Manchester Metropolitan University

e-space

Manchester Metropolitan University's Research Repository

Please cite the Published Version

Butt, Shariq Aziz, Jamal, Tauseef, Azad, Muhammad Ajmal, Ali, Arshad and Safa, Nader Sohrabi (2022) A multivariant secure framework for smart mobile health application. Transactions on Emerging Telecommunications Technologies, 33 (8). e3684 ISSN 2161-3915

DOI: https://doi.org/10.1002/ett.3684

Publisher: Wiley

Version: Accepted Version

Downloaded from: https://e-space.mmu.ac.uk/633266/

Usage rights: © In Copyright

Additional Information: This is the peer reviewed version of the following article: Butt, SA, Jamal, T, Azad, MA, Ali, A, Safa, NS. A multivariant secure framework for smart mobile health application. Trans Emerging Tel Tech. 2022;e3684, which has been published in final form at https://doi.org/10.1002/ett.3684. This article may be used for non-commercial purposes in accordance with Wiley Terms and Conditions for Use of Self-Archived Versions. This article may not be enhanced, enriched or otherwise transformed into a derivative work, without express permission from Wiley or by statutory rights under applicable legislation. Copyright notices must not be removed, obscured or modified. The article must be linked to Wiley's version of record on Wiley Online Library and any embedding, framing or otherwise making available the article or pages thereof by third parties from platforms, services and websites other than Wiley Online Library must be prohibited.

Enquiries:
If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines)

A multivariant secure framework for smart mobile health application

Shariq Aziz Butt, Tauseef Jamal, Muhammad Ajmal Azad, Arshad Ali, Nader Sohrabi Safa

Abstract

Wireless sensor network enables remote connectivity of technological devices such as smart mobile with the internet. Due to its low cost as well as easy availability of data sharing and accessing devices, the Internet of Things (IoT) has grown exponentially during the past few years. The availability of these devices plays a remarkable role in the new era of mHealth. In mHealth, the sensors generate enormous amounts of data and the context-aware computing has proven to collect and manage the data. The context aware computing is a new domain to be aware of context of involved devices. The context-aware computing is playing a very significant part in the development of smart mobile health applications to monitor the health of patients more efficiently. Security is one of the key challenges in IoT-based mHealth application development. The wireless nature of IoT devices motivates attackers to attack on application; these vulnerable attacks can be denial of service attack, sinkhole attack, and select forwarding attack. These attacks lead intruders to disrupt the application's functionality, data packet drops to malicious end and changes the route of data and forwards the data packet to other location. There is a need to timely detect and prevent these threats in mobile health applications. Existing work includes many security frameworks to secure the mobile health applications but all have some drawbacks. This paper presents existing frameworks, the impact of threats on applications, on information, and different security levels. From this line of research, we propose a security framework with two algorithms, ie, (i) patient priority autonomous call and (ii) location distance based switch, for mobile health applications and make a comparative analysis of the proposed framework with the existing ones.

1 INTRODUCTION

The Internet of Things (IoT) is blended of two kinds of systems, ie, (i) wired and (ii) wireless, to connect with the internet. However, the wireless part is mostly used on account of its easy availability at most of the places. Market of IoT is growing exponentially due to low cost and easy availability of IoT devices.[1] This makes mHealth more feasible to monitor the person's health and poses new research challenges to the research community.[2-4]

FIGURE 1 Context-aware system under threats

The monitoring sensors in health are producing huge amount of data. The context-aware computing, a new domain of research, plays a vital role in managing the patient's data. The context-aware computing is gaining popularity due to its unique features, such as dealing with the current context environment, timely reaction to current situation, data

presentation to the user, and data collection from sensors. It is used to track the status of smart technological objects such as people, mobile, and sensors. Context-awareness includes all types of information about various kinds of contexts such as object, location, activities, temperature, body movement, environment sensing, and monitoring.[5-7]

However, mHealth environment faces many threats from intruders due to wireless connectivity,[8-10] which can affect the overall performance of the system as well as lead to data modification, revealing, and deletion. Figure 1, context-aware system under threats, shows an example of a context-aware system levels under threats, ie, system and hardware level, data security level, authentication access/administrative level, and physical level.

In **System and Hardware Level,** a person wears different kinds of incorporated sensors that are used for data transmission. The control gadget works as a gateway between sensors inside the system and the context of outside world. The hardware part of the system faces server and operating system threats. Therefore, during the development of frame- works for health monitoring applications, multiple aspects and functionality of the applications are required to be considered.[11-13]

The **Data Security Level** is the most targeted level by intruders because health applications contain medical as well as personal data. Hence, placing huge amount of valuable and confidential data on health care applications, the data is at serious hazards to steal, misuse, and manipulate.[5,11,14]

The **Authentication Access/Administrative Level** is required for effective security control to manage the system. At this level, the most vulnerable threat is to get unauthorized access to the system. Therefore, the system needs a strong authentication approach to secure the system from intruders.[5,15]

The **Physical Level** includes controlling access to physical devices and stealing and tempering information in the system. Mostly, the devices are vulnerable to wear and tear. Similarly, the system may malfunction and present major issues to the overall operations and tasks in case of occurrence of anomalies. Thus, there is a need of careful designing of devices to make the tempering verification vital. However, it is true that avoiding physical tempering of devices is difficult to accomplish. Another preventive measure is that only the authorized persons are allowed to physically handle the devices.[11,16]

With the purpose of securing mHealth applications, many security frameworks have been proposed such as Office of the National Coordinator (ONC) National Framework, Health Privacy Project (HPP) Best principles, HPP Best Practices, Markle: Common Framework, and General Data Protection Regulation (GDPR). However, existing frameworks have some limitations to secure mHealth applications.

The rest of this paper is structured as follows. Section 1.1 presents background of context-aware computing. Section 1.2 discusses the motivation and contribution. Section 2 explains the context-aware scenarios for smart health systems. Section 3 presents security threats with impact on application. Section 4 explains the existing frameworks for mobile applications. Section 5 explains proposed framework. Section 6 explains the difference between the existing frameworks and the proposed framework, and Section 7 presents the conclusion.

1.1 Background

The ability of any system to understand its environment to adopt behavior according to a particular situation is known as context awareness.[1] The context is a situation about the environment of the user that computer is able to understand.[17] Another definition found in the literature is that "context is the type of information that can be used to describe orcharacterize the overall situation of entities which is related to the user and application interaction, which includes user and application itself."[18] As defined in the works of Sharif et al[19] and Bradeško et al,[20] two different dimensions of context aware, ie, internal context and the external context, are provided. The external context is defined as physical context such as measurement of temperature, heat, and location. Internal context purely depends on user-specified dimensions. This is captured by observing the user interactions with systems such as business context or emotions. Many context-aware systems use an external or internal factor like the location of the particular user in that particular situation. According to Yürür et al[21] and Celdrán et al,[22] we must distinguish and deal with three entities, namely, places (rooms, buildings, etc), things (computer components, physical objects), and people (groups, individual, etc). These entities have further subattributes like status (means activity, an intrinsic property of that entity), identity (has some extraordinary identifier), area (position, co-area, closeness, and so forth), and time (timestamps are utilized to characterize the correct circumstance or requesting). The context-aware computing is currently used in many real-time applications such as security tracking, data security, military security, and temperature sensing, but the most important application is intelligent health context-based systems for health monitoring.[23-25] The context aware computing has the concept of multiagent systems for intelligent environment acquisition, abstraction, and application. In the multiagent context aware system, the agent means that sensors work as cooperative network and monitor an environment. These multiagent systems perform dif- ferent kind of activities such as sensing, interaction with the users, interaction with other sensors in the system, and information processing and controlling. In mHealth systems, the multiagent systems are mostly self-organized.[26-28]

1.2 Motivation and contribution

IoT is becoming a very vast field for research community due to its involvement in wired and wireless networks. Today, everything is connecting with the internet and making everything smart such as smart cities, smart hospitals, smart high- way, smart factory, and smart health.[29-31] The mHealth is enormous domain in the IoT due to its relation with the smart health and human's life. The smart mHealth monitoring can save patient's life and support in medication remotely.[32-34] In smart mHealth, the context aware computing is playing very important role for health monitoring due to its intelli- gent concepts to make application adoptive to the environment.[7,24] The most important requirement from the context aware application is to provide multivariant functionalities for mHealth monitoring.[13,35,36] The multivariant means var- ious functionalities like securing of data, continuous monitoring with static and remote states, and deny unauthorized user access. As evident from Figure 2, technical scenario 1, intensive care, and Figure 3, technical scenario 2, normal health care, there are two scenarios to monitor the patient's health, ie, static and remote. For both of these two states, the application should be multivariant to support monitoring and adopt any situation either static or remote. Therefore, the system or applications should be designed to provide the multivariant functionalities to support continuous monitor- ing. There are many existing frameworks to design and develop the smart mHealth monitoring applications but all have some drawbacks such as traditional secure authorization mechanism, lack of trustworthy staff, third party security risks, and monitoring for a specific state.[37-39] Therefore, we propose a multivariant functionality framework to overcome all these issues from mHealth monitoring. The proposed framework targets the data traffic management on application, con- tinuous monitoring support, threats detection, new alert approach, new authentication approach, and location distance control.

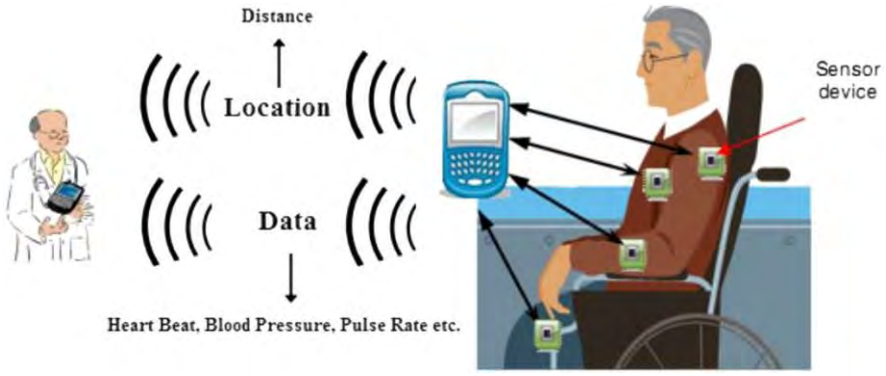

FIGURE 2 Technical Scenario 1, intensive care

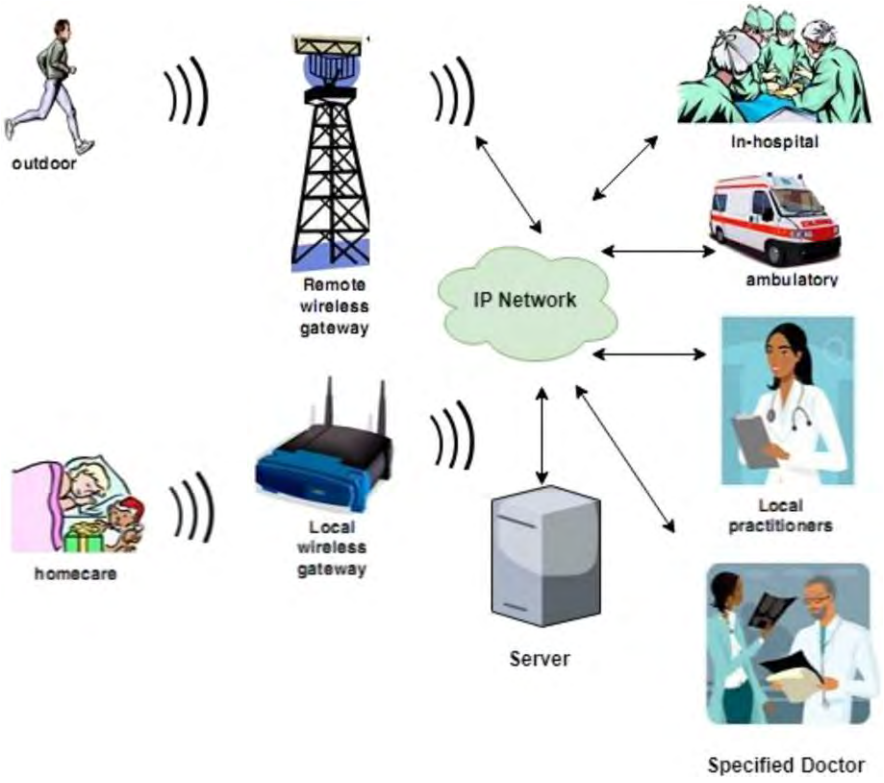

FIGURE 3 Technical Scenario 2,
normal health care

2 SMART HEALTH APPLICATIONS

There are two technical scenarios to understand the concept of context-aware computing in health systems. In Figure 2, technical scenario 1, intensive care, the first technical scenario refers to intensive care. A patient sits on fully automated wheelchair with planted sensors to sense the activities of the patient that can be temperature, blood pressure, heartbeat, pulse rate, etc. This type of context-aware health application is developed for disable persons known as intensive care scenario. The sensors monitor the activities and send results to a smart mobile device. The medium of communication is wireless between the patient and end destination. The sensed data is delivered to the doctor with the location of the patient and activities. The patient's data can include blood pressure, temperature; pulse rate, heart beat, etc. The doctor is notified in case of any abnormality to take an appropriate action to maintain the patient health.[2,11]

In Figure 3, technical Scenario 2, normal health care, the second technical scenario refers to normal health care. The person can be at any place and can do any activities, either outdoor or at home. The person wears some smart gadgets or planted sensors in the body to observe the activities. In this example, the destination of patient data in any emergency case is predecided. Data can be delivered to the nearest hospital at that time, can be delivered to nearest ambulance service center with the current location of the patient, can be sent to local doctor clinic, and can be sent to the family doctor or any family member. The location and receiver of the data can be set with the need of application.[2,11]

The distance matters a lot between the patient and receiver for efficient health monitoring. In both scenarios, the patient has more complex situation for efficient health monitoring due to single receiver and distance. If the receiver is not accessible, then the patient can face many complex situations.

3 SECURITY THREATS IN SMART HEALTH SYSTEMS

Due to the data security and privacy the healthcare application has several threats with there impact on application. Some of these threats that target the functionalities of the health care systems[10,40,41] are mentioned below in Table 1, threats in mHealth.[29,42,43]

- The **Confidentiality Loss** ensures the authentication/authorization of the unknown user to the information of the patient.

TABLE 1 Threats in mHealth[29,42,43]

Threats	Type of Feature/Functionality	Impact
Reveal of information	Confidentiality loss	Patient data is show to unauthorized person, loss of trust.
Withholding information and services	Availability loss	Financial loss, less support of services, less monitoring.
Information modification	Integrity loss	Loss of data consistency, data accuracy, data modification, wrong Treatment of the patient.
Repudiation	Systems loss	Less control to track the user actions, forging of new actions.
Nonauditable	Fault tolerance loss	System failure, system recovery, services loss.

- The **Availability Loss** ensures the system services available all the time when the authorized person needs to access the system even in the case of any attack on the system.
- The **Integrity Loss** guarantees the information is not adjusted in the transmission mode in case of any adversary.
- The **Systems Loss** is the assurance that a node cannot deny the data validity.
- The **Fault Tolerance Loss** is the assurance that the system/node should provide services in any case (ie, system failure, software failure).

4 EXISTING PRIVACY FRAMEWORKS

In this section, we discuss existing frameworks such as Office of the National Coordinator (ONC) National Framework, Health Privacy Project (HPP) Best principles, Health Privacy (HPP) Best Practices, Markle: Common Framework, and General Data Protection Regulation (GDPR).

4.1 ONC national framework

The Office of the National Coordinator (ONC) Framework is for securing mHealth applications. It was introduced by the US department of Health and Human Services for the development of secure health systems and applications. It is used in the usage of the Strategic Health IT Advanced Research Projects (SHARP). It plans under the principles and standards of the ONC system. In this, challenges are for shared, organizational optional EHR information utilization. The ONC national framework is described in Table 2, ONC national framework principles.[44,45]

TABLE 2 Office of the National Coordinator (ONC) national framework principles

1. ONC National Framework[43-45]	
Principles	**Description**
ONC1 Individual access	The Access to person should be given a basic and on time intends to give access and acquire their identity for health data in a readable and understandable form.
ONC2 Correction	Patients should be given with time that means to the argument the precision or reliability of their exclusively identify health data, and to have incorrect data adjusted or to have a dispute reported document on the off chance that their requests are denied.
ONC3 Openness and transparency	The strategies, methodology, and innovations with new technologies that directly influence patients and additionally their separately identi fiable health data have to be open and transparent.
ONC4 Individual choice	Individual should to be given a sensible chance and capacity to plan good decisions about the gathering, utilizing, and disclosure of their individual identity health data.
ONC5 collection, use and disclosure limitation	People identity health data should be gathered, utilized, or potentially revealed just to the extent important to achieve a specified goal and never to segregate improperly.
ONC6 Data quality and integrity	People and entities should make sensible moves to guarantee that individual identity health data is finished, accurate, and up to date to the degree important for the individual's or entity's expected objectives and has not been changed or removed in an unapproved way.
ONC7 Safeguards	People health identity data should be secured with sensible authoritative, specialized, and physical protections to guarantee its confi dentiality, trustworthiness, and accessibility. Further more to safe unapproved or unseemly access, utilize, or revelation.
ONC8 Accountability	These benchmarks ought to be completed, and adherence ensured, all through legitimate watching and distinctive methods and strategies ought to be set up to report and mitigate non adherence and breaks.

TABLE 3 Health privacy project (HPP) best framework principles

	2. HPP Best Principles[46-48]
HPP 1	For all uses of health data, health care associations should eliminate individual identifiers to the complete extent possible, consistent with keeping up the usability of the data.
HPP 2	Protection Policies should be following the information/data.
HPP 3	An individual has full access to his/her information to check the status of health data and also have access to addition it.
HPP 4	Individuals should lean notice concerning the utilization and revealing of their health information and their rights with relevance to that information.
HPP 5	Health care associations should execute security shields for the capacity, utilize, and exposure to Health care data.
HPP 6	Personal recognizable health information should not be uncovered while not enough approval, aside from in restricted conditions. Health care organizations should give patients with beyond any doubt decisions concerning the usage and uncovering of their health data.
HPP 7	Health care associations have to build up policies also review systems with respect to the gathering, utilize and revelation of health data.
HPP 8	Health care organizations should utilize a target and furthermore, adjusted procedure to review the utilization and exposure of personally identifiable health data for research and examine.
HPP 9	Human services associations have not revealed uncover by and by recognizable health information to law approval specialists, missing a fundamental legal procedure, for instance, a warrant or court request.
HPP 10	Health privacy protections should be actualized so as to improve existing laws prohibiting discrimination.
HPP 11	Solid and compelling solutions for violations of security protections should be built up.
	3. HPP Best Principles[46-48]
HPP 1	For all uses of health data, health care associations should eliminate individual identifiers to the complete extent possible, consistent with keeping up the usability of the data.
HPP 2	Protection Policies should be following the information/data.
HPP 3	An individual has full access to his/her information to check the status of health data and also have access to addition it.
HPP 4	Individuals should lean notice concerning the utilization and revealing of their health information and their rights with relevance to that information.
HPP 5	Health care associations should execute security shields for the capacity, utilize, and exposure to Health care data.
HPP 6	Personal recognizable health information should not be uncovered while not enough approval, aside from in restricted conditions. Health care organizations should give patients with beyond any doubt decisions concerning the usage and uncovering of their health data.
HPP 7	Health care associations have to build up policies also review systems with respect to the gathering, utilize and revelation of health data.
HPP 8	Health care organizations should utilize a target and furthermore, adjusted procedure to review the utilization and exposure of personally identi fiable health data for research and examine.
HPP 9	Human services associations have not revealed uncover by and by recognizable health information to law approval specialists, missing a fundamental legal procedure, for instance, a warrant or court request.
HPP 10	Health privacy protections should be actualized so as to improve existing laws prohibiting discrimination.
HPP 11	Solid and compelling solutions for violations of security protections should be built up.

4.2 Health privacy project (HPP) best principles

The health privacy is a working group to introduce framework for secure health monitoring called health privacy project (HPP) best principles framework. It has been adopted by the Center for Democracy and Technology (CDT). The projec-t's main goal was to promote the public policies that make sure individual privacy because health information shared electronically. The principles of the HPP best are provided in Table 3, HPP best framework principles.[47,48]

4.3 Health privacy project (HPP) best practices

The HPP best practices framework was introduced by the same group working on health services. The framework mostly targets the group who take care of patient data records (PHRs) and defined some principles for securing access to health monitoring application.[46,49] Currently, the cloud computing is integrating service providers with the mHealth for data storage and privacy. The HPP best practices are detailed in Table 4, HPP best practices framework principles.[9]

TABLE 4 HPP best practices framework principles

4. HPP Best Practices[43,46]	
bp 1 Transparency and notice	The security suppliers ought to be immediate about their inspirations driving offering a Personal Heath Record to representatives and all techniques that apply to the Personal Heath Record. Businesses ought to give information Policy Statement or Notice that clearly spreads out the propensities by which data in the Personal Heath Record will be utilized and verified. Businesses should join the Notice into their therapeutic favorable circumstances programs, and should make it open in a layered sort out a short brief shape to keep running with a continuously separated one. Representatives ought to be in framed of any updates to the methodologies.
bp 2 Education	Employees should to be sufficiently instructed about the advantages, limits, and substance of the individual health records. Information about the individual's health records should be communicated from different viewpoints to build both learning and trust.
bp 3 Employees can choose which content is included in the personal health records	Employees ought to be in a situation to pick the substance of the PHR, including which suppliers and plans add to it. Specialists ought to in all likelihood elucidate the records exhibited by others, further enter their own data, with laborer entered learning checked in that capacity. The conspicuous confirmation of wellsprings of all near and dear health information inside the individual health data ought to be speedily plainly obvious.
bp 4 Employees control access to and use of the personal health record	A. Employees should control who is allowed to get entry to their personal health info's. Employers must now not get access to or use personnel' individually-identi able health information from the personal health record. B. employees have to pick out, with out condition, whether or not to furnish access to private health data within their personal health record for any "secondary uses". An audit trail that suggests who has accessed the personal health record should be easy to be had to employees.
bp 5 Employees can designate proxies to act on their behalf	Employees should decide who, including relatives and parental figures, should to have guide access to their Personal health record for their behalf. Where conceivable, Employees should have the capacity to give intermediary access to full or halfway data in their Personal health records, incorporating access to crisis conditions.
bp 6 Chain of trust: Information policies extend to the data chain of trust understandings that require business accessories to hold quickly to the business partners	The information procedures and practices of employers Personal health records should to complete employer's useful methodologies and practices.
bp 7 Data security	Safety providers should to give a solid level of security to protect the data in the Personal health records frameworks. A robust confirmation process for access to Personal health records should to be required, in extension to a review trail that shows who has gotten data and when.
bp 8 Data management	Safety Providers should to guarantee that the Personal health record frameworks they give have exhaustive information management procedures that secure the information including information maintenance approaches.
bp 9 Enforcement and remedies	Employers ought to develop oversight and obligation frameworks for holding quickly to their Personal health record systems and practices. Bosses should institute a way to deal with quickly educate delegates regarding any wrong access to or usage of information contained in an Employee's Personal health record, perceive the methods which have been made to address the inappropriate move, and make resources open to workers to help them in tending to impacts of the unacceptable action.
bp 10 Portability	Employers should present Personal health record that is transferable, to the degree practical, enabling representatives to keep up or move the PHR as well as the information it contains even after employment or scope finishes or changes.

4.4 Markle: common framework

The Markle Foundation introduced a framework called **Markle: Common Framework**. The project was supported and funded by the Markle Foundation. It is utilized in the undertaking Distributed Surveillance Taskforce for Real-time Influenza Burden Tracking and Evaluation (DiSTRIBuTE) venture. The task fundamental objective was sharing of information between the national influenza reconnaissance and bio observation practices with the contemplations of confinements included: production of various separate information storehouses, absence of input to unique infor- mation holders, legitimate and limitations to sharing individual recognizable data, delays in getting to or spreading gathered information, extensive expense to procurement of information, information security over state, and neigh- borhood jurisdictional self-governance. The principles of the framework are explained in Table 5, Markle: common framework principles.[47,50]

TABLE 5 Markle: common framework principles

4. Markle: Common Framework[43,48,50]	
CF 1 Openness and transparency	Customer should to have the ability to appreciate what information has been gathered about them, the purpose its usage, who can get to and use it, and where it locates. They should to similarly be instructed about how they may secure access to information gathered about them and how they may control who approaches it.
CF 2 Purpose specification	The reasons for which individual information is gathered should be specified at the time of accumulation, and ensuing the use should be constrained to those reasons, or others that are specified on each event of the progress of reason.
CF 3 Collection limitation and data minimization	Patient health data should to just be aggregated for deciding purposes and should be gotten by legitimate and reasonable strategies. The personal health information should be limited for storage and collection to that information necessary for use.
CF 4 Use limitation	Personal information should not be revealed, made accessible, or generally utilized for purposes other than those speci ed.
CF 5 Individual participation and control	Patients ought to have the ability to control access to their individual information. They should realize who is sparing what information on them, and how that information is being used. They ought to similarly be prepared to audit the way in which their information is being used or spared.
CF 6 Data quality and integrity	All personal data gathered should be important to the reasons for which they are to be utilized and should to be precise, finish, and up to date.
CF 7 Security safeguards and controls	Sensible safeguards should secure individual information against such dangers as misfortune or unapproved access to, utilize, modi fication, or disclosure.
CF 8 Accountability and oversight	Persons or organizations are responsible for individual health data must be held responsible for actualizing these standards.
CF 9 Remedies	Cures must exist to address security or protection infringements.

4.5 General data protection regulation

This framework is introduced by the Federal Trade Commission (FTC) USA. The General Data Protection Regulation (GDPR) defines security as the rights and commitments of people and organizations as for there uses and maintenance of patient's data. The principles of the framework are given in Table 6, general data protection regulation framework principles.[46,53,54]

TABLE 6 General data protection regulation framework principles

5. General Data Protection Regulation[9,51,52]	
Fairness, lawfulness, and transparency	The preparing of individual information must be done in a reasonable and clear way. Information subjects must be given data concerning that is required for their information in an unmistakable way. This should be done before any information is merged and changes are done. The GDPR besides specifies particular conditions for arranging solitary information including (in any case, not limited to) the assent of the information subject.
Purpose limitation	Every single individual information gathered by the information controller or processor must be done in a way which is specific, express and authentic for the reason it was gathered.
Data minimization	All the individual data should be gathered in such a way that it should be to its limited purposes.
Accuracy	Every single individual data which are gathered should be exact and stayed up with the latest and measures should be set up to recognize mistaken information.
Storage limitation	Every individual information gathered should be stored in such a way which permits the identification of the information subjects for a measure of time no longer than is expected to finish the tasks which the information was gathered for.
Integrity and Confidentiality	Every single individual data gathered must be prepared by strategies that ensure suitable security and protection shields that will stop unapproved and unlawful use as well as protect against unexpected misfortune or harm.
Accountability	The information controller is in charge of guaranteeing (also illustrating) consistence with the standards above. This incorporates different information administration and responsibility commitments, for example, reporting the gathering of consent; executing specialized and hierarchi cal measures to sufficiently secure individual information (eg, pseudonymisation); taking an information security (protection) by plan and default way to deal with information handling; leading information security affect appraisals; and detailing individual information insurance breaks.

5 PROPOSED FRAMEWORK

This work proposes a security framework for smart mHealth applications in IoT. The smart mHealth applications can be prevented from threats by adopting the principles provided in the proposed framework for design and development of applications. The framework mainly focuses prevention from intruders and secures the remote patient's information with continuous monitoring. As mentioned earlier in Section 5, there are many threats to health applications, which directly affect the application's services, health monitoring, data modification, and reveal of information. In this framework, we give some principles that limit the security attacks and make health monitoring ingenious. Figure 4, proposed security framework, presents our proposed framework called **"Secure Health Principles (SHP)"**. The principles of SHP are provided in Table 7 proposed framework's principles. We provide seven principles with new approaches and concepts to secure the mHealth applications; in the first principle, we suggest user access to application with the voice authentication method; in the second principle, we present the data presentation format for both patient and doctor; in the third principle, we provide Call alert message approach for any update, delete, modify, and abnormality with respect to information; in the fourth principle, we present that the application have some intelligent sensors schema in which the sensors at the doctor end perform some activities such as autonomous information update and modifications rather then third entity; in the fifth principle, we suggest the patient priority approach on the basis of their disease to reduce the traffic load from application with the continuous monitoring; in the sixth principle, we provide that there is no administration or third party such as cloud for data store and control; and in the last seventh principle, we provide a new concept for mobility of patients that includes location and distance of patient.

We set a priority level of patients on the basis of their diseases and then set an autonomous time-based call mechanism to get the update status of the patient's health with continuous monitoring. This way, the sensor in application can timely predict any type of delay in data transformation due to security threats.[55,56] The autonomous call functionality ensures the continuity of healthcare in remote areas and improves the connectivity between the patients and doctor. In the first phase, the doctor sets the disease priority based on patient's health condition and disease seriousness (see Figure 5, patient disease prioritization with time filtration). In the second phase, the doctor sets a time scale filtration for updated status for patient's health. The time span can be different from patient to patient and disease to disease. As mentioned in the work of Kakria et al,[57] a patient can have more than one disease to monitor and the application has to take preprogrammed actions. The reason of this time difference is to reduce the complexity of application's functionality and quick response from the doctor to diagnose different patients.[58-60] Furthermore, the traffic due to continuous monitoring is always high, resulting in slow data transformation and reduction in quality of service. The data transmission can be slower due to low connectivity of wireless network.[61] As mentioned in the work of Lloret et al,[60] it is expected to achieve 50 billion pervasive devices associated to the smart mobile network until 2020. Beside this, the traffic from cell phones will represent around 66% of the complete IP traffic. Hence, the limit of the systems needs to be significantly expanded to fulfill these high data rates to satisfy the needs of the clients without decreasing the quality of service. Therefore, the time-based filtration manages these types of aspects of application to make it more qualitative and support the continuous monitoring. The doctor can set the time scale for new update status by using

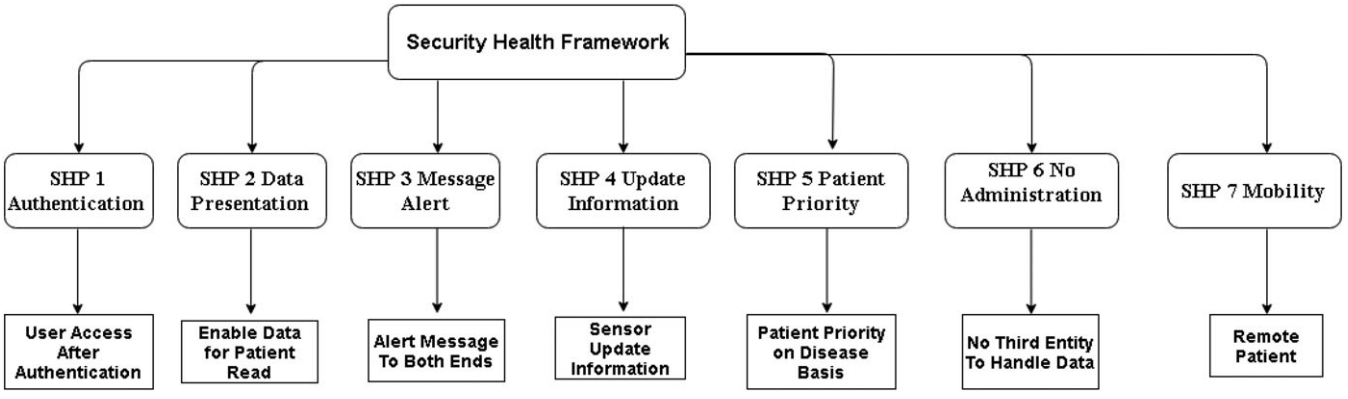

FIGURE 4 Proposed security framework

TABLE 7 Proposed framework's principles

Secure Health Principles (SHPs) 2018	
Principles	**Description**
SHP 1 Authentication	The sender and receiver can get access to application by using voice authentication approach and verify their identity. The voice authentication approach is more secure than any other traditional access approach. It is a robust authentication process to secure information.
SHP 2 Data Presentation	Information presentation is made easier, therefore a patient can view status, read information and understand it. In the case of any serious change in information, patient can take an action. This principle maintains the data quality and presentation.
SHP 3 Message Alert Call	There is an alert call information message in application. When any abnormality in the patient's information is monitored, then call alert message is sent at both sides, ie, doctor and patient. This principle monitors the abnormalities such as threats, data modifications, data drop and deny of application services.
SHP 4 Intelligent Agent (Sensor)	Only intelligent sensors can update the information of patient. There is no individual information update, if any individual wishes to update, change or delete any information then he/she has to get permission from the other party. There is no direct human involvement in it.
SHP 5 Patient Priority	In this principle a Time-Span for status is set with respect to patient priority on the basis of their diseases. It means that after a specific time period the intelligent sensor gets the update status of patient health. If the information does not send to doctor by sensor after that specified time period then the sensor generates a call on a patient end to get the new status of the patient's health. The purpose of this principle is that when an attacker does any malicious activity then this new call concept enables in knowing the abnormalities in application.
SHP 6 No Safeguards and Organization	There are no safeguards, administrative body, employees, technical, and cloud safeguards to secure the information. The reason is that the attacker can be internal and can reveal information. Therefore there should be no safeguards to secure the patient's data. The only sensors secure the information in mHealth applications.
SHP 7 Mobility	Patient mobility includes the location and distance of the patient from doctor or any medical facility. Due to mobility of the patients, it is very important to facilitate the patient accurately and timely at their current location. In this principle our framework works for quick medication facility within short time and distance.

Algorithm 1. In smart health application, doctor just needs to select the time difference against any disease and patient. This time-based filtration also protects the healthcare application from threats that need to mitigate. These security threats in smart remote mHealthcare environment can be sinkhole attack, denial of service attack (DoS), and select forwarding attack.[62,63]

Algorithm 1 Patient priority autonomous call

Input: T_l : Last Time, T_n : New Time. T_d : Time Difference, P : Patient, D : Doctor, P_r : Prioritization, D_i : Diseases

Output: Autonomous Call to Patient for Update Status

1. **Start**
2. Let **D** to set P_r of P with respect to their D_i
3. Set T_d for every D_i for status
4. **Check** Continuous Monitoring of patient
5. **For** $T_d = T_l - T_n$= 2 Minutes
6. *If* T_d is ≥ 2 Minutes and no update status **then** do
7. Automatically Call to P
8. Repeat Call until patient response
9. **end** *if*
10. End
11. **Return** Update Status Via Call

- The **DoS attack** in healthcare disrupts the application functionality to monitor the patient health.[64]
- In **sinkhole attack,** the data packet is dropped to malicious end and it also affects the other sensors in network, this attack is very hard to detect timely.[65]
- In the **select forwarding attack,** the attacker changes the route of data and forwards the data packet to other location.[66-68]

Therefore, our proposed time-based scaling algorithm helps the application to detect any malicious threat such as data drop to false location, DoS, and alteration in the route of the data. It helps to protect the application from many other security threats that are hard to detect on time. As a result, it manages data traffic, reduces the complexity of system, and detects malicious behavior.

5.1 Formal modeling of autonomous call algorithm 1

Algorithm 1 is designed for the principle patient priority call. In this algorithm, the key inputs are T_n, T_l, and D_t. T_l is the last time, T_n is the new time, and D_t is the difference of the new and the last time, ie, T_n-T_l. The D_t works as trigger for sensor to generate an autonomous call. The D_t can vary in diseases D_i and is set manually by the doctor **D** for every

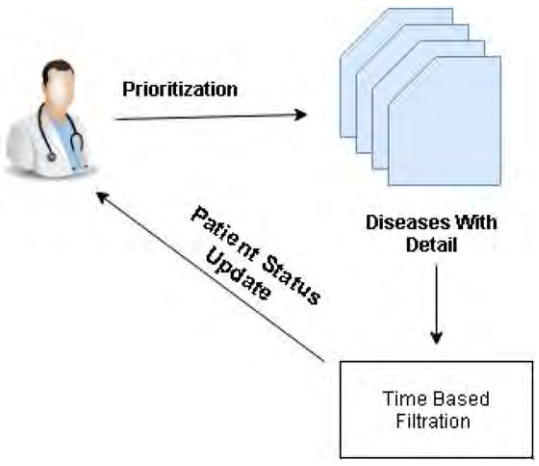

FIGURE 5 Patient disease prioritization with time filtration

patient **P.** Using the algorithm, **D** can set P_r for P_s according to their disease type. Here, we set time difference D_t as 2 minutes in algorithm to present our schema. After every 2 minutes, the system checks the update status of the patient. If there is no update about the information or any abnormalities in the status information, then the system autonomously calls the patient for an update. The main goal of the algorithm is to reduce the complexity of the system, manage patient monitoring with disease priority. As mentioned in the work of Kakria et al,[57] a patient can have many diseases to monitor at a single time, which can be fever, blood pressure, heart beat monitoring, etc. An application can have many users including the patients, doctors, and nurses and can generate huge amount of data traffic that can cause some challenges in terms of complexity and timeliness. To solve these issues, there is a need to design and develop systems with new approaches.[69] Therefore, we propose the decision-making algorithm to overcome these issues in mHealth application with priotization concept. The Algorithm 1 not only sends call alert message but also controls the status updates. The conventional way of alert message in mobile smart health environment is short messages service (SMS), where an SMS is delivered at specified location in any abnormality situation. The issues with SMS approach are late delivery of message, message size, and unreadable messages. Our proposed framework overcomes these alert messages challenges and alerts are sent via call.[70,71]

Acronyms	Meaning
P	Patient
D	Doctor
T_l	Last Time
T_n	New Time
T_d	Time Difference
P_r	Pririotization
D_i	Diseases
S	Store Distance
T_f	First Time
T_h	Half Time
Ont	Ontology
C	Categorization
d	Distance
T_w	Wait Time

5.2 Location distance-based switch Algorithm 2

In the patient mobility, the distance and location of the patient matters to take the right decision to facilitate the patient timely. In the mobile health smart applications, there is a need to calculate the **distance** of the nearest medical facility with **time** to reach that medication to patient. As mentioned in the work of Kakria et al,[57] the existing mobile smart health applications are working on patient's location with the use of the Google maps. When there is any abnormality, the only doctor will send medication to patient at current location. However, the issues with this concept are as follows.
(1) Distance of the patient from the doctor (means how far the doctor is away from the patient). (2) How much time is required by medication facility to reach to patient? (3) What kind of disease the patient has? Does this disease need urgent medication? These are some challenges with the existing approaches that need to address.

In the existing frameworks, only the doctor can send the medication facility to the patient. Therefore, there is a need of modifications to facilitate the patient timely. We propose Algorithm 2 to enhance this facility in mobile health applications. In this algorithm, we categorize the medication facility ontology (eg, doctor, clinic, ambulance service, hospital) with respect to the disease of the patient. When there is any abnormality, the mobile application first filter the ontology based on disease, then measures the individual distance of each ontology from patient's location and store all distances for future correspondence. After this, the application sends alert to the nearest with the shortest distance ontology for medication facility. After sending the alert message, the application measures the time of send alert and waits for medication facility to reach; if not, then the application wait for half time of the first send alert time. Otherwise, the application switches to the next nearest medication facility and repeats this until the medication facility reaches to the patient. When the medication facility reaches to the patient, then the application generates a new message to those ontologies that also received medication support alert message. This stops the multimedication facilities to reach the patient and improve the application intelligent decision making.

Algorithm 2 Location distance based switch

Input: **S** : Store Distances, T_f : First Time, T_h : Half Time., ***P*** : Patient, **Ont** : Ontology, **C** : Categorization, **d** : Diseases, T_w : Wait Time

Output: Get Medication Facility within short time

Start

1. First set **C** of **Ont** with respect to D_i **then**
2. compute the **d** for all **Ont** & **S then** do
3. send alert to **Ont** with shortest distance
4. **Check** the T_f of alert send message to **Ont**
5. ***for*** Calculate T_w the each **Ont** first time and Half time
   $$T_w = \frac{T_f}{T_h}$$
6. **Wait** for the T_w to reach the medication to ***P***
7. ***if*** the medication do not reach to ***P*** **then**
8. **Switch** to next shortest distance **Ont** from the **S**
9. repeat until the medication reach to ***P***
10. **end** ***if***
11. **end** ***for***
12. Send stop message to other **Ont** for not come when the ***P*** get medication

13. **END**
14. **Return**

6 DISCUSSION AND COMPARISONS

This section is explaining the difference between the key features and principles of the proposed framework with the existing frameworks. We explained the principles with name and key attributes of various existing frameworks in Section 5.

In Table 8, sign **X** shows that the principle does not exist in the frameworks. In the individual access feature, the ONC 1, HPP 3, bp 4 and CF 1 follow the traditional way of user access to application. However, in our framework SHP 1, we provide an authentication access approach, which a user can access the application and data. Our access approach will secure the system from any kind of unauthorized person. In our approach, a user (patient and doctor) can use its smart phone speaker to authenticate through voice and get access to application. This can secure the application from the intruders to get access to application. The openness and transparency included in the ONC 3, bp 1 and 1 are clarifying that the data should be open and the security approaches, strategies should be characterized and pursued. However, in our framework, we dispose of this. The reason is that, when the data will be on receptiveness mode, then it provides a chance to intruders for any pernicious action with the data and system. The information disclosure and notification features of our framework has similarity with the existing frameworks as ONC4, HPP 1, HPP 4, CF 4, and SHP 3. All frameworks highlight that there should be a notification process in the system to inform the patient about his information (change, delete, or update). However, we adopt a new approach, ie, call alert using the Algorithm 1 for patient and doctor. The autonomous call is done by the intelligent agent (sensor). The safeguard feature in ONC 7, HPP5, bp 7, CF 7, and 6 is presenting that there should be a safeguard third party in the form of administration/organization to manage the data, as, currently, the cloud computing concept is used for it.[9,38,39] It is a traditional way to store and secure the data on cloud. Nevertheless, it makes easy way for intruders and third party associated risks.[72,73] Therefore, in our framework, the SHP 4 and SHP 6 deny storing data on any third party and prefer to storing data on agent (sensor). The data presentation feature is present in CF 6, we propose SHP 2 principle that the data should be in such presented form that a patient can understand it. The main reason of readable data presentation is to inform the patient about the data so that, when ever any data modification is done, the patient can predict it. Our propose framework in SHP 4 only provides the intelligent agents (sensors) feature. In this, the data processing activities should be done and monitor by the sensors only to secure data processing. The patient priority SHP 5 suggested that due to the intensive health situation of a patient, as mentioned earlier in Figure 2, technical Scenario 1, intensive care. The information collection and its use by other feature exist in ONC 5, bp 4, and CF 3 but does not exist in our proposed framework, due to the data sensitivity and security breaches. The continuous monitoring of patient in

TABLE 8 Comparison of Principles for Smart Health Privacy

Features	ONC	HPP Best Principles	HPP Best Practices	Markle: Common Framework	General Data Protection Regulation	Proposed Framework
Individual Access	ONC 1	HPP 3	BP 4	CF 1	X	SHP 1
Openness and Transparency	ONC 3	X	BP1	X	1	X
Information Disclosure and Notification.	ONC4	HPP 1, HPP 4	X	CF 4	X	SHP 3
Safeguards/Third Party	ONC 7	HPP5	BP 7	CF 7	6	SHP 4 and SHP 6
Data Presentation	X	X	X	CF 6	X	SHP 2
Intelligent Sensors	X	X	X	X	X	SHP 4
Patient Priority	X	X	X	X	X	SHP 5
Information Collection and Use by Other	ONC 5	X	BP 4	CF 3	X	X
Patient Mobility	X	X	X	X	X	SHP 7

mobility mode should be a major component of mobile health application. The existing mobile health frameworks do not have any principle or mechanism for remote patient medical facilitation; however, in the proposed framework, the mobility is considered as a key component, due to the need of continuous monitoring considering patients' mobility. The patient mobility has some major characteristics such as location, distance, and data traffic on application due to continuous monitoring. In the propose framework, we provide a principle for patient mobility while considering all these characteristics of application. The comparative analysis of features with the existing framework is shown later in Table 8 comparison of principles for smart health privacy.

6.1 Research findings

6.1.1 Access control

Access control is an important factor in the mHealth to secure the access of the application from the malicious persons. Access control should be done with focus on patient centric. The access should be on role basis with the role of data access and limitations to patient's data.[46,49,74]

6.1.2 Authentication

The authentication is the check for any person to get access to the system. The authentication should be done by the unique ID and password that is only known by the user, a controller.[46,49,74]

6.1.3 Security

The security principles must be considered when devising the mHealth applications. The security parameters make the whole application secure from the intruders. Different security approaches must be suggested and implemented to make the system secured from any malicious activity.[46,49,74]

6.1.4 Inform patient

There should be functionality in the application of how it responds to the patient about the collection, usage, and change of his/her information. This functionality will enhance data security and data quality. This functionality should be easy to implement and understandable by the patient. This functionality should breach the notification to patient and doctor about any change in data.[46,49,74]

6.1.5 Mobility

Mobility management plays an important role in context-aware systems since the data demands of moving nodes have been increasing. Therefore, mobility needs to be considered in health systems to alleviate situations such as load balancing, timely service, and service disruption. This will enable all entities (doctor, patient, facilitation center, etc) of the system to roam between networks without application loss. In our opinion, the health system should also include various mobility models based on daily routine of patient and previous history.[75,76]

6.1.6 Connectivity

In IoT, the wireless network is mostly used due to its remote connectivity of devices (sensors) from anywhere. Thus, the mobile health systems are expanding rapidly. This leads to various issues related to Quality of Service (QoS), such as interference, energy, congestion, processing delay, capacity, throughput, collisions, and contentions.[77]

Resource depletion may lead to poor QoS or DoS attack.[78] In order to address the QoS related issues, there is a need to improve various access and routing protocols (such as in IEEE 802.15.6 std). Efficient resource management schemes need to be devised to increase the throughput and capacity of overall network.[79]

Another thing, we need to assure the always-connected situation to enable constant observation of the patient. We also need to consider the disaster situation, eg, if there is no infrastructure. In our opinion, the mHealth application should also work in absence of operator, either using cooperation[80,81] or D2D (device to device) or heterogeneous network (HetNet). This way, a patient in infrastructure-less area can communicate and cooperate via health application to other users in vicinity. If any of the other users is in infrastructure area (or move to infrastructure), the information can be forwarded to facilitation center on behalf of the patient.

7 CONCLUSION AND FUTURE WORK

The smart context aware health focuses globally around society since all humans need health assistance or can be a patient in lifetime. In this paper, the context aware computing is playing a vital role to make the mHealth more viable. However, the mHealth application has many threats that makes it unsecure to use for health monitoring. There are many existing frameworks such as ONC National Framework, Health Privacy Project (HPP) Best principles, HPP Best Practices, and Markle: Common Framework and General Data Protection Regulation. These all frameworks target different security environment for securing the mHealth application from any kind of threats. However, all these frameworks have some limitations to secure the mHealth applications; thus, we provide a security framework to make the mHealth application more secure from any kind of threats. In this paper, we comparatively analyze these frameworks with our proposed framework.

The generalization and adoption of the strategy of smart health will profit society as an entire. In the future, we are interested in implementing a health application based on our framework and test on real-time patients. In addition, we aim to provide analytical comparison of all frameworks, finding some flaws in these frameworks and divert these to a new direction to secure the health application with better functionalities. There is also a need to explore connectivity features of framework to enhance the QoS. This way, the individuals will enormously profit by the idea of health since they will increase the way of life quality, way of life and freedom, whereas their medicines turn out to be progressively proficient and less expensive.

ORCID

Tauseef Jamal https://orcid.org/0000-0003-4965-0322
Muhammad Ajmal Azad https://orcid.org/0000-0003-1707-018X

REFERENCES

1. Brézillon P, Gonzalez AJ, eds. *The Context in Computing: a Cross-Disciplinary Approach for Modeling the Real World*. New York, NY: Springer; 2014.
2. Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of things (IoT): a vision, architectural elements, and future directions. *Future Gener Comput Syst*. 2013;29(7):1645-1660.
3. Jamal T, Amaral P, Khan A, Zameer A, Ullah K, Butt SA. Denial of service attack in wireless LAN. Paper presented at: The Twelfth International Conference on Digital Society and eGovernments; 2018; Rome, Italy.

4. Perera C, Barhamgi M, Bandara AK, Ajmal M, Price B, Nuseibeh B. Designing privacy-aware internet of things applications. 2017. arXiv preprint arXiv:1703.03892.
5. Pang Z. *Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being* [Phd dissertation]. Stockholm, Sweden: KTH Royal Institute of Technology; 2013.
6. Alemdar H, Ersoy C. Wireless sensor networks for healthcare: a survey. *Computer Networks*. 2010;54(15):2688-2710.
7. Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context aware computing for the internet of things: a survey. *IEEE Commun Surv Tutor*. 2014;16(1):414-454.
8. Suo H, Wan J, Zou C, Liu J. Security in the internet of things: a review. Paper presented at: 2012 International Conference on Computer Science and Electronics Engineering; 2012; Hangzhou, China.
9. Ahmed A, Latif R, Latif S, Abbas H, Khan FA. Malicious insiders attack in IoT based multi-cloud e-healthcare environment: a systematic literature review. *Multimed Tools Appl*. 2018;77(17):21947-21965.
10. Jamal T, Butt SA. Malicious node analysis in MANETS. *Int J Inf Technol*. 2018;1-9.
11. Al Ameen M, Liu J, Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. *J Med Syst*. 2012;36(1):93-101.
12. Altamimi AM. Security and privacy issues in eHealthcare systems: towards trusted services. *Int J Adv Comput Sci Appl*. 2016;9(9).
13. Roman R, Lopez J, Mambo M. Mobile edge computing, fog et al.: a survey and analysis of security threats and challenges. *Future Gener Comput Syst*. 2018;78:680-698.
14. Li M, Lou W, Ren K. Data security and privacy in wireless body area networks. *IEEE Wirel Commun*. 2010;17(1):51-58.
15. Gope P, Hwang T. BSN-care: a secure IoT-based modern healthcare system using body sensor network. *IEEE Sens J*. 2016;16(5):1368-1376.
16. Gupta PK, Maharaj BT, Malekian R. A novel and secure IoT based cloud centric architecture to perform predictive analysis of users activities in sustainable health centres. *Multimed Tools Appl*. 2017;76(18):18489-18512.
17. Ko J, Lu C, Srivastava MB, Stankovic JA, Terzis A, Welsh M. Wireless sensor networks for healthcare. *Proc IEEE*. 2010;98(11):1947-1960.
18. Codina V, Ricci F, Ceccaroni L. Distributional semantic pre-filtering in context-aware recommender systems. *User Model User-Adapt Interact*. 2016;26(1):1-32.
19. Sharif M, Asghar Alesheikh A, Kaffash Charandabi N. Context-aware pattern discovery for moving object trajectories. In: Proceedings of the ICA; 2018; Singapore.
20. Bradeško L, Starc J, Mladenic D, Grobelnik M, Witbrock M. Curious cat conversational crowd based and context aware knowledge acquisition chat bot. Paper presented at: 2016 IEEE 8th International Conference on Intelligent Systems (IS); 2016; Sofia, Bulgaria.
21. Yürür Ö, Liu CH, Sheng Z, Leung VC, Moreno W, Leung KK. Context-awareness for mobile sensing: a survey and future directions. *IEEE Commun Surv Tutor*. 2016;18(1):68-93.
22. Celdrán AH, Clemente FJG, Pérez MG, Pérez GM. SeCoMan: a semantic-aware policy framework for developing privacy-preserving and context-aware smart applications. *IEEE Syst J*. 2016;10(3):1111-1124.
23. Rahmani AM, Gia TN, Negash B, et al. Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach. *Future Gener Comput Syst*. 2018;78:641-658.
24. Solanas A, Patsakis C, Conti M, et al. Smart health: a context-aware health paradigm within smart cities. *IEEE Commun Mag*. 2014;52(8):74-81.
25. Bhattacharyya S, Saravanagru RA, Thangavelu A. Context aware healthcare application. *IJCA-Int J Comput Appl*. 2011;22(3):1-6.
26. Aielli F, Ancona D, Caianiello P, Costantini S, De Gasperis G, Di Marco A, Mascardi V. FRIENDLY & KIND with your health: human-friendly knowledge-intensive dynamic systems for the e-health domain. Paper presented at: International Conference on Practical Applications of Agents and Multi-Agent Systems; 2016; Seville, Spain.
27. Rosa JH, Barbosa JL, Kich M, Brito L. A multi-temporal context-aware system for competences management. *Int J Artif Intell Educ*. 2015;25(4):455-492.
28. Vianna HD, Barbosa JLV. A model for ubiquitous care of noncommunicable diseases. *IEEE J Biomed Health Inform*.2014;18(5):1597-1606.
29. Kumar P, Lee HJ. Security issues in healthcare applications using wireless medical sensor networks: a survey. *Sensors*. 2011;12(1):55-91.
30. Ashraf A, Rajput A, Mussadiq M, Chowdhry BS, Hashmani M. SNR based digital estimation of security in wireless sensor networks. Paper presented at: International Conference on Communications Infrastructure. Systems and Applications in Europe; 2009; London, UK.
31. Hammi B, Khatoun R, Zeadally S, Fayad A, Khoukhi L. IoT technologies for smart cities. *IET Networks*. 2017;7(1):1-13.
32. Jara AJ, Zamora-Izquierdo MA, Skarmeta AF. Interconnection framework for mHealth and remote monitoring based on the internet of things. *IEEE J Sel Areas Commun*. 2013;31(9):47-65.
33. Jamal T, Mendes P. Cooperative relaying in user-centric networking under interference conditions, *Proc IEEE Commun Mag*. 2014;52(12):18-24.
34. Kai K, Pang ZB, Cong W. Security and privacy mechanism for health internet of things. *J China Univ Posts Telecommun*. 2013;20:64-68.
35. Jamal T, Butt SA. Cooperative cloudlet for pervasive networks. *Proc Asia Pac J Multidiscip Res*. 2017;5(3):42-26.
36. Ibrahim M, Bajwa I. Design and application of a multi-variant expert system using apache Hadoop framework. *Sustainability*. 2018;10(11):4280.
37. Mathur A, Newe T, Rao M. Defence against black hole and selective forwarding attacks for medical WSNs in the IoT. *Sensors*. 2016;16(1):118.
38. Yang Y. Attribute-based data retrieval with semantic keyword search for e-health cloud. *J Cloud Comput*. 2015;4(1):10.
39. Loheswaran K, Premalatha J. Renaissance system model improving security and third party auditing in cloud computing. *Wirel Pers Commun*. 2016;90(2):1051-1066.

40. Bricon-Souf N, Newman CR. Context awareness in health care: a review. *Int J Med Inform*. 2007;76(1):2-12.
41. Ng HS, Sim ML, Tan CM. Security issues of wireless sensor networks in healthcare applications. *BT Technol J*. 2006;24(2):138-144.
42. Islam SR, Kwak D, Kabir MH, Hossain M, Kwak KS. The internet of things for health care: a comprehensive survey. *IEEE Access*. 2015;3:678-708.
43. Theoharidou M, Tsalis N, Gritzalis D. Smart home solutions: privacy issues. *Handbook of Smart Homes, Health Care and Well-Being*. Cham, Switzerland: Springer; 2017:67-81.
44. Rea S, Pathak J, Savova G, et al. Building a robust, scalable and standards-driven infrastructure for secondary use of EHR data: the SHARPn project. *J Biomed Inform*. 2012;45(4):763-771.
45. Blumenthal D. Implementation of the federal health information technology initiative. *N EnglJ Med*. 2011;365(25):2426-2431.
46. Jusob FR, George C, Mapp G. Exploring the need for a suitable privacy framework for mHealth when managing chronic diseases. *J Reliab Intell Environ*. 2017;3(4):243-256.
47. McGraw D. Privacy and health information technology. *J Law Med Ethics*. 2009;37:121-149.
48. Avancha S, Baxi A, Kotz D. Privacy in mobile technology for personal healthcare. *ACM Comput Surv (CSUR)*. 2012;45(1):3.
49. Kotz D, Avancha S, Baxi A. A privacy framework for mobile health and home-care systems. In: Proceedings of the First ACM Workshop on Security and Privacy in Medical and Home-Care Systems; 2009; Chicago, IL.
50. Olson DR, Paladini M, Lober WB, Buckeridge DL. ISDS Distribute Working Group. Applying a new model for sharing population health data to national syndromic influenza surveillance: DiSTRIBuTE project proof of concept, 2006 to 2009. *PLOS Currents*. 2011;3:RRN1251.
51. Nyrén O, Stenbeck M, Grönberg H. The European Parliament proposal for the new EU general data protection regulation may severely restrict European epidemiological research. *Eur J Epidemiol*. 2014;29(4):227-230.
52. Muchagata J, Ferreira A. Translating GDPR into the mHealth practice. Paper presented at: 2018 International Carnahan Conference on Security Technology (ICCST); 2018; Montreal, Canada.
53. Doukas C, Maglogiannis I, Koufi V, Malamateniou F, Vassilacopoulos G. Enabling data protection through PKI encryption in IoT m-health devices. Paper presented at: 2012 IEEE 12th International Conference on Bioinformatics & Bioengineering (BIBE); 2012; Larnaca, Cyprus.
54. Prosch M. Protecting personal information using generally accepted privacy principles (GAPP) and continuous control monitoring to enhance corporate governance. *Int J Discl Gov*. 2008;5(2):153-166.
55. Vilpert S, Monod S, Ruedin HJ, et al. Differences in triage category, priority level and hospitalization rate between young-old and old-old patients visiting the emergency department. *BMC Health Serv Res*. 2018;18(1):456.
56. Kalid N, Zaidan AA, Zaidan BB, Salman OH, Hashim M, Muzammil H. Based real time remote health monitoring systems: a review on patients prioritization and related "big data" using body sensors information and communication technology. *J Med Syst*. 2018;42(2):30.
57. Kakria P, Tripathi NK, Kitipawang P. A real-time health monitoring system for remote cardiac patients using smartphone and wearable sensors. *Int J Telemed Appl*. 2015;2015.
58. Ciman M, Wac K. Individuals' stress assessment using human-smartphone interaction analysis. *IEEE Trans Affect Comput*. 2018;9(1):51-65.
59. Majumder S, Aghayi E, Noferesti M, et al. Smart homes for elderly healthcare—recent advances and research challenges. *Sensors*. 2017;17(11):2496.
60. Lloret J, Parra L, Taha M, Tomás J. An architecture and protocol for smart continuous eHealth monitoring using 5G. *Computer Networks*. 2017;129:340-351.
61. Simplicio MA, Iwaya LH, Barros BM, Carvalho TC, Näslund M. SecourHealth: a delay-tolerant security framework for mobile health data collection. *IEEE J Biomed Health Inform*. 2015;19(2):761-772.
62. Rughoobur P, Nagowah L. A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. Paper presented at: 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS); 2017; Dubai, UAE.
63. Butt SA, Jamal T. Study of black hole attack in AODV. *Proc Int J Future Gener Commun Netw*. 2017;10(9):37-48.
64. Ünsal E, Çebi Y. Denial of service attacks in WSN. Paper presented at: 1st International Symposium on Computing in Science & Engineering (ISCSE); 2013; Izmir, Turkey.
65. Karchowdhury S, Sen M. Survey on attacks on wireless body area network. *Int J Comput Intell IoT Forthcom*. https://ssrn.com/abstract=3358378. 2019.
66. Strielkina A, Kharchenko V, Uzun D. Availability models for healthcare IoT systems: classification and research considering attacks on vulnerabilities. Paper presented at: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT); 2018; Kiev, Ukraine.
67. Jamal T, Alam M, Umair MM. Detection and prevention against RTS attacks in wireless LANs. Paper presented at: 2017 International Conference on Communication, Computing and Digital Systems (C-CODE); 2017; Islamabad, Pakistan.
68. Al-Janabi S, Al-Shourbaji I, Shojafar M, Shamshirband S. Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications. *Egypt Inform J*. 2017;18(2):113-122.
69. Ma X, Wang Z, Zhou S, Wen H, Zhang Y. Intelligent healthcare systems assisted by data analytics and mobile computing. *Wirel Commun Mobile Comput*. 2018;2018:https://doi.org/10.1155/2018/3928080
70. Varshney U. A model for improving quality of decisions in mobile health. *Decis Support Syst*. 2014;62:66-77.
71. Iribarren SJ, Brown W III, Giguere R, et al. Scoping review and evaluation of SMS/text messaging platforms for mHealth projects or clinical interventions. *Int J Med Inform*. 2017;101:28-40.
72. Chaturvedi A, Lone FA. Analysis of big data security schemes for detection and prevention from intruder attacks in cloud computing. *Int J Comput Appl*. 2017;158(5).

73. Masud M, Hossain MS. Secure data-exchange protocol in a cloud-based collaborative health care environment. *Multimed Tools Appl*. 2018;77:11121-11135.
74. Martínez-Pérez B, De La Torre-Díez I, López-Coronado M. Privacy and security in mobile health apps: a review and recommendations. *J Med Syst*. 2015;39(1):181.
75. Srinivasan V, Stankovic J, Whitehouse K. A fingerprint and timing-based snooping attack on residential sensor systems. *ACM SIGBED Rev*. 2008;5(1):28.
76. Di Pietro R, Mancini LV, Soriente C, Spognardi A, Tsudik G. Catch me (if you can): data survival in unattended sensor networks. Paper presented at: 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom); 2008; Hong Kong.
77. Jamal T, Amaral P, Abbas K. Flow Table congestion in software defined networks. Paper presented at: The Twelfth International Conference on Digital Society and eGovernments; 2018; Rome Italy.
78. Jamal T and Haider Z, Denial of service attack in cooperative networks. 2018. arXiv preprint arXiv:1810.11070.
79. Azad MA, Bag S, Hao F. PrivBox: verifiable decentralized reputation system for online marketplaces. *Future Gener Comput Syst*. 2018;89:44-57.
80. Jamal T, Mendes P. Relay selection approaches for wireless cooperative networks. Paper presented at: 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications; 2010; Niagara Falls, Canada.
81. Azad MA, Bag S, Parkinson S, Hao F. TrustVote: privacy-preserving node ranking in vehicular networks. *IEEE Internet Things J*. 2018. Early access.