technologies

MDPI

Article

Vehicular Alarm System Using mHealth Data and Lightweight Security Algorithms

James Jin Kang [1,*], Sazia Parvin [2], Kiran Fahd [2] and Sitalakshmi Venkatraman [2]

[1] School of Information Technology, Deakin University, 221 Burwood Highway, Burwood, VIC 3125, Australia
[2] Department of IT, Melbourne Polytechnic, Preston, VIC 3072, Australia; saziaparvin@melbournepolytechnic.edu.au (S.P.); kiranfahd@melbournepolytechnic.edu.au (K.F.); sitavenkat@melbournepolytechnic.edu.au (S.V.)
* Correspondence: j.kang@deakin.edu.au; Tel.: +61-439-192-855

Received: 23 January 2019; Accepted: 14 February 2019; Published: 17 February 2019

Abstract: Among the various factors affecting long distance driving are the risks imposed by a driver's health, which could result in road accidents. Internet of Things (IoT) and mobile health (mHealth) technologies are increasingly being recognized for their role in monitoring various health parameters of such drivers. IoT devices such as wearable devices could be used efficiently in vehicles by professional long-distance drivers. However, the adoption of such technologies is limited by security and privacy issues. This paper proposes a novel vehicular alarm notification system by integrating mHealth data of the driver with vehicular data for improving vehicle safety. The purpose of the system is to minimize road accidents by integrating the emerging mHealth technologies with the vehicular information system (VIS) using wireless body area network sensors and devices in a secure and lightweight framework. An integrated secure system could facilitate adoptability to provide timely notifications of emergencies to drivers in order to avoid road accidents and take appropriate follow-up actions. Furthermore, the information gathered by the integrated system could assist health service providers to address the driver's root cause of potential health risks. The lightweight security framework adopted in this study is based on an efficient trust model that can improve the adoption of an mHealth integrated vehicular alarm notification system. Our contribution is to provide a real-time alarm notification service to avoid potential traffic accidents by monitoring the health status of long-distance drivers, achieved through incorporating an affordable and lightweight security system to secure health data transfer.

Keywords: mobile health (mHealth); mobile healthcare (mHealthcare) system; vehicular information system (VIS); wearable devices; emergency alarm system; road accidents; wireless body area network (WBAN); lightweight security; security algorithm

1. Introduction

Road traffic injuries have increased considerably and contribute to one of the main causes of death across all age groups worldwide, as reported by the World Health Organization (WHO) [1]. Long distance professional truck drivers have been identified as a high-risk group vulnerable to an increased risk of road accidents. A report claims that truck drivers have a life expectancy 10 to 15 years lower than the average male in the United States [2]. Due to a stressful workload with long periods of sedentary driving, health issues related to these drivers could result in road accidents.

With the advancement of Internet of Things (IoT) and mobile health (mHealth) technologies, intelligent wearable devices could help monitor the health parameters of long-distance drivers in real time. However, there is a lack of trust and health education in adopting mHealth solutions that can be integrated with vehicular information systems (VIS). Since mHealth network resources have

constraints of battery power, it is not practical to implement a full capacity security system. For example, an attacker may intervene the data transfer from the smartphone to the cloud as a man-in-the middle attack, and a time-based verification model to detect the MITM attacks [3] can be utilized to handle this situation. This paper is aimed to address these issues by applying an integrated approach to both the driver health monitoring system as well as the vehicle safety system using mHealth devices such as wearable devices utilizing a lightweight security framework. Figure 1 depicts the idea of integrating an mHealth network with a VIS that collects road and vehicular information to connect with smart devices, which are a medium to mHealth. It is intended to use the mHealth network to transfer data from sensors to a cloud server via a smartphone, which integrates the VIS into the mHealth network. Hence, the information flow and security measures are mainly focused on the mHealth application rather than the VIS, which transfers data to the smartphone.

The paper is structured as follows. Section 2 provides the background of the study and the gap in the literature. Section 3 proposes an integrated vehicular sensor design with the use of multiple sensor devices, including vehicular sensors, mHealth wearable sensors, and smart devices of the driver. Section 4 describes the application of such a wireless sensor design to integrate data from various sensors to activate the alarm in response to emergency situations that may arise. Section 5 proposes a lightweight security algorithm and Section 6 describes the simulation results. Lastly, the conclusions and direction of future research are described in Sections 7 and 8 respectively.

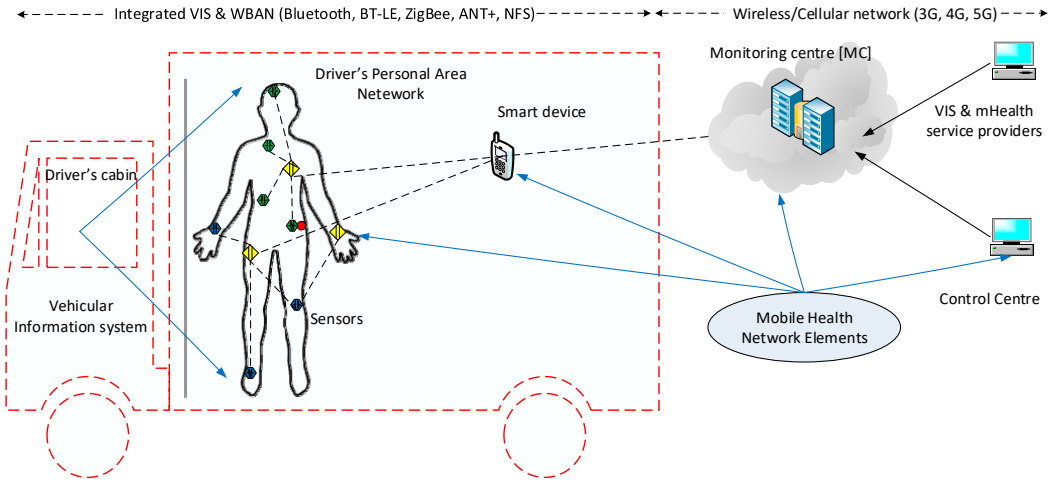

Figure 1. Integrated mHealth and vehicular information system.

2. Related Works

Many studies into vehicle road accidents have been conducted and have focused on the aspects surrounding the circumstance or accidental outcomes of the incident as opposed to addressing the viewpoint of safe vehicle operation. Many factors such as the driver's training, speed judgment, substance or alcohol consumption, hours driven, health, stress from driving, and other lifestyle factors have been studied in the literature. Of these, the driver's health, their speed judgment, and training are the main contributing factors in road accidents. Studies have shown that fatigue is a main contributing factor in two-thirds of accidents and is therefore of importance in safety considerations [4]. Regardless of a driver's level of training in vehicle operation, fatigue impairs speed judgment and is related to the driver's health.

In general, long distance drivers are referred to as over the road (OTR) drivers or long-haul truck drivers who drive for long periods of time with minimal resting periods, e.g., 5.5 h with 15 min of rest, 8 h for half an hour and 11 h with a 1-h break [5]. When driving, drivers are in a seated posture and are relatively sedentary with little movement as compared to being out of the driver's seat. Therefore, health-related data (HD) such as heart rate (HR), respiration rate (RR), blood pressure (BP),

body temperature (BT), Electrocardiology (ECG), Electroencephalogram (EEG), Electromyography (EMG), and Blood Oxygen are expected to have little variation over this long duration and may show consistency. In addition, there may be some unique patterns that emerge with little variance in the driver's health data, which can be implicated in the detection of emergency situations by integrating evolving and emerging technologies such as the mHealth network, personal health devices (PHD), biosensors, wearables, contactless sensing for vehicular applications, and emergency alarm systems.

Sensors are now evolving to accommodate requirements from health and vehicular applications with increased compactness, efficient computation, and data transmission capabilities, and overall increases in quality, accuracy, and cost affordability.

Wearable devices provide motion tracking and health-related data collection such as measuring human movements of falling, sitting, walking, and running to encourage users to move and exercise as well as monitoring the posture. These are used with smartphones, which transmit data to cloud servers or other networks like vehicular application systems.

PHD sensors collect health data measurements such as vital signs as well as chronic disease related devices, which may include implanted sensors and devices including pacemakers.

Sensors for vehicular applications have been used for fuel control, parking, safety, in-cabin convenience, speed monitoring, oxygen sensing, and engine monitoring. For example, a gas composition sensor along with humidity and temperature sensors checks air quality, monitors the air intake, and adjusts the heating, ventilation, and air conditioning (HVAC) system as required. However, health applications such as monitoring the driver's health data and notifying when there is an imminent risk of falling asleep have not been fully addressed. Vehicular applications can also detect early or real-time warnings for unexpected driving emergencies such as engine failure, jammed accelerator, shattered windscreen, tire blowouts, or animals causing a collision.

Due to the evolution of sensor devices and emerging technologies of vehicular and health informatics, it is feasible to sense data, collect, transfer, process, and determine an action in real-time. Furthermore, it is possible to send an alarm notification to the driver and their head office before a potential health condition deterioration occurs by analyzing health data against a prescribed health threshold index of the user [6].

Rapid technology advancement and innovation have resulted in a fast-growing global market that currently offers more than 1.5 million different mobile medical devices for self-monitoring personal health. To date, health device manufacturers have primarily provided products and services for consumers who are either fitness or health conscious, or who are chronically ill and require regular monitoring of their health status. In addition, due to the increasing aging population and overload of healthcare systems, there arises a need for ubiquitous healthcare services with mobile devices to facilitate remote monitoring and diagnosis through computer-based mobile healthcare (mHealthcare) systems for effectively managing a person's health. In addition, with the emergence of wearable devices and smart phones, the younger population is also motivated towards personalized health. Certain health conditions such as sleep apnea are often found with greater incidence in truck drivers resulting in excessive daytime sleepiness due to their sedentary lifestyle. However, mHealth technologies have not been explored in combination with vehicular technologies.

A survey to integrate the internet of things (IoT) network for healthcare technologies proposed a network architecture including various platforms and applications using the protocol stack of IPv6 and low-power wireless personal area networks (6LoWPAN) [7]. They also proposed an intelligent security model, which looks at security requirements, attacks taxonomies and threat models, and is important to minimize security risks in healthcare systems.

The Wireless body area network (WBAN) and Vehicular Ad hoc Networks (VANETs) can be combined to detect various human states such as drowsiness levels, intoxication, distractibility, and disorders of emotion using physiological information inputs [8]. This can be further extended to detect other states using sensed vitals data and other physiological statuses, as we proposed in this paper.

Security is critical in dealing with health data, and methods to provide optimal security measures for WBAN alongside the reduction of energy consumption in sensor devices have been comprehensively reviewed [9]. This paper further investigates and proposes the enhancement of security aspects when mHealth is integrated with VANETs.

Previous studies have been conducted to find the percentage of accidents with drivers who fall under the category of snorers, apneic or controls, or other non-health related factors such as the number of years of similar driving experience, age, and other demographic factors. Similarly, vehicular characteristics have also been studied to improve the design of vehicles for long distance driving. However, there is a lack of research in combining the data from both the driver's mHealth technologies as well as vehicular sensors, which can provide more scope to address the vehicular safety problems in addressing road accidents. This forms the prime motivation for this research to propose a novel vehicular sensor system that integrates data from the driver's mHealth wearable devices as well as sensors mounted in the vehicle to provide timely warnings and/or alarms for drivers to take necessary actions and safety precautions before the possibility of a potential road accident. When the driver is not responding to the alarm notification, or unable to take an action suggested, the proposed system will actuate or take appropriate actions, according to pre-defined procedures.

3. Proposed Integrated Vehicular Monitoring Sensor Design

mHealth Sensors can be distributed in the driver's home, placed on the body, or even implanted within the body. Human observation of physiological values has practical limitations and may not be suitable for certain measurements. On the other hand, sensors measure a person's health characteristics and convert them into raw digital data for monitoring, where the application plays an important role in collecting relevant and accurate data for analysis. mHealthcare systems offering a number of software solutions or smart device applications can provide a convenient and economical means for new modalities of self-administered patient care and well-being. Different devices related to a particular experiment to be performed on the patient are designed differently since they collect data in different forms and with varied procedures. Some monitoring systems make observations from multiple distributed sensors that are communicated over a network to a point of aggregation and analysis, or even to actuators for performing certain actions. Figure 2 shows the device interoperability standards required by mHealth devices for integrating with vehicular devices.

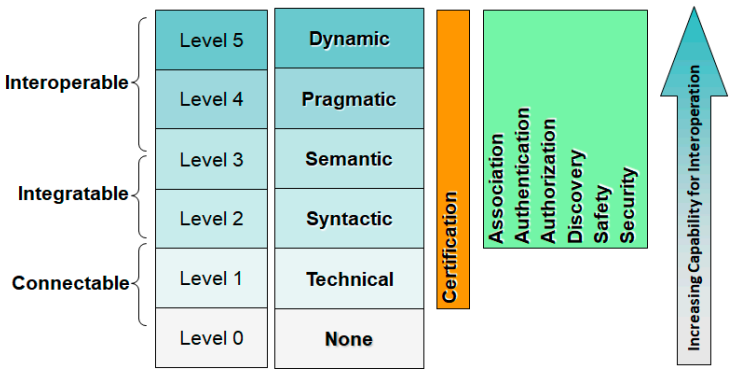

Figure 2. mHealth device interoperability standards framework.

While the purpose of vehicular application is different from mHealth, sensors, and monitoring devices can be used for both applications and can complement each other. PHD sensors can be used for invasive and non-invasive procedures in medical treatment. Invasive techniques involve incision or entering the body or the removal of tissue, while non-invasive techniques avoid penetrating the skin. Most PHD devices are non-invasive. However, some devices such as pacemakers are implanted inside the body. For the purpose of vehicular informatics, invasive interventions are considered as

ones involving physical contact with the skin while non-invasive interventions can operate remotely without touching the skin [10].

Some sensors equipped in most smartphones capture basic health data such as heart rate and motion, whereas dedicated PHD devices are used more for health applications. These devices can be worn on the body or attached as wearables in the form of a watch, clothing, glasses, or accessories to capture physical data from the body's movement. Contactless sensors are located in the cabin for remote sensing such as sound, visual sensing, motion, and temperature. Some of these sensors can have contact with the skin, e.g. handle, seat etc. from time to time and sense data accordingly.

Table 1 shows sensors and their functionalities that can be used in vehicular and mHealth applications. Smartphones are used to connect vehicular and mHealth networks integrated with various sensors and monitoring devices.

Table 1. Integrated sensor devices [11,12].

Vehicular	Personal Health	Smartphone
Distance	Pulse Oximeter	Accelerometer
Radar	Blood Pressure Monitor	Gyroscope
Camera vision	Thermometer	Compass
Ultrasonic	Weighing Scale	Heart Rate
Proximity	Glucose Meter	Barometer
Night vision	Body composition analyzer	Proximity
Speed	Peak flow	Pedometer
Angular rate	Cardiovascular	Magnetic field
Linear acceleration	Strength fitness equipment	Orientation
GPS	Independent living activity hub	Pressure
Gas composition	Medication monitor	Ambient light
Humidity	Basic ECG	Gravity
Temperature	Respiration rate monitor	Temperature
Navigation	INR (blood coagulation)	Global positioning system
Seated weight	Insulin pump	Microphone and camera

Figure 3 shows the sensor locations in the cabin that can connect to a smartphone, which processes and transfers this information along with physiological data obtained from mHealth devices to a cloud server. The accuracy of an integrated system depends upon how well the data in different formats sent from the mHealth wearable devices and mobile sensors are processed. The appropriate alerts are sent to the driver, the vehicle, and healthcare provider of the driver for future follow-ups with the driver's health as well as vehicle maintenance. Figure 4 provides an overview framework of an integrated vehicular alarm system, which is presented in the following section.

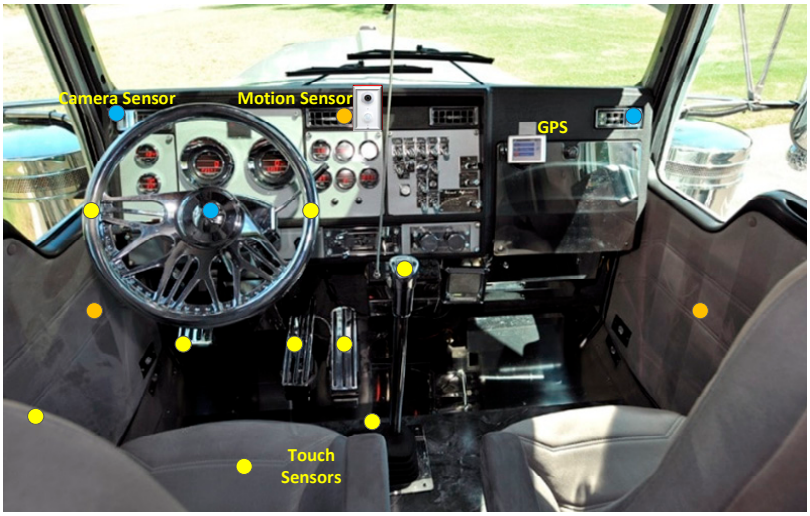

Figure 3. Sensor positions of vehicular information systems (Image adapted from Reference [13]).

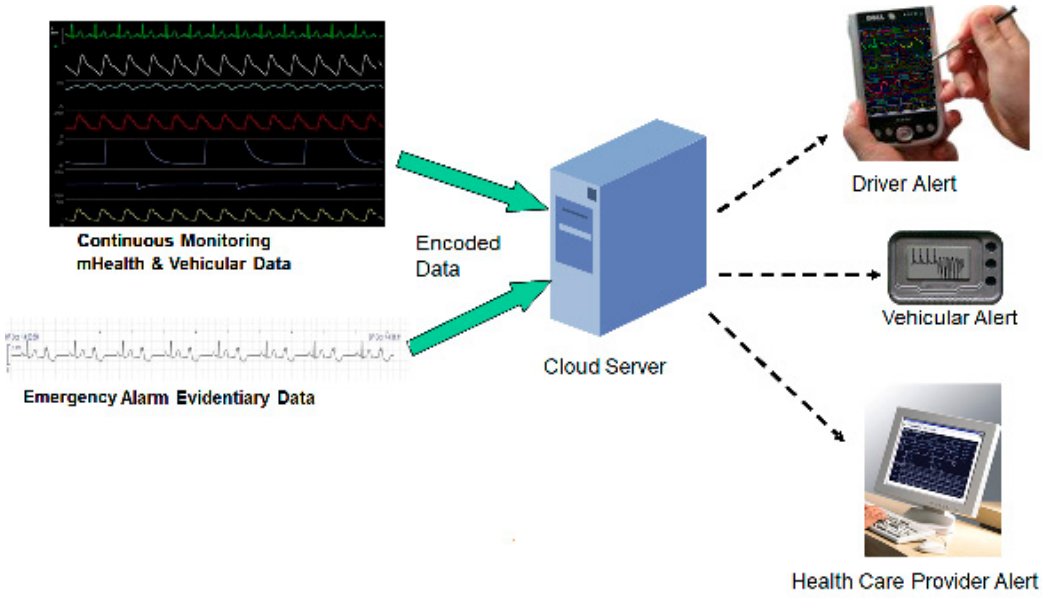

Figure 4. Integrated vehicular alarm system.

4. mHealth Integrated Vehicular Alarm System

There have been frequently reported cases of drivers that have collapsed behind the wheel including passenger vehicles, taxis, buses, lorries, and even train drivers caused by health issues such as a heart attack [14], sudden death [15], or other medical causes. Non-traumatic acute aortic dissection (AAD) occurring behind the wheel is one of the causes and include symptoms which include chest and/or back pain and syncope [16]. The consequences can result in catastrophic motor vehicle collisions with severe casualties.

Distracted driving such as reading or sending a text is another cause of fatal consequences. In 2016 alone, 3450 deaths and 391,000 people were injured in car crashes in 2015 that involved distraction in the USA. Distracted driving using a mobile phone caused 26% of all crashes [17,18].

Using an emergency alarming system [6], it is possible to send a notification to warn or actuate vehicular application to enforce the vehicle to safely stop and trigger help requests to various parties, including healthcare providers of the driver. To create alarm thresholds to determine an alarm situation, an inference system is required. We provide the factors to be considered for this inference system.

4.1. Inference Factors

1. Health data (HD) of a driver may settle and become consistent over the driving duration e.g., 10 min into driving, HD may show the same or similar patterns, i.e., a relationship with one another. After each hour, HD may show regular/typical patterns.
2. Drivers who travel the same paths/routes regularly such as truck drivers travelling between Melbourne and Sydney in Australia, which has a distance of approximately 900 km may show consistent HD patterns against time and space (geography).
3. Speed and road conditions (straight, curved, and undulated) or vehicle velocity may affect the HD and their patterns.
4. Room temperature may affect the HD.

Table 2 shows an example of an alarm threshold for vitals including BP (mmHg), HR (beats per minute), BT (Celsius), and RR (breaths per minute). In addition to the conditions of the vitals, other health data are used to determine the alarm, e.g., motion sensors for eye blinking (sleepiness levels), cellphone use (distraction), body postures, and more.

Table 2. Alarm threshold of sensed data suggested. These data are provided by a medical practitioner for a general purpose [19].

Data Types	Acceptable		Warning		Severe		Critical	
	Low	High	Low	High	Low	High	Low	High
BP	91	169	90	170	80	185	65	220
HR	51	139	50	140	40	180	32	210
BT	34.1	37.9	34	38	32	40	30	42
RR	11	29	10	30	8	36	6	45

There are two actions that can be taken in the case of an emergency, which includes alarm notification and actuation as described below.

4.2. Alarm Notification

If an alarm notification is triggered, it can be sent to the relevant parties with multiple phases of communication. This is categorized into two phases including the warning phase and alarm phase.

Warning phase—a warning notification is issued to alert the driver when distraction is detected. These could include movements such as checking a phone, deteriorating health conditions such as fatigue, and the cabin environment, e.g., faulty HVAC. The warnings can be raised by sound or visual cues e.g., playing a warning message from the mobile phone or vehicle or a flickering light.

Alarm phase—an alarm notification is issued to the driver as well as the relevant parties such as company headquarters and health service providers when the health condition of the driver is not suitable for driving. For example, the heart rate may be out of the threshold limits and a heart attack is envisioned. A paramedic may be dispatched to the site in case of emergency even though the driver is not in a position of sending for help as per pre-scheduled processes of an emergency situation. To avoid faulty alarms, there may be a confirmation message to the driver's smartphone requesting a reply via voice prompts and voice recognition with a timeout period, which will trigger the alarm if the reply is not received within the pre-set timer value. When the driver is not available to reply on the phone even though the truck is in a stopped or parked condition, they may be able to reply by voice recognition.

4.3. Actuation

In the event that an emergency arises, such as a heart attack or a seizure, the vehicular application system will force the vehicle to stop (and turn off the engine after a timeout period) as well as send an alarm to the relevant parties. If required, the system can also force the vehicle to be immobile to avoid a dangerous situation until the situation has been rectified. Lighting or sound cues may be used to attract attention around the vehicle so that others can check on the driver. A monitoring camera may be turned on to record the situation and transfer to the relevant parties along with the mHealth system, which will capture the health data and transfer them to the monitoring center. Activity recognition (AR) sensors when used will help find the posture of the driver.

4.4. Emergency Situation Determination

The Emergency Situation Determination is required to determine emergency situations when it occurs, which can be caused by various situations such as deteriorated health conditions, distractions, and unexpected changes in the weather or road conditions. Tuokko et al. [20] found that health-related symptoms are related to difficulties of driving. They found that functions related to both the spine (42%) and lower body (29%) were among the most commonly reported symptoms and resulted in difficulties of driving function involving these parts of the body. This result makes sense since long distance drivers maintain the same posture for the upper body, which affects the spine as well as the

lower body when sitting. When sensors recognize a health situation or distraction, the previously mentioned actions will be taken such as sending warnings, alarm notification, and/or an actuation.

A comprehensive set of health-related symptoms need to be included in the HD of the inference system. Some of the commonly used health related symptoms are: musculoskeletal, cardio/pulmonary, neurological, endocrine, visual, sleeping disorders, upper/lower body discomfort, central nervous system, heart attack, sudden collapse, and unconsciousness.

In addition to health-related symptoms, other factors that could lead to an accident include distractions, which should be avoided. Some of the possible distractions are: talking, texting, handling a GPS device, adjusting music and controls, not looking at the road, and zoning out.

The data collected using our proposed mHealth integrated vehicular system is distributed over various servers and networks in the cloud. In such an interdisciplinary domain covering healthcare, sensor technologies, vehicles, and road traffic, data privacy is of the utmost importance and laws in different countries regulate data privacy. To address these privacy and security issues, data must be tagged to the right driver and encrypted, authenticated, and made accessible to the authorized people. We present a novel and trust-based security framework that could be applied to our proposed mHealth integrated vehicular notification system.

5. Security Algorithms with Lightweight Security

Security is defined as the techniques and procedures required to prevent unauthorized access to the information.

Previous studies have been conducted regarding research in general issues linked to mHealth security and privacy. The authors in Reference [21] proposed several security and privacy recommendations in terms of a technical perspective for mHealth developers and, as a result, nine aspects of security are considered, which are outlined below.

- Access control—Mechanisms that help users ought to be able to enable or deny access to patient-centered data at any moment.
- Authentication—Authentication allows users to use data/mechanisms with a unique ID and password (or multi-factor authentication) so that no unauthenticated access can occur in the system. Passwords should reach appropriate levels of security.
- Security and confidentiality—Proper use of encryption mechanisms with appropriate parameter configurations (i.e., key size) so that confidentiality of message transmission will be guaranteed.
- Integrity—Secure and privacy-aware data collection through usage of message authentication codes and digital signatures in Mobile Health Systems.
- Inform patients—Confirmation of privacy policy to users before collection of data that informs about the user rights and specifies the purposes of data collection and processing.
- Data transfer—Transferring of data among entities through the use of secure communication channels (e.g., TLS, VPNs) and inform users about data transfers.
- Data retention—Informing users about their retention policy. Availability of the data should be allowed only for the necessary time in order to accomplish the initial purpose. User should be notified when data is deleted and be able to check the confirmation of data deletion.
- Body Area Network communication—Establishing secure communication channels among devices based on the security mechanisms for authentication and key distribution among sensors and smart-phones.
- Breach notification—Competent authorities and users should be notified in case of data breaches. Entities should help users in order to relieve the consequences and restore possible damages.

All data must be properly encrypted before transmission to/from the server in order to protect in-transit information in mHealth networks. In addition, the protection mechanisms verify whether the information received came from an authenticated user and prevent unauthorized entities from

injecting data into the system's database. However, any conventional mechanisms for establishing secure connections (e.g., TLS/SSL) may not be appropriate for mHealth data delivery because there is a difference in communication infrastructure between heterogeneous networks and WBAN devices, which have limited resources such as battery and computational power. The complexity arises because data temporarily stored in the device needs to be encrypted and, therefore, adds additional overhead from providing an extra security layer. Hence, the aim is to provide a solution that can be independent of secure communication tunnels for data delivery, but also ensures the data that travels between sensors and the mobile device in mHealth networks.

We propose a trust oriented digital signature-based authentication scheme for secure communication so that nodes in mHealth networks possess all the features of public key encryption. It can also provide several technical advantages such as a less complicated key management system to provide a lightweight security mechanism as well as easily detecting unwanted accidental asynchrony that occurs in nodes based on the justification of trust values.

5.1. System Topology

The security framework is proposed in Figure 5 where the vehicle information system is coming from different sensors positioned at different locations in the vehicle, as depicted in Figure 3. The proposed architecture shows that the different sensors located at different positions in the vehicle will be connected through a smart phone (or other devices) and will transfer the collected information from mHealth devices to the cloud network. However, unauthorized/compromised entities (intruders) can inject modified information into the mHealth system's message to compromise the whole network's activity. To avoid such problems, the sensors' identity or transmitted messages should be checked to ensure that it is coming from authenticated users. Hence, we propose a lightweight secure mechanism so that only authenticated data will be transmitted. We propose to implement the lightweight security framework for mHealth networks. In our system architecture, there are two areas including the wireless cognitive radio network (WCRN) and the vehicle information system. The security mechanism is applied in the WCRN only. In this network, there are three entities, which are outlined below.

1. Certificate Authority (CA)
2. Primary User Base Station (PUBS) (Primary mHealth Base Station)
3. Primary and Secondary Users (mHealth nodes)

Cognitive sensor nodes in the WCRN can use the radio more efficiently for transmission in the wireless network. It allows us to construct a network based on the available radio with the combination of cognitive radio nodes and improves the speed and availability of channels for wireless networks. The benefit of using a cognitive radio is its efficient utilization of the spectrum such that the radio can always be available for secondary users when primary users are not using the radio bandwidth. The two types of users include primary users and secondary users. Primary users are those who access the radio network at a high demand, such as ECG sensors in the vehicle information system, which transmit heart-related information frequently. These primary sensors need to send the information with priority. Sensors that do not need to send information urgently such as motion sensors will be considered as secondary users. Depending on the users' radio usage priority, there will be two networks: primary user network (PUN) and secondary user network (SUN) in the proposed architecture. However, each user's identity or transmitted message from the user will be checked to verify the source as an authenticated primary or secondary user. There are three advantages of using cognitive radio (CR) architecture in mHealth networks, which are discussed below.

- A CR automatically senses a spectrum hole and requires *trust* from the existing system (i.e., primary system) and regulator to dynamically access the spectrum for information transmission, without creating interference to the primary station (PS).
- A CR may want to leverage another existing cognitive radio to route its packets, even though another CR is not the targeted recipient terminal. It requires *trust* from another CR.

- A CR can leverage the PS to forward its packets to realize the goal of packet switching networks. It requires *trust* from the PS, not only at a network level, but also in the service provider level.

Considering these advantages of a CRN trust-based authentication infrastructure, the following are included in the mHealth network architecture for secure communication.

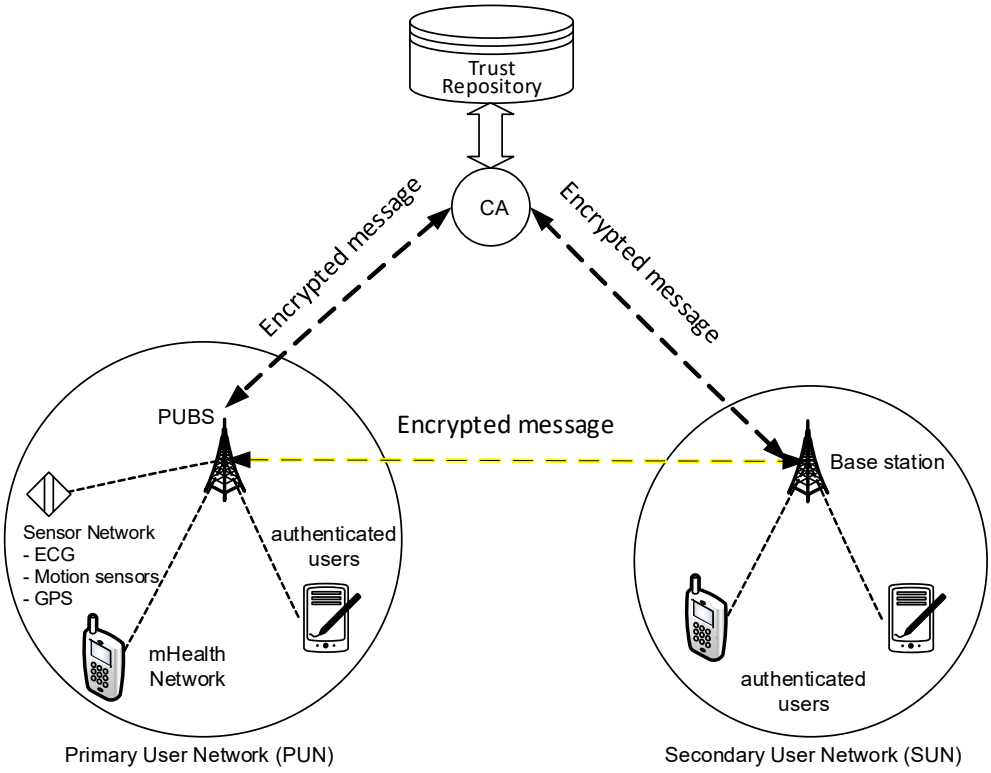

Figure 5. Security system architecture. Adapted from Reference [22].

5.1.1. Certification Authority

In our architecture, a certification authority is an entity that is connected to the PUBS and secondary user base station (SUBS). The CA will act as a trust repository for every node in the mHealth network for trust calculation, and it issues certificates for all members. Both SUBS and PUBS have full trust on CA.

5.1.2. Primary User Base Station

The base station is defined as the central point of contact between the two different types of users, which are primary and secondary mHealth nodes. Primary users (PU) are connected to the PUBS whereas Secondary users (SU) are connected to the SUBS. If there is any change of a member node's public key, the base station is informed. Then the base station sends the new public key to CA and the CA securely registers the new public key.

5.1.3. Primary and Secondary Users (mHealth Nodes)

Both primary and secondary nodes are connected to their respective base stations. The secondary user uses a sensing algorithm to detect the presence of a primary user's transmission. If the transmission is free, it sends an encrypted message to SUBS. After the message has been decoded and detached from the signature, SUBS sends the SU request message to the PUBS through an established control channel. This flow is depicted in Figure 6.

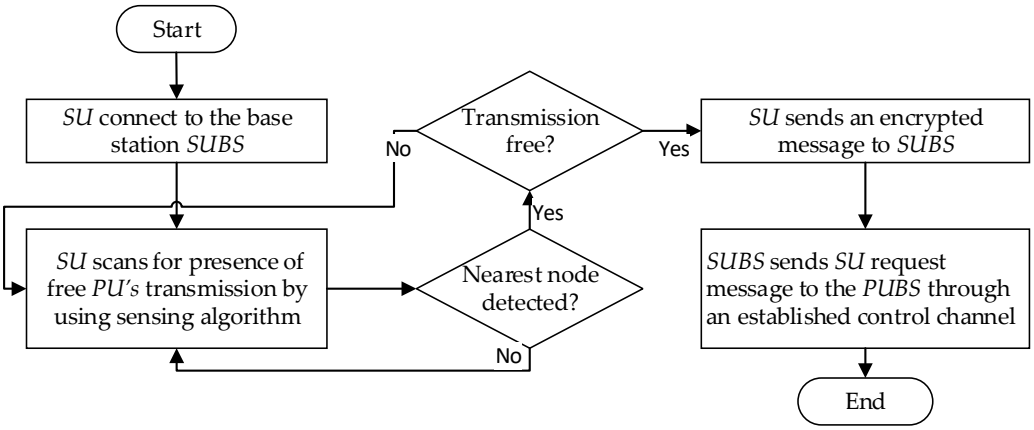

Figure 6. Flow of trust calculation for member nodes.

In this system architecture, member nodes are initially registered as authenticated users using the digital signature to their respective network. Nodes communicate with each other and the base stations using encryption techniques to ensure secure communication in CRNs.

5.2. Trust Calculation for Member Nodes in mHealth Networks

The basic trust calculation methods are described for both networks in this section. Both SUBS and PUBS calculate trust for their member nodes depending on past behaviors. We give an overview of the trust measurement approach below.

Direct trust calculation: The base station computes the trust value of a member node in its mHealth network if a past interaction experience exists between the member node itself. This is denoted by TDirecttrust.

Indirect trust calculation: Indirect trust calculation is used to establish the trust value of the member node by the base station in case of the absence of any direct past interaction experience between the base station and member node. The base station will send a request to other member nodes and seek assistance to send recommendations to it about the requesting node. Upon receiving the recommendations from all member nodes, the trust value of the candidate is computed. The TIndirecttrust denotes the computed trust value.

Integrated trust calculation: The base station combines both the direct and indirect trust values in order to compute the trust value of the candidate node in situations where both exist, according to the preferences of the nodes. This is done by the integrated trust calculation method and the TIntegtrust denoted the computed trust value.

Both base stations keep storage of these calculated trust values for their member nodes and send the values to CA. Thus, the CA will have a trust repository for keeping the trust record of every member node in the mHealth network. In this study, we used a digital signature to ensure authenticity of each mHealth member node so that any unauthorized user cannot have access to the network communication. We also use the trust value to check the requesting member node's previous behavior.

5.3. Authentication Procedure

We use the RSA algorithm to generate the asymmetric keys for the authentication process. We assume that there are m numbers of SUs in the mHealth network. ID_i denotes the unique identity of SU_i.

Request and Acknowledgement denote the packet request and the packet response, respectively. $\text{Sign}_A()$ denotes signature mechanism of user A, Cert_A denotes the certificate of user A, and $P_{PK}(.)$ denotes the encrypting process using the public key (PK).

The authentication procedure is shown in Figure 7 for each step. Figure 8 illustrates the workflow of the working procedure using a digital signature to use PU's free spectrum.

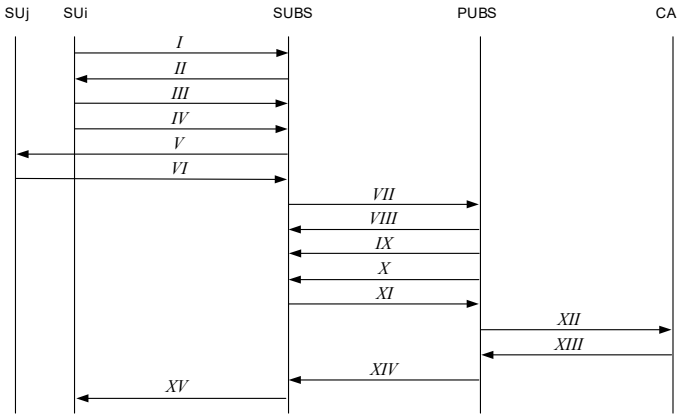

Figure 7. Information flow of the authentication procedure with each step.

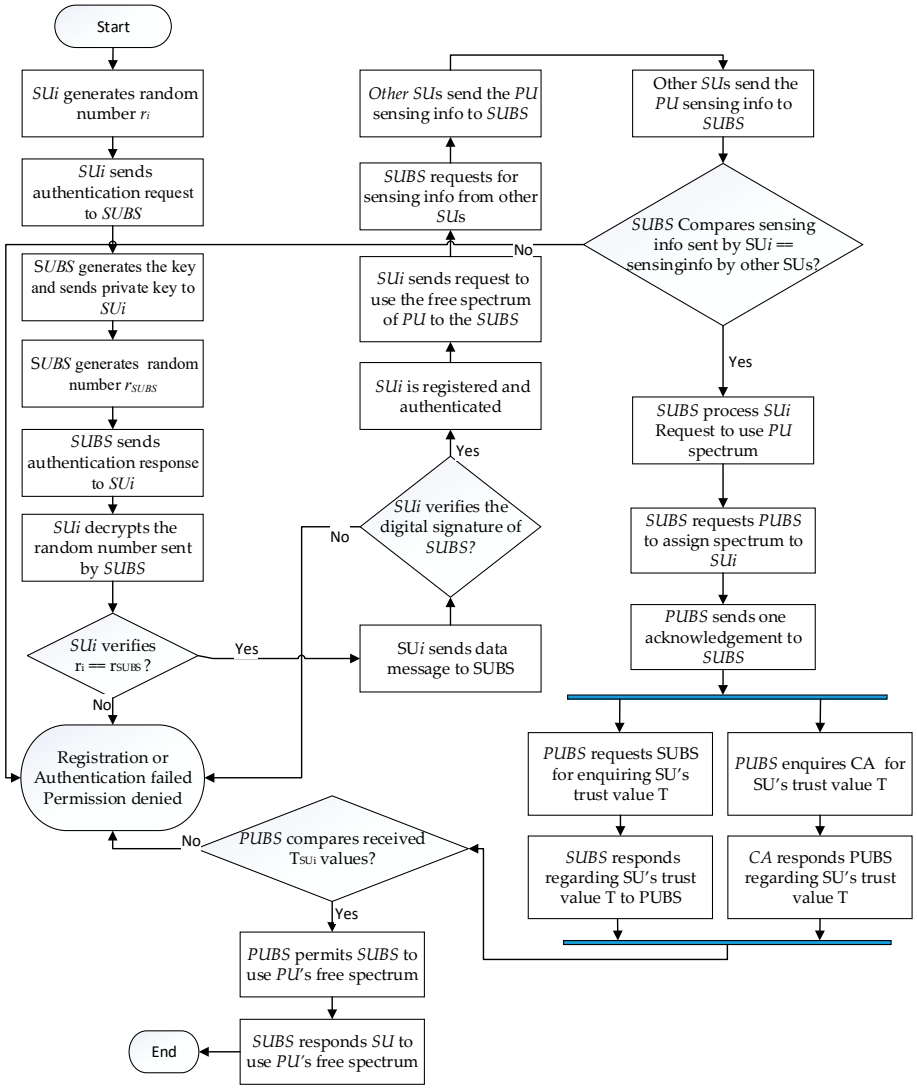

Figure 8. Workflow of the procedure with a digital signature.

In this subsection, we present the steps of the authentication procedure as follows.

Step 1: SU_i generates a random number r_i by pseudo random generator and sends the request packet to SUBS, $I = (Request,\ ID_i, r_i)$.

Step 2: SUBS generates the public-private key (pu_i, pr_i) by the RSA algorithm and sends the private key (pr_i) to SU_i by a secure channel. SUBS generate a random number r_{SUBS} by using a pseudo random generator. SUBS then sends the respond packet to SU_i, $II = P_{pr_i}(\ ID_i, ID_{SUBS},\ r_i,\ r_{SUBS})$.

Step 3: SU_i decrypts the data packet by using SUBS's public key pu_i to retrieve the random number r_{SUBS}. SU_i verifies whether the generated random number is similar to the received random number or not. If both numbers are identical, SU_i sends the data packet to SUBS. $\mathrm{SU_i}$

$$III = (Cert_{SUi},\ r_i,\ ID_{SUBS},\ Sign_{SUi}(r_i,\ \ r_{SUBS},\ ID_{SUBS}))$$

SUBS verifies the digital signature of SU_i. If it is a valid signature, then SU_i is registered and authenticated to communicate with SUBS and use PU's spectrum.

Step 4: SU_i sends requests to use the free spectrum of PU to the SUBS.

$$IV = \left(Request,\ \ sensing_{info},\ ID_i, r_i\right)$$

Step 5: SUBS sends requests to other secondary users SU_j to send sensing information $sensing_{info}$ about the primary users.

$$V = P_{pr_i}\ (ID_{SUBS},\ r_{SUBS,}\ ID_j)$$

Step 6: SU_j decrypts the data packet by using SUBS's public key (pu_i) to retrieve the random number r_{SUBS}. SU_j sends the data packet to SUBS.

$$VI = \left(Cert_{SUj},\ r_j,\ ID_{SUBS},\ Sign_{SUj}\left(r_j,\ \ r_{SUBS},\ ID_{SUBS},\ sensing_{info}\right)\right)$$

SUBS verifies both sensing information received from SU_j and SU_i. If both are identical, then it will process SU_i's spectrum request.

Step 7: SUBS send requests to PUBS for assigning spectrum to SU_i.

$$VII = (Request,\ ID_{SUBS},\ ID_i,\ r_{SUBS})$$

Step 8: PUBS send one acknowledgement to SUBS.

$$VIII = (\mathrm{ACK},\ \ ID_{PUBS},\ r_{PUBS})$$

Step 9: PUBS send the data packet to SUBS for enquiring SU_i's trust value $\mathrm{T_{Sui}}$.

$$IX = P_{pu_j}(ID_{PUBS}, ID_{SUBS}, \mathrm{T_{Sui}},\ r_{SUBS},\ r_{PUBS}).$$

Step 10: PUBS generates the public-private key (pr_j, pu_j) by the RSA algorithm and sends the public key (pu_j) to SUBS by a secure channel.

$$X = P_{pu_j}(ID_{PUBS}, ID_{SUBS}, \mathrm{T_{Sui}},\ r_{SUBS},\ r_{PUBS}).$$

Step 11: SUBS sends the respond packet regarding $\mathrm{T_{Sui}}$ to PUBS.

$$XI = (Cert_{SUBS},\ r_{SUBS},\ ID_{PUBS},\ Sign_{SUBS}(r_{SUBS},\ \ r_{PUBS},\ \mathrm{T_{Sui}}, ID_{PUBS}))$$

Step 12: PUBS also sends one data packet to CA for enquiring the SU_i' trust value $\mathrm{T_{Sui}}$.

$$XII = \left(Cert_{PUBS},\ r_{PUBS},\ ID_{CA},\ P_{pu_j}(\mathrm{T_{Sui}})\right)$$

Step 13: CA generates the public-private key ($\mathrm{pr_{CA}}$, $\mathrm{pu_{CA}}$) by the RSA algorithm and sends the public key ($\mathrm{pu_{CA}}$) to PUBS by a secure channel. CA sends a response packet to PUBS for informing SU_i's trust value $\mathrm{T_{Sui}}$ encrypting by its private key.

$$XIII = P_{\mathrm{pr_{CA}}}(ID_{SUBS},\ ID_{CA},\ \mathrm{T_{Sui}},\ r_{CA},\ r_{PUBS}).$$

PUBS decrypts the message from CA using CA's public key and receives SU_i's trust value $\mathrm{T_{Sui}}$ from both SUBS and CA. It checks the trust value for integrity purposes and, if it is identical and passes a certain threshold value, it sends a digitally signed message to give permission to the requesting SU to use the PU's free spectrum.

Step 14: PUBS sends a response packet to SUBS for the permission to user PU's free spectrum.

$$XIV = (Cert_{PUBS},\ r_{PUBS},\ ID_{SUBS},\ Sign_{PUBS}(r_{SUBS},\ r_{PUBS},\ ID_{SUBS}))$$

Step 15: After receiving permission from PUBS, SUBS sends one response packet to the requesting SU_i to allow the use of PU's free spectrum.

$$XV = \left(P_{pr_i}(ID_{SUBS}, ID_i,\ r_{SUBS},\ r_i)\right)$$

5.4. Algorithm Development for the Authentication Procedure

The RSA algorithm employs a key pair consisting of a public key and a private key to generate the asymmetric keys for the authentication process that was described in Section 5.3. All messages will be encrypted using the public key and all encrypted messages will be decrypted using the associated private key.

The algorithms will use the java security, *java.security*. Additional functions such as *java.security.Key*, *java.security.KeyPair*, *java.security.KeyPairGenerator*, and *java.security.Security* contain the methods to generate keys and key pairs (Algorithm 1), to encrypt (Algorithm 2), and to decrypt the data by the generated key pair (Algorithm 3).

Algorithm 1. Generate key pairs

```
function generateKeyPair ( )
//The following sets the RSA KeyPairGenerator instance. It initializes with a bit size of 256 bits.
   SecureRandom random = new SecureRandom( )
   KeyPairGenerator generator = KeyPairGenerator.getInstance("RSA")
   KeyPair pair = generator.
   generateKeyPair( ) generator.initialize(256, random)
   return pair
end function
```

Algorithm 2. Encrypt message

```
function encryptMessage (KeyPair pair, byte[ ] message)
//It encrypts the original message by using the public key
   Key pubKey = pair.getPublic( )
   Cipher cipherText = Cipher.getInstance("RSA")
   cipherText.init(Cipher.ENCRYPT_MODE, pubKey)
   byte[ ]encryptedCipher = cipherText.doFinal(message.getBytes( ))
   return encryptedCipher
end function
```

Algorithm 3. Decrypt message

```
function decryptMessage (Key privKey, byte[ ] demessage)
//It decrypts the cipher text and returns the original message
    Cipher deCipher = Cipher.getInstance("RSA")
    deCipher.init(Cipher.DECRYPT_MODE, privKey)
    byte[ ] originalMessage = cipher.doFinal(demessage)
    return new String(originalMessage)
end function
```

The public-private key pair is also used to generate and verify the digital signature (Algorithm 4). The data is signed by using the private key, which can be verified by the public key for data integrity and authenticity. *java.security.Signature* contains the methods to sign the data and verify the signature of the received data.

Algorithm 4. Verify digital certificate

```
function verifySignature(byte[ ] dataText, Key pubKey, byte[ ] signature)
//the following verifies the digital certificate by using RSA and returns a true or false result
    Signature sig = Signature.getInstance("SHA256withRSA");
    sig.initVerify(pubKey);
    sig.update(dataText);
    boolean result= sig.verify(signature);
    return result
end function
```

Figure 9 illustrates the process of authentication for a specific secondary node with unique identity of *SUi* in *m* numbers of SUs in the mHealth network.

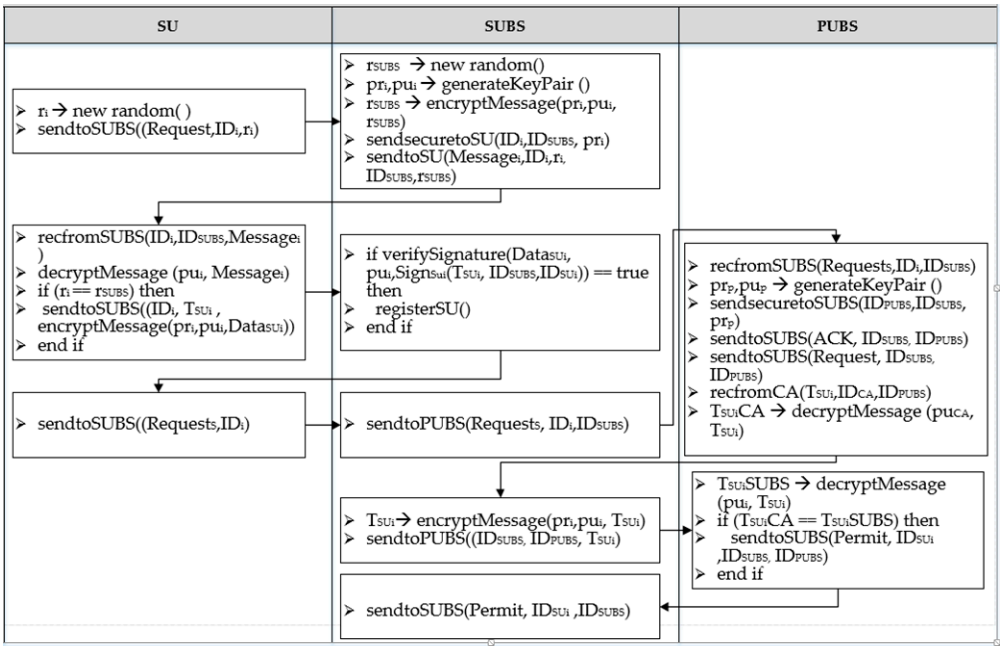

Figure 9. Authentication process.

6. Simulation Results

The proposed scheme was simulated using a network simulator (ns-2). Two networks (primary network and secondary network) were set up in the mHealth network to transmit a short message.

The first test involved transmitting the message without any authentication process, while the second test involved transmitting the same message using an authentication process. The message was transmitted between two entities in the mHealth network known as PUBS and SUBS. Trust value was not considered to reduce complexity.

The snapshots of the ns-2 environment in Figure 10 presents the required time against the packet size of the transmitted message without an authentication process and with the authentication process from SUBS to PUBS in the mHealth network. It is observed that message transmission with authentication requires a longer duration of time in comparison to transmitting without the authentication process. However, it is more secure. Therefore, it increases the difficulty for adversaries to obtain the private key from a known public key and to slow down the network performance.

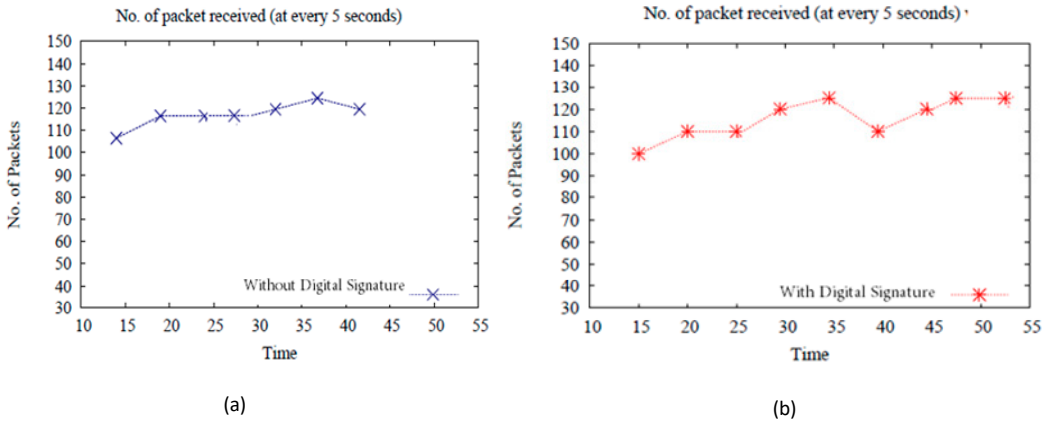

Figure 10. Message transfer without (**a**) and with (**b**) digital signature.

7. Conclusions

This paper contributed an idea of an integrated mHealth and VIS to predict and notify alarms for long-distance drivers based on real-time parameters of the driver's health condition as well as the road circumstances. We proposed a trust-based security framework to sense and securely transmit the driver's health data as well as change vehicular and road conditions via a centralized monitoring center using a novel integration model. Apart from providing alarms in advance to the driver, this system aims to facilitate other relevant parties such as healthcare providers and road assistance services to undertake an appropriate action based on the real-time intelligently integrated computational model. This novel proposal has the advantage of a continuous monitoring inference system for mHealth wearable devices and IoT vehicular sensors with a trust-based authentication model to predict and send alarms accurately. The health care providers, road transportation, and other relevant parties could make use of such a safe and intelligent alarm system to support the driver and the vehicle, without causing any inconvenience to the road traffic system. This paper considered the technologies, interfacing standards, privacy and security aspects in the design, and presented future works of the system development. Overall, this work is the first of its kind in proposing a vehicle safety alarm system designed to combine mHealth data of the driver and vehicular sensor data using a lightweight security framework. With this modest step forward, our work generates research interest in this multi-disciplinary problem of integrating mHealth and VIS for improving road safety.

8. Future Works

Future work of this ongoing research would involve a prototype development of our proposed design model of the mHealth integrated vehicular alarm system using the trust-based authentication and security framework. Some of the key activities envisioned to be undertaken are described below.

Software and algorithm development—in addition to the security algorithms proposed, further defining of the thresholds of each personalized health data to determine the abnormality levels is

required. These threshold levels will be determined in consultation with the health experts and physicians of the user (driver). For example, the normal resting heart rate of 60 to 100 beats per minute may not be relevant to a particular user due to variables such as medications. In addition, the HR may change in different situations such as the user's activity level, fitness level, environmental factors such as air temperature, body posture (e.g., standing, sitting, lying down), emotional state, body size, and medications [23]. Robust software algorithms require development and verification to handle these personalized data within the inference engine of the integrated alarm system. To secure health data exchange between sensor nodes and the cloud servers, we propose to use trusted time-servers to detect man-in-the-middle attacks [3]. This can be integrated with the lightweight security algorithms this paper proposed for real-time detection of attacks and an emergency alarm system for physiological sensors [6].

Database collection/creation/management/queries—when sensed data from IoT devices are sent to the cloud server, data wrangling and transparency of the data should be verified. How much of the data can be trustworthy? What is the validity of the data received and the maximum expiry? When further data are required, how does the system automatically authenticate, perform a query, and collect the data? All these questions need to be addressed before accepting the data from sensor devices within the trust-based security framework including data compliance between mHealth and integrated vehicular networks.

Data analysis/visualization/presentation using machine learning and statistical approaches—data visualization facilitates quicker inferencing and decision-making for providing timely and accurate alarms to the driver and the relevant parties. Applying and testing appropriate machine learning algorithms is crucial to avoid false alarms in order to enhance adoptability. The evaluation and benchmarking of the system would involve measuring how accurate the alarm notification is triggered and validated in different circumstances.

Mobile app development—as smartphones will be used to connect the two networks (mHealth and VIS) for end-to-end connections, mobile app development should include modules for the integration of mHealthcare systems with vehicular applications. Existing interfaces such as WBAN for mHealth and Vehicular Ad-hoc Networks would be appropriate to establish communication among these. However, other networks such as IoT or Satellite networks would also be required to interface via mobile apps. Standardization of the interfaces as well as privacy and security protocols adhering to the proposed security framework will be applied, checked, and verified for mobile app development and its interfaces.

Management support—since the proposed system handles the driver's health data, appropriate ethics approvals will be sought within the existing healthcare system of privacy and security. Different government agencies and states may adopt different policies and practices and it is therefore important to seek approval from all relevant parties to conduct the research.

Author Contributions: J.J.K. conceived and reviewed related works, designed the solution and application, wrote the original draft, and reviewed and edited the draft. S.P. wrote security frameworks. K.F. wrote algorithms. S.V. supervised the overall quality of the article.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. World Health Organization. Number of Road Traffic Deaths. Available online: http://www.who.int/gho/road_safety/mortality/traffic_deaths_number/en/ (accessed on 29 August 2018).
2. Roemer, N. Trucking Insurance Industry Journal, The Roemer Report: Trucker Life Expectancy 10–15 Years Less Than Average American Male. Available online: https://www.prweb.com/releases/2008/03/prweb762664.htm (accessed on 16 January 2019).
3. Kang, J.J.; Fahd, K.; Venkatraman, S. Trusted Time-Based Verification Model for Automatic Man-in-the-Middle Attack Detection in Cybersecurity. *Cryptography* **2018**, *2*, 38. [CrossRef]

4. Bates L., J.; Davey, J.; Watson, B.; King, M.J.; Armstrong, K. Factors Contributing to Crashes among Young Drivers. *Sultan Qaboos Univ. Med. J.* **2014**, *14*, e297–e305. [PubMed]
5. National Transport Commission (Road Transport Legislation—Driving Hours Regulations) Regulations 2006. Available online: https://www.legislation.gov.au/Details/F2006L00250 (accessed on 7 August 2018).
6. Kang, J.; Larkin, H. Application of an emergency alarm system for physiological sensors utilizing smart devices. *Technologies* **2017**, *5*, 26. [CrossRef]
7. Islam, S.M.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]
8. Reyes-Muñoz, A.; Domingo, M.; López-Trinidad, M.; Delgado, J. Integration of Body Sensor Networks and Vehicular Ad-hoc Networks for Traffic Safety. *Sensors* **2016**, *16*, 107. [CrossRef] [PubMed]
9. Kang, J.J.; Adibi, S. A Review of Security Protocols in mHealth Wireless Body Area Networks (WBAN). In Proceedings of the International Conference on Future Network Systems and Security, Paris, France, 11–13 June 2015; pp. 61–83.
10. Adibi, S.; Wickramasinghe, N. Contactless Biomedical Sensing for Vehicular Applications. In Proceedings of the First IEEE Healthcare Technology Conference: Translational Engineering in Health & Medicine, Houston, TX, USA, 7–9 November 2012.
11. IEEE. *Health Informatics—Personal health Device Communication—Part 20601: Application Profile—Optimized Exchange Protocol*; IEEE Std 11073-20601-2014 (Revision of ISO/IEEE 11073-20601:2010); IEEE: Piscataway, NJ, USA, 2014; pp. 1–253.
12. Abdelhamid, S.; Hassanein, H.S.; Takahara, G. Vehicle as a Mobile Sensor. *Procedia Comput. Sci.* **2014**, *34*, 286–295. [CrossRef]
13. Farber, J. Top 6 Best Driving Seat Cushions for OTR Truckers, Cars, RVs. Available online: https://www.painawaydevices.com/best-car-seat-cushions/ (accessed on 5 August 2018).
14. Defino, T. Heart Problems Prompt Fainting Behind the Wheel. Available online: https://www.webmd.com/heart-disease/news/20000517/heart-problems-linked-to-fainting-behind-wheel#1 (accessed on 7 August 2018).
15. Regan, T. Passenger Takes Wheel of Transit Bus after Driver Collapses, Later Dies. Available online: https://www.ajc.com/news/local/passenger-takes-wheel-transit-bus-after-driver-collapses-later-dies/rLsbZ0LkrB4Z1Vd3r5KDVN/ (accessed on 7 August 2018).
16. Yoshizaki, T.; Kimura, N.; Hirano, T.; Yamaguchi, A.; Adachi, H. Acute Aortic Dissection Occurring "Behind The Wheel", Report of 11 Cases. *Ann. Vasc. Dis.* **2016**, *9*, 205–208. [CrossRef] [PubMed]
17. Engelberg, J.K.; Hill, L.L.; Rybar, J.; Styer, T. Distracted driving behaviors related to cell phone use among middle-aged adults. *J. Transp. Health* **2015**, *2*, 434–440. [CrossRef]
18. National Highway Traffic Safety Administration (NHTSA). Distracted Driving. Available online: https://www.nhtsa.gov/risky-driving/distracted-driving (accessed on 7 August 2018).
19. Kang, J.J. An Inference System Framework for Personal Sensor Devices in Mobile Health and Internet of Things Networks. Ph.D. Thesis, Deakin University, Burwood, Australia, 2017.
20. Tuokko, H.A.; Rhodes, R.E.; Dean, R. Health conditions, health symptoms and driving difficulties in older adults. *Age Ageing* **2007**, *36*, 389–394. [CrossRef] [PubMed]
21. 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*, 181. [CrossRef] [PubMed]
22. Parvin, S.; Hussain, F.K.; Hussain, O.K. Digital signature-based authentication framework in cognitive radio networks. In Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia (MoMM '12), Bali, Indonesia, 3–5 December 2012; pp. 136–142.
23. Laskowski, E.R. What's a Normal Resting Heart Rate? Available online: https://www.mayoclinic.org/healthy-lifestyle/fitness/expert-answers/heart-rate/faq-20057979 (accessed on 29 August 2018).