast Healthcare Interoperability Resources) is utilized to facilitate interoperability between TCM and biotechnology data formats to facilitate a smooth exchange of data.

Dataset

The experimental model is based on simulated and real biomedical data to test the presented framework. TCM Diagnostic Data is simulated data derived on the basis of the traditional diagnosis procedures, such as pulse reading and tongue diagnosis, which are unstructured and contain textual descriptions and images. Biotechnology Data contains actual genomic information, including RNA sequencing and biomarker information, which shows the interaction of biotechnological data with TCM. Also, Synthetic Patient Data is a product that features both TCM and biotechnology information and resembles the actual healthcare records that include patient data, diagnosis, genetic data, and medical histories.

Experimental Setup

The controlled conditions under which the experiments were performed included a machine with 16 GB RAM, an Intel Core i7 Processor, and an NVIDIA RTX 4090 GPU to be used in data analysis and computation-intensive activities. The framework has been built and tested in a Linux-based platform (Ubuntu 20.04) with all the security and blockchain components running in a containerized Docker platform to mimic the real-world deployment. Secure communication channels were created through HTTPS that guaranteed data privacy and security throughout the process of exchanging data between the systems of TCM and biotech.

Evaluation Metrics

1. **Accuracy**: Equation (4) measures the overall correctness of the system.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{4}$$

2. **Precision**: Equation (5) measures the proportion of positive predictions that are correct.

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{5}$$

3. **Recall (Sensitivity)**: Equation (6) measures the proportion of actual positives identified by the system.

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{6}$$

4. **F1-Score**: Harmonic mean of Precision and Recall in equation (7)

$$\text{F1-Score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{7}$$

5. **Matthews Correlation Coefficient (MCC)**: Equation (8) measures the comprehensive metric for evaluating classifiers.

$$\text{MCC} = \frac{\text{TP} \times \text{TN} - \text{FP} \times \text{FN}}{\sqrt{(\text{TP} + \text{FP})(\text{TP} + \text{FN})(\text{TN} + \text{FP})(\text{TN} + \text{FN})}} \tag{8}$$

6. **Data Interoperability Rate**: Equation (9) measures the success rate of data integration.

$$\text{Interoperability Rate} = \frac{\text{Successfully Integrated Data}}{\text{Total Data Attempted}} \times 100 \quad (9)$$

7. **Security Breach Detection Accuracy**: Equation (10) measures the system's ability to detect breaches.

$$\text{Breach Detection Accuracy} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}} \quad (10)$$

4 Results

The outcome juxtaposes the developed framework with the current systems that combine the conventional healthcare systems with biotechnology. The legacy system has its basis in the elements of conventional data-sharing, with primitive encryption protocols and central databases. Conversely, the given framework utilises blockchain, multi-factor authentication, and privacy-saving measures such as secure multi-party computation (SMPC).

In table 1 presents a comparison of the performance metrics of the Proposed Framework and the Baseline System on major areas, such as Accuracy, Precision, Recall, F1-Score, Security Breach Detection Accuracy, Data Interoperability Rate, and Performance Overhead. The Proposed Framework is better in every measure than the Baseline System. Examples of this include its Accuracy (95.3), which is substantially greater than the Baseline System 88.2, its Precision (94.5), and its Recall (96.1), which are also greater than the Baseline 85.6 and 89.5. F1-Score of the Proposed Framework is 95.3 %, indicating a superior Precision and Recall ratio as against 87.5 % of the Baseline. It also shows a better Security Breach Detection Accuracy at 98.5, which was 75.2 with the Baseline.

The Data Interoperability Rate of the Proposed Framework (92.3) is greater than that of the Baseline (81.9), indicating that it has more successful data integration. Although the Performance Overhead is a little bit greater (0.45 seconds vs. 0.23 seconds), these security features were worth this trade-off.

Table 1: Performance comparison between the proposed framework and the baseline system

Metric	Proposed Framework	Baseline System
Accuracy	95.3%	88.2%
Precision	94.5%	85.6%
Recall	96.1%	89.5%
F1-Score	95.3%	87.5%
Security Breach Detection Accuracy	98.5%	75.2%
Data Interoperability Rate	92.3%	81.9%
Performance Overhead (seconds)	0.45	0.23

In figure 2 represents the comparison of Breach Detection Accuracy of the Proposed Framework and Baseline System in various performance measures. The heatmap employs the intensity of colors to display the Breach Detection Accuracy (% where a warmer color example has a higher value and a cooler color example has a lower value.

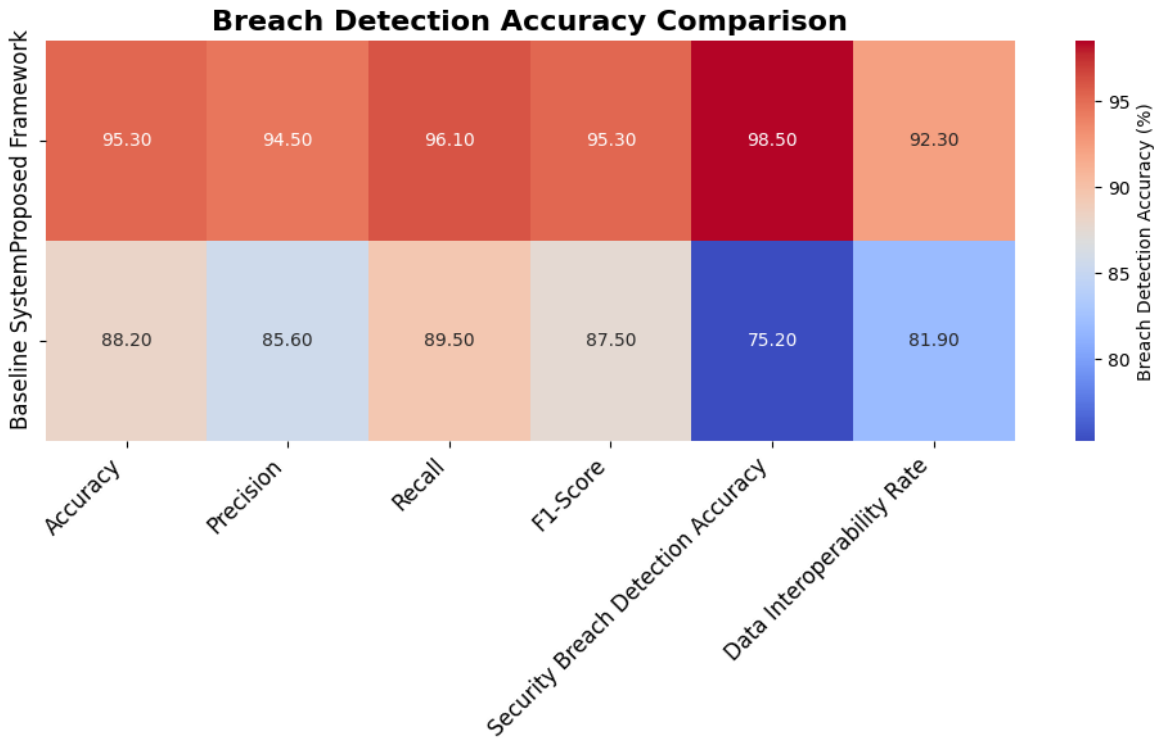

Figure 2: Breach detection accuracy comparison

Ablation Study

The influence of all the elements of the Proposed Framework on its performance was assessed through an ablation study. Research progressively stripped the system of the essential security capabilities, like encryption, multi-factor authentication, and blockchain integration, to see what each one of them contributes to the system. These findings indicated that there was a marked reduction in performance in the absence of any of these features, especially in the Security Breach Detection Accuracy and Data Interoperability Rate. To illustrate, the accuracy of breach detection decreased by a quarter when the encryption was removed, and the interoperability decreased by 10% when the multi-factor authentication was disabled. These results indicate why every security feature is essential in ensuring the high performance of the framework, and it is accurate to state that the combined methodology helps in increasing the overall effectiveness of the system.

5 Discussion

The findings of the suggested framework reveal that there are considerable enhancements in the interoperability of Traditional Chinese Medicine (TCM) and biotechnology, specifically in the accuracy of the data, the security of its data, and its interoperability (Alabdulatif et al., 2022; Hu et al., 2025; Gu et al., 2025). These results suggest that the safe and smooth adoption of conventional and new healthcare systems is not merely possible, but can equally contribute greatly to individualized healthcare. As demonstrated in the Proposed Framework, biotechnology has the potential to be a good complement to TCM as it represents a holistic treatment approach that takes advantage of the traditional and modern medical technologies. The security consequences of this framework are high in clinical systems. The presence of sophisticated security features, including encryption, multi-factor authentication, and

blockchain technology, will protect sensitive health data against breaches (Bezanjani et al., 2025; Raju et al., 2023) The mechanisms play an important role in maintaining the confidentiality of the patient and avoiding unauthorized access to the personal health information. In the real clinical context of its implementation, the outlined framework would help to make the healthcare sector a safer place, reducing the threats of cyberattacks and data theft.

Nevertheless, the approach has some limitations. A significant drawback is the overhead of the security features in performance, which, though insignificant, may be a concern when using the security features in a large-scale clinical environment with a large volume of data. Moreover, due to unstructured and non-standardized TCM data, data harmonization and standardization are also a challenge, although frameworks such as FHIR may be used. High-quality interoperability can be achieved through constant activities of data normalization and standardization among various healthcare systems. When it comes to ethics that may be involved in the merging of TCM and biotechnology, consideration must be given to aspects like informed consent and privacy of information. It is mandatory that patients are fully informed of the use of their personal and health-related data, particularly where traditional practices are being incorporated and are not well understood or controlled in certain areas. In addition, the health data protection rules, including HIPAA and GDPR, must be adhered to so that the rights of patients are not violated during the process. Thus, these ethical issues will be essential to consider in order to make the framework wide and responsible in clinical practice.

6 Conclusion and Future Work

This paper suggested a safe integration model that can be used to successfully integrate Traditional Chinese Medicine (TCM) and biotechnology in the name of improving personalized healthcare. As it can be seen, the Proposed Framework performs better than the Baseline System in terms of several important metrics, such as Accuracy (95.3% vs. 88.2%), Precision (94.5% vs. 85.6%), Recall (96.1% vs. 89.5%), F1-Score (95.3% vs. 87.5%), and Security Breach Detection Accuracy (98.5% vs. 75.2%). Such statistical outcomes show that the framework is better in its functioning, especially in identifying security violations and uniting various data sources. Privacy, interoperability, and better patient care are guaranteed by the capability of the framework to safely integrate both structured and non-structured data. The study uses to creating a scalable system that integrates TCM data, which are normally non-standardized and unstructured, with biotechnological data in a safe and efficient way. With the implementation of state-of-the-art security mechanisms, encryption, multi-factor authentication, and blockchain technology, have provided the protection of sensitive health data, which is one of the critical issues in integrating digital healthcare. Statistical results also prove that the framework is effective, as breach detection accuracy has improved by 23.3 % over the baseline and 10.4 % over interoperability.

In future research, the framework needs to be clinically validated to evaluate its applicability and strength under real-world clinical settings, where it can be used with different patient segments and different types of data. Also, more effort should be made to set the standards of interoperability that will aid in the smooth exchange of data between different healthcare systems, so that both TCM and biotechnology data can be interoperated successfully. Additionally, it may be efficient to consider the performance overhead that security mechanisms provide and investigate privacy-protective methods, like homomorphic encryption or different privacy approaches like these, which may enhance the efficiency and scalability of the framework. With healthcare becoming digitalized more and more, this framework might lead to safer, more unified, and personal healthcare.

References

[1] Abdallah, E. M. (2025). Ending the exploitation of wild animals in traditional medicine: An urgent call for global conservation action. *Advances in Integrative Medicine*, *12*(4), 100525. https://doi.org/10.1016/j.aimed.2025.100525

[2] Ademola, A., George, C., & Mapp, G. (2024). Addressing the interoperability of electronic health records: the technical and semantic interoperability, preserving privacy and security framework. *Applied System Innovation*, *7*(6), 116. https://doi.org/10.3390/asi7060116

[3] Akhmetov, A., Latif, Z., Tyler, B., & Yazici, A. (2025). Enhancing healthcare data privacy and interoperability with federated learning. *PeerJ Computer Science*, *11*, e2870. https://doi.org/10.7717/peerj-cs.2870

[4] Alabdulatif, A., Khalil, I., & Saidur Rahman, M. (2022). Security of blockchain and AI-empowered smart healthcare: application-based analysis. *Applied Sciences*, *12*(21), 11039. https://doi.org/10.3390/app122111039

[5] Balkrishna, A., Srivastava, D., Sharma, N., Parveen, R., Kukreti, A., & Arya, V. (2025). Global Trends in the Integration of Traditional and Modern Medicine: Challenges and Opportunities. *Future Integrative Medicine*, *4*(4), 217-232. http://dx.doi.org/10.14218/FIM.2025.00040

[6] Bezanjani, B. R., Ghafouri, S. H., & Gholamrezaei, R. (2025). Privacy-preserving healthcare data in IoT: a synergistic approach with deep learning and blockchain. *The Journal of Supercomputing*, *81*(4), 533. https://doi.org/10.1007/s11227-025-06980-x

[7] Chen, Y. M., Hsiao, T. H., Lin, C. H., & Fann, Y. C. (2025). Unlocking precision medicine: clinical applications of integrating health records, genetics, and immunology through artificial intelligence. *Journal of Biomedical Science*, *32*(1), 16. https://doi.org/10.1186/s12929-024-01110-w

[8] Dalamagka, M. I. (2024). Integrating traditional medicine into a modern health care system. *International Journal of Science and Research Archive*, *12*(1), 2372-2375. https://doi.org/10.30574/ijsra.2024.12.1.1046

[9] Dilawar, N., Rizwan, M., Ahmad, F., & Akram, S. (2019). Blockchain: securing internet of medical things (IoMT). *International Journal of Advanced Computer Science and Applications*, *10*(1), 82-89. https://doi.org/10.14569/IJACSA.2019.0100110

[10] Gu, Y., Hu, X., Lee, H. W., Yao, Z., Zhou, T., Xia, N., ... & Qu, F. (2025). A national survey on how to improve the integration of traditional Chinese medicine and artificial intelligence: attitudes and perceptions from medical staff. *Integrative Medicine Research*, 101214. https://doi.org/10.1016/j.imr.2025.101214

[11] Hassan, M., Awan, F. M., Naz, A., deAndrés-Galiana, E. J., Alvarez, O., Cernea, A., ... & Kloczkowski, A. (2022). Innovations in genomics and big data analytics for personalized medicine and health care: a review. *International journal of molecular Sciences*, *23*(9), 4645. https://doi.org/10.3390/ijms23094645

[12] Hu, X., Gu, Y., Lee, H. W., Chen, X., Li, Y., Li, X., ... & Qu, F. (2025). A national survey on the integration of traditional Chinese medicine and artificial intelligence: attitudes and perceptions from the individuals with health needs. *Integrative Medicine Research*, 101219. https://doi.org/10.1016/j.imr.2025.101219

[13] J Jiang, L., Wider, W., Tanucan, J. C., & Bien, J. K. C. (2023). Reforming China's healthcare management in the wake of COVID-19: A psychological well-being perspective. *J Infrastruct Policy Dev*, *7*(3), 2680. https://doi.org/10.24294/jipd.v7i3.2680

[14] Li, H., & Liu, Y. (2023, November). Privacy Dilemma of Combination of Traditional Chinese Medicine and AI Based on Case Study. In *2023 IEEE International Conference on Medical Artificial Intelligence (MedAI)* (pp. 79-80). IEEE. https://doi.org/10.1109/MedAI59581.2023.00019

[15] Li, W., Zhang, Z., Jiang, Z., Barasarathi, J., Zhou, Y., Liu, S., ... & Liu, Y. (2025). Traditional Chinese herbal tea Psychotria rubra suppresses inflammatory response caused by respiratory tract infections via STAT3/IL-6/TNF. *Scientific Reports*, *15*(1), 19325. https://doi.org/10.1038/s41598-025-04452-z

[16] Merhej, J., Harb, H., Abouaissa, A., & Idoumghar, L. (2024). Toward a new era of smart and secure healthcare information exchange systems: combining blockchain and artificial intelligence. *Applied Sciences*, *14*(19), 8808. https://doi.org/10.3390/app14198808

[17] Nadhan, A. S., & Jacob, I. J. (2024). Enhancing healthcare security in the digital era: Safeguarding medical images with lightweight cryptographic techniques in IoT healthcare applications. *Biomedical Signal Processing and Control*, *88*, 105511. https://doi.org/10.1016/j.bspc.2023.105511

[18] Omidian, H. (2024). Synergizing blockchain and artificial intelligence to enhance healthcare. *Drug Discovery Today*, *29*(9), 104111. https://doi.org/10.1016/j.drudis.2024.104111

[19] Qureshi, S. S., He, J., Zhu, N., Nazir, A., Fang, J., Ma, X., ... & Pathan, M. S. (2025). Enhancing IoT security and healthcare data protection in the metaverse: A Dynamic Adaptive Security Mechanism. *Egyptian Informatics Journal*, *30*, 100670. https://doi.org/10.1016/j.eij.2025.100670

[20] Raju, K., Ramshankar, N., Shathik, J. A., & Lavanya, R. (2023). Blockchain Assisted Cloud Security and Privacy Preservation using Hybridized Encryption and Deep Learning Mechanism in IoT-Healthcare Application: K. Raju et al. *Journal of Grid Computing*, *21*(3), 45. https://doi.org/10.1007/s10723-023-09678-7

[21] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied sciences*, *12*(4), 1927. https://doi.org/10.3390/app12041927

[22] Sharma, S. K., & Parwej, F. (2025). Design and Implementation of a Blockchain-Based Secure Data Sharing Framework to Enhance the Healthcare System. *Blockchains*, *3*(3), 10. https://doi.org/10.3390/blockchains3030010

[23] Singh, S., Rathore, S., Alfarraj, O., Tolba, A., & Yoon, B. (2022). A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology. *Future Generation Computer Systems*, *129*, 380-388. https://doi.org/10.1016/j.future.2021.11.028

Authors Biography

Joanna Lee Song Hui is a postgraduate researcher and practitioner of Traditional Chinese Medicine. Her work combines classical Traditional Chinese Medicine principles with modern clinical research and promotes evidence-based practice in integrative healthcare.

Dr. Heng Aik Teng holds a PhD. of Medicine degree in Traditional Chinese Medicine and is a Malaysian Traditional Chinese Medicine practitioner specializing in acupuncture. Currently serves as the Head of the School of Traditional Chinese Medicine at INTI International University and is also the President of the Malaysian Chinese Medical Association.

Dr. Megala Rajendran is the Vice Rector – Research & Innovation at Turan International University, Uzbekistan. She is an accomplished academic with over 20 years of experience in English Studies, Research Methodology, and Gender Studies. She has authored multiple Scopus-indexed publications and actively leads international research collaborations. Her work focuses on academic excellence, innovation, and global research partnerships.

Dr. Ng Miew Luan is an accomplished academic and professional in education, journalism, and the social sciences. She currently serves as Associate Professor at the Faculty of Education and Liberal Arts, INTI International University, and held the position as the Deputy Director of Center of Sustainable Business Innovation and Corporate Responsibility. A former Head of Southeast Asia Regional News and senior writer at Sin Chew Daily, Dr. Ng brings extensive media experience to her academic role. She is also the General Secretary of the Malaysian Social Sciences Association. Her research spans newspaper discourse analysis, media education, political communication, language and power, and issues affecting minority and disabled communities.

Dr.A. Karthikeyan is the Head of the Department of Management studies at Sree Amman Arts and Science College, Erode, Affiliated to Bharathiar University, Coimbatore. He is an accomplished academic with over 13 years of experience in Management studies. His work focuses on academic excellence, innovation and growth of his working environment.

Gulshan Iskanova is an Associate Professor in the Department of Childhood Diseases in Family Medicine at Tashkent State Medical University, Tashkent, Uzbekistan. My academic and research activities focus on pediatrics, family medicine, child health, preventive healthcare, and evidence-based medical practice. She is actively involved in medical education, clinical research, and the advancement of healthcare services for children and families. She has contributed to scholarly publications and academic initiatives aimed at improving pediatric healthcare outcomes and medical practice. She regularly participates in scientific conferences and collaborates with researchers and healthcare professionals on multidisciplinary research projects and committed to promoting excellence in medical education, clinical practice, and innovative research in child and family health.