Chapter 15
Fog Computing Application for Biometric-Based Secure Access to Healthcare Data

Sreekantha Desai Karanam, Shashank Shetty, and Kurup U. G. Nithin

15.1 Introduction

Healthcare 4.0 industry standards promote a patient-centric healthcare service delivery at his doorsteps. Fog computing paradigm leverages us to deploy the power of cloud computing at the edge devices in IoT networks to leverage cost-effective communication, storage, and computations. “Fog computing is a term created by Cisco that refers to extending cloud computing to the edge of an enterprise’s network.”

“Fog Computing also is known as Edge Computing or fogging facilitates the operation of computing, storage, and networking services between end devices and cloud computing data centers.” Edge computing also enables security, mobility, privacy, network bandwidth, and low latency features in IoT networks. These features are essential to design a real-time healthcare management system. A biometric security system ensures secure and perfect access to a system compared to alphanumeric-based passwords in the digital world. Biometric security can be further strengthened by adopting multi-model authentication. In the IoT domain, every edge device will have a unique network address assigned by the IPV6 system. Only the authorized end-users can access and control these edge devices to access IoT-enabled services protecting their privacy. These edge devices provide secure access for authenticated users through a biometric mechanism by verifying their digital credentials in real time. This secure access mechanism can also be made context-aware to understand user-specific requirements. High-security systems can

S. Desai Karanam (✉) · S. Shetty
Department of CSE, NMAM Institute of Technology, Nitte, Udiupi Dist., Karnataka, India
e-mail: sreekantha@nitte.edu.in; shashankshetty@nitte.edu.in

K. U. G. Nithin
Department of CSE, VCET, Puttur, Karnataka, India

S. Tanwar (ed.), *Fog Computing for Healthcare 4.0 Environments*,
Signals and Communication Technology,
https://doi.org/10.1007/978-3-030-46197-3_15

implement a combination of fingerprint, face recognition, and iris scanning to assure the highest safety and privacy for authentication of the end-users.

15.1.1 Evolution of Technological Shift from Healthcare 1.0 to Healthcare 4.0 Standards

The major focus of Healthcare 1.0 is to reduce the manual and paperwork to enhance productivity. Healthcare 2.0 focused on data processing and sharing with organizations. Healthcare 3.0 introduced patient-oriented IT solutions, while healthcare 4.0 objective was to provide real-time tracking of patient conditions and provide on-site medical assistance. Healthcare 1.0 has progressed from the computerization of healthcare data processing to real-time, on-site patient healthcare diagnostics and context-aware AI-based solutions. The healthcare data/information sharing is initiated within the hospitals and extended to the cluster of healthcare providers across the country. Healthcare 4.0 promotes healthcare data sharing across the globe conforming to technical and statutory standards. The technologies for Healthcare 1.0 were information technology solutions for hospital administration, extended to Electronic Data Interchange (EDI), cloud computing, big data, big data analytics, fog computing, IoT, Electronic Medical Records (EMR), wearable devices, block chain, and artificial intelligence technologies. Today the major challenges faced in Healthcare 4.0 are interoperability, conforming technical standards and ensuring privacy, security, and confidentiality of data as per prevailing statutory framework [38].

15.1.2 Fog Computing for Enhancing Biometric Security

The edge computing helps us to solve the difficulties connected with safety and confidentiality of biometric signatures by improving security and privacy of critical patient information. The intrinsic properties of fog computing permit additional advantages of computing features which are essential for ensuring the privacy and security-sensitive data access by computing important data at the fog nodes and transmitting the secure and encoded data to cloud after processing.

15.2 Review of Recent Related Literature

Researchers have carried out an extensive survey of research papers on healthcare 4.0, fog and cloud computing applications from Springier and Elsevier publications since the year 2007. The findings are revealed in the following discussion. A healthcare 4.0 architecture having three processing layers based on fog computing was presented [1]. This architecture is used to implement an analysis of patient-centric healthcare data. Two case studies were presented to confirm the effectiveness of this system. It is mandatory to assure the security and confidentiality of data on the health of a patient by law. In healthcare domain, providing secure access to information is the most critical aspect.

The biometric features are used for authentication of end-users of health data, since these personal features will not be forgotten, hired, purchased and also are very hard to duplicate [2]. Ensuring data security in pathology labs is most crucial in the design of smart medical systems [3]. The generation of a binary string of varying length of bits, corresponding to the range of patient heart beat rate to incorporate quality and security features in Wireless Body Sensor Networks (WBSN) using Random Binary Sequences (RBS) generation method is called adaptive computing. A protocol based on the Squared Secure Biometric Authentication (SSBA) metric is used in a cloud platform. This protocol protects the confidentiality of the critical data and ensures a safe identity in the cloud computing infrastructure [4]. Governments are promoting unique biometrics-based identification for their citizens for authentication purposes to provides passport services, driving license, voter cards, and public and social applications.

The demand is to develop a robust, secure and cost-effective authorization system to protect privacy using multi-model biometric signatures [5]. After the successful implementation of One Time Passwords (OTP), the application of biometrics that is cancelable is highly recommended instead of conventional biometrics to promote secure and private data sharing. Today cancelable or revocable biometric methods are employed as these are more accurate and increase the privacy of data [5, 6]. Considering biometric signatures and stored specimen templates as public data in the authentication process leads to a weak security level, since the server stores the original template and can be tampered by malicious hackers. This biometrics sketch can be encoded as a binary string of constant size and saved in a tamper-proof smart card to ensure better authentication. The suggestions on implementation of Broadband Remote Access (BRA) systems to ensure a two-factor authentication system to store additional data in a tamper-proof smart card as a second factor were made by the authors [7].

A simple security protocol for securing the privacy of the data having cost-effective packet transmission with three stages was proposed [8]. In the first stage, the attacks are detected to eradicate the intruder attacks such as Wormhole, Sybil, and Sinkhole. In the second stage, data is classified and ranked using WPM based on its sensitivity and sends the nascent data to the MNS. In the last stage, an enhanced Elliptic Curve Cryptography (ECC) would provide secure authentication services between the interconnected end-users.

This method achieves the Packet Delivery Ratio (PDR) of 97%. The hardware implementation of biometric-based authentication is very secure and withstands regular attacks. This model was tested in real time and is applicable in many domains [9]. The evaluation of the effectiveness of security to counter the wolf attack was computed using WAP (Wolf Attack Probability). The attacker in the wolf attack tries to differentiate a user without knowing the user's biometric signature. The WAP provides the least level of security for the biometric authentication system [10].

Ensuring the identity, privacy, and anonymity in a transaction using unique biometric signatures are critical challenges. This protocol assumes that a secure sketch and biometric signature template are publicly available entities. An end-user need not have to save their private information and record data at the user's sensors level [11]. Designing of various models for integrating biometrics with smart cards like On-Card Biometric Comparison, Store-on-Card, System-on-Card, and Work-sharing procedure is experimented. These models are still in the design phase. Each of these models is designed with a specific objective having pros and cons.

The authors discussed e-passports and Electronic Spanish National ID Card [12]. The design of security systems is carried out using hardware and software co-design and it is also cost-effective [13]. This system identification is designed considering the mobility of smart interconnected devices in ad-hoc networks. Application of pi-calculus and the ProVerif verification tools are used in the design of biometric authentication using Chen, Pearson, and Vamvakas (CPV) 02 protocol [14]. The results have demonstrated that this protocol is effective, secure, and also correct [15].

The study is carried out on user's behavioral patterns, keystroke dynamics, and texting of SMS messages, which are used as inputs for a multi-mode biometric method in cell phones. The experimental results have revealed that these multi-mode profiles can uniquely identify a user with high accuracy. A user authentication protocol was designed using IBE (Identity Based Encryption) mechanism which provides high security and improves WSNs authentication [16]. The proposal on sensor forge resilience: liveness sensors and age-dependent sensors were explored to check the feasibility of designing duplicate sensors to prevent forgeries of original sensors [17].

A random orthonormal biometric remote authentication model which is not susceptible to counter advanced attack in an open network was designed [18]. This model applies the user's biometric signatures along with other authentication factors to attain higher security levels. A protocol that is not anonymous is to be designed to implement the services of anonymous and un-linkable for various types of intruders [19]. This protocol is efficient in processing, ensuring security and provides extended services. The bio-keys captured from different subjects are quite random and unique to secure the Internet of Medical Things (IoMT) [20]. These bio-keys are applied in medical data encryption to decrease resource requirements. The results showed that this mechanism reduces the economics of healthcare services and ensures safe medical data transfer between end-users and service providers. A new authentication scheme for a cloud server was proposed [21]. Experimental results of a security analysis performed on this model reveal that this proposed scheme performs computationally and economically better. The symmetric cryptography protocol shares end-to-end secret data between the nodes having restricted resources of any particular remote entity [22]. The evaluation of this protocol showed that it is safe, secure and saves the cost of energy.

The proposal to permit an authenticated end-user to change the passwords and biometric signatures without consulting the authorized administrator was presented [23]. This proposal also gives a revocation policy to terminate the misbehaving nodes in a network. The analysis of security aspects of this policy is carried out using Burrows Abadi Needham (BAN) logic and random oracle model using the popular Real-Or-Random model. The results derived from the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool revealed that this model is tolerant to man in middle attacks. The proposal on the "Anonymous Privacy-Preserving scheme with Authentication (APPA)" to IoT fog enabled model is device-oriented [24]. Authors realized a multiple layered device authentication using certification by pseudonym and anonymity. This scheme enables independent update of certificate by SDs and pseudonym ensuring the confidentiality of data sensed.

Cloud-based biometric authentication system BAMHealthCloud was discussed [25]. A dedicated component of this system takes care of the security aspect. ALGO Health Security check was performed on this model and results were found satisfactory. The development of a secure healthcare framework is compatible with cloud and mobiles platforms [26]. This framework considers security at inter-sensor communication and patient's data levels. This system employs multi-mode biometrics signatures for inter-sensor communication through public keys. Evaluation of this system showed that it is a feasible solution for future cellular healthcare systems. System architecture based on smart e-health gateways with distribution to verify the end-user's authentication is proposed [27]. This method decreases the workload on the medical sensors ensuring good security. This architecture depends on Datagram Transport Layer Security (DTLS) handshake protocol which is certificate-based. Analysis of security of this architecture reveals that it is highly secure and also tolerant to Denial of Service Attack (DoS) attacks. A low weight protocol having many features for remote end-user authentication was proposed [28]. This protocol facilitates end-users to register using a gateway node in an IoT environment.

After registration users can interconnect to the required sensor nodes through IoT devices to avail every service directly. This protocol has less weight since it is unidirectional and perceptual hash mathematical and XOR functions. This protocol is less intensive in computing and hence very much suitable for the IoT environment, where the capacities of resources are limited. The authors have analyzed the security features using AVISPA tool to discover that it can tolerate various security breaches. This protocol mainly concentrates on providing features such as privacy, security, and integrity of the applications deployed in the cloud environment. These applications are typically implemented on virtual machines enabling trusted computing pools [29].

The Authenticated Key Agreement Protocol (AKAP) scheme for providing security to remote users ECC in mobile client and server environments was presented [30]. The authors discussed the security features of a random oracle model with Elliptic Curve Discrete Logarithm Problem (ECDLP) and Curve Decisional

Diffie-Hellman Problem (CDHP). Analyzing security features showed that this scheme is tolerant of security threats.

The performance also revealed that this scheme is computationally less intensive and has less communication cost compared to other schemes. A secure protocol having a key establishment mechanism with mutual authentication in IoT-enabled WSNs with better performance was designed [31]. The cryptanalysis conducted on this protocol using the BAN logic model revealed that it tolerates various security threats. A biometric template model for generating a biometric certificate for user authentication was proposed [32]. This mechanism resists the users from generating or extracting the other user's biometric digital key pairs legally. This model enables only the authenticated users to generate the keys. A quantitative analysis of security features of Context Aware Security by Hierarchical Multilevel Architectures (CASHMA), a multi-model biometric authentication system using ADversary VIew Security Evaluation (ADVISE) formalism was carried out [33].

Authors studied the human factors that become threats for the authentication of biometric systems [34]. FaceFirst is a tool to generate a completely automatic, easy to use, face recognition system. This tool sends a message whenever a captured face sample matches a face template stored in a database. The tool works in low-resolution environments and enables real-time operations [35].

15.2.1 Literature on Iris Recognition based Biometric Security

The colored circular section in the human eye is called iris and this can be seen with the normal eye. Iris is comprised of muscles that modify the pupil's size and also controls the quantity of light coming into the eye. Quantity of melatonin pigment contributes to various colors in the formation of iris of humans. The iris muscle foldings covering the ring generate a structure giving a greater level of detail. The creation process of muscle structure is stochastic and it will not follow any specific rules to govern the formation of structure in a human's eye. This muscle structure once created remains permanent throughout the life of the person. Each person's iris is unique and has a distinct pattern for each eye. These properties are considered for individual recognition. A high-quality digital camera can scan the details of iris muscle structures. The iris recognition system uses near-infrared (NIR: 700–900 nm) radiation to capture iris structure. The iris recognition software is installed in a dedicated system to get efficiency and security purposes. A camera captures the image of this structure of iris muscles and its quality is improved by the image enhancement procedures. Every iris formation is unique even the two iris of a person are not identical and there are variations in iris of twins also [36, 37].

This improved image is processed by the recognition system to identify the distinct features to create a biometric template. Matching the sample current iris data with this stored iris template confirms the identity of the person under consideration. Iris recognition offers minimum cost of implementation with high security and user-friendliness. Iris recognition has been implemented by border control agencies of the United Arab Emirates at border security checkpoints. All the foreign travelers with visitor visas have to undergo an iris recognition system for entry into UAE. CANPASS Air program based on iris recognition is operational in several Canadian airports.

Aadhaar, a citizen identification system from the government of India’s program is the unique method, where the biometric signatures are extensively used for citizen identification and linked to all public services. Iris identification of a person using iris is very effective in many applications.

15.2.2 Literature on Retina Recognition based Biometric Security

The neural cells constitute a tissue of a thin layer in the eye called the retina. The retina is situated inside of the human eye. The system of blood vessels carrying blood to this thin layered tissue is represented by a specific structure, which serves as a unique identification of a person. The structure of blood vessels is considered distinct for every person. A special device is needed to capture this structure.

The high cost of usage and highly invasive nature of retina recognition makes its less popular personal identification method and is only applied in highly secure implementations such as defense and war fields. The infrared light having low energy is used to capture the retinal patterns. The blood capillaries pass infrared light and other tissues reflect this light. This reflected light is sensed and the image is formed by the retina recognition system. This image is processed to create a retina template representing the person’s retina signature. This retina image capturing process is called biometric enrollment. The person’s identification may be proved by capturing a new retinal sample and comparing it against the enrolled retina template. Many government agencies like NASA, CIA, FBI, etc. are using retinal recognition for personal identification purposes. Ensuring the privacy of data, precise authentication, and anonymity of end-users identity is very critical in healthcare domain. A framework for providing data abstraction with anonymity of end-user is proposed using a paradigm named anonymous credentials. This framework is implemented using blind signatures [39]. The survey on methods of processing and storage of data in fog environment was carried out. This survey revealed the various challenges and complications in carrying out fog data analytics. Authors have designed a prototype to manage various parameters like ease of access, scaling, communications and collaboration among the nodes, and non-homogeneity. The functioning of this prototype has been explained using two cases [40].

15.2.3 Statutory Requirements for Protecting the Patient Data

15.2.3.1 International Statutory Requirements

“Health Insurance Portability and Accountability ACT (HIPAA)” Standards are developed by US. Department of Health and Human Services (HHS) to assure the security and privacy of data and securing specific health information. The HIPAA privacy rules and national regulations are designed to protect patient data and other personal health data privacy of health programs, healthcare providers and healthcare clearing centers. These entities share medical data to offer online healthcare facilities. The objective of these standards is to establish mandatory precautions to secure patient medical health data privacy.

They define terms for usage, sharing, and disclosing of patient data after taking patient approval. These national regulations enable the patient to exercise their rights over their health data records. The HIPPA security rule enforces proper administration, infrastructural and technological precautions to guarantee the privacy, unity, and safety of digitally secured health data [38].

HIPAA standards compliant business companies which are consuming delicate and secured health data should enforce these standards in infrastructure, networks, safety, regulations and operations [41, 42]. China has also enforced many laws and regulations for protecting healthcare data. The written consent of the patient is mandatory for collecting, using, and sharing the medical and personal data. The recent Cybersecurity Law enacted on May 1, 2017 prohibits the people of China from using digital technologies to breach the privacy of patients and collect personal information unlawfully. European Union (EU) has enacted General Data Protection Regulation (GDPR) from 25th May 2018. This act prohibits any company from gathering and processing medical data from EU or non-EU residents. Japan has established Protection of Personal Information (APPI) act from 30th May 2017 [41].

15.2.3.2 Statutory Requirements for Healthcare Data Security in India

Govt. of India, Ministry of Health and Family Welfare is working on Digital Information Security in Healthcare Act (DISHA). DISHA provides security, privacy, standardization, and confidentiality for electronic health data. The aim is to set up a National Digital Health Authority to exchange information related to health. National Health Policy leverages National Health Information Network to share Aadhaar mapped health records electronically. At present, Indian data privacy laws are not planned for protecting the medical data. The section 43A of the Information Technology Act, 2000 enforces general reasonable security practices, procedures for sharing personal data which is sensitive [43, 44].

15.2.4 Consolidated Summary of Review of Literature

Authors have carried out the comparative study of all surveyed research papers and highlighted the various methods, results, and applications of biometric-based authentication systems as shown in Table 15.1.

15.2.5 Findings from Review of Literature

Authors after a survey of recent literature have discovered that many diverse methods and protocols are used for authentication using multi-model biometric techniques. The implementation using software, hardware using IoT microprocessor boards in real time and experimentation was discussed in very few instances of multi-model biometric signatures concerning Healthcare 4.0 standards. This research gap has motivated researchers to research this area of authentication in the healthcare 4.0 domain.

Authors found that biometric security systems have been successfully implemented in banks, passports, visa offices, and many organizations. The collaboration with KSHEMA Medical Colleges of Nitte Deemed to be University was planned for successful implementation of this prototype. The authors have carried out the experiments in labs and involving their staff and students for biometric signatures.

15.3 Proposed User Authentication System

The main objective of this chapter is to design a patient unique identification system for secure access to patient healthcare data. Authors aimed at developing a hybrid security mechanism at the edge devices to protect healthcare data from intruders. Online home-based healthcare services are provided by smart hospitals to patients at their homes. Patients shall enroll in accessing online healthcare solutions from hospitals. The patients can avail of healthcare monitoring and consultancy services from their smart home. The health conditions of the patient are recorded and monitored by these smart wearable medical healthcare devices.

The wearable medical devices will sense abnormal patient's health conditions and send mobile notifications to the patient caregiver's mobiles and hospital authorities instantly. The patient's healthcare data is private and sensitive, so furnishing security and ensuring the confidentiality of this healthcare data is very critical. Patient's data needs to be accessed only by authenticated doctors and hospitals securely, to the extent permitted by law.

Any violations in securing the privacy of healthcare data lead to breaching of statutory obligations. This paper proposed a biometric authentication model to verify that only authenticated users are accessing the data.

Table 15.1 Consolidated Summary of Review Papers

Ref. No	Methodology Applied	Findings and Results	Areas of Application
1.	Healthcare 4.0 architecture	Doctors can make intelligent healthcare decisions in case of emergency in real time	Patient-centric medical data analysis systems
2.	Biometric features and fast identity standards	Physiological biometrics are more stable than behavioral biometrics	Smart medical systems
3.	Uniqueness and randomness RBSs, is measured using metrics of hamming distances	This method is threefold faster for heart rate	This method has significance for real-time and intelligent healthcare devices.
4.	Homomorphic encryption scheme	Protects the confidentiality of the critical data and ensures the safe identity	The biometric authentication process in the cloud environment
5.	Multi-model biometric signatures	Promotes secure and private data sharing	Passport services, driving license, voter cards, public and social applications
6.	Cancelable or revocable biometric scheme	It has a minimal equal error rate compared with those of the state-of-the-art techniques.	Suitable for IoT environments
7.	Biometrics sketch is encoded as a binary string	Better authentication.	Tamper-proof smart card
8.	Designed a model to detect Sybil, sinkhole, and wormhole attacks under different conditions.	Data packets delivery ratio is 97% and cost-effective packet transmission	Ambulatory care unit for healthcare
9.	Hardware implementation of biometric-based authentication	Very secure and withstands regular attacks	Applicable in many security domains
10.	Secure sketch and biometric signature template	Finger vein pattern algorithm to detect wolf attacks	Secure biometric authentication systems

11.	Specially designed architecture and security prototype for biometric authentication policies	An end-user neither registers nor stores any private data at the client sensor	Identity privacy and transaction anonymity applications
12.	System-on-card, store-on-card, on-card comparing biometric data and sharing	The biometric data and processes are protected using security methods	e-passports and electronic Spanish national ID card
13.	Interconnected security architecture for the system of smart devices	Cost-effective, viable secure system for smart devices that is 35% quicker and 5% increased load efficiency	A security framework for security systems
14.	Pi-calculus and the ProVerif tool	CPV02 biometric authentication protocol, is effective, secure and are also correct	Online banking
15.	Behavior-based biometric methods for SMS texting actions and communications	Matching fusion will improve the classification accuracy by 8%	Create a reliable biometric security system
16.	IBE mechanism WSNs authentication	This protocol for authenticating a user has better security features	Applicable in high-security wire fewer sensor networks
17.	Liveness sensors, age-dependent sensors	Accuracy depends on applied unforgeability and sensing technologies	Forge-resilient secure biometric systems
18.	Unsusceptible biometric-based remote authentication model	Countering advanced attacks in open network	Complex computations are decreased without losing accuracy in biometric systems
19.	An attribute-based non-anonymous and fully anonymous scheme	Performance comparison of this scheme with other similar schemes revealed its out-performance	Appropriate for usage in resource-constrained devices
20.	Secure it, ECG data from 40 healthy patients are collected and public data set, i.e., physionet	The outcome of the study revealed that this method reduces process time and power consumption	Real-time healthcare applications

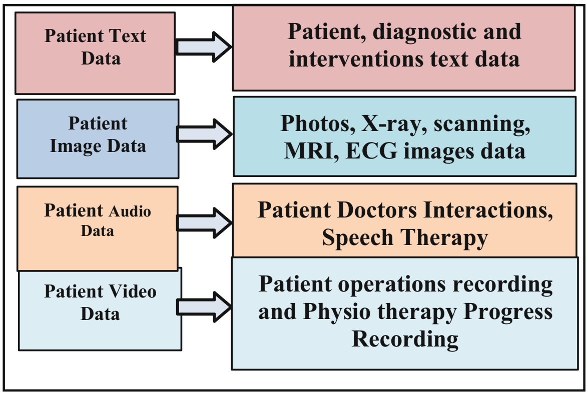
(continued)

Table 15.2 (continued)

Ref. No	Methodology Applied	Findings and Results	Areas of Application
21.	Sensing of patient heartbeats through ECG signals using wearable healthcare devices. Design of biometric security frames for devices with resource constraints	The outcome of the study revealed that this method reduces process time and power consumption	This biometric security design has business importance and relevant to society real-life healthcare domain
22	Symmetric cryptography protocol	Safe, secure and saves the cost of energy.	Scheme performs computationally and economically better
23	Authenticating users using ECC in wireless sensor networks in the healthcare domain	Facilitates better security Revoking stolen or lost cards and effective security code words and updating the biometric data. Dynamically adding sensor nodes	e-authentication protocol using wireless sensor networks
24	Anonymous privacy-preserving scheme with authentication (APPA)	Model is tolerant to replay and man in the middle attacks	Confidentiality in sensed data can be ensured
25.	Biometric authentication system BAMHealthCloud	BAMHealthCloud provides 0.12 EER, 0.98 sensitivity, 0.95 specificity	BAMHealthCloud, a biometric authentication system for educational healthcare, defense, and banking sectors
26	Secure healthcare framework which is compatible with cloud and mobiles. Security of inter-sensor communication	This framework is feasible future cell phone-based healthcare applications	A ubiquitous and cloud-based security framework for wearable healthcare solutions
27	Multi-mode biometrics signatures in distributed smart e-health gateways	Facilitates important security features, measures using extremely efficient key creation methods	A feasible solution for future cellular healthcare systems
28	DTLS handshake certificate-based protocol	Highly secure and also tolerant of DoS attacks	Intruder detection systems
29	Perceptual hash mathematical functions and XOR instructions	Less intensive in computing and hence very much suitable for IoT environment	Virtual machines and enabling trusted computing pools

30	AKAP scheme for providing security to remote users ECC in mobile client and server environments	The scheme is tolerant of security threats, computationally less intensive	Mobile client-server environments
31	Key establishment for mutual authentication in IoT	Cryptanalysis reveals that this technique has improved performance and also tolerates many security attacks	Secure data sharing protocol cloud computing applications
32	BAN logic model	Tolerates various security threats.	The fingerprint data is used in Aadhaar card ID, criminals identification cards ID, and access control cards
33	Digital key creation and extraction technique which are biometric-based	One can’t lawfully create or pull out other users’ digital biometric key pairs	Biometric authentication systems
34	A multi-mode biometric authentication system CASHMA’s security assessment	The security features are assessed with 0.1 confidence interval and 99% confidence level	Biometric authentication systems
35	FaceFirst is a tool for face recognition	Support vector machine	Face recognition systems
36, 37.	Iris recognition system	Iris recognition is noninvasive and cost of operations is low, user’s attention and consent are essential	CANPASS air program is operational in several Canadian airports. The United Arab Emirates at border security checkpoints

Fig. 15.1 Patient data types


Patient Text Data
Patient, diagnostic and interventions text data
Patient Image Data
Photos, X-ray, scanning, MRI, ECG images data
Patient Audio Data
Patient Doctors Interactions, Speech Therapy
Patient Video Data
Patient operations recording and Physio therapy Progress Recording

Authorized doctors can access these patient wearable devices for accessing recorded healthcare data. After carrying out remote diagnosis, the doctors can also interact and advise patients in real time.

15.3.1 Proposed Methodology

Authors proposed a fog computing based biometric solution for authentication of end-users to access patient's healthcare data. This healthcare data is managed in a database mounted on the smart home server. Only authenticated end-users can access this data. The healthcare data is multimedia data, and the patient's details such as name, address, and contacts comprise text data. The x-rays, ECG, and scan reports are the image data. The patient's and doctors' interactions and speech theory progress of patients are audio data. The video data consists of a recording of the operations, the progress of physiotherapy exercises, etc. The health data types and examples are shown in Fig. 15.1.

15.3.2 Stakeholders of Healthcare Data

The patient healthcare data would be used by different stakeholders as shown in Fig. 15.2 for various purposes.

- The patient keeps track of his/her healthcare data for personal information and monitoring purposes.
- Doctors would like to access the patient data for diagnosis, intervention, and progress tracking purposes.

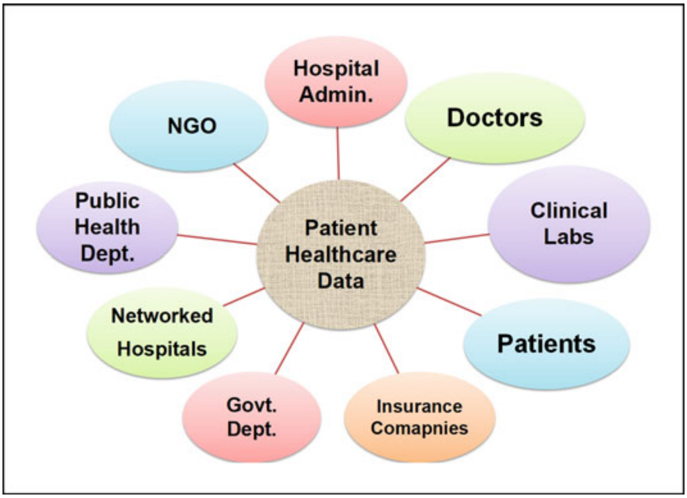


Fig. 15.2 Stakeholders of healthcare data

- Clinical or pathology labs would like to access the health data for analysis and reporting to doctors and patients.
- Hospital administration also accesses the patient's data for billing.
- Govt. authorities also access the patient's healthcare data for planning and reporting purposes.
- The insurance company also accesses the healthcare data for processing the insurance claims.

15.3.3 Architecture of Proposed User Authentication System

The authors have designed a layered architecture for providing authentication to access the patient healthcare data securely as shown in Fig. 15.3.

15.3.3.1 Patient Data Layer

The patient is residing in his smart home or lying on smart bed when she/he is not feel well. This patient health condition data is the innermost core layer in the architecture (Fig. 15.3), where data is captured by the wearable medical devices attached to the patient's body or smart bed.

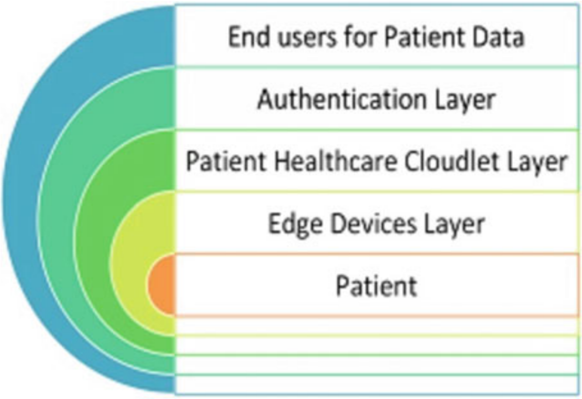


Fig. 15.3 Layered architecture

15.3.3.2 Edge Device Layer

The various health data capturing wearable medical devices are attached to the patient body. These devices monitor the patient body conditions and record health data continuously. Wearable medical devices are configured to send notifications to patients, caregiver's mobiles, and hospitals where a patient has enrolled in case of a medical emergency.

15.3.3.3 Patient Cloudlet Layer

The health data captured is stored securely either in the patient's mobile that plays the role of secure storage edge space or cloudlet. This proposed system can also be configured in such a way that the healthcare data can also be stored in the cloudlet space dedicated to the smart home server of the patient.

15.3.3.4 Authentication Layer

The patient healthcare data needs to be shared by different end-users for different purposes. Ensuring that only authorized users will access patient data to the extent required and permitted by law is most important. In this context, authentication of healthcare data plays a very important role.

The authors have designed a multi-mode biometric authentication system prototype for protecting this data.

The user's authentication is provided by capturing text based on username and password, a biometric image of the fingerprint, face recognition, and iris recognition depending on the data type and significance of data that needs to be accessed.

15.3.3.5 End-User Layers

The end-users of data are discussed and shown in Fig. 15.2 who can access the healthcare data of the patient by proving their identity. The authentication requirements for accessing the data varies on the criticality and type of data. The text data is least critical and hence less secure, while image data and video data have increasing levels of criticality and security.

15.3.4 *The Block Diagram for End-User Authentication*

The biometric authentication system block diagram is organized and nested blocks as shown in Fig. 15.4.

15.3.4.1 Patient Smart Home Block

The innermost block is the patient smart home block which has four sub-blocks. The patient sub-block comprises a patient with wearable medical devices. The edge devices sub-block is to pre-process the captured data. The authentication sub-block is to verify the identity of users and authenticate the user's access.

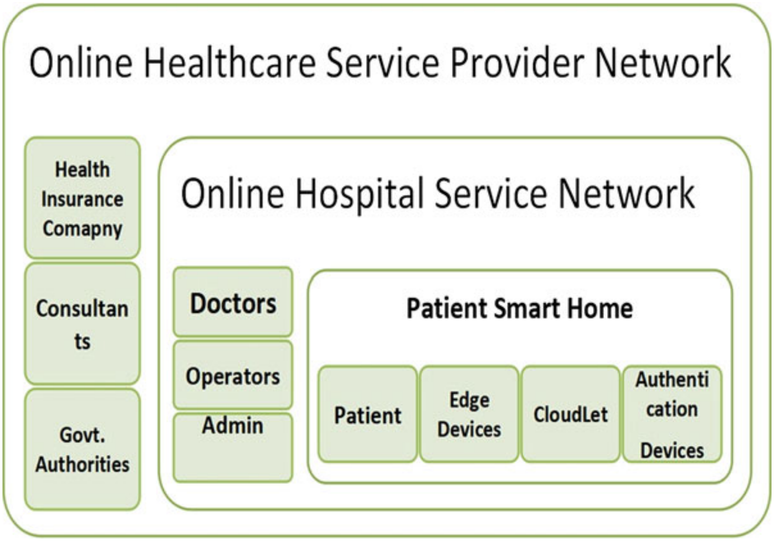


Fig. 15.4 Block diagram of an authentication

15.3.4.2 Hospital Online Services Block

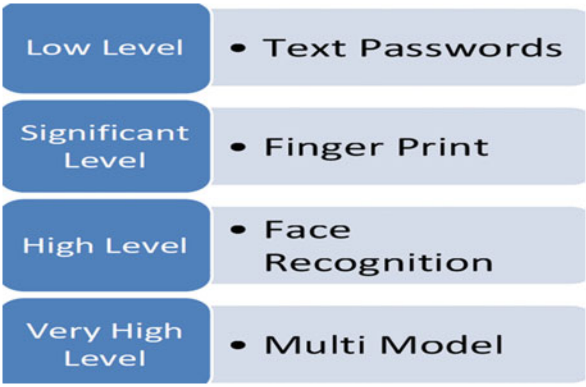
The patients and old age people of smart homes have to enroll in accessing online services with smart hospitals. The enrolled patients are provided with online healthcare and consultancy services. The patients are connected to the hospital through their medical wearable devices. Only authenticated doctors can monitor and diagnose the patients online. The access to patient's data and interactions with health professionals is secured by the proper authentication mechanism. Hospitals have to identify themselves with user code to sign in to patient data account. The authorized doctors and medical professionals can retrieve the patient data to the extent they are allowed to access after verification of their authentication.

15.3.4.3 Healthcare Services Providers

The insurance authorities, consultants, and Govt. authorities would also require to access the patient healthcare data. These bodies can access patient data after providing proper authentication online.

15.3.5 Safety and Privacy Levels of Data

The privacy and security of health data can be ensured by proper authentication using biometric signatures. The authors proposed distinct levels of security for various types of data as shown in Figs. 15.5, 15.6, and 15.7. Text passwords and user names represent the lowest level of security. Images and video recordings require the highest level of security features.



Low Level	• Text Passwords
Significant Level	• Finger Print
High Level	• Face Recognition
Very High Level	• Multi Model

Fig. 15.5 Security levels and data types

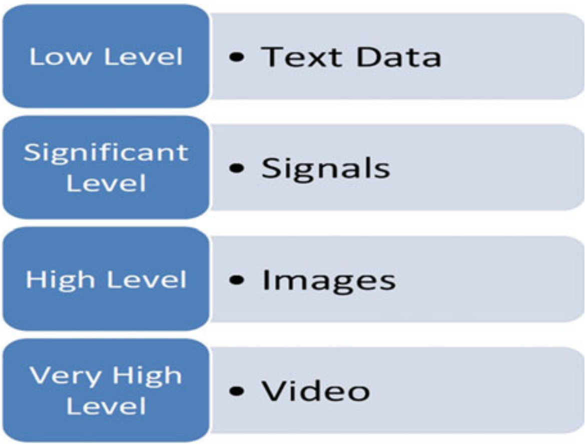


Fig. 15.6 Security levels, biometric signatures

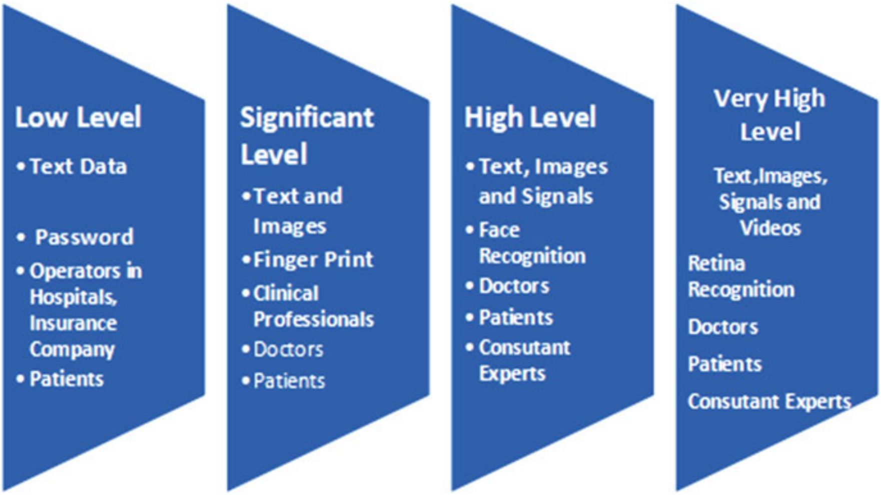


Fig. 15.7 Integrated security levels, biometric signatures and end-users

15.3.6 End-Users Enrollment Procedure for Authentication Purposes

15.3.6.1 Patient Enrollment

The hospital would broadcast the information on available online services through their website. Patients shall register/enroll for accessing online healthcare services on the website of the hospital. The patient's fingerprint, face recognition, and retina signatures are captured during patient registration.

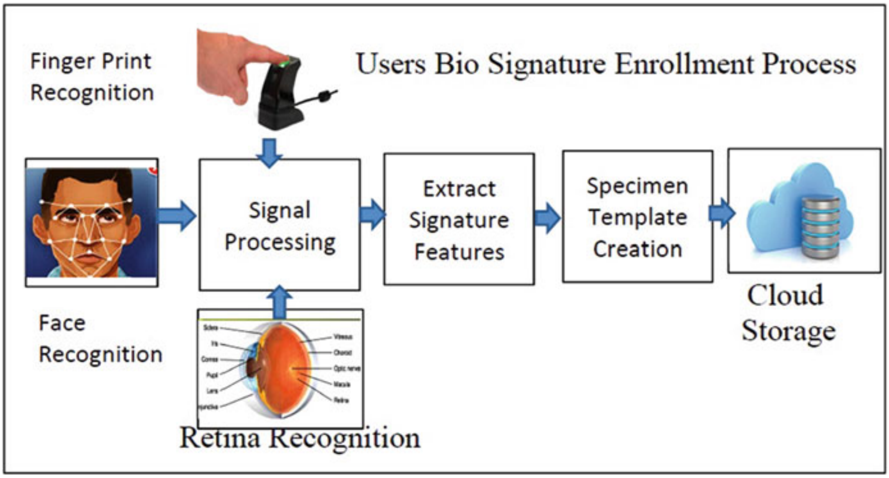

Finger Print Recognition
Users Bio Signature Enrollment Process
Signal Processing
Extract Signature Features
Specimen Template Creation
Cloud Storage
Face Recognition
Retina Recognition

Fig. 15.8 Users biometric enrollment

15.3.6.2 Hospital Authentication

Hospitals will assign a unique identification code for patients who have enrolled in online healthcare services. The hospital staff authentication codes and biometric signatures are securely stored in patient smart spaces also. These authentication codes are cross-checked and confirmed at the patient's location before providing access to the patient's health data.

Fog computing has a very significant role in authenticating end-user identity to ensure that authorized users are accessing the data. End-user's biosignatures are captured by fingerprint readers, face recognition and iris reader devices during the enrollment process. These are images pre-processed and transformed into a standard template with unique identification code and stored in the signature database in edge devices after encryption and compression as shown in Fig. 15.8.

15.3.6.3 End-User Authentication Procedure

The end-users who would like to access patient data need to identify themselves by providing their bioauthentication depending on the type and extent of data to be accessed. These biosignatures captured from end-users are pre-processed. The extracted features of the biosignature are matched with that of enrolled end-user stored signatures. The system compares all the features of user specimen signature with a stored template; if the exact match is found, then only the end-user is allowed to proceed; otherwise, user's data access request will be rejected. If authentication is successful, the user will be able to proceed with data access. The entire process is depicted in Fig. 15.9. The fog and cloud architecture for securing the patient data is shown in Fig. 15.10.

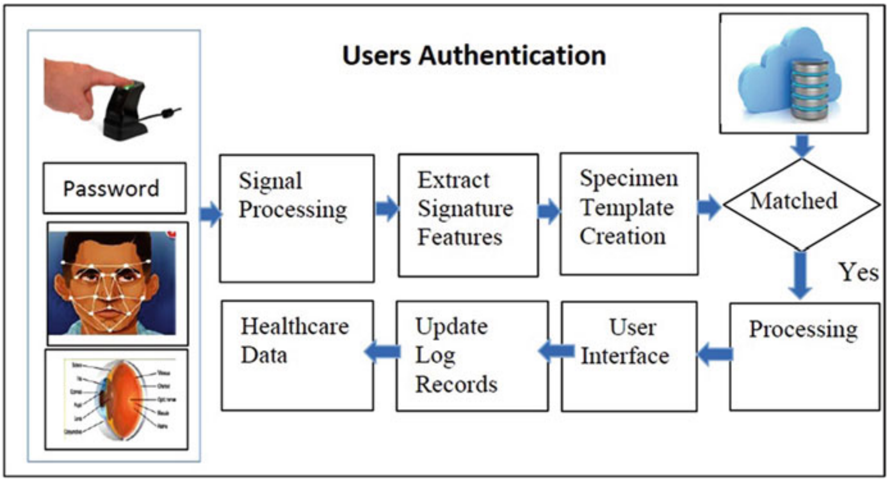


Fig. 15.9 Authentication verification process flow

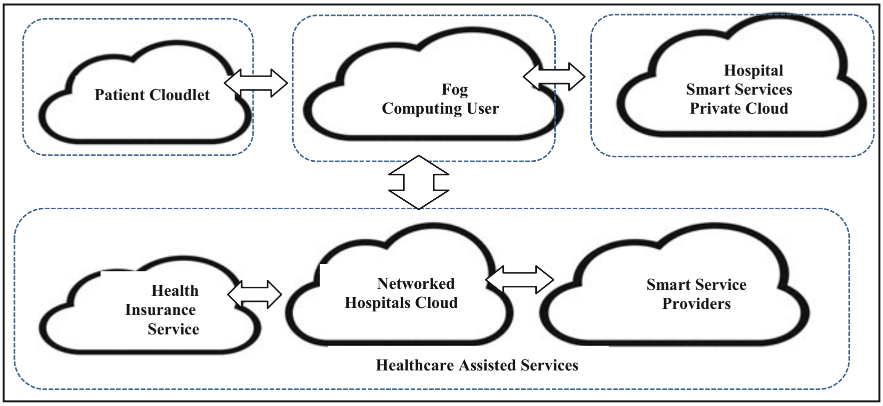

Patient Cloudlet
Fog Computing User
Hospital Smart Services Private Cloud
Health Insurance Service
Networked Hospitals Cloud
Smart Service Providers
Healthcare Assisted Services

Fig. 15.10 Fog and cloud architecture diagram for securing patient data

15.3.6.4 Summary of Step-by-Step Procedure for Authentication

1. Hospitals publishing their smart healthcare online services
2. Patients subscribing for online smart healthcare services
3. Patient biometric enrollment process (finger, face, and iris signatures registration) for authentication purposes
4. Doctors and medical staff authentication for accessing the patient data
5. Patient registering their medical insurance company representatives and their authentication
6. Hospital admin registration and authentication to access the patient data

7. Govt. Public health representatives registration with hospitals for accessing the patient data
8. Patient's registration with networked smart hospitals to share patient healthcare data
9. Registration of patient's IoT smart home service providers for secure healthcare data transmission
10. Registration and authentication of diagnostic labs for patient's medical test data

15.4 Implementation of Proposed Methodology

The authors have designed an experimental prototype setup for verifying the authentication of users using a face recognition technique shown in Fig. 15.11. A web portal is designed to enroll users. Users use this portal for enrollment to services as shown in Fig. 15.12. Raspberry Pi-3 and Pi camera are interfaced with this web portal. The portal is developed in PHP and implemented Haar-cascade face recognition for security purposes. The user's face is exposed to Pi cameras during the enrollment process. This system is trained to recognize the end-user's face. The face recognition algorithms extract the features of the end-user's face and prepare a specimen template.

During the testing phase when users are exposed to Pi camera the sample face features are compared with stored sample face features. If the correct match is found, then user face recognition is successful and the user is permitted to access the patient health data, otherwise, the user is denied access to the data. The screenshots of registered user recognition and display of user names are shown in Fig. 15.13.

The unregistered users not recognized are shown in Fig. 15.14. An alert message and image of the unrecognized user are sent to the administrator as shown in Fig. 15.15. To improve the accuracy of the recognition, maximum three testing attempts are provided for the users for authentication. If more than three attempts are made, then the notification is sent to system administration along with the sample of the captured image and other details. Researchers are working on the user

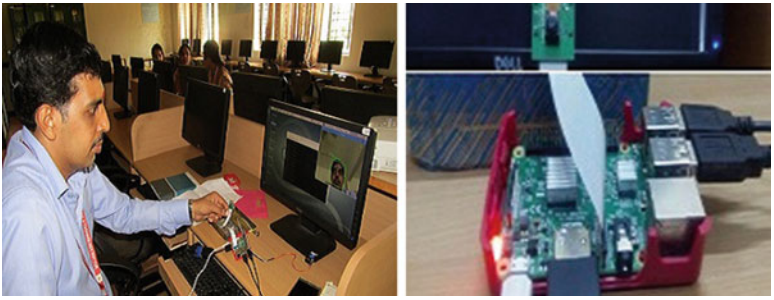


Fig. 15.11 The experimental setup for face recognition

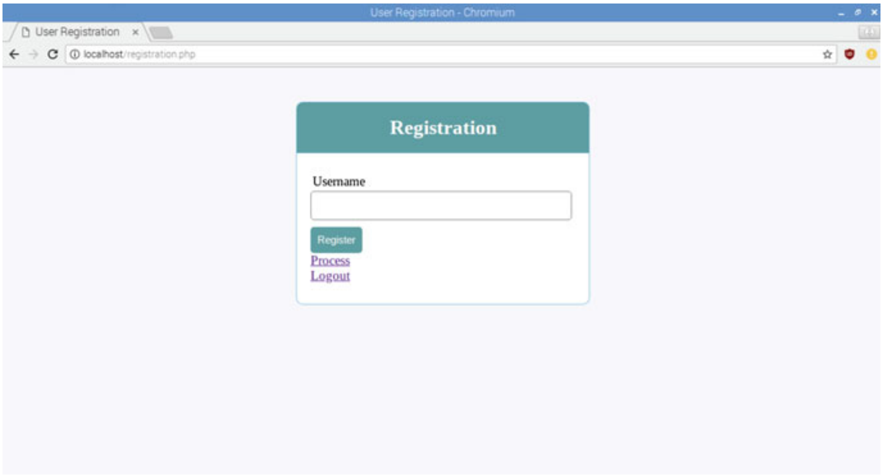
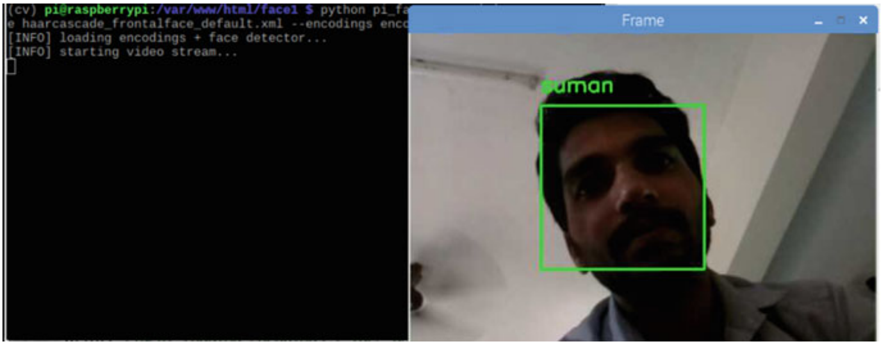


Fig. 15.12 User registration into portal



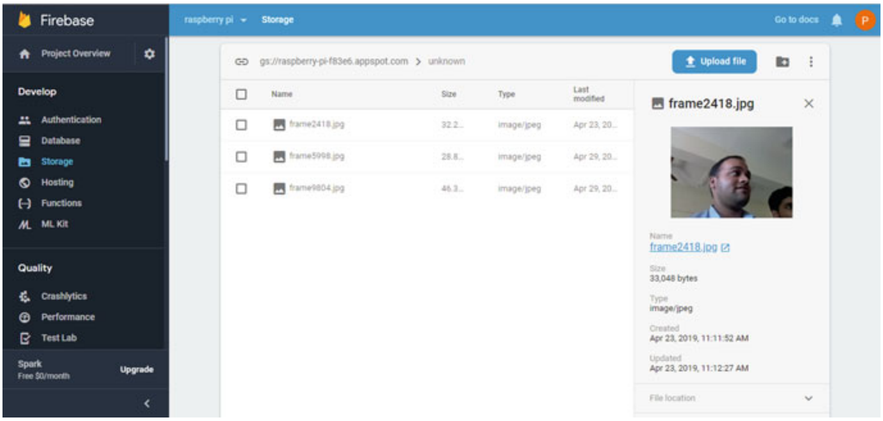
```
(cv) pi@raspberrypi:/var/www/html/face1 $ python pi_fa
e haarcascade_frontalface_default.xml --encodings enco
[INFO] loading encodings + face detector...
[INFO] starting video stream...
```

Fig. 15.13 User recognition

authentication process using fingerprint and iris signature recognition on similar lines of face recognition.

15.4.1 Conducting Experiments and Result Discussion

This authentication prototype is tested using the staff and students in our department as users. The authors used a Raspberry Pi camera for capturing the face images of end-users. Authors have selected end-users with different age groups, gender, and categories. Ninety end-user's biometric signatures were captured in this training process. For each end-user, five face sample images with slightly different postures are captured and stored in the edge device. At the testing phase randomly users



gs://raspberry-pi-f83e6.appspot.com > unknown

Name	Size	Type	Last modified
frame2418.jpg	32.2...	image/jpeg	Apr 23, 20...
frame5998.jpg	28.8...	image/jpeg	Apr 29, 20...
frame9804.jpg	46.3...	image/jpeg	Apr 29, 20...

frame2418.jpg

Name
frame2418.jpg

Size
33,048 bytes

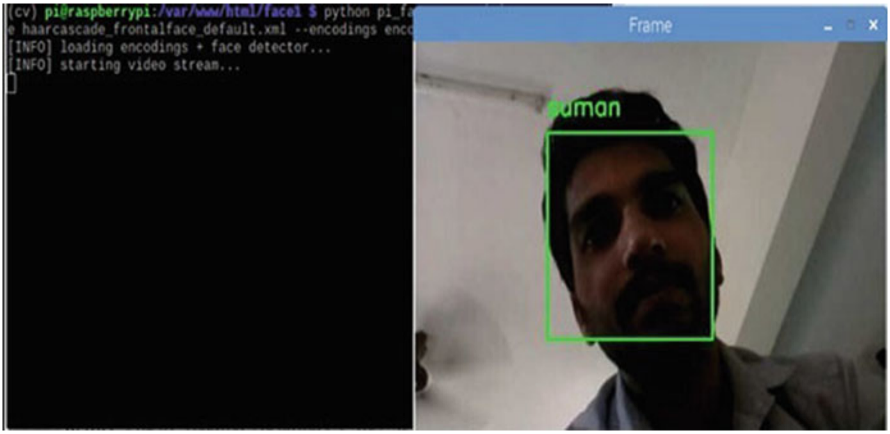
Type
image/jpeg

Created
Apr 23, 2019, 11:11:52 AM

Updated
Apr 23, 2019, 11:12:27 AM

File location

Fig. 15.14 Unknown user recognition



```
(cv) pi@raspberrypi:/var/www/html/face1 $ python pi_fa
e haarcascade_frontalface_default.xml --encodings enc
[INFO] loading encodings + face detector...
[INFO] starting video stream...
```

Fig. 15.15 Alert to system administer

Table 15.2 Data set samples and results recorded

Persons Type	Female	Age	Male	Age	Accuracy in %
Lab instructors	8	25–30	15	30–35	95
Faculties	12	28–35	15	28–40	96
Students	20	19–21	20	19–21	97

are called for face recognition. This system could recognize their faces accurately. The face recognition accuracy achieved is about 95% and above. Authors are experimenting with fingerprint and iris recognition modules and would like to integrate all biometric signatures into one system. The details of the sample data set and results in correct recognition are shown in Table 15.2.

Authors have experimented with a set of users in the department and found that the system gives satisfactory recognition results of about 95% accuracy.

15.4.2 Case Study and Challenges Faced in Fog Computing Implementations in Healthcare 4.0

The patient is residing in his smart home or lying in the smart bed. The wearable medical devices attached to his/her body will sense and transmit data about the health conditions of the patient to edge device. The edge devices may be the smart phone or any edge device with fog computing capability in the patient vicinity. This edge device will process the data received from wearable devices and if any heath data values are abnormal and critical then notifications will be sent to smart hospitals authorities where patient has enrolled for smart services.

The doctors of smart hospitals can access the patient's wearable devices data after verifying their proper authentication. The edge will transmit the data to smart hospitals. The hospital authorities will call the patient/caregiver and explain the conditions of health and advice course of actions to be followed by the patient. This patient heath data is also shared with clinical laboratories for further investigation and accessing the patient data remotely with proper authentication.

Healthcare 4.0 facilitates remote monitoring of heath conditions of the patient with human interventions. Patient can be altered and advised about medication by the medical professional remotely through smart technologies.

The challenges in implementation are the following:

1. Optimizing the cost of healthcare
2. Infrastructure limitations to support real-time operations
3. Building trust in patients on smart healthcare services
4. Managing the interoperability of devices in fog and IoT network domains
5. Compliance with healthcare regulatory standards
6. Providing fool proof authentication mechanisms
7. Managing and sharing healthcare big data with high security and flexibility

15.5 Conclusions

Healthcare 4.0 standards leverage online health data sharing across the globe conforming to technical and statutory standards. Healthcare 4.0 paradigm promotes a patient-centric healthcare service delivery at his doorstep. The foolproof authentication mechanism is essential to prevent any intrusions into the healthcare systems. Authors have carried out the comparative study of all surveyed research papers and highlighted the various methods, results, and applications of biometric-based authentications systems. A biometric security system is adopted to ensure secure access to a system. Biometric security can be further strengthened by adopting multi-model authentication. This paper discussed national and international status of healthcare data protection acts and tools used for biometric authentication. Authors have discussed the prototype design for authentication of end-users of healthcare data and carried out a face recognition experiment for authentication. The authors have designed a layered architecture for providing authentication to access the patient healthcare data securely. Authors have experimented with a set of users and demonstrated satisfactory recognition results.

Future Scope Authors are collaborating with Nitte (Deemed to be) University and KS Hegde Medical Academy, Mangalore, Karnataka for real-time patient data management and data analytics. Authors are planning to implement this system in the AB Shetty Dental College since authors have developed a web portal to capture patient data which is being implemented in this hospital.

References

1. Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2018). Fog computing for healthcare 4.0 environment: Opportunities and challenges. *Computers and Electrical Engineering, 72*, 1–13. https://doi.org/10.1016/j.compeleceng.2018.08.015.
2. Hamidi, H. (2019). An approach to developing smart health using the internet of things and authentication based on biometric technology. *Future Generation Computer Systems, 91*, 434–449. https://doi.org/10.1016/j.future.2018.09.024.
3. Wu, W., Pirbhulal, S., & Li, G. Adaptive computing-based biometric security for intelligent medical applications. *Neural Computing and Applications*. https://doi.org/10.1007/s00521-018-3855-9.
4. Kok Seng, Wong Myung, Ho Kim. (2012). *Secure biometric based authentication for cloud computing* (pp. 86-101). Second international conference, CLOSER, Porto, Portugal, April 18-21. doi:10.1007/978-3-319-04519-1_6.
5. J. Wayman, A. Jain, D. Maltoni, D. Maio, An introduction to biometric authentication systems, Biometric Systems. pp. 1-20, Springer, London, (2005), [Online]. doi:https://doi.org/10.1007/1-84628-064-8_1.
6. Punithavathi, P., Geetha, S., Marimuthu, K., Hafizul Islam, S. K., Hassan, M. M., & Choo, K.-K. R. (2019). A lightweight machine learning based authentication framework for smart IoT devices. *Information Sciences, 484*, 255–268. https://doi.org/10.1016/j.ins.2019.01.073.
7. Sarier, N. D., Meadows, C., & Fernandez, G. C. (2012). Security notions of biometric remote authentication revisited, STM, 2011. *LNCS, 7170*, 72–89. https://doi.org/10.1007/978-3-642-29963-6_7.
8. Vaniprabha, A., & Poongodi, P. (2017). Augmented lightweight security scheme with access control model for wireless medical sensor networks. *Cluster Computing, 22*(1), 1–12. https://doi.org/10.1007/s10586-017-1669-7.
9. Maneesh, U., Anoop, M., Namboodiri, K., & Srinathan, C. V. J. (2009). Efficient biometric verification in the encrypted domain, ICB 2009. *LNCS, 5558*, 899–908. https://doi.org/10.1007/978-3-642-01793-3_91.
10. Une, M., Otsuka, A., & Imai, H. (2007). Wolf attack probability: A new security measure in biometric authentication systems, ICB 2. *LNCS., 4642*, 396–406. https://doi.org/10.1007/978-3-540-74549-5_42.

11. Tang, Q., Bringer, J., Chabanne, H., & Pointcheval, D. (2008). A formal study of the privacy concerns in biometric-based remote authentication schemes. In: L. Chen, Y. Mu, W. Susilo (Eds.,) *Information Security Practice and Experience*. ISPEC 2008. Lecture Notes in Computer Science (pp. 56-70), Berlin: Springer. doi: 10.1007/978-3-540-79104-1_5.
12. Sanchez-Reillo, R., Alonso-Moreno, R., & Liu-Jimenez, J. (2013). Smart cards to enhance security and privacy in biometrics. In: Campisi P. (Ed.,) *Security and privacy in biometrics* (pp. 239-274). London: Springer. doi: 10.1007/978-1-4471-5230-9_10
13. Awad, A. I., Hassanien, A. E., & Baba, K. (2013). *A secure framework for OTA smart device ecosystems using ECC encryption and biometrics*. Berlin: Springer. https://doi.org/10.1007/978-3-642-40597-6_18.
14. Salaiwarakul, M. D., & Ryan, C. L. (2008). Verification of integrity and secrecy properties of a biometric authentication protocol. In W. Susilo (Ed.), *ISPEC LNCS* (pp. 1–13). Berlin: Springer. https://doi.org/10.1007/978-3-540-79104-1_1.
15. Hataichanok, S., & Theoharidou, M. (2012). Multi-modal Behavioural Biometric Authentication for Mobile Devices, SEC 2012. *IFIP AICT, 376*, 465–474. Retrieved from https://link.springer.com/content/pdf/10.1007%2F978-3-642-30436-1_38.pdf.
16. Quan, Z., Chunming, T., Xianghan, Z., et al. (2015). A secure user authentication protocol for sensor network in data capturing. *J Cloud Comp, 4*, 6. https://doi.org/10.1186/s13677-015-0030-z.
17. Phan, R. C. W., Whitley, J. N., & Parish, D. J. (2009). On the Design of *Forgiving* Biometric Security Systems. In J. Camenisch & D. Kesdogan (Eds.), *iNetSec 2009 – Open research problems in network security. IFIP advances in information and communication technology* (Vol. 309). Berlin: Springer. https://doi.org/10.1007/978-3-642-05437-2_1.
18. Tran, N., & Dang, K. (2015). A multi-factor biometric-based remote authentication using fuzzy commitment and non-invertible transformation. *IFIP International Federation for Information Processing, 9357*, 77–88. https://doi.org/10.1007/978-3-319-24315-3_8.
19. Hamada, M., Ibrahim, S. K., Ashok, K. D., & Odelu, V. (2018). Attribute-based authentication on the cloud for thin clients. *Journal of Super-computing, 74*, 5813–5845. https://doi.org/10.1007/s11227-016-1948-8.
20. Pirbhulal, S., Oluwarotimi, W. S., Wu, W., Sangaiah, A. K., & Li, G. (2019). A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Generation Computer Systems, 95*, 382–391. https://doi.org/10.1016/j.future.2019.01.008.
21. Jigna Hathaliya, J., Tanwar, S., Tyagi, S., & Kumar, N. Securing electronic healthcare records in healthcare 4.0: A biometric based approach. doi: 10.1016/j.compeleceng.2019.04.017.
22. Abdmeziem, M. R., & Tandjaoui, D. (2015). An end-to-end secure key management protocol for e-health applications. *Computers, and Electrical Engineering, 44*, 184–197. https://doi.org/10.1016/j.ins.2019.01.073.
23. Challa, S., Das, A. K., Odelu, V., Kumar, N., Kumari, S., Khane, M. K., & Athanasios Vasilakos, V. (2018). An efficient ECC based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks. *Computers, and Electrical Engineering, 69*, 534–554. https://doi.org/10.1016/j.compeleceng.2017.08.003.
24. Guan, Z., Zhang, Y., Wu, L., Wu, J., Li, J., Yinglong, M., & Jingjing, H. (2019). APPA: An anonymous and privacy-preserving data aggregation scheme for fog-enhanced IoT. *Journal of Network and Computer Applications, 125*, 82–92. https://doi.org/10.1016/j.jnca.2018.09.019.
25. Kashish Shakil, A., Farhana Zareen, J., Alam, M., Jabin, S., & BAMHealthCloud. (2017). A biometric authentication and data management system for healthcare data in Cloud, Journal of King Saud University. *Computer and Information Sciences, 32*, 57. https://doi.org/10.1016/j.jksuci.2017.07.001.
26. Farrukh Aslam Khana, Aftab Alia, Haider Abbasb, Nur Al, Hasan Haldar. *A cloud-based healthcare framework for security and patient's data privacy using wireless body area networks*. The 2nd International Workshop on Communications and Sensor Networks (ComSense-2014). Retrieved from http://creativecommons.org/licenses/by-nc-nd/3.0/

27. Sanaz Rahimi Moosavi, Tuan Nguyen Gia, Amir, Mohammad Rahmani, Ethiopia Nigussie, Seppo Virtanen, Jouni Isoaho, Hannu Tenhunen. (2015). SEA: A secure and efficient authentication and authorization architecture for IoT based healthcare using smart gateways. Retrieved from http://creativecommons.org/licenses/by-nc-nd/4.0/
28. Dhillon, P. K., & Kalra, S. (2017). A lightweight biometrics based remote user authentication scheme for IoT services. *Journal of Information Security and Applications, 34*, 255–270. Retrieved from https://daneshyari.com/article/preview/4955718.pdf.
29. Yeluri, R., & Castro-Leon, E. (2014). Identity Management and Control for Clouds. In *Building the Infrastructure for Cloud Security* (pp. 141–159). Berkeley, CA: Apress. https://doi.org/10.1007/978-1-4302-6146-9_7.
30. Mo, J., Hu, Z., & Lin, Y. (2018). Remote user authentication and key agreement for the mobile client-server environments on elliptic curve cryptography. *The Journal of Super-computing, 74*, 5927–5943. https://doi.org/10.1007/s11227-018-2507-2.
31. Dheerendra, M., Vijayakumar, P., Venkatasamy, S., Ruhul, K., Hafizul, A., Islam, S. K., & Gope, P. (2018). Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. *Multimed Tools Applications, 77*, 18295–18325. https://doi.org/10.1007/s11042-017-5376-4.
32. Lin, J. L., Hsu, H. L., Jong, T. L., & Hsu, W. H. (2011). Biometric authentication. In P. S. P. Wang (Ed.), *Pattern recognition, machine intelligence and biometrics* (pp. 607–631). Berlin: Springer. https://doi.org/10.1007/978-3-642-22407-2_23.
33. Lee, H. W., & Kwon, T. (2007). Biometric digital key mechanisms for Telebiometric authentication based on biometric certificate. In C. Stephanidis (Ed.), *Universal Acess in human computer interaction. Coping with diversity. UAHCI 2007* (Lecture notes in computer science) (Vol. 4554). Berlin: Springer. https://doi.org/10.1007/978-3-540-73279-2_48.
34. Montecchi, L., Lollini, P., Bondavalli, A., & La Mattina, E. (2012). Quantitative security evaluation of a multi-biometric authentication system. In F. Ortmeier & P. Daniel (Eds.), *Computer safety, reliability, and security. SAFECOMP 2012* (Lecture notes in computer science) (Vol. 7613). Berlin: Springer. https://doi.org/10.1007/978-3-642-33675-1_19.
35. Michel Owayjan, Amer Dergham, Gerges Haber, Nidal Fakih, Ahmad Hamoush, Elie Abdo. Face recognition security system, Springer, Berlin (2013). Retrieved from https://www.researchgate.net/publication/259027363
36. Ali Alheeti, K. M. (2011). Biometric Iris recognition based on hybrid technique. *International Journal on Soft Computing (IJSC), 2*(4). https://doi.org/10.5121/ijsc.2011.24011.
37. Shubhika Ranjan, Prabu S, Swarnalatha P, Magesh G, Ravee Sundararajan, Iris Recognition System, International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395–0056, Vol: 04, Issue: 12, (2017). Retrieved from https://www.ijeat.org/wp-content/uploads/papers/v8i5S3/E11030785S319.pdf
38. Chanchaichujit, J., Tan, A., Meng, F., Eaimkhong, S. *Healthcare 4.0: Next generation processes with the latest technologies*. Retrieved from https://link.springer.com/book/10.1007/978-981-13-8114-0
39. J. Vora, P. Dev Murari, S. Tanwar, S. Tyagi, N. Kumar and M. S. Obaidat. Blind signatures based secured e-healthcare system International Conference On Computer, Information and Telecommunication Systems (CITS), Colmar, 2018, pp. 1–5. Retrieved from https://ieeexplore.ieee.org/document/8440186
40. Kumari, A., Tanwar, S., Tyagi, S., Kumar, N., Parizi, R., & Choo, R. (2018). Fog data analytics: A taxonomy and process model. *Journal of Network and Computer Applications, 128*(2019), 90–104. https://doi.org/10.1016/j.jnca.2018.12.013.
41. Summary of the HIPAA Security Rule. HHS.gov. Retrieved November 30, 2019, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations
42. HIPAA Privacy Rule - HHS.gov. Retrieved November 30, 2019, from https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

43. The future of governance of health data in India. Ikigai Law. Retrieved November 30, 2019, from https://www.ikigailaw.com/disha-and-the-draft-personal-data-protection-bill-2018-looking-at-the-future-of-governance-of-health-data-in-india.
44. DISHA and the draft Personal Data Protection Bill ... - Ikigai Law. Retrieved November 30, 2019, from https://marksmanhealthcare.com/indias-disha-different-global-patient-data-protection-laws