scientific reports

OPEN

Enhancing patient admission efficiency through a hybrid cloud framework for medical record sharing

Mona Abughazalah[1]✉, Wafaa Alsaggaf[1], Shireen Saifuddin[1] & Shahenda Sarhan[2,3]

The fragmentation of patient data across multiple healthcare institutions presents a significant challenge to realizing timely and effective treatment. Although electronic medical records have replaced traditional paper records, they often remain isolated within individual hospital information systems, limiting data exchange and preventing physicians from accessing complete medical histories during patient admission. These restrictions hinder the efficiency of diagnosis and treatment, particularly in critical care settings, such as emergency departments. Cloud computing provides a promising solution by enabling controlled electronic medical record sharing, thereby improving the continuity and quality of care. This study presents a system-level, multi-layered hybrid cloud architecture framework designed to facilitate seamless and managed exchange of electronic medical records among healthcare organizations. To further enhance operational efficiency, the system integrates fingerprint authentication based on hashed identifiers for rapid patient identification and an Internet of Things bracelet for real-time monitoring of vital signs. System performance was evaluated using discrete-event simulation implemented in the OMNeT++ framework, with simulation parameters informed by real emergency department data from three hospitals in Saudi Arabia. The evaluation considers multiple workflow scenarios and incorporates repeated simulation runs to assess performance stability. The simulation results indicate consistent reductions in average patient waiting times, while treatment durations remain stable and patient throughput increases. These findings highlight the potential of the proposed framework to enhance electronic medical record management, streamline clinical workflows, and improve operational efficiency in time-critical environments.

Keywords Cloud computing, Hybrid cloud computing, Electronic medical records, Fingerprint, IoT

Advances in information technology have a tangible impact on reshaping healthcare[1]. Specifically, innovations like cloud computing have made multiple healthcare services accessible to patients, including secure storage, seamless data exchange, and remote access to medical information[2].

To provide these services, healthcare providers require rapid access to medical information, particularly in medical emergencies[3]. Traditional hospital information systems (HISs) have limitations because they are hospital-based platforms, not designed for data sharing across institutions, and operate in isolation[4]. This isolation prevents data sharing across institutions, making it difficult for external hospitals to access patient information[5].

Cloud computing has emerged as an innovative technology to address this challenge by providing a scalable, secure, and flexible infrastructure that enables healthcare institutions to exchange electronic medical records (EMRs) efficiently across diverse healthcare systems[6].

Cloud EMR exchange benefits the users of the medical system by enabling hospitals to manage a large volume of patient EMRs more efficiently and reducing the need for repeated lab tests, X-rays, and magnetic resonance imaging (MRIs)[7]. This prevents patients from recurring exposure to harmful medical procedures[8].

[1]Department of Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia. [2]Computer Science Department, Faculty of Computers and Information, Mansoura University, Mansoura 35516, Egypt. [3]School of Computer Science & Technologies, VIZJA University, Warsaw, Poland. ✉email: mabughazaleh@kau.edu.sa

Patients can benefit from the availability of their medical information across hospitals, enabling accurate diagnosis and effective treatment[9]. Physicians can make more informed therapeutic decisions and spend less time on consultations when they have access to a comprehensive and integrated medical history. This accelerates patient care and makes it more efficient[10].

Cloud computing in healthcare has evolved around two predominant deployment paradigms: centralized and decentralized cloud architectures. Centralized models combine data storage and processing within a single data center, providing ease of management and efficient system integration, but remain prone to single points of failure, limited scalability, and potential security vulnerabilities[11].

Conversely, decentralized architectures distribute data and computational workloads across multiple nodes. This enhances fault tolerance and reduces latency, but often leads to increased complexity in synchronization and cost management[12].

Building on the differences between centralized and decentralized cloud architectures, the hybrid cloud represents an intermediate approach that combines the advantages of both. It facilitates the sharing of patient information among medical organizations via cloud computing platforms[13].

Several studies have examined the exchange of EMRs using cloud computing to address the problem of isolated HIS environments and the resulting barriers to accessing comprehensive patient information.

However, comparatively limited attention has been paid to examining the direct, system-level impact of integrated medical data on healthcare service efficiency, particularly in terms of patient flow and waiting times within automated admission and clinical workflows.

While hybrid cloud infrastructures have been previously explored in healthcare, this work does not aim to introduce new cloud layers or deployment models. Instead, it focuses on the functional separation of private, community, and government cloud roles, and examines how this separation influences emergency department workflows in environments where inter-hospital EMR exchange does not currently exist.

The proposed architecture is employed as a design framework to evaluate system-level changes in patient flow and waiting time, rather than as an infrastructure-centric contribution. This distinction differentiates the present study from prior cloud-based EMR solutions that primarily evaluate data exchange capabilities in isolation.

To address these limitations, this study presents a multi-layered hybrid cloud framework for exchanging patient EMRs across hospitals. This framework integrates several private clouds, a shared community cloud, and a government cloud to establish a robust infrastructure for medical data exchange.

A private cloud is one of the cloud computing deployment models that provides a secure environment and strong control over data by dedicating resources to a single organization[14].In the framework, each hospital has a dedicated private cloud to store and process medical information. Private clouds are used because they provide privacy and a secure environment, and only authorized persons can access them[15].

A community cloud is a shared computing infrastructure utilized by several institutions with similar interests. It enables resource sharing, data exchange, and service coordination[16,17]. In the framework, the community cloud serves as a shared directory service for hospitals, maintaining metadata on the location of patient EMRs across participating hospitals. This facilitates rapid, real-time access to data for authorized healthcare providers for accurate diagnosis and timely treatment.

Governments worldwide are increasingly adopting cloud computing to deliver citizen-centered services[18]. Cloud services can help governments save money on hosting data and applications because they are not required to pay for an entire physical IT infrastructure. Cloud computing enables governments to store, manage, process, and share data and applications in a flexible manner. This enables them to develop new, cost-effective, and reliable solutions for scalability[19].

The government cloud in the proposed framework facilitates the creation of EMR by automating the retrieval of patient demographic data from national databases. This automation replaces the traditional manual registration process in hospitals, reducing reliance on manual registration processes and minimizing human errors during data entry, which may contribute to improved admission efficiency.

In addition to the cloud infrastructure, the proposed framework incorporates two integrated technologies that enhance accuracy and patient experience. First, fingerprint authentication is utilized for patient identification at hospital entry points. Because each person has a unique fingerprint pattern, this biometric method provides a fast, cost-effective, and highly secure authentication mechanism, reducing the risk of fraud or misidentification[20]. Fingerprint authentication only requires a simple touch to process, is affordable, and integrates easily with any system[21].

Fingerprint authentication reduces medical errors by linking patients directly to their EMR and facilitating accurate identification of patients[22]. Furthermore, it enables safe and traceable access to sensitive health data[23]. It also streamlines patient registration and minimizes administrative delays.

Second, the system utilizes an Internet of Things (IoT) bracelet that continuously monitors patients' vital signs, including heart rate, blood pressure, and body temperature, and automatically transmits the data to the hospital's private cloud. This real-time monitoring helps reduce the need for repetitive manual vital-sign measurements and supports timely clinical awareness when abnormal readings are detected. Importantly, the IoT bracelet is intended to augment clinical workflows and support healthcare staff, rather than replace human judgment or clinical decision-making during triage.

By integrating these components: private, community, and government clouds, along with fingerprint authentication and an IoT bracelet, the proposed hybrid cloud framework aims to enhance the efficiency of healthcare services. It provides a unified and secure environment for exchanging medical data, improving diagnostic accuracy, reducing patient waiting times, and enhancing the overall quality of healthcare delivery, thereby strengthening the patient experience and ensuring continuous and effective care.

While the proposed framework is intended for use across general healthcare settings, the Emergency Department (ED) was chosen as the primary evaluation setting due to its dynamic, time-critical workflows[24].

The ED is characterized by highly variable patient arrival patterns[25], frequent encounters involving patients from multiple healthcare providers[26], and minimal tolerance for delays in clinical decision-making[27].In such environments, delays related to fragmented medical records and manual admission procedures can have immediate operational implications for patient flow and waiting times. Evaluating the framework within the ED, therefore, provides a rigorous context for examining system-level efficiency effects under demanding operational conditions.

The remainder of this paper is organized as follows. The "Related Work" section surveys prior related work on existing cloud-based patient information exchange. The "Proposed Framework" section describes the proposed multi-layered framework for a healthcare system. The "Security and Privacy Considerations" section outlines the Security and Privacy in the framework. The "Simulation Setting" section outlines the simulation methodology, which is calibrated using emergency department data from real hospitals. The "Dataset" section presents the dataset and its characteristics. The "Evaluation Metrics" section explains the mathematical equations used to compute the system average treatment and waiting time, as well as the theoretical maximum patient number in the simulation. The "Results" section presents the analysis of real emergency department data alongside simulation results. The "Discussion" section discusses the simulation experimental results. The "Limitation" section outlines the constraints of the present study, while the "Future Work" section identifies opportunities for extending the proposed framework. Finally, the "Conclusion" section concludes the paper.

Related work

Recent technological advances have made significant contributions to the quality of health care, particularly in the exchange of patients' medical information. Many previous studies have focused on the challenges of integrating healthcare organizations and making access to patient records distributed across hospital environments easy, fast, and timely. In this section, we review previous studies that addressed these challenges and proposed many solutions to facilitate a quick and effective EMR sharing across many healthcare organizations.

Centralized cloud-based system

The research conducted by Ademola et al.[28] introduced a centralized cloud-based system, technical and semantic interoperability, preserving privacy and security (TASIPPS), to facilitate the exchange of electronic health records (EHRs). TASIPPS incorporates robust security and privacy protocols, ensuring secure real-time access to EHR. This enhances diagnostic accuracy and facilitates timely treatment interventions. However, this architecture uses a patient's unique identifier to retrieve their medical records from interconnected healthcare systems. Discrepancies or errors in ID assignment may lead to inaccurate record retrieval.

Furthermore, Ou and Tsai[29] proposed a flow-based mechanism for accessing and sharing patient data across healthcare organizations via a centralized cloud computing system. They developed a web-based system that primarily focuses on patient registration and doctor appointments. Although the system improves workflow and ensures a smooth and intuitive process for managing appointments and medical records, it relies on personal identification health ID cards for identity verification. This dependency may pose challenges if the cards are lost, damaged, or forgotten.

In another study conducted in Taiwan, Wu et al.[30] evaluated the impact of a centralized cloud-based information exchange system, called MediCloud, on the quality of patient care in the emergency department. They discovered remarkable improvements after implementing MediCloud in the healthcare system, which reduced waiting times and accelerated treatment decisions.

Symvoulidis et al.[31] proposed a centralized cloud-based EHR system that leverages architecture to securely store and manage EHR for emergency healthcare scenarios. The authors highlighted that in critical emergencies, where even seconds are vital, the proposed system ensures rapid retrieval of health data. However, they rely on QR codes to enable healthcare professionals to access a user's EHR during emergencies. However, in critical emergencies where the patient is unconscious or unable to provide the QR code, accessing their EMR could be impossible.

The study by Saleh et al.[32] was conducted with the Sijilli system, which uses centralized cloud computing to store and exchange health information for refugees. The Sijilli enables healthcare providers worldwide to access refugees' medical information and ensure continuity of care during and after migration. However, a notable limitation is that the health records are handed to the refugee on a key-shaped flash drive, which is susceptible to loss or damage.

Similarly, the authors in[33] implemented a centralized cloud-based system to enable efficient exchange of EMR across hospitals in Taiwan. Although their system improves healthcare, they rely on traditional methods for accessing EMR, using an integrated circuit card to identify patients and physicians, which can be vulnerable to damage or loss.

Hybrid cloud-based systems

McOwiti et al.[34] proposed a hybrid cloud data lake architecture to integrate clinical and genomic data for oncology research. The hybrid cloud enables scalable storage of large genomic datasets in the cloud while maintaining sensitive clinical data securely on-premises. This design enhances data accessibility and supports precision medicine while maintaining privacy compliance. However, the system's search function primarily depends on metadata quality and lacks real-time performance, limiting its suitability for time-sensitive clinical applications.

Naz et al.[35] focused on designing a hybrid cloud framework that combines centralized indexing with decentralized storage to enable secure and efficient exchange of medical records across hospitals. Their contribution lies in the architectural design for global healthcare data management. However, the system relies on predetermined code sets and a unique 13-digit citizen identification number for patient identification, which limits international applicability, as identification systems vary across countries. Additionally, depending on the use of a unique 13-digit citizen patient identification number during the search process increase the risk of typing errors, potentially leading to incorrect or failed record retrieval.

Another work by Vellela et al.[36] proposed an integrated e-healthcare system using a dynamic hybrid cloud platform for EMR exchange. The system collects patient information from biosensors, user inputs, and audio/video streams, storing and processing all data in the cloud for secure access. The study highlights the potential of hybrid cloud infrastructures; however, its reliance on patient IDs may lead to misidentification.

Javaid et al.[37] reported that cloud computing plays a pivotal role in enhancing healthcare delivery by enabling real-time exchange of patient records across hospitals and healthcare providers. The study emphasized that such data sharing reduces treatment delays by granting clinicians immediate access to medical histories, laboratory results, and imaging data. This practice improves the quality and efficiency of healthcare services through better coordination, remote consultations, and reduced duplication of diagnostic tests.

Brown et al.[38] proposed a hybrid cloud-based model designed to securely link large-scale healthcare datasets across healthcare institutions while preserving patient privacy. The system stores sensitive information locally and performs encrypted data matching in the cloud using cryptographic hashing techniques, ensuring that no identifiable information is exposed. This approach enables scalable, privacy-preserving record linkage, supporting data integration for research and health analytics. However, one major limitation is that the model primarily depends on the quality and accuracy of the original data; errors in names, dates, or formatting can significantly reduce linkage accuracy.

Finally, Yang et al.[39] addressed the challenges of legacy EHR systems by introducing MedShare, a hybrid cloud-based solution designed to enable secure sharing of medical resources among autonomous healthcare providers. The authentication process involves scanning the patient's ID card. However, this work was limited to resource sharing between independent providers, specifically dialysis centers.

Although previous studies have explored the use of both centralized and hybrid cloud models for exchanging EMRs across hospitals and have demonstrated the benefits of cloud-based EMR exchange, most have focused primarily on the data exchange process itself. Moreover, centralized cloud models often suffer from security vulnerabilities, single points of failure, and limited control over sensitive information. These limitations motivate the adoption of hybrid cloud approaches as a potentially more robust and flexible solution for modern healthcare environments.

While reductions in patient waiting times following cloud-based EMR adoption have been reported in prior studies, such improvements are not novel in isolation. Unlike prior work that treats EMR exchange as a standalone function, this study examines the system-level implications of integrating multiple components within a unified hybrid cloud architecture. Specifically, the proposed framework considers the combined roles of private clouds for secure data management, a community cloud for selective record discovery, a government cloud for identity initialization and coordination, biometric fingerprint authentication for patient admission, and IoT-based vital-sign monitoring to support pre-consultation workflows. This integrated perspective enables an assessment of how coordinated system components influence patient flow, admission efficiency, and waiting times in ED settings beyond isolated EMR exchange mechanisms.

To contextualize the proposed framework within existing EMR exchange paradigms, Table 1 provides a high-level comparison of centralized, conventional hybrid, and blockchain-based EMR systems alongside the proposed BioCareCloud framework.

Proposed framework

The proposed framework, referred to as BioCareCloud, is designed to support system-level integration and workflow analysis across multiple healthcare institutions. Most existing EMR exchange systems rely on health ID cards, national identification numbers, or QR code identifiers to access and share patient data. Although these methods can ensure accurate record retrieval, they also have limitations, such as the risk of card loss or damage. In contrast, the proposed framework utilizes fingerprint-based authentication using hashed identifiers to support reliable patient verification without storing biometric images. This approach enhances security and accuracy, reduces the risk of data misuse, and simplifies the patient verification process. The proposed framework is presented in detail in the following sections, with each component and layer thoroughly described.

Hybrid cloud computing architecture has emerged as a strategic approach that integrates multiple cloud models to deliver robust and flexible solutions that meet healthcare requirements[40]. The architecture of the proposed healthcare system employs a multi-layered hybrid cloud framework to facilitate EMR integration across various hospitals. The framework comprises several cloud components, each playing a crucial role in

Feature	Centralized cloud	Conventional hybrid cloud	Blockchain-based EMR	Proposed BioCareCloud
Data storage	Fully centralized	Distributed but shared	Distributed ledger	Distributed, hospital-owned
Record discovery mechanism	Central database	Direct querying	Ledger lookup	Index-only Community Cloud
Privacy exposure	Relatively high	Medium	Medium	Lower exposure (no EMR stored in Community Cloud)
Emergency workflow suitability	Limited	Moderate	Low (latency)	Designed for ED workflows
Selective record access	No	Limited	Limited	Yes (scenario-based)
Patient identity resolution	Local/manual	Local/manual	Key-based	Government Cloud–assisted
Workflow differentiation	No	No	No	Yes (scenario-based)

Table 1. Comparison of EMR exchange architectures.

Component	Primary role in the framework
Hospital Information System (HIS)	Manages local EMRs, supports patient registration, clinical documentation, and synchronization with the private cloud.
Private cloud	Securely stores and manages hospital EMRs, coordinates communication with other clouds, and integrates biometric and IoT data.
Community cloud	Maintains patient metadata and indexing information to identify hospitals holding relevant EMRs without storing clinical data.
Government cloud	Provides verified demographic data and supports automated EMR creation using fingerprint-based identification.
Fingerprint authentication	Enables secure and accurate patient identification during admission using privacy-preserving biometric hashing.
IoT wearable bracelet	Collects and transmits real-time vital signs to support pre-consultation clinical preparation and monitoring.

Table 2. Summary of the main components of the proposed hybrid cloud framework and their roles.

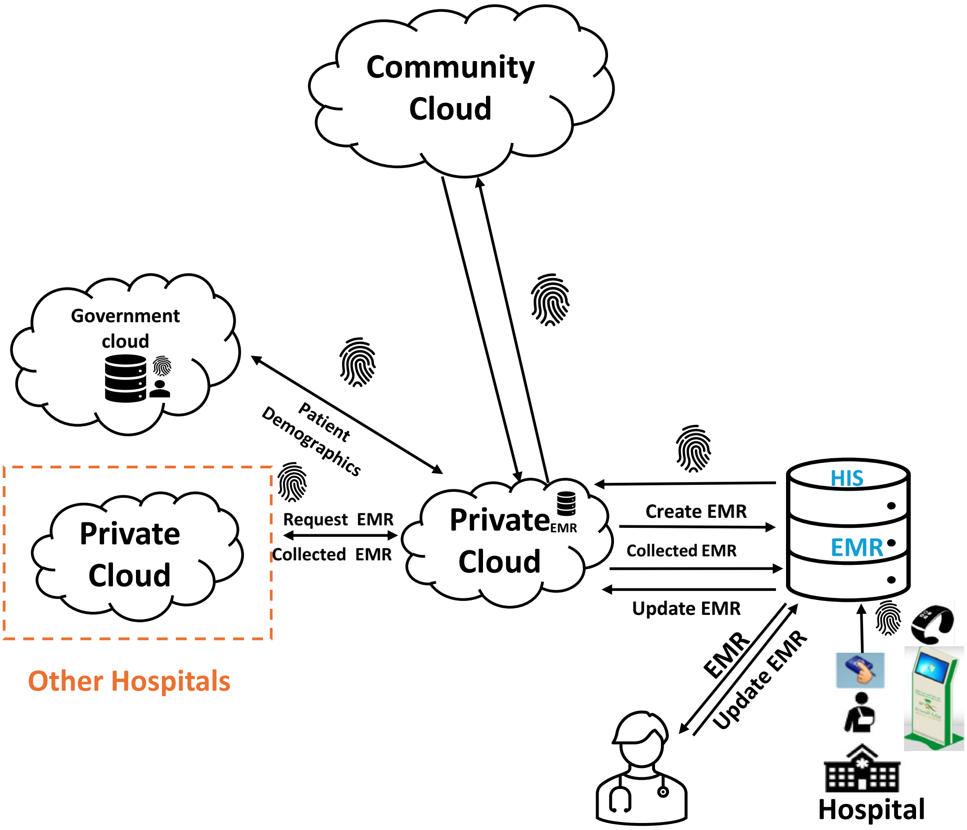

Fig. 1. The proposed framework.

supporting secure data exchange and coordinated clinical workflows. Table 2 provides a concise summary of the main components of the proposed framework and their respective roles.

The framework includes the following components: first, a private cloud for each hospital, which protects sensitive patient information by maintaining it within a secure and controlled environment. Second, a shared community cloud serves as a coordination layer that supports inter-hospital communication and record discovery. Finally, a government cloud is integrated to support automated EMR initialization and system-level coordination, reducing reliance on manual data entry and supporting overall workflow efficiency across institutions. Figure 1 illustrates the components of the proposed hybrid cloud architecture framework.

Private cloud layer

In the proposed BioCareCloud framework, each hospital operates an independent private cloud that serves as the secure virtual infrastructure for storing and managing its EMRs. The private cloud functions as a coordination layer that enables controlled interaction between the HIS, the community cloud, the government cloud, and other hospitals' private clouds, thereby supporting secure and efficient EMR exchange within a distributed healthcare environment.

The private cloud integrates directly with the HIS through internal application programming interfaces (APIs)[41], supporting the creation, modification, and synchronization of EMRs while ensuring data consistency and reliability within the hospital system. In addition, the private cloud manages real-time data streams received from fingerprint authentication devices and IoT wearable bracelets, enabling the secure processing and storage of biometric identifiers and vital-sign measurements.

During patient admission, when a fingerprint is captured, the HIS first checks for the existence of a corresponding local EMR. If no record is found, the private cloud issues a secure API request to the government cloud to retrieve verified demographic information, which is then used to automatically create a new EMR. In parallel, the private cloud queries the community cloud to determine whether the patient has existing medical records at other participating hospitals. Upon receiving a list of relevant hospitals, the private cloud establishes secure, direct API-based communication only with those institutions to request the associated EMRs.

All EMRs are stored locally within a relational database in each hospital's private cloud to ensure referential integrity, transactional consistency, and high data reliability. Any updates performed within the HIS are immediately synchronized with the private cloud, maintaining alignment between operational clinical systems and cloud-based data management.

From a system-level perspective, the private cloud architecture supports scalable and modular operation. Each hospital's private cloud functions as a self-contained unit that can be integrated into the broader network through standardized APIs, enabling horizontal scalability without requiring architectural restructuring. As additional hospitals join the system, new private clouds can be registered with the community cloud's indexing service, allowing seamless expansion of the network.

By distributing data storage and processing across hospital-owned private clouds, the framework balances computational and storage loads across the system. This decentralized, API-driven design supports stable performance, flexibility, and service continuity as healthcare data volumes and institutional participation increase within the hybrid cloud environment.

Community cloud layer

In the proposed BioCareCloud framework, the community cloud functions as a federated coordination layer that maintains patient-level metadata to support efficient EMR discovery across multiple hospitals. Rather than storing clinical records, the community cloud manages reference information, including a privacy-preserving fingerprint hash for each patient and a list of hospitals that currently hold the patient's EMRs.

The primary role of the community cloud is to enable inter-hospital record discovery without transferring or replicating sensitive medical data. Each participating hospital retains full ownership of its EMRs within its private cloud, while the community cloud operates as an intermediary that facilitates record location through metadata indexing. This design separates data storage from coordination, reducing privacy exposure and limiting unnecessary data movement.

When a patient arrives at a hospital, the hospital's private cloud submits the patient's fingerprint hash to the community cloud to determine whether prior records exist. The community cloud matches the query against its metadata index and identifies the hospitals that hold relevant EMRs. It then returns a list of these hospitals to the requesting private cloud, which subsequently retrieves the records directly through secure, API-based communication channels. By directing requests only to relevant institutions, the framework reduces network overhead and improves retrieval efficiency.

If the patient has no prior record within the system, the community cloud creates a new metadata reference and registers the current hospital as the initial record holder. If prior records exist, the community cloud updates the patient's index by appending the current hospital to the list of associated institutions. At no point does the community cloud access, store, or process clinical content; its functionality is strictly limited to metadata management.

From a system-level perspective, this metadata-driven coordination model reduces synchronization overhead by eliminating the need for centralized EMR repositories or continuous bulk data replication. Instead, only lightweight index updates are exchanged following relevant patient interactions. As a result, the system achieves faster record discovery, lower communication overhead, and improved responsiveness in distributed healthcare environments.

In the proposed framework, updates to the community cloud are event-driven and occur immediately after relevant patient interactions. Following each hospital visit, the community cloud is updated via API communication to either create a new patient reference or register the current hospital in an existing index. This design supports timely, on-demand record discovery in time-critical clinical workflows.

Government cloud layer

The government cloud in the proposed hybrid healthcare architecture functions as a government-controlled digital infrastructure that operates independently of hospital systems but interacts with them to manage and verify patient demographic data.

This cloud serves as a national demographic reference, maintaining a centralized database that stores essential non-clinical information, such as fingerprint hashes, national ID numbers, names, birth dates, gender, and other identification attributes, used to uniquely identify patients across all healthcare institutions.

The government cloud is not managed or controlled by individual hospitals; rather, it is a part of the national health information infrastructure and is accessed only when needed. Specifically, communication with the government cloud is established when a patient visits a hospital for the first time. In this case, the hospital's private cloud securely transmits the patient's fingerprint to the government cloud through an API request.

The government cloud processes this request by searching its demographic repository to verify whether a record already exists for the patient. If a match is found, the corresponding demographic data are returned to the hospital's private cloud. The system then automatically creates a new EMR for the patient.

This automated system helps reduce reliance on manual intervention and reduces the risk of input errors through the use of fingerprint verification. Furthermore, it helps reduce waiting at hospital reception desks for administrative registration.

From a technical perspective, the communication is implemented through API messages that ensure data confidentiality and integrity. These APIs are designed to operate under strict authentication protocols, ensuring that only authorized hospital systems can access government cloud services. Additionally, the government cloud supports consistency and reliability throughout the healthcare ecosystem. Establishing a single source for patient demographics helps prevent duplicate identity data across hospitals.

From an architectural perspective, the government cloud is essential for maintaining data integrity and unifying patient identity in a hybrid healthcare environment. It allows hospitals to automatically retrieve verified demographic data using a patient's fingerprint, supporting accurate and standardized EMR creation nationwide. By integrating fingerprint verification, secure APIs, and centralized data governance, the government cloud strengthens consistency in national healthcare data and supports the automation of clinical workflows, while maintaining strong security and privacy protections.

In this study, the government cloud is modeled as a national demographic support service for system-level workflow analysis. The interaction with the government cloud is represented using an abstracted service delay that is treated as a configurable simulation parameter. This parameter is introduced to capture the role and timing impact of centralized demographic verification within the admission workflow, while avoiding assumptions of instantaneous access or guaranteed response times in real-world national systems.

Fingerprint authentication

The proposed model includes several self-service kiosks at the hospital gate to streamline automated patient onboarding and avoid waiting in line. To ensure accuracy and effective patient identification, the framework utilizes fingerprint authentication.

The fingerprint scanner plays a central technical role in the proposed hybrid healthcare architecture, serving as a biometric authentication interface between patients and the hospital's digital infrastructure. It reduces reliance on traditional manual identification processes, such as entering a national ID or medical record number, by employing a secure fingerprint-based verification mechanism that supports accurate and efficient patient identification.

From a technical perspective, the fingerprint scanner is implemented as an independent module that acquires, processes, and validates fingerprint data during patient registration and authentication. When a patient arrives at the hospital, they interact with a self-service kiosk, where the scanner captures the patient's fingerprint and converts it into a unique digital hash. This hash serves as a consistent reference identifier for the patient across the healthcare system.

To preserve biometric privacy, the system does not store or transmit raw fingerprint images. Instead, distinctive features are extracted from the captured fingerprint and transformed into a fixed-length hash via a one-way hashing process. This hash functions as a privacy-preserving identifier and cannot be reversed to reconstruct the original fingerprint. During authentication, newly captured fingerprints are processed in the same manner and matched against stored hashes, ensuring secure identification without exposing sensitive biometric data.

Once the fingerprint is captured, it is transmitted to the HIS. The HIS checks whether a corresponding EMR exists. If no record is found, the fingerprint is securely sent via API calls to the government cloud to create a new EMR.

Internally, the fingerprint scanner module is designed with parameters that define its operational behavior, including scanning time and accuracy rate. These performance indicators enable real-time monitoring of the fingerprint scanner's efficiency and reliability. Upon receiving a scan request, the scanner initiates a timed biometric capture process. Once complete, it generates a response message containing the patient's fingerprint hash, timestamp, and a success flag, which is then transmitted to the HIS through a secure channel. When biometric authentication fails, a fallback manual verification process is triggered, modeled as an additional time penalty in the simulation framework, introducing an extra processing step in the admission workflow.

This biometric-based identification mechanism helps enhance both security and usability By linking each patient to a unique fingerprint hash, the system helps reduce the risk of duplicate or erroneous patient identities. It also helps prevent unauthorized access, as fingerprint data is bound to the individual and cannot be falsified through traditional credential theft. Moreover, automated fingerprint recognition reduces the need for manual data entry in most admission cases. The patient onboarding process becomes more streamlined, enabling patients to authenticate themselves directly at the kiosk. This reduces wait time at the reception desk, thereby improving hospital throughput and the patient experience.

Technically, the fingerprint scanner operates as an input device within the hospital's infrastructure and communicates with the private cloud through the HIS. When a patient's fingerprint is captured, the scanner transmits the fingerprint data to the HIS, which then forwards it to the hospital's private cloud via secure API interactions. All communications occur over encrypted channels to ensure the confidentiality and integrity of biometric information during transmission. This design ensures that the fingerprint data remains protected and accessible only to authorized system components.

In summary, the fingerprint scanner serves as the technological gateway that bridges the physical presence of patients with the digital healthcare infrastructure. It provides a fast, secure, and reliable mechanism for patient identification and record creation, supporting integration with HIS, private, community, and government cloud components. Through fingerprint precision, automated data handling, and real-time system feedback, the fingerprint scanner enhances operational efficiency, improves data accuracy, and supports the broader goal of secure, automated patient management in the distributed healthcare environment.

IoT wearable bracelet

Wearable bracelets monitor physiological data at regular intervals, including heart rate, body temperature, blood pressure, and oxygen saturation, using integrated sensors. These IoT devices automatically transmit the collected data to cloud platforms[42].

The traditional method of recording vital signs involves nurses manually measuring, recording, or entering patient vital signs into the HIS, which is time-consuming and error-prone[43,44]. To address this challenge, IoT smart bracelets are employed to continuously measure vital signs and transmit them directly to the cloud.

To begin the procedure, all patients are requested to use the fingerprint scanner. Upon successful fingerprint reading, a digital consent message[45] will be displayed on the kiosk screen to ensure compliance with data privacy regulations and ethical standards. This message informs the patient that their biometric and health data will be collected, stored, and securely shared within the healthcare cloud infrastructure. To continue, the patient must provide their approval by selecting "Agree".

Upon this, if the patient has an EMR in the HIS, the kiosk will dispense a disposable smart IoT bracelet to the patient. For patients visiting the hospital for the first time and who do not have an existing EMR, the kiosk will display a message: "Please wait while we create your EMR". The disposable IoT bracelet will be issued only after the EMR has been successfully created.

When the patient receives the IoT bracelet and wears it properly, the kiosk will display a confirmation message indicating successful pairing. The system will then begin real-time monitoring of the patient's vital signs, which will be securely transmitted to the hospital's private cloud and stored in the patient's EMR.

This automated workflow improves the consistency of clinical data, supports the initial collection of vital signs before clinical triage, and helps reduce repetitive manual measurements, thereby supporting nursing workflows while preserving the essential role of human clinical judgment and triage decisions. By contrast, if a patient disagrees with the consent, they will need to visit the hospital reception and follow the traditional onboarding method.

Abnormal readings from the bracelet can generate alerts for medical staff, facilitate timely clinical attention, and improve situational awareness. Beyond supporting immediate clinical response, the disposable nature of the bracelet promotes infection control protocols[46], minimizing the risk of cross-contamination between patients. In addition, these real-time vital sign readings are made available to the physician upon the patient's arrival at the clinic, supporting informed clinical decision-making while streamlining the onboarding process for real-time health monitoring.

In this study, the wearable bracelet is modeled at a functional level to support system-level workflow analysis. Hardware-specific characteristics, such as device cost, battery lifetime, and low-level communication protocols, are abstracted, as the focus of this work is on evaluating admission and monitoring workflows rather than detailed device implementation.

Data flow and communication workflow

The proposed system creates a patient-centered workflow that automates identity verification through an integrated biometric fingerprint, retrieves and exchanges EMR, and enables real-time health monitoring through an IoT bracelet, all supported by a multi-layered hybrid cloud infrastructure. The data exchange mechanism is designed to support efficiency, scalability, and confidentiality in communication among different hospitals. The framework has four cases for patients. In the next section, we will discuss and explain these cases.Table 3 illustrates the four scenarios.

It is important to note that the four cases defined in this framework do not correspond to pre-existing categories in the real-world hospital data. Rather, they represent logical workflow scenarios introduced by the proposed hybrid cloud architecture and the Community Cloud indexing mechanism. In the current hospital setting, where no inter-hospital EMR exchange exists, patients are not differentiated based on record availability across institutions.

Case 0: workflow when no EMR exists in local HIS or other hospitals

If the patient's EMR is not found in the local HIS after fingerprint authentication, the system initiates a secondary workflow to create a new record. First, the hospital's Private Cloud (PC) sends the fingerprint to the Government Cloud (GC) to retrieve patient demographic data. If a match is found, the GC returns demographic data, including national ID, name, age, and gender, to the PC, which then forwards this information to the HIS. The HIS uses these verified demographics to create a new EMR record for the patient automatically.

Simultaneously, the patient's fingerprint is sent to the community cloud (CC). The CC searches its database and finds no existing patient record. Based on this, the CC creates a new reference entry for the patient in its database, storing the patient's encrypted fingerprint along with the current hospital ID. The CC then sends a response code "0" to the PC, indicating that no existing record for the patient was found in any other hospital.

Case type	Explanation
Case 0	Represents a new patient who does not have an EMR in HIS or a record in the community cloud.
Case 1	Represents a patient with a local EMR in HIS and one record in the community cloud, with no previous visits to other hospitals.
Case 2	Represents a patient with a local EMR in HIS and a record in the community cloud, which reveals previous visits to other hospitals.
Case 3	Represents a new patient who does not have an EMR in HIS but has a record in the community cloud, which reveals previous visits to other hospitals.

Table 3. Patient case types.

This code confirms that the patient is new to the shared healthcare environment and triggers the appropriate workflow for first-time patient registration.

While the patient waits for their clinical consultation, the PC continues to collect real-time vital signs via the wearable IoT bracelet. These readings are transmitted to the HIS when the patient is called for consultation. The HIS then compiles the new EMR along with the collected vital signs and transmits it to the attending physician.

During the medical consultation, the physician may update the patient's EMR with diagnosis notes, prescriptions, or other relevant medical entries. These updates are saved to the HIS, which subsequently synchronizes the updated EMR with the PC, ensuring consistency across the system and preparing the record for future access or inter-hospital sharing if needed. Figures 2 and 3 illustrate the flowchart and workflow of Case 0, respectively.

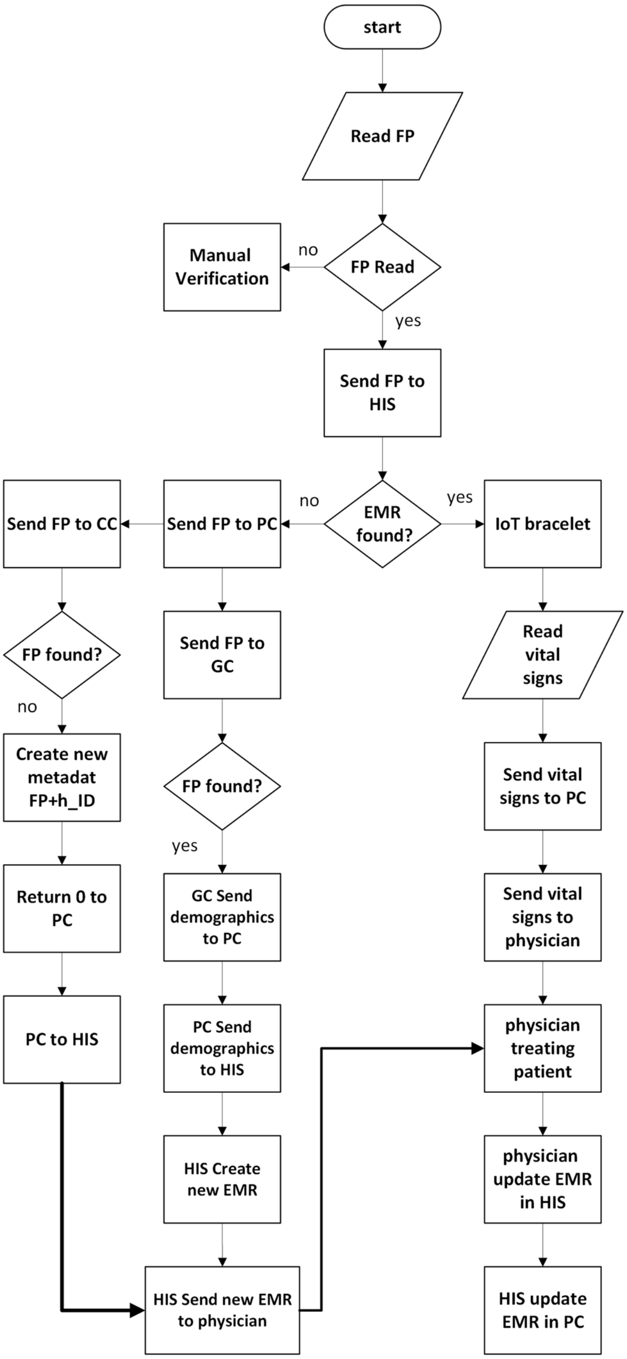

Fig. 2. Case 0 flowchart.

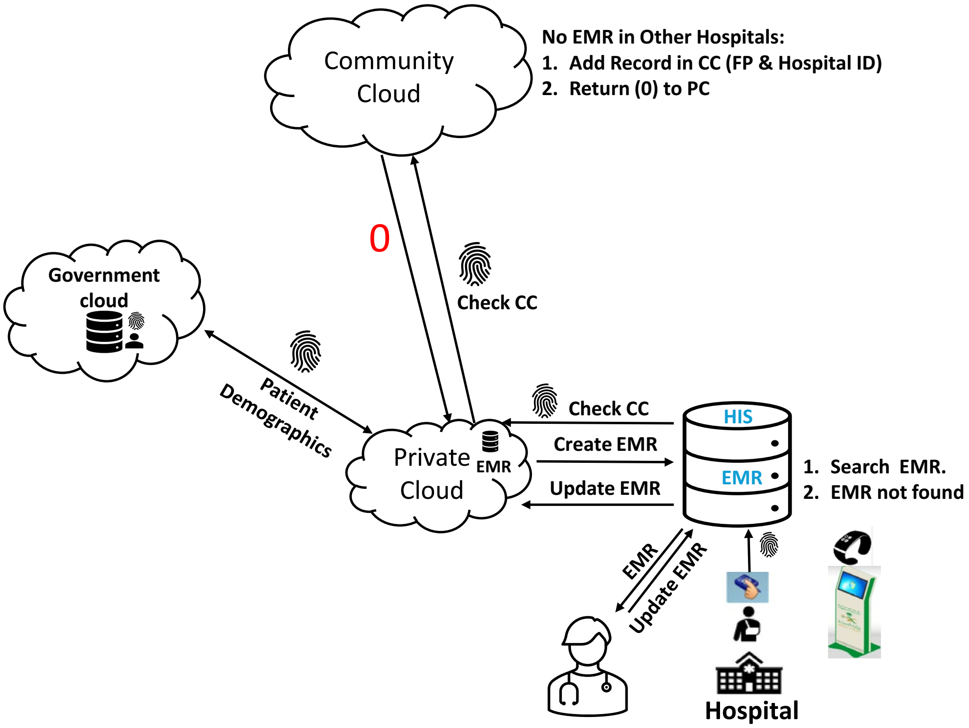

Fig. 3. Case 0 workflow.

Case 1: workflow when EMR is found locally and no external records are identified
If the patient's EMR is found in the local HIS following fingerprint authentication, the hospital PC forwards the patient's fingerprint to the CC. Even when a local EMR exists, the CC is queried to confirm whether the patient has records in other hospitals, as the absence of external records is determined only after this verification step. Case 1 is therefore identified based on the CC response, rather than being assumed a priori.

The CC searches its database and finds only one hospital's information along with the patient's fingerprint. Based on this, the CC will send a response code "1" to the PC, indicating that the patient has a prior medical record stored only in the same hospital that sent the request. Consequently, a copy of the patient's EMR, stored in the hospital's HIS, is securely transmitted to the attending physician.

While the patient waits for the clinical consultation, the patient's real-time vital signs are collected and incorporated into the EMR, making them available to the physician during the consultation.

Additionally, the physician updates the patient's EMR during the consultation, and the revised record is saved in the HIS and synchronized with the hospital's PC, ensuring consistency across the system and preparing the record for future access or inter-hospital sharing if needed. Figures 4 and 5 illustrate the flowchart and workflow of Case 1, respectively.

Case 2: workflow when EMRs exist in HIS and in multiple external hospitals
When a patient's EMR is found in the local HIS, the fingerprint is sent to the CC to check for other EMRs across the healthcare network. The CC sends a response code "2" to the PC, along with a list of hospitals that the patient has previously visited. The list includes the hospital's ID. This list is forwarded to the requesting hospital's PC. The PC verifies that its institution is included in the list, then proceeds to initiate secure communication with the other hospital's PC to request a copy of the patient's EMRs.

While the patient is waiting, real-time vital signs are collected via the assigned wearable IoT bracelet. These readings are transmitted to the HIS when the patient is called for consultation. The HIS compiles all relevant information, including the local hospital's EMR, the external collected EMRs from other hospitals, and the newly recorded vital signs, into a unified record. This comprehensive medical history is then presented to the physician in a smart interface before the examination.

The physician's clinical updates are persistently stored in the HIS and subsequently synchronized with the PC to ensure the consistency and authenticity of inter-institutional patient referencing. Figures 6 and 7 illustrate the flowchart and workflow of Case 2, respectively.

Case 3: workflow when EMR is not found locally, but exists in other hospitals
This scenario represents a hybrid case that combines Cases 0 and 2. The patient does not have an EMR in the HIS, which indicates that this is their first visit to the current hospital. Consequently, the PC initiates a request to the GC to retrieve the patient's demographic data required to create a new EMR in the HIS.

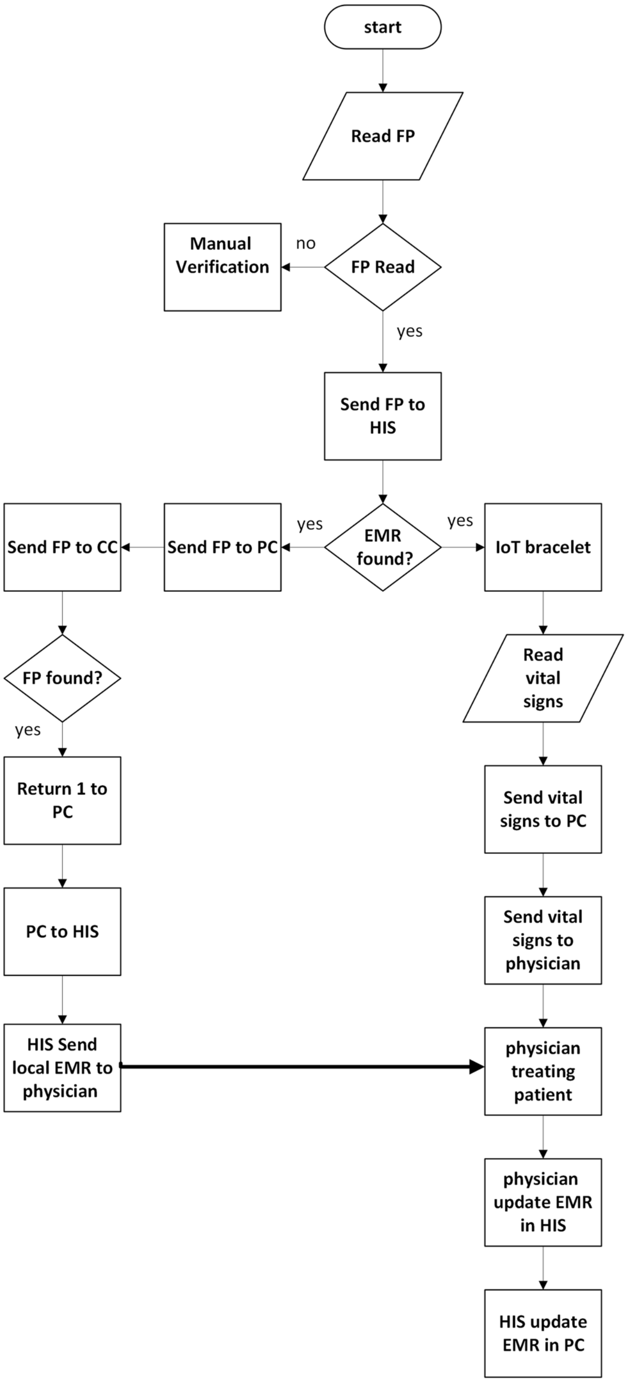

Fig. 4. Case 1 flowchart.

Simultaneously, the PC communicates with the CC to determine whether the patient has visited other hospitals previously. Upon receiving a response code “3” from the CC, along with a list of hospital IDs, the PC establishes secure connections with the identified hospitals to request copies of the patient’s EMR.

Thus, this case executes both workflows in parallel: (1) the creation of a new EMR based on fingerprint verification and (2) the aggregation of distributed medical records from previously visited institutions. This approach supports the availability of a more complete clinical profile for first-time visitors at the point of care.

While this process occurs, real-time vital signs are collected by the PC. When the patient is called for clinical consultation, the PC sends the vital signs to the HIS. The HIS compiles all relevant information, including the newly created local hospital’s EMR, the externally collected EMRs from other hospitals, and the newly recorded vital signs, into a unified record. This comprehensive medical history is then presented to the physician in a smart interface before the examination.

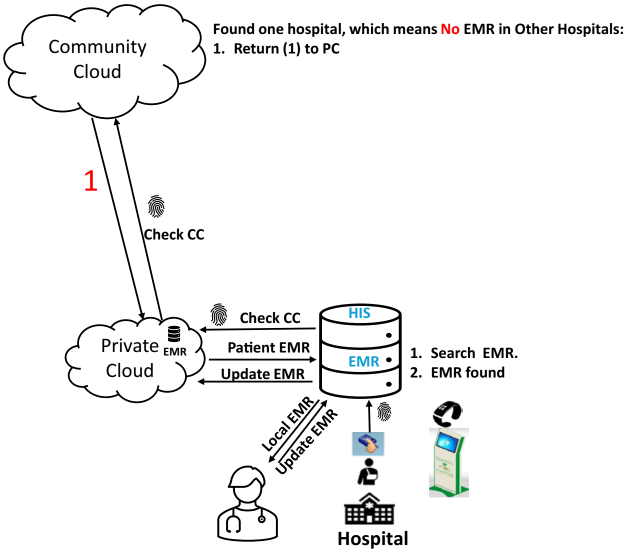

Fig. 5. Case 1 workflow.

After the consultation, the physician updates the EMR with diagnostic notes, prescriptions, or follow-up instructions. The updated EMR is saved in the HIS and forwarded to the PC to ensure synchronization and up-to-date referencing for future hospital visits. Figures 8 and 9 illustrate the flowchart and workflow of Case 3, respectively.

Security and privacy considerations

Biometric fingerprint data integrity and protection

In the proposed framework, fingerprint authentication is employed as a privacy-preserving alternative to traditional patient identification methods commonly used in hospitals. To protect biometric privacy, raw fingerprint images are neither stored nor transmitted across system components.

Instead, distinctive fingerprint features are locally extracted and transformed into a fixed-length, one-way cryptographic hash. This hashed representation functions as an anonymized identifier that cannot be reversed to reconstruct the original fingerprint, thereby preserving biometric confidentiality and identity integrity.

Only hashed identifiers are used during inter-system communication between the hospital private cloud, the community cloud, and the government cloud. All such communications are assumed to occur over encrypted channels using standard secure communication protocols. The community cloud stores only hashed identifiers and hospital references and contains no clinical or demographic patient information.

By relying on hashed biometric identifiers and encrypted communication, the framework reduces the risk of biometric exposure, limits unnecessary data propagation, and ensures that medical record transactions remain securely linked to verified patient identities. These secure communication mechanisms apply to all API-based interactions described in the Proposed Framework.

Attack surface and threat considerations

Although the community cloud stores only hashed biometric identifiers and hospital references, specific attack vectors may still be considered at the metadata level. For example, linkage attacks could infer patient movement patterns by correlating repeated hash appearances with timestamps or hospital identifiers. To mitigate such risks, the proposed framework limits the information stored in the community cloud to the minimum necessary for record discovery and avoids storing clinical, demographic, or temporal data.

Replay or spoofing attacks based on compromised hash values are mitigated by performing fingerprint capture and feature extraction locally within trusted hospital environments, combined with secure channel communication and authentication controls. The framework assumes that biometric verification is always coupled with live fingerprint capture rather than static identifier reuse.

Cryptographic mechanisms such as salting, key rotation, or collision-resistant hash selection are considered implementation-level concerns and are therefore abstracted in this system-level study. The framework assumes the use of standard, well-established cryptographic primitives without prescribing specific algorithms.

Simulation settings

This study evaluates the performance of the proposed framework by comparing real-world hospital data with simulation-derived outcomes. The study evaluates the weekly average treatment and waiting times and estimates the theoretical maximum number of patients that the hospital's ED can accommodate within 1 h.

The simulation was conducted over a 1-week period of ED arrivals, and its results were then compared with the corresponding real hospital data to examine the framework's operational behavior and applicability.

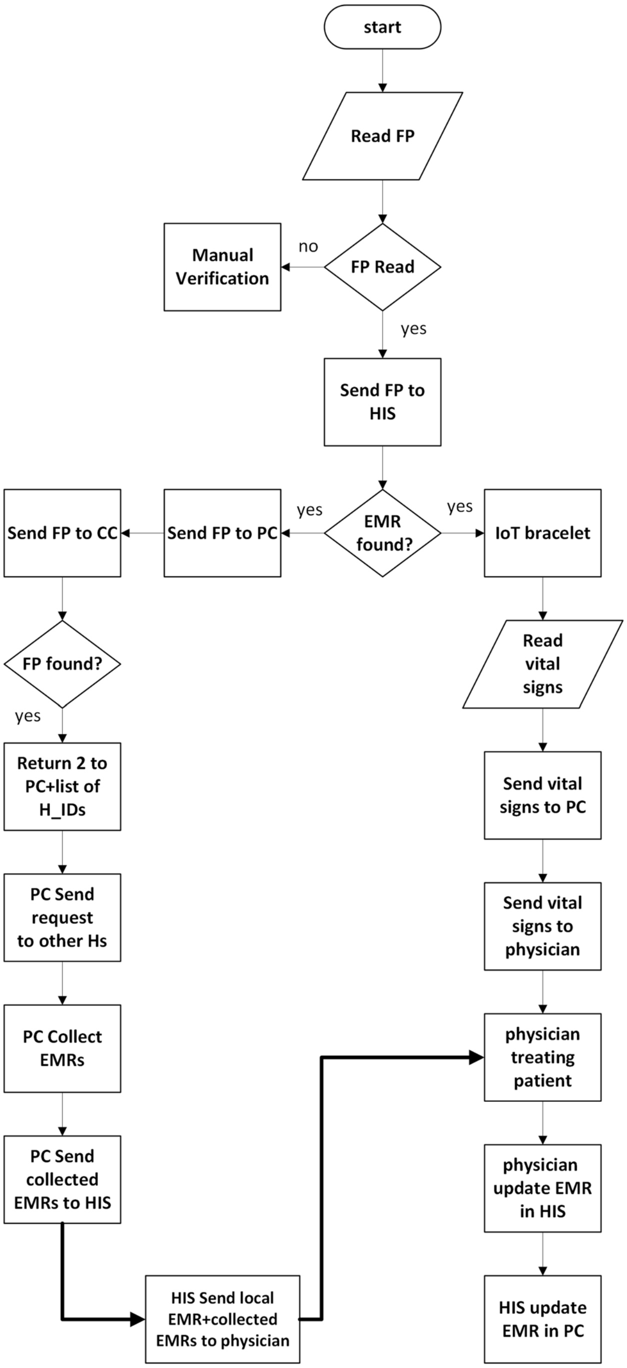
start
Read FP
FP Read
no
Manual Verification
yes
Send FP to HIS
EMR found?
yes
Send FP to PC
Send FP to CC
yes
IoT bracelet
FP found?
yes
Return 2 to PC+list of H_IDs
PC Send request to other Hs
PC Collect EMRs
PC Send collected EMRs to HIS
HIS Send local EMR+collected EMRs to physician
Read vital signs
Send vital signs to PC
Send vital signs to physician
physician treating patient
physician update EMR in HIS
HIS update EMR in PC

Fig. 6. Case 2 flowchart.

Using a week as a temporal feature is well suited compared to extended periods, such as months or years, because weekly features offer finer temporal resolution. This granularity enables the identification of variations in patient volumes on specific weekdays and weekend patterns that are occasionally obscured when data is aggregated over prolonged durations. Moreover, weekly information aligns well with common operational practices of ED, where physician and nursing schedules, as well as resource planning, are typically organized weekly[47].

Therefore, weekly features offer a balanced approach by capturing fine-grained and recurring temporal dynamics, such as differences across weekdays, holidays, or even specific hours of the day, rather than relying solely on generalized averages derived from longer-term aggregations, such as months[48–50].

We used OMNeT++ as the simulation environment because it is a modular, event-driven framework that supports discrete-event models for complex networked systems and service operations[51]. The EMR simulation network was designed to represent a connected healthcare environment involving multiple hospitals, medical devices, and centralized modules. The network comprised three hospitals, each containing six functional

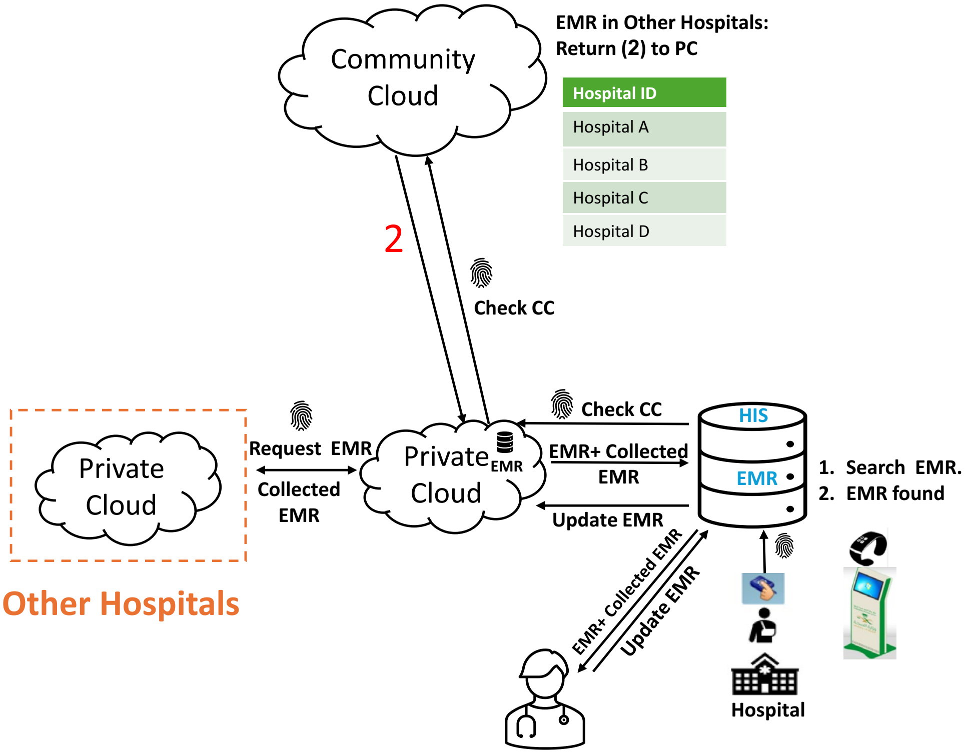

Fig. 7. Case 2 workflow.

modules: Patient, Fingerprint Scanner, IoT Bracelet, HIS, Private Cloud, and Doctor. Additionally, three shared modules, CC, GC, and other hospitals' cloud, managed data exchange and system coordination, resulting in a total of 12 interconnected modules. Table 4 presents the simulation environment and network topology used to build the simulation.

The reported simulation time represents a logical execution window sufficient to process all modeled events rather than a real-time duration. This choice reflects the discrete-event nature of the simulation, where system performance is evaluated based on event ordering and workflow interactions rather than wall-clock execution time.

Table 5 summarizes the key operational and modeling assumptions used in the simulation, complementing the infrastructure parameters reported in Table 4.

In the simulation, the Government Cloud (GC) is represented as a national demographic support service accessed during first-time hospital visits. To enable system-level workflow evaluation rather than infrastructure-level performance analysis, the GC is modeled using abstracted configuration parameters, as summarized in Table 4. These parameters are introduced to represent the functional role of centralized demographic support within the admission workflow and do not assume perfect data availability, instantaneous access, or guaranteed response times in real-world national systems. Accordingly, GC-related delays are explicitly reflected as part of the onboarding process in the simulation, allowing their impact on patient admission flow to be examined under the modeled assumptions without making claims about the operational performance of any specific national deployment.

For non-governmental system components, such as local hospital modules and community cloud services, the simulated network and database delays represent abstracted lower-bound timings consistent with modern hospital IT environments. In practice, many hospital information systems operate on local or regional networks with high-speed connectivity and indexed data access, resulting in millisecond-scale internal communication and query delays. These values are used to provide internally consistent timing relationships between system components, rather than to model the exact performance of specific hospital deployments.

Patient arrival volumes used in the simulation were derived directly from real-world emergency department data collected from the three hospitals, as summarized in Table 7. For each simulation run, the day of the week is specified, and the corresponding patient arrival volumes are applied accordingly.

The four workflow cases represent design-level scenarios introduced by the proposed hybrid cloud architecture and Community Cloud indexing mechanism, rather than empirically observed categories in the original hospital data. Patient allocation across these cases is therefore generated probabilistically.

All remaining operational and modeling parameters are fixed and fully specified in Tables 4 and 5. Randomness arising from patient allocation and treatment-time generation is mitigated through repeated simulation runs. Accordingly, the simulation emphasizes comparative system-level workflow evaluation rather than precise prediction of absolute system response times in specific hospital infrastructures.

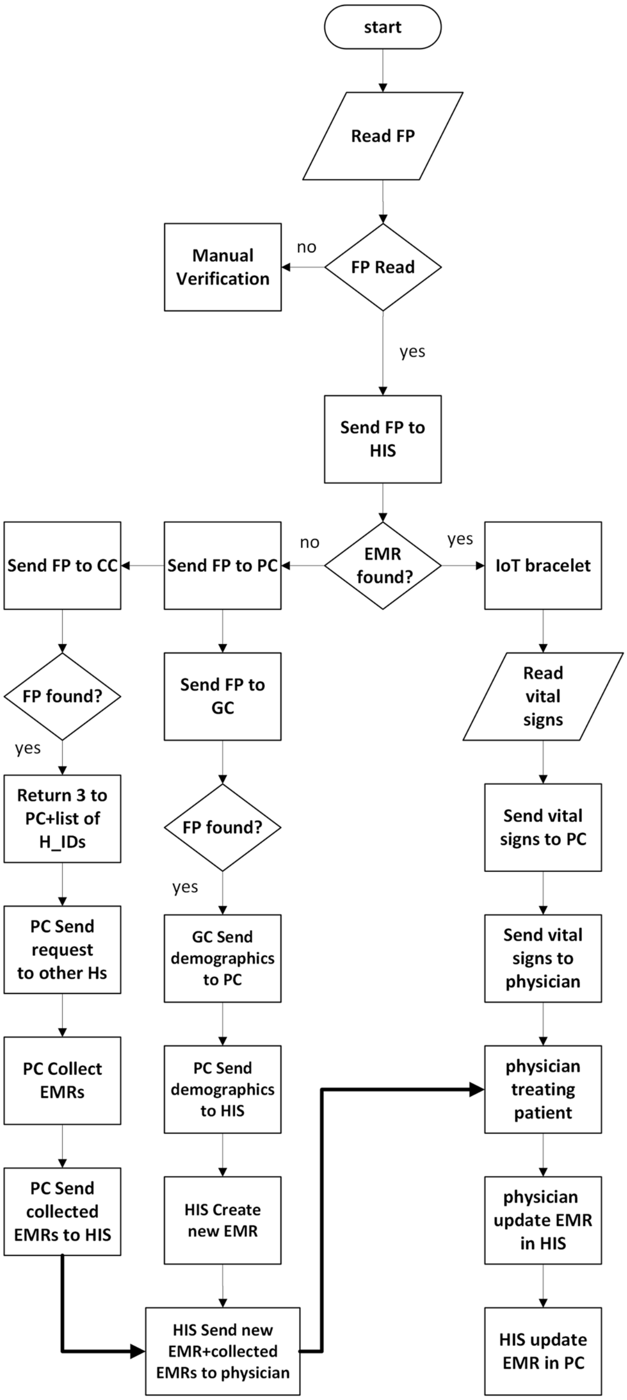
start
Read FP
FP Read
no
Manual Verification
yes
Send FP to HIS
EMR found?
no
yes
Send FP to CC
Send FP to PC
IoT bracelet
FP found?
yes
Send FP to GC
Read vital signs
Return 3 to PC+list of H_IDs
FP found?
yes
Send vital signs to PC
PC Send request to other Hs
GC Send demographics to PC
Send vital signs to physician
PC Collect EMRs
PC Send demographics to HIS
physician treating patient
PC Send collected EMRs to HIS
HIS Create new EMR
physician update EMR in HIS
HIS Send new EMR+collected EMRs to physician
HIS update EMR in PC

Fig. 8. Case 3 flowchart.

Biometric authentication failure modeling

Fingerprint-based biometric authentication systems are subject to non-zero false rejection rates (FRR), implying that a subset of valid authentication attempts may fail and require fallback procedures. In this study, biometric authentication behavior is represented within a discrete-event simulation framework. Biometric failures are incorporated probabilistically based on literature-informed FRR parameters, and no real-world biometric measurements are used. For each patient admission in the simulation, a single biometric authentication attempt is modeled. A failure is triggered randomly according to the specified FRR probability. When a failure occurs, the admission workflow transitions directly to a manual identity verification step. The FRR therefore defines the probability of invoking this fallback procedure, while the additional processing time is introduced by the manual verification step itself. Published benchmark evaluations of fingerprint recognition systems report FRR values on the order of several percentage points under specific datasets and operating thresholds. For example, FRR values

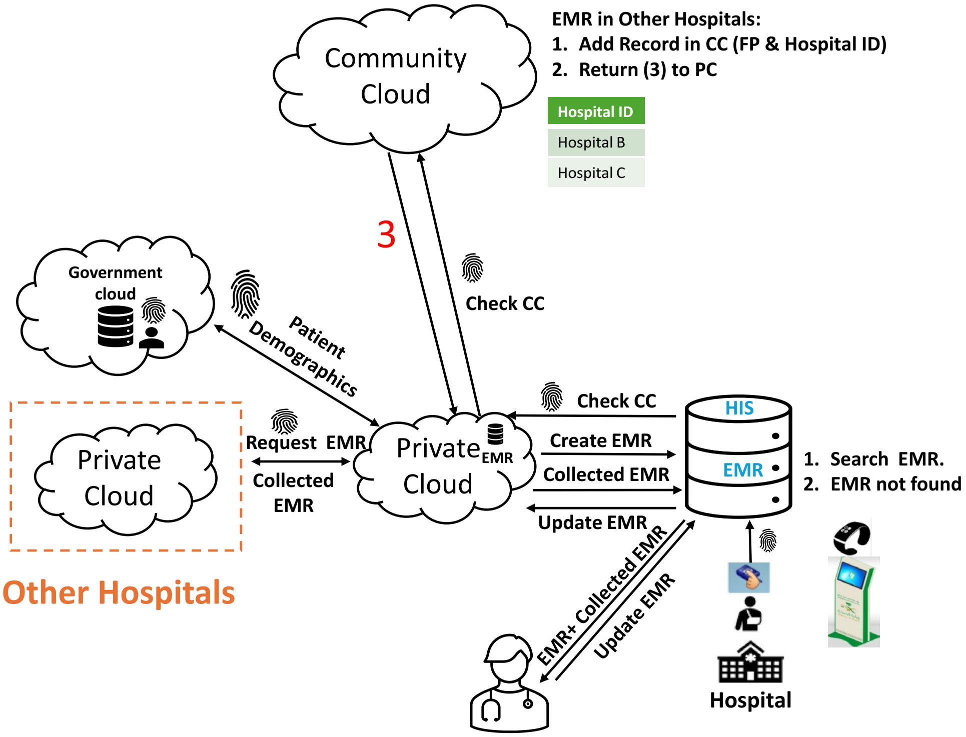

Fig. 9. Case 3 workflow.

Category	Item	Specification
Environment	Simulator	OMNeT++ v6.0
	Programming standard	C++17
	Operating system	Windows 10
	EMR framework	Custom-built EMR framework
	Total simulation time	60 seconds
Network topology	Hospitals	3 hospitals
	Modules per hospital (6)	Patient, Fingerprint Scanner, IoT Bracelet, HIS, Private Cloud, Doctor
	Shared modules (3)	Community Cloud, Government Cloud, Other Hospitals Private Cloud
	Total modules	12 interconnected modules
Network configuration	Base latency	2 ms
	Bandwidth	1 Gbps
	Packet loss rate	0.1%
	Max concurrent connections	1000
Database parameters	Local Database	Query time 1 ms; 100K records per hospital
	Community Cloud Database	Query time 2 ms; 10M records
	Government Cloud Database	Service delay 500 ms; Demographic repository scale 50M records
Server configuration	Local Server	CPU 1.0; 32 GB RAM; Disk 500 MB/s; 50 concurrent tasks
	Community Cloud Server	CPU 2.0; 128 GB RAM; Disk 1000 MB/s; 200 concurrent tasks
	Government Cloud Server	CPU 0.8; 64 GB RAM; Disk 300 MB/s; 100 concurrent tasks

Table 4. Simulation environment and network configuration of the hybrid cloud framework.

of approximately 7.75% have been reported in controlled evaluations[52]. Consistent with these reports, biometric authentication failures are modeled as rare, randomly occurring events rather than systematic occurrences.

In the simulation, the manual identity verification step is represented as an additional fixed processing delay of 7 minutes. This value is adopted as a conservative modeling assumption informed by durations reported in prior studies of manual patient registration processes[53]. The selected delay is used solely for simulation purposes and does not represent a measured, validated, or site-specific real-world processing time.

Parameter	Specification
Simulation horizon	7 consecutive days (24 hours/day)
Patient arrival input	Daily patient volumes derived from real ED data (Table 7)
Physician capacity	9 concurrent physicians (fixed across all days)
Number of simulation runs	30 independent runs per day
Service-time distribution	Gamma distribution ($k = 2, \theta = \mu/k$)
Service-time bounds	Truncated to [20, 80] minutes
Patient case allocation	Dirichlet distribution with fixed concentration parameter ($\alpha = 2$)
Definition of waiting time	Admission time to start of physician consultation
Definition of treatment time	Start of physician consultation to discharge
Workflow cases	Design-level scenarios (Cases 0–3), not empirical patient categories
Simulation objective	Comparative system-level workflow evaluation

Table 5. Key operational and modeling parameters used in the simulation.

False acceptance rates (FAR) are not modeled as a source of additional processing delay, as they do not interrupt the admission workflow or trigger manual identity verification steps. Accordingly, the simulation focuses on false rejection events as the mechanism by which biometric authentication failures introduce additional processing time. Under these assumptions, biometric authentication failures and associated fallback procedures are explicitly represented in the simulation to reflect their impact on admission workflows at the system level.

Dataset

In this study, real-world data were collected from three public Saudi hospitals in the emergency department over one year, from January to December 2024: King Fahd Armed Forces Hospital, King Abdullah Medical Complex, and Heraa General Hospital.

The required data from these hospitals included all patient visits during the data collection period. Although the request was not limited to the emergency department, the data obtained pertained to emergency visits, given their frequency and time sensitivity. Such visits are typically documented with precise records of admission, physician interaction, and discharge times.

Emergency department data are particularly relevant for emergency care research owing to their focus on time-sensitive, high-acuity cases, and they are typically collected at high frequency (e.g., daily), allowing for granular analysis of waiting and treatment times. These advantages make emergency department data more robust and comparable to aggregated hospital-wide datasets[54,55]. For these reasons, emergency department data provide an appropriate and demanding context for evaluating system-level performance improvements related to admission efficiency and medical record availability. The recorded data for each patient visit included the day, arrival time at the hospital, and start and end times of treatment. The operation hours were 24 h per day, 7 days a week. They have three shifts, each with nine doctors. Emergency Department data were selected to represent a high-load and high-variability operational scenario, enabling evaluation of the proposed framework under peak clinical pressure.

Due to strict data governance and privacy policies imposed by the participating hospitals, the available dataset was limited to time-stamped records of emergency department visits. Specifically, the data include patient arrival times, waiting times, treatment start and end times, and daily patient counts. More detailed statistical descriptors, such as variance measures, hourly arrival distributions, or peak-load statistics, were not available in the provided dataset. Nevertheless, the provided temporal data were sufficient to derive weekly averages and throughput metrics used in the simulation and comparative performance analysis.

Ethical considerations

This study was approved by the Institutional Review Board of the Ministry of Health in Jeddah (IRB Log No. A02122) and was conducted in accordance with the guidelines outlined in the Declaration of Helsinki. The study did not involve any human experiments or experimental protocols. Instead, it relied exclusively on retrospective, fully anonymized operational hospital data that contained no personal, clinical, or identifiable information and involved no direct patient contact. Accordingly, the requirement for informed consent was waived by the IRB.

Evaluation metrics

This section describes the methodology for computing the system-average treatment and waiting times, as well as the theoretical maximum number of patients that the system can serve across three hospitals in the simulation.

Average patient number

The system-level evaluation of average treatment time involves three main steps: (i) calculating the average patient number across the three hospitals, (ii) distributing the average patient number across the four workflow cases, and (iii) generating treatment times from a Gamma distribution and computing the weighted average treatment time.

In our simulation framework, we first calculated the average number of patients across the three hospitals included in the study. This baseline measure normalizes hospital sizes and enables system-level modeling by treating the three hospitals as a single integrated unit before evaluating treatment performance[56,57].

The average number of patients visiting the three hospitals was computed on a per-day basis using the formula provided by Ross[58] and Montgomery et al.[59], as expressed in Equation 1.

$$N_{\text{AvgPatientNum}} = \frac{\sum_{i=1}^{n} x_i}{n}, \qquad n = 3 \tag{1}$$

Equation 1 represents the calculation of the average daily number of patients across the participating hospitals, where x_i denotes the patient count at the i-th hospital and n is the total number of hospitals. This average patient volume is subsequently used as an input parameter to the discrete-event simulation for system-level workflow evaluation.

Distribution of patients across cases

To allocate patients across the four workflow cases, a Dirichlet distribution was employed[60]. The Dirichlet distribution is a multivariate generalization of the Beta distribution and is widely used to model proportions across multiple categories whose values are constrained to sum to one[61,62]. This makes it suitable for probabilistic allocation of patients across the defined cases within the simulation.

Because the four workflow cases are architectural scenarios introduced by the proposed hybrid cloud framework, they do not correspond to pre-existing categories in the collected hospital data. As a result, no empirical distribution of patients across these cases can be derived from real-world records. The Dirichlet distribution is therefore used as a neutral modeling mechanism to generate patient allocations across cases without assuming fixed or observed proportions.

The probability density function of the Dirichlet distribution is given in Equation 2.

$$p(\boldsymbol{\pi}) = \frac{\Gamma\left(\sum_{i=1}^{k} \alpha_i\right)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \prod_{i=1}^{k} \pi_i^{\alpha_i - 1} \tag{2}$$

The concentration parameter controls how evenly patients are distributed across cases. In this study, a moderate value ($\alpha = 2$) was selected for all cases to avoid highly extreme allocations while still allowing variability across simulation runs. This choice supports system-level workflow evaluation under uncertain patient routing conditions, rather than estimation of real-world case frequencies.

Generating a patient number per case

To estimate the number of patients assigned to each case, we employed a proportional allocation approach[63] based on probability weights derived from the Dirichlet distribution. According to Blien et al.[64], the general formula used to calculate the number of patients per case is defined in Equation 3.

$$N_i = N_{\text{AvgPatientNum}} \times C_i \tag{3}$$

Equation 3 expresses the proportional allocation used to distribute the average number of patients across the four cases. Here, N_i represents the number of patients allocated to case i, $N_{\text{AvgPatientNum}}$ denotes the average number of patients, which is calculated in Equation 1, and C_i is the proportion assigned to Case i, which was generated from a Dirichlet distribution in Equation 2. This approach ensures that the average number of patients is distributed across cases in proportion to their relative weights.

Generating treatment times using a gamma distribution

In this study, treatment times are modeled using a Gamma distribution as a system-level service-time representation. Emergency department service processes are widely recognized to exhibit right-skewed behavior, characterized by a large number of short visits and a smaller number of prolonged, complex cases. Consistent with established practice in discrete-event simulation and healthcare operations modeling, the Gamma distribution is commonly adopted to capture such skewness while ensuring non-negative service times and realistic variability in treatment duration[65,66].

The parameters of the Gamma distribution were selected to preserve the empirically observed average treatment times reported in Table 7 while introducing stochastic variability at the patient level. Because patient-level timestamps are heterogeneous across hospitals, a fixed shape parameter was adopted to provide a transparent and reproducible modeling assumption suitable for system-level evaluation.

$$f_X(x) = \begin{cases} \dfrac{1}{\Gamma(k)\,\theta^k}\, x^{k-1} e^{-x/\theta}, & x > 0, \\ 0, & \text{otherwise.} \end{cases} \tag{4}$$

Equation 4 defines the probability density function of the Gamma distribution, where k is the shape parameter, θ is the scale parameter, and $\Gamma(\cdot)$ denotes the Gamma function. The Gamma distribution ensures non-negative treatment times and introduces controlled right-skewness consistent with emergency department service dynamics.

In the adopted service-time model, the shape parameter was fixed to $k = 2$, a commonly adopted choice in healthcare service-time modeling when only mean treatment durations are available. The scale parameter θ was computed as $\theta = \mu/k$, where μ denotes the empirically observed average treatment time for the corresponding day reported in Table 7. This parameterization ensures that the expected treatment time satisfies $\mathbb{E}[X] = k\theta = \mu$.

To maintain consistency with observed clinical practice, the parameters of the Gamma distribution were selected based on the empirically observed range of average treatment times in the hospital data, spanning approximately 20 to 80 minutes.

The Gamma service-time model is used to characterize treatment-time variability within the simulation, while all reported numerical results are obtained empirically from the discrete-event simulation runs.

Weighted average treatment time

To estimate the average treatment time across the three hospitals, the weighted average formula was applied. This method was selected because the patient numbers in each case were not equal. By using weights proportional to patient numbers in each case, the formula ensures that cases with higher patient numbers have a proportionally greater impact on the overall treatment time.

According to Finch et al.[67], Kirchner[68], and Cochran et al.[69], we have used the weighted averages formula to calculate the average treatment time by using the following formula:

$$\bar{T} \;=\; \frac{\sum_{i=1}^{n} N_i\, FX_i}{N_{\text{AvgPatientNum}}}, \qquad n \in \{1, 2, 3, 4\} \tag{5}$$

Equation 5 computes the average treatment time $\bar{T}$ as a weighted mean across *n* cases. Here, N_i is the number of patients allocated to Case *i* calculated in Equation 3, FX_i is the treatment time for Case *i* calculated in Equation 4, and $N_{\text{AvgPatientNum}}$ is the average number of patients calculated in Equation 1. The index set $n \in \{1, 2, 3, 4\}$ indicates the four cases. This approach provides a more representative measure of performance by accounting for variations in patient volume across hospitals and reflects the overall system efficiency more accurately.

Equation 5 is used to define the system-level evaluation metric, whereas all numerical values are obtained from the discrete-event simulation results.

Queueing-based analytical reference

To establish an analytical reference for system loading and stability, we employ classical queueing theory formulations. Queueing theory provides a well-established mathematical framework for characterizing congestion and server utilization in service systems[70]. Following Yaduvanshi et al. [71] and Qandeel et al. [72], Erlang-*C* expressions are presented solely as an analytical reference under idealized assumptions.

$$\lambda \;=\; \frac{N}{T} \tag{6}$$

Equation 6 defines the patient arrival rate[71]. Here, λ denotes the arrival rate (patients/min), *N* denotes the total number of arriving patients, and *T* denotes the operating time in minutes (24 h × 60 min).

$$\mu \;=\; \frac{1}{\bar{T}} \tag{7}$$

Equation 7 defines the service rate per physician[73]. Here, μ represents the service rate (patients/min) for a single physician, and $\bar{T}$ represents the average treatment time calculated in Equation 5.

$$a \;=\; \frac{\lambda}{\mu} \;=\; \lambda\,\bar{T} \tag{8}$$

Equation 8 defines the total offered traffic[71]. Here, *a* denotes the offered load, λ denotes the patient arrival rate (patients/min), μ denotes the per-physician service rate (patients/min), and $\bar{T}$ denotes the average treatment time calculated in Equation 5.

$$\rho \;=\; \frac{\lambda}{c\,\mu} \tag{9}$$

Equation 9 defines the server utilization factor[74]. Here, *c* denotes the number of physicians concurrently available per shift. In the emergency department under study, staffing is organized into three consecutive shifts with nine physicians per shift; therefore, $c = 9$ is used in the waiting-time analysis. Because physicians operate in non-overlapping shifts, only one shift is active at any given time; therefore, the effective number of concurrently available physicians is $c = 9$ rather than 27. For system stability, the utilization condition $\rho < 1$ must hold.

$$P_0 = \left[\sum_{n=0}^{c-1} \frac{a^n}{n!} \;+\; \frac{a^c}{c!}\,\frac{1}{1-\rho}\right]^{-1} \tag{10}$$

In Equation 10, P_0 represents the steady-state probability of the system being empty in a queue[74].

$$P_{\text{wait}} = P_0 \, \frac{a^c}{(1-\rho)\, c!} \tag{11}$$

In Equation 11, P_{wait} represents the probability of a patient waiting in a queue[72].

It is essential to emphasize that the analytical queueing expressions presented in Eqs. (6 – 11) are not used to compute average waiting times in this study. Classical Erlang-*C* models assume exponential service times, whereas the simulation model employs Gamma-distributed treatment times calibrated to empirically observed daily averages. Consequently, all waiting-time results reported in this work are obtained directly from discrete-event simulation outputs. The queueing-based analysis is included solely to provide a conceptual reference for system loading and stability, rather than as a predictive or computational model of emergency department waiting behavior.

For clarity, Table 6 summarizes the notation used in the queuing-based waiting-time analysis.

Theoretical maximum patient number

The theoretical capacity of a healthcare system, which means how many patients the system can serve per hour, can be estimated using the following formula:

$$TC \;=\; \frac{c\,T}{\bar{T}} \tag{12}$$

Here, TC denotes the theoretical capacity (number of patients that can be treated) over time T, $\bar{T}$ denotes the average treatment time calculated in Equation 5, and c represents the total number of physician-shifts available over a 24-hour period, distinct from the number of concurrently available physicians per shift.

Specifically, the emergency department operates with three consecutive shifts of nine physicians each, resulting in a total of 27 physician-shifts per day. The resulting capacity is normalized and reported on a 1-hour basis for comparability and should not be interpreted as the number of physicians concurrently available in a single shift.

This formulation is a direct application of the general definition of maximum capacity in operations management, as discussed by Green et al[75]. Accordingly, this capacity estimate reflects a daily-level theoretical maximum rather than instantaneous staffing levels.

Results

This section presents results derived from real-world ED data and discrete-event simulation analysis. Empirical data collected from three hospitals were first analyzed to establish baseline performance characteristics of existing clinical workflows. The dataset comprised daily patient visit records with timestamps for hospital admission, physician encounter, and discharge from the clinic. From these records, key performance indicators were computed, including the average number of patients per day, average waiting time, average treatment duration, and estimated patient throughput expressed as patients per hour.

Discrete-event simulation was configured using patient arrival volumes, staffing assumptions, and operating conditions derived from the empirical data. The simulation produced corresponding performance metrics under controlled and repeatable conditions. Each scenario was executed over multiple independent runs to capture stochastic variability in arrivals and service durations. Results are reported using mean values and variability measures to enable consistent comparison between empirical observations and simulation-based outcomes. Analytical queueing expressions are included solely as a conceptual reference for system loading and stability. At the same time, all reported performance metrics are obtained exclusively from real-world measurements and discrete-event simulation outputs. All reported simulation results incorporate biometric authentication failures and their associated manual fallback procedures.

The results are presented in a set of tables contrasting empirical observations with simulation-derived outcomes. These tables report mean values together with measures of variability, enabling a direct and consistent comparison between observed hospital performance and simulated system behavior under the proposed framework. The reported average number of patients represents an aggregated system-level demand profile obtained by averaging daily patient volumes across the three hospitals, rather than the workload of a single hospital.

Symbol	Description
λ	Patient arrival rate (patients/min)
μ	Service rate per physician (patients/min)
$\bar{T}$	Average treatment time per patient (minutes)
c	Number of physicians available per shift
ρ	System utilization factor
P_0	Probability that the system is empty
P_{wait}	Probability that a patient has to wait

Table 6. Notation used in the queueing parameters.

Day	Hospital Name	Number of patients	Avg.number of patients	Avg.waiting time (min)	Avg.treatment time (min)	Patients/h
Sunday	King Abdullah Medical Complex	118	197	43	76	21
	Heraa General Hospital	155				
	King Fahd Armed Forces Hospital	317				
Monday	King Abdullah Medical Complex	119	191	45	67	24
	Heraa General Hospital	152				
	King Fahd Armed Forces Hospital	301				
Tuesday	King Abdullah Medical Complex	86	203	41	76	21
	Heraa General Hospital	179				
	King Fahd Armed Forces Hospital	345				
Wednesday	King Abdullah Medical Complex	76	146	49	71	23
	Heraa General Hospital	128				
	King Fahd Armed Forces Hospital	235				
Thursday	King Abdullah Medical Complex	87	174	42	75	22
	Heraa General Hospital	157				
	King Fahd Armed Forces Hospital	279				
Friday	King Abdullah Medical Complex	128	190	36	65	25
	Heraa General Hospital	200				
	King Fahd Armed Forces Hospital	242				
Saturday	King Abdullah Medical Complex	122	184	41	75	22
	Heraa General Hospital	198				
	King Fahd Armed Forces Hospital	232				

Table 7. Real-world emergency department performance metrics collected from three hospitals. This table provides baseline performance metrics derived from real-world hospital data and serves as a reference for quantifying relative changes observed in the simulation-based results.

Day	Avg. number of patients	Avg. treatment time (min)	Treatment SD	Lower CI	Upper CI	Patients/h
Sunday	197	58.17	1.82	57.25	58.82	28
Monday	191	54.78	2.00	54.06	55.49	30
Tuesday	203	58.70	1.80	57.43	58.73	28
Wednesday	146	56.59	2.17	55.81	57.36	29
Thursday	174	57.91	2.02	57.18	58.63	28
Friday	190	53.93	2.02	53.20	54.65	30
Saturday	184	57.81	2.00	57.09	58.53	28

Table 8. Day-of-week variation in emergency department treatment times (minutes): simulation results (30 runs). While average treatment times remain relatively consistent across all days, the simulation results show an increase in the number of patients served per hour compared with the real-world baseline. This improvement in patients served per hour is consistent with enhanced system utilization and patient flow efficiency under the fixed clinical service assumptions of the simulation, rather than changes in treatment duration.

Table 7 summarizes real-world ED performance metrics collected from three hospitals. For each hospital, daily average waiting and treatment times were computed for each day of the week based on one year of ED visit records. The reported daily values represent the arithmetic mean of the corresponding daily averages across the three hospitals, without weighting by hospital size or patient volume.

This aggregation approach provides a system-level representation of current ED performance, without assigning differential weights to individual hospitals. The resulting metrics serve as baseline reference values for comparison with the simulation-based results of the proposed framework. The patients-per-hour metric was estimated using a capacity formulation 12 based on physician availability and service duration. This metric represents an estimated operational throughput and is not a directly observed empirical measurement.

Table 8 reports the treatment-time statistics used to characterize treatment duration in the simulation. Treatment times remain relatively stable across days, reflecting calibration of the treatment-time distribution to empirical averages. This stability is consistent with a 24-hour emergency department operating under fixed concurrent physician staffing, where day-to-day performance differences are driven primarily by variations in patient arrivals rather than changes in treatment duration. The low standard deviation values observed across all days indicate limited run-to-run variability in the simulation outcomes. Furthermore, the substantial overlap among the 95% confidence intervals suggests that the small numerical differences in average treatment times are not statistically significant. These results demonstrate that treatment duration remains structurally stable within the model, and that observed differences in patient throughput arise from system-level workflow and arrival-pattern effects rather than from changes in clinical service time.

Table 9 presents the average waiting times obtained from the discrete-event simulation based on 30 independent runs for each day of the week. The results demonstrate clear day-of-week variability, primarily driven by differences in daily patient arrivals under a fixed concurrent physician capacity ($c = 9$). Days with higher patient volumes (e.g., Tuesday and Sunday) exhibit longer waiting times due to increased system utilization, whereas lower-demand days result in substantially shorter waiting times.

In particular, the low waiting times observed on Wednesday can be explained by the relatively lower average number of patient arrivals on that day compared with the fixed number of available physicians. Under these conditions, patient demand remains below service capacity, resulting in limited queue formation and short waiting times. This behavior is consistent with expected operational dynamics under low utilization and supports the internal consistency of the simulation results. Notably, the observed waiting times reflect demand-driven effects rather than changes in staffing, as physician capacity remains constant across all days.

The standard deviation values indicate moderate run-to-run variability in waiting times, which is expected given the stochastic nature of patient arrivals and queue formation in the emergency department. The 95% confidence intervals are sufficiently narrow to support the reliability of the reported mean waiting times, while their limited overlap across high- and low-demand days reflects meaningful demand-driven differences rather than random simulation noise. These results indicate that the observed variation in waiting time is consistent with differences in patient arrival volumes under a fixed physician capacity.

Taken together, the results presented in Tables 7, 8, and 9 provide insight into system behavior under the proposed simulation framework. Treatment times remain relatively consistent due to calibration to empirical averages, while variations in waiting times and patient throughput are primarily associated with differences in demand levels and system utilization across days. These findings indicate that the observed performance changes arise from demand-driven effects rather than changes in clinical service duration. In particular, the observed improvements reflect system-level efficiencies related to information availability and admission coordination within the simulated hybrid cloud architecture, rather than modifications to medical decision-making or care delivery processes.

Discussion

The simulation results provide a basis for interpreting system-level behavior across different demand conditions throughout the week. These results are used to estimate key performance indicators, including average treatment time, average patient waiting time, and the number of patients served per hour. The following discussion interprets these results to explain the observed performance patterns and their operational implications.

A comparison between the real-world hospital data reported in Table 7 and the simulation-based results presented in Tables 8 and 9 highlights notable differences in system-level performance, particularly in patient throughput and waiting dynamics. In the empirical data, treatment times are relatively long and patient throughput remains limited, reflecting operational conditions observed across the three hospitals. These conditions are consistent with environments characterized by fragmented information availability and heterogeneous patient processing workflows, which motivate the design assumptions underlying the proposed framework.

In contrast, the simulation results demonstrate more efficient patient flow under the proposed framework. While average treatment times in the simulation remain stable and aligned with empirical service-duration characteristics, the system is able to serve a higher number of patients per hour. This improvement is primarily attributable to reduced waiting times and improved admission coordination and information availability rather than changes in clinical service duration.

Overall, the observed differences illustrate the potential impact of enhanced information accessibility and workflow integration on emergency department efficiency at the system level. At the same time, it is acknowledged that real-world performance is also influenced by additional clinical, staffing, and organizational factors that are beyond the scope of the current simulation.

Day	Avg. number of patients	Avg.waiting time (min)	Waiting SD	Lower CI	Upper CI
Sunday	197	18.74	15.32	13.26	24.23
Monday	191	8.82	6.77	6.40	11.25
Tuesday	203	23.38	18.58	17.09	30.39
Wednesday	146	1.88	1.27	1.43	2.34
Thursday	174	6.95	4.47	5.35	8.55
Friday	190	7.46	5.25	5.58	9.34
Saturday	184	10.52	8.32	7.54	13.50

Table 9. Day-of-week variation in emergency department waiting times (minutes): simulation results (30 runs). Compared with the real-world baseline reported in Table 7, the simulation results indicate an overall reduction in average waiting times across all days of the week. The magnitude of improvement varies by day and is more pronounced during lower-demand periods, reflecting reduced queue formation under the proposed framework.

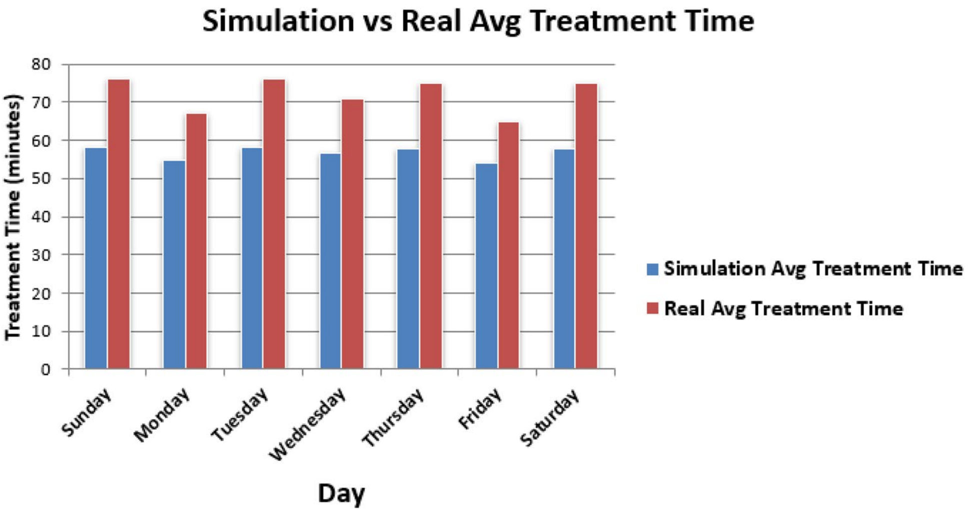

Fig. 10. Comparison of simulated and real average treatment times across days of the week. The results illustrate the relative stability of treatment duration in the simulation, aligned with empirically observed service characteristics.

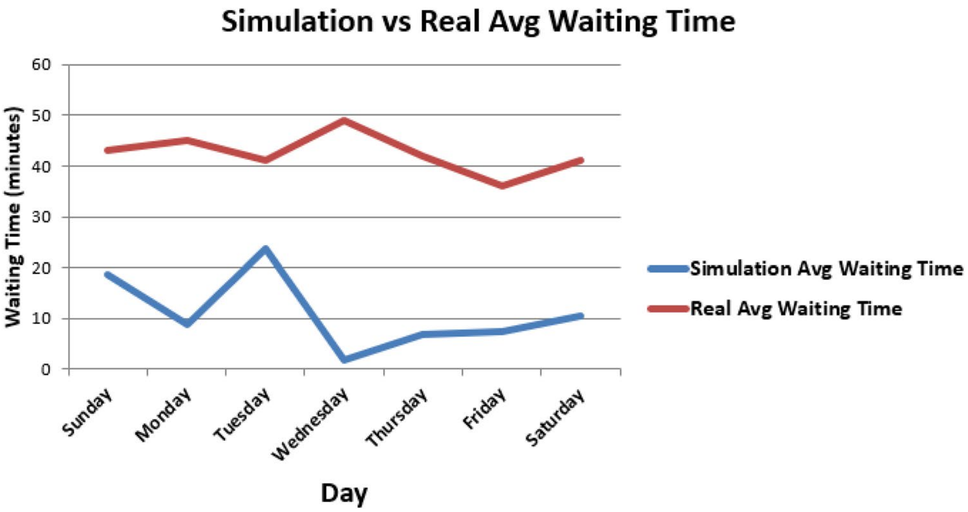

Fig. 11. Comparison of simulated and real average waiting times across days of the week. Line plots are used to highlight day-to-day variations and demand-driven differences between simulated and empirical results.

The observed reductions in waiting times, together with the increase in patient throughput, can be largely explained by specific system-level design features of the proposed framework. Fingerprint-based patient identification reduces manual registration steps and minimizes delays associated with demographic data entry and identity verification during patient admission, without altering clinical assessment processes. In parallel, the Community Cloud indexing mechanism enables selective discovery of external medical records, allowing hospitals to retrieve patient information only from relevant institutions rather than issuing broad, unnecessary requests. This targeted record retrieval reduces communication overhead and accelerates record availability for clinicians. Together, these design choices contribute to improved admission coordination and information availability at the system level, which is reflected in reduced waiting times and increased throughput rather than changes in clinical service duration.

Furthermore, integrating IoT-based vital-sign monitoring supports pre-consultation clinical preparation by enabling early collection of patient data during waiting periods. Collectively, these mechanisms streamline admission and information access workflows, allowing physicians to begin consultations with a more complete patient context, thereby reducing waiting times and improving overall system throughput without altering clinical service duration.

Figures 10, 11 and 12 summarize the comparative behavior of treatment time, waiting time, and patient throughput between the simulated framework and the empirical baseline.

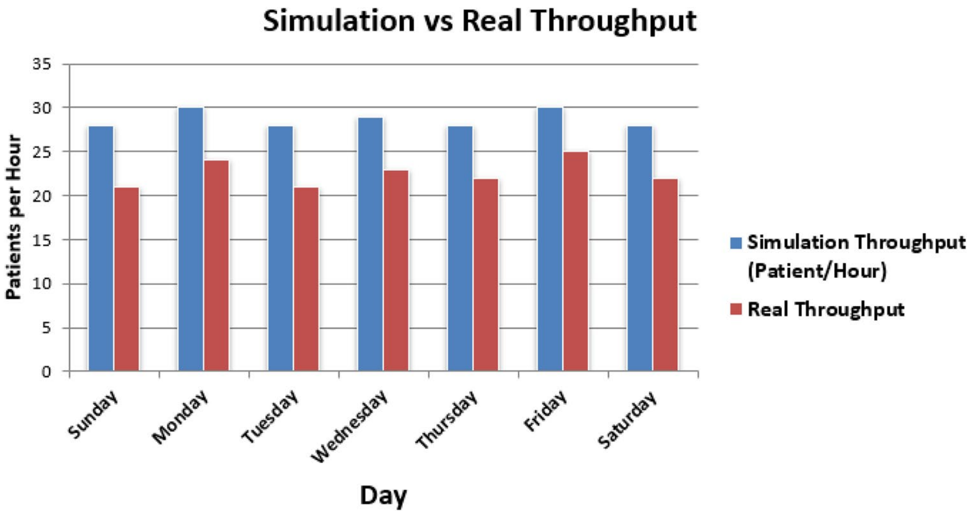

Fig. 12. Comparison of simulated and real patient throughput measured as the number of patients served per hour across days of the week. The simulated results indicate higher throughput under improved system coordination.

Importantly, the performance improvements observed in this study emerge from the coordinated interaction of identification, record discovery, record aggregation, and pre-consultation monitoring, rather than from EMR exchange alone.

As illustrated in Fig. 10, treatment times remain relatively stable across all days in both the real and simulated scenarios. This stability reflects the calibration of the treatment-time distribution to empirical service characteristics and confirms that the proposed framework does not alter clinical service duration. Consequently, observed performance improvements in other metrics cannot be attributed to changes in treatment time.

Figure 11 highlights demand-driven variations in waiting time across days of the week. The simulated results consistently exhibit lower waiting times compared with the empirical baseline, particularly on high-demand days, indicating improved system-level coordination and reduced queue formation under the proposed framework.

As shown in Fig. 12, the reduction in waiting time under the simulated framework is accompanied by increased patient throughput. This relationship reflects improved utilization of fixed physician capacity rather than changes in staffing levels or clinical service processes.

Across the evaluated days, the simulation results indicate an overall reduction in average waiting time relative to the empirical baseline, with improvements ranging from approximately tens of percent, depending on daily demand levels. These reductions are accompanied by corresponding increases in patient throughput, reflecting more efficient utilization of fixed service capacity rather than changes in clinical treatment duration.

The proposed hybrid cloud framework addresses several limitations of both centralized and conventional hybrid architectures, particularly in data security, patient identification, and system reliability, by distributing sensitive data across private, community, and government cloud components while supporting selective record access and robust identity verification.

As discussed in the Related Work section, several studies[28–33] have investigated the use of centralized cloud systems for sharing patient files across healthcare institutions. These systems have demonstrated notable potential in enhancing the efficiency of medical data exchange and improving access to EMRs. Nevertheless, centralized architectures present several limitations, including single points of failure, scalability constraints, and increased vulnerability to security breaches and privacy violations. In addition, most of these systems rely on a patient health ID card or a patient identifier for patient identification and data retrieval, which can increase the risk of unauthorized access and be prone to errors. These limitations motivate the need for alternative architectures that enhance fault tolerance, strengthen identity verification, and reduce reliance on centralized identifiers while maintaining efficient data sharing across institutions.

In this context, many researchers[34–39] have shifted toward hybrid cloud models that integrate private and public cloud components to balance performance, cost, and data protection. Although these hybrid configurations offer improved flexibility and partial mitigation of security risks, their continued dependence on public cloud services for sensitive data handling may introduce residual security and privacy concerns when compared with more controlled deployment environments. Moreover, many of these systems continue to rely on patient ID-based or QR code–based search mechanisms for patient identification and record retrieval, thereby maintaining potential exposure to privacy risks and identification errors.

In response to these challenges, the proposed framework introduces an alternative hybrid cloud architecture that integrates a Private Cloud with a Community Cloud, rather than relying on a public cloud. This design aims to strengthen data security and privacy protection by enabling controlled collaboration among trusted healthcare entities within a defined community environment. Furthermore, the system replaces traditional patient identifiers with fingerprint-based biometric authentication, providing a robust identity verification mechanism that supports accurate patient identification without relying on centralized identifier databases. By minimizing dependence on manual, identifier-based search processes, the framework also reduces the potential for human error during medical record retrieval.

Within the proposed architecture, the Government Cloud serves as a trusted coordination and oversight layer that supports system reliability and inter-institutional trust without participating in routine clinical data exchange.

While the evaluation was conducted using ED data, the observed performance improvements are not inherently limited to this setting. The ED was intentionally used as a stress-test environment to examine the framework under time-critical and high-variability conditions. Similar mechanisms for selective record retrieval and automated admission can be applied to other clinical settings, such as outpatient clinics or inpatient admissions, where workflows are typically less time-sensitive.

Overall, the proposed framework builds upon existing hybrid cloud approaches by integrating Community Cloud coordination and fingerprint-based identity verification, while also incorporating a Government Cloud component to support trusted governance and system-level oversight. Together, these design choices provide a more secure, resilient, and scalable infrastructure for exchanging medical data across healthcare environments.

Limitations

While the simulation results are promising, the observed outcomes may differ in real-world implementations. Hospitals may encounter human and operational challenges, such as patient delays, staffing constraints, or limited availability of self-service kiosks, which could introduce new queues or affect patient flow if system resources are not properly distributed. Technical issues, including potential malfunctions of fingerprint scanners, IoT bracelets, or other hardware components, as well as network instability, could also affect system continuity and the timely transmission of patient data. In addition, interoperability challenges among heterogeneous hospital information systems and organizational resistance to adopting new digital workflows may limit the practical effectiveness of the proposed framework. Finally, while real-world emergency department data from three hospitals were used to inform patient arrival volumes and baseline performance indicators, detailed measurements of internal network latency, database response times, and server performance within these hospitals were not available. As a result, the simulation does not explicitly model low-level infrastructure delays, which may influence system behavior in real-world deployments

Future work

Several future directions can be explored to enhance the effectiveness of the proposed system and broaden its scope. The system can be expanded to include more hospitals, thereby strengthening national-level healthcare integration. Such expansion would also test the system's ability to handle a greater number of patients. Additionally, artificial intelligence and machine learning techniques may be leveraged to analyze aggregated medical records from various hospitals, providing physicians with intelligent decision support. This could include predicting potential complications or suggesting personalized treatment protocols for each patient. In the future, interactive patient interfaces may be developed through mobile applications, enabling patients to view appointments, test results, and real-time updates on their health status. Future work may also explore implementation-level security aspects of the proposed framework, including the evaluation of specific hashing algorithms, encryption standards, and key management mechanisms, as part of deployment-oriented studies in real hospital environments.

Conclusion

This study examined how a hybrid cloud framework can support system-level improvements in emergency department operations by integrating private, community, and government cloud components with biometric fingerprint authentication and IoT-based vital-sign monitoring. Using real-world emergency department data from three hospitals and discrete-event simulation implemented in OMNeT++, the proposed framework was evaluated under multiple workflow scenarios.

The findings indicate consistent reductions in patient waiting times and increased patient throughput, while treatment durations remain stable and aligned with empirical service characteristics. These improvements arise from enhanced admission coordination, selective medical record retrieval through the community cloud, and improved information availability for clinicians, rather than from changes in clinical service delivery.

The proposed system architecture mitigates administrative bottlenecks by streamlining patient identification, automating record initialization, and supporting early collection of vital-sign data. As a result, physicians can access a more complete patient context at the start of consultations, supporting informed clinical decision-making and reducing redundant procedures. These system-level enhancements improve patient experience and support the workflows of both medical and administrative staff.

Overall, this research demonstrates that integrating hybrid cloud technologies with biometric identification and IoT-based monitoring offers a practical and scalable approach for improving operational efficiency in time-critical healthcare environments. The proposed framework also provides a foundation for future extensions, including deployment across additional hospitals and integration with broader regional or national healthcare information infrastructures.

Data availability

Raw patient-level data cannot be publicly shared due to institutional data-use restrictions. However, all derived simulation inputs and modeling assumptions required to replicate the simulation setup are fully specified in the manuscript. These include daily patient arrival volumes derived from real emergency department data Table 7, the design-based case allocation mechanism, service-time bounds, staffing assumptions, and all system configuration parameters Tables 4 and 5. Additional implementation details may be provided upon reasonable request to the corresponding author, subject to institutional approval.

Received: 13 November 2025; Accepted: 1 January 2026
Published online: 09 January 2026

References

1. Bevere, D. & Faccilongo, N. Shaping the future of healthcare: integrating ecology and digital innovation. *Sustainability***16**, 3835 (2024).
2. Wynn, R., Gabarron, E., Johnsen, J.-A. K. & Traver, V. Special issue on e-health services (2020).
3. Callahan, J. M. et al. Access to critical health information for children during emergencies: Emergency information forms and beyond. *Pediatrics***151**, e2022060970 (2023).
4. Saberi, M. A., Mcheick, H. & Adda, M. From data silos to health records without borders: A systematic survey on patient-centered data interoperability. *Information***16**, 106 (2025).
5. Kinnear, N. Comment on'electronic medical records–a disappointing mirage for clinicians and research'. *BJU international***133** (2024).
6. Jang, J.-S., Kim, N. & Lee, S.-H. Scalable and interoperable platform for precision medicine: Cloud-based hospital information systems. *Healthc. Inf. Res.***28**, 285–286 (2022).
7. Sachdeva, S. *et al.* Unraveling the role of cloud computing in health care system and biomedical sciences. *Heliyon***10** (2024).
8. Chen, J. et al. Radiation exposure in recurrent medical imaging: Identifying drivers and high-risk populations. *Front. Public Health***13**, 1626906 (2025).
9. Tuler de Oliveira, M., Amorim Reis, L. H., Marquering, H., Zwinderman, A. H. & Delgado Olabarriaga, S. Perceptions of a secure cloud-based solution for data sharing during acute stroke care: Qualitative interview study. *JMIR Format. Res.***6**, e40061 (2022).
10. Moharraq, T. M. Y. et al. Revolutionizing medical imaging: The integration and impact of pacs (picture archiving and communication systems). *J. Int. Crisis Risk Commun. Res.***7**, 1205 (2024).
11. Liu, G., Xie, H., Wang, W. & Huang, H. A secure and efficient electronic medical record data sharing scheme based on blockchain and proxy re-encryption. *J. Cloud Computing***13**, 44 (2024).
12. Tseng, C.-H., Hsieh, Y.-H., Lin, H.-Y. & Yuan, S.-M. Emr-chain: Decentralized electronic medical record exchange system. *Technologies***13**, 446 (2025).
13. Pampattiwar, K. & Chavan, P. A secure and scalable blockchain-based model for electronic health record management. *Sci. Rep.***15**, 11612 (2025).
14. Abdulsalam, Y. S. & Hedabou, M. Security and privacy in cloud computing: technical review. *Future Internet***14**, 11 (2021).
15. Sivan, R. & Zukarnain, Z. A. Security and privacy in cloud-based e-health system. *Symmetry***13**, 742 (2021).
16. Aldahwan, N. S. & Ramzan, M. S. Descriptive literature review and classification of community cloud computing research. *Sci. Programming***2022**, 8194140 (2022).
17. Valluripally, S. *et al.* Community cloud architecture to improve use accessibility with security compliance in health big data applications. In *Proceedings of the 20th International Conference on Distributed Computing and Networking*, 377–380 (2019).
18. Raghavan, A., Demircioglu, M. A. & Taeihagh, A. Public health innovation through cloud adoption: A comparative analysis of drivers and barriers in japan, south korea, and singapore. *Int. J. Environ. Res. Public Health***18**, 334 (2021).
19. Vu, K., Hartley, K. & Kankanhalli, A. Predictors of cloud computing adoption: A cross-country study. *Telematics Inf.***52**, 101426 (2020).
20. Patil, V. & Ingle, D. An association between fingerprint patterns with blood group and lifestyle based diseases: A review. *Artif. Intell. Rev.***54**, 1803–1839 (2021).
21. Yang, W. et al. Biometrics for internet-of-things security: A review. *Sensors***21**, 6163 (2021).
22. Ahamed, F. et al. An intelligent multimodal biometric authentication model for personalised healthcare services. *Future Internet***14**, 222 (2022).
23. Sohn, J. W. et al. Clinical study of using biometrics to identify patient and procedure. *Front. Oncol.***10**, 586232 (2020).
24. Østervang, C., Jensen, C. M., Coyne, E., Dieperink, K. B. & Lassen, A. Usability and evaluation of a health information system in the emergency department: Mixed methods study. *JMIR Human Factors***11**, e48445 (2024).
25. Sudarshan, V. K., Brabrand, M., Range, T. M. & Wiil, U. K. Performance evaluation of emergency department patient arrivals forecasting models by including meteorological and calendar information: A comparative study. *Computers Biol. Med.***135**, 104541 (2021).
26. Pek, P. P. et al. Nationwide study of the characteristics of frequent attenders with multiple emergency department attendance patterns. *Ann Acad Med Singap***51**, 483–492 (2022).
27. Chang, H. & Cha, W. C. Artificial intelligence decision points in an emergency department. *Clin. Exp. Emergency Med.***9**, 165 (2022).
28. Ademola, A., George, C. & Mapp, G. Addressing the interoperability of electronic health records: the technical and semantic interoperability, preserving privacy and security framework. *Appl. Syst. Innov.***7**, 116 (2024).
29. Ou, T.-Y. & Tsai, W.-L. Designing a flow-based mechanism for accessing electronic health records on a cloud environment. *J. Web Eng.***21**, 1491–1517 (2022).
30. Wu, D.-C., Lin, H.-L., Cheng, C.-G., Yu, C.-P. & Cheng, C.-A. Improvement the healthcare quality of emergency department after the cloud-based system of medical information-exchange implementation. In *Healthcare*, vol. 9, 1032 (MDPI, 2021).
31. Symvoulidis, C., Kiourtis, A., Mavrogiorgou, A. & Kyriazis, D. Healthcare provision in the cloud: An ehr object store-based cloud used for emergency. *Healthinf***1**, 435–442 (2021).
32. Saleh, S. et al. Sijilli: a scalable model of cloud-based electronic health records for migrating populations in low-resource settings. *J. Med. Internet Res.***22**, e18183 (2020).
33. Wu, C. H., Chiu, R. K., Yeh, H. M. & Wang, D. W. Implementation of a cloud-based electronic medical record exchange system in compliance with the integrating healthcare enterprise's cross-enterprise document sharing integration profile. *Int. J. Med. Inf.***107**, 30–39 (2017).
34. McOwiti, A., Dowst, H., Zheng, F., Hilsenbeck, S. & Amos, C. A hybrid cloud data lake architecture supporting the integration of clinical and genomics data. *Health Inf. J.***31**, 14604582251353440 (2025).
35. Naz, A., Ali, M., Cheema, S. M. & Pires, I. M. Cloud-based framework for data exchange to enhance global healthcare. *Procedia Computer Sci.***241**, 570–575 (2024).
36. Vellela, S. S., Reddy, B. V., Chaitanya, K. K. & Rao, M. V. An integrated approach to improve e-healthcare system using dynamic cloud computing platform. In *2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT)*, 776–782 (IEEE, 2023).
37. Javaid, M. et al. Evolutionary trends in progressive cloud computing based healthcare: Ideas, enablers, and barriers. *Int. J. Cognitive Computing Eng.***3**, 124–135 (2022).
38. Brown, A. P. & Randall, S. M. Secure record linkage of large health data sets: Evaluation of a hybrid cloud model. *JMIR Med. Inf.***8**, e18920 (2020).

39. Yang, Y. et al. Medshare: a novel hybrid cloud for medical resource sharing among autonomous healthcare providers. *IEEe Access***6**, 46949–46961 (2018).
40. Son, H. X., Nguyen, M. H., Vo, H. K. & Nguyen, T. P. Toward an privacy protection based on access control model in hybrid cloud for healthcare systems. In *Computational Intelligence in Security for Information Systems Conference*, 77–86 (Springer, 2019).
41. Grossman, R. L. et al. A framework for the interoperability of cloud platforms: towards fair data in safe environments. *Scientific Data***11**, 241 (2024).
42. Hariharan, U., Rajkumar, K., Akilan, T. & Jeyavel, J. Smart wearable devices for remote patient monitoring in healthcare 4.0. In *Internet of Medical Things: Remote Healthcare Systems and Applications*, 117–135 (Springer, 2021).
43. Dall'Ora, C., Griffiths, P., Hope, J., Barker, H. & Smith, G. B. What is the nursing time and workload involved in taking and recording patients' vital signs? a systematic review. *J. Clin. Nursing***29**, 2053–2068 (2020).
44. van Graan, A. C., Scrooby, B. & Bruin, Y. Recording and interpretation of vital signs in a selected private hospital in the kwazulu-natal province of South Africa. *Int. J. Africa Nursing Sci.***12**, 100199 (2020).
45. Turvey, C. L. et al. Racial differences in patient consent policy preferences for electronic health information exchange. *J. Am. Med. Inf. Assoc.***27**, 717–725 (2020).
46. Pasquale, L. et al. Infection prevention in endoscopy practice: Comparative evaluation of re-usable vs single-use endoscopic valves. *Infection Prevent. Practice***3**, 100123 (2021).
47. Wang, X., Matta, A., Geng, N., Zhou, L. & Jiang, Z. Simulation-based emergency department staffing and scheduling optimization considering part-time work shifts. *Eur. J. Op. Res.***321**, 631–643 (2025).
48. Porto, B. M. & Fogliatto, F. S. Enhanced forecasting of emergency department patient arrivals using feature engineering approach and machine learning. *BMC Med. Inf. Decision Making***24**, 377 (2024).
49. Rostami-Tabar, B., Browell, J. & Svetunkov, I. Probabilistic forecasting of hourly emergency department arrivals. *Health Syst.***13**, 133–149 (2024).
50. Radhakrishnan, L. Seasonal trends in emergency department visits for mental and behavioral health conditions among children and adolescents aged 5–17 years-united states, january 2018-june 2023. *MMWR. Morbidity Mortality Weekly Rep.***72**, 1032–1040 (2023).
51. Khan, U. H. et al. Secure edge-based iomt framework for icu monitoring with tinyml and post-quantum cryptography. *Sci. Rep.***15**, 36195 (2025).
52. Jennifer, T. & Kanagalakshmi, K. Generation of cancellable and irrevocable fingerprint biometric templates using quadrant shift modulation transformation. *Eng., Technol. Appl. Sci. Res.***15**, 28165–28171 (2025).
53. Oktamianiza, O., Ilahi, V., Putri, K. A., Yulia, Y. & Rahmadhani, R. Design of computerized patient registration application system at tanjung pati health center. *J. Ind. Health Policy Admin.***9**, 2 (2024).
54. Paling, S., Lambert, J., Clouting, J., González-Esquerré, J. & Auterson, T. Waiting times in emergency departments: Exploring the factors associated with longer patient waits for emergency care in england using routinely collected daily data. *Emergency Med. J.***37**, 781–786 (2020).
55. Nyce, A. et al. Association of emergency department waiting times with patient experience in admitted and discharged patients. *J. Patient Exp.***8**, 23743735211011404 (2021).
56. Hartz, A. J., Kuhn, E. M. & Krakauer, H. The relationship of the value of outcome comparisons to the number of patients per provider. *Int. J. Quality Health Care***9**, 247–254 (1997).
57. Keele, L. J., Ben-Michael, E., Feller, A., Kelz, R. & Miratrix, L. Hospital quality risk standardization via approximate balancing weights. *Ann. Appl. Stat.***17**, 901–928 (2023).
58. Sheldon, M. Ross: Introduction to probability and statistics for engineers and scientists. *Elsevier Academic Press, 3rd Edition***185**, 499 (2004).
59. Montgomery, D. C. & Runger, G. C. *Applied statistics and probability for engineers* (John wiley & sons, 2010).
60. Teh, Y. W. Dirichlet process. In *Encyclopedia of machine learning and data mining*, 361–370 (Springer, 2017).
61. Gelman, A., Carlin, J. B., Stern, H. S. & Rubin, D. B. *Bayesian data analysis* (Chapman and Hall/CRC, 1995).
62. Feng, S. *Introduction, 3–14* (Springer, Berlin Heidelberg, 2010).
63. Ross, S. M. *Introduction to probability models* (Academic press, 2014).
64. Blien, U. & Hirschenauer, F. Formula allocation. In *EALE Conference, Lisbon* (2004).
65. Law, A. M., Kelton, W. D. & Kelton, W. D. *Simulation modeling and analysis*, vol. 3 (Mcgraw-hill New York, 2007).
66. Veazie, P., Intrator, O., Kinosian, B. & Phibbs, C. S. Better performance for right-skewed data using an alternative gamma model. *BMC Med. Res. Methodol.***23**, 298 (2023).
67. Finch, T. Incremental calculation of weighted mean and variance. *University of Cambridge***4**, 41–42 (2009).
68. Kirchner, J. Weighted averages and their uncertainties (2006).
69. Cochran, W. G. *Sampling techniques* (john wiley & sons, 1977).
70. Joseph, J. W. Queuing theory and modeling emergency department resource utilization. *Emerg. Med. Clin.***38**, 563–572 (2020).
71. Yaduvanshi, D., Sharma, A. & More, P. Application of queuing theory to optimize waiting-time in hospital operations. *Op. Supply Chain Manag.: An Int. J.***12**, 165–174 (2019).
72. Qandeel, M. S. et al. Analyzing the queuing theory at the emergency department at king hussein cancer center. *BMC Emerg. Med.***23**, 22 (2023).
73. Thomopoulos, N. T. *Fundamentals of queuing systems: statistical methods for analyzing queuing models* (Springer Science & Business Media, 2012).
74. Hinestroza, T. M. A. *et al.* Queuing theory & discrete simulation as a tool to improve medicine deliver center service levels. *Yugoslav Journal of Operations Research* 15–15 (2025).
75. Green, L. Queueing analysis in healthcare. In *Patient flow: reducing delay in healthcare delivery*, 281–307 (Springer, 2006).
76. Baru, C., Bhandarkar, M., Nambiar, R., Poess, M. & Rabl, T. Big data benchmarking. In *Proceedings of the 2012 Workshop on Management of Big Data Systems*, MBDS '12, 39–40, https://doi.org/10.1145/2378356.2378368 (Association for Computing Machinery, New York, NY, USA, 2012).

Acknowledgements

The project was funded by KAU Endowment (WAQF) at king Abdulaziz University, Jeddah, Saudi Arabia. The authors, therefore, acknowledge with thanks WAQF and the Deanship of Scientific Research (DSR) for technical and financial sup-port.

Author contributions

M.A. and S.S. (Shahenda Sarhan) contributed to the conceptualization, methodology, M.A. data collection and curation, and software and experimental work and writing, M.A., W.A., and S.S. (Shahenda Sarhan); formal analysis, W.A., S.S. (Shahenda Sarhan), S.S. (Shireen Saifuddin); participated in review and editing and supervision. All authors reviewed and approved the final version of the manuscript

Funding

The project was funded by KAU Endowment (WAQF) at king Abdulaziz University, Jeddah, Saudi Arabia. The authors, therefore, acknowledge with thanks WAQF and the Deanship of Scientific Research (DSR) for technical and financial sup-port.

Declarations

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to M.A.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.