IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 13, 2019, accepted June 1, 2019, date of publication June 5, 2019, date of current version June 24, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920850

Fingerprint Access Control for Wireless Insulin Pump Systems Using Cancelable Delaunay Triangulations

GUANGLOU ZHENG[1], (Member, IEEE), WENCHENG YANG[1], CRAIG VALLI[1], RAJAN SHANKARAN[2], HAIDER ABBAS[3], (Senior Member, IEEE), GUANGHE ZHANG[4], GENGFA FANG[5], JUNAID CHAUDHRY[6], AND LI QIAO[7]

[1]Security Research Institute, Edith Cowan University, Perth, WA 6027, Australia
[2]Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
[3]Department of Information Security, National University of Sciences and Technology, Rawalpindi 46000, Pakistan
[4]School of Computer and Information Engineering, Jiangxi Normal University, Nanchang 330022, China
[5]School of Electrical and Data Engineering, University of Technology Sydney, NSW 2007, Australia
[6]College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ 86301, USA
[7]School of Engineering and Information Technology, University of New South Wales, Canberra, ACT 2610, Australia

Corresponding author: Wencheng Yang (w.yang@ecu.edu.au)

This work was supported by the National Natural Science Foundation of China (NSFC) under Grant 61562043.

ABSTRACT An insulin pump is a small wearable medical gadget which can mimic the way a healthy pancreas functions by providing continuous subcutaneous insulin infusion for the patient. However, in the current products, the access to the pump is not securely controlled, rendering the pump insecure to harmful or even lethal attacks, such as those that lead to the privacy breach of the patient and the delivery of abnormal dosage of insulin to the patient. In a conventional symmetric key-based security solution, how to distribute and manage the key is quite challenging, since the patient bearing an insulin pump may visit any hospital or clinic to receive treatment from any qualified doctor. In order to prevent malicious access to the pump, in this paper, we propose a Fingerprint-based Insulin Pump security (FIPsec) scheme which requires an entity to first pass the fingerprint authentication process before it is allowed to access the insulin pump. With this scheme, the request from an adversary to access the pump will be blocked thereby protecting the pump from the possibility of being subjected to serious attacks during the post-request period. In the scheme, a cancelable Delaunay triangle-based fingerprint matching algorithm is proposed for the insulin pump, which has capabilities to resist against nonlinear fingerprint image distortion and the influence of missing or spurious minutiae. In order to evaluate the performance of the proposed fingerprint matching algorithm, we perform comprehensive experiments on FVC2002 DB1 and DB2 fingerprint databases. The results show that the FIPsec scheme can achieve a reasonably low equal error rate and thus becomes a viable solution to thwarting unauthorized access to the insulin pump.

INDEX TERMS Biomedical informatics, wearable sensors, implantable biomedical devices, insulin pump system, artificial pancreas, cyber security, authentication, access control.

I. INTRODUCTION

An insulin pump is a small medical gadget which can be easily carried on the body of a patient with diabetes, e.g., on a belt, inside a pocket, or even attached to a bra [1]–[3]. In other words, it facilitates a discreet therapy service that is convenient for these patients. Insulin delivery with pumps, also known as continuous subcutaneous insulin infusion (CSII), can mimic the way a healthy pancreas functions and deliver precise doses of rapid-acting insulin 24 hours a day to closely match the physiological demands of the body [4], [5]. A typical Insulin Pump System (IPS) is composed of a Continuous Glucose Monitor (CGM), an insulin pump and an infusion set. The CGM can provide real-time glucose readings to the pump. So, the pump can mimic a healthy pancreas to infuse the insulin accordingly.

The associate editor coordinating the review of this manuscript and approving it for publication was Ilsun You.

Nonetheless, the current IPS lacks sufficient security mechanisms to protect the patients from malicious attacks. In particular, the access to the pump does not have to pass any rigorous authentication process, which render the patient insecure to many harmful or lethal attacks [6], [7]. Firstly, adversaries can gain access to the sensitive information stored in the pump, including the patient's personal information (name, age, ID, contact number, etc.) and related medical information (insulin infusion recordings, insulin delivery configurations, etc.). Furthermore, this illegal access to the pump can even modify the therapy related settings in the pump, triggering the pump to deliver abnormal dosage of insulin to the patient. The overdosage of insulin can result in low blood glucose levels in the patient's blood thereby causing hypoglycemia which may lead to dizziness, seizures, loss of consciousness or even death. In contrast, the underdosage of insulin can cause abnormally high blood glucose level in the blood, leading to a condition called hyperglycemia that can be fatal to the patient. For patient's safety reasons, the U.S. Food and Drug Administration (FDA) requires the IPS to have preset minimum and maximum dosage and infusion rate settings in the pump. Nevertheless, these settings could be tampered with by attackers via the wireless link. As demonstrated by Barnaby Jack [8], with customized radio equipment and software, the attacker can seize control of any insulin pump within a radius of 300 feet and subject the pump to unauthorized commands such as dispensing its entire reservoir of insulin to the patient. A conventional symmetric key based security solution, in which the key has to be deployed beforehand, is not viable here. This is because a patient bearing an IPS may need to visit any hospital or clinic for treatment, especially in a medical emergency scenario. It is quite challenging to distribute the key to the very hospital or clinic in a timely manner and manage the key securely thereafter [9], [10].

In order to safeguard the therapy related settings in the insulin pump, Hei *et al.* [6] proposed a personalized patient infusion pattern-based access control (PIPAC) scheme in which supervised learning approaches are employed to learn the insulin infusion patterns by performing training on infusion logs in the pump. Any attack which aims to deliver abnormal dosage of insulin to the patient will not fit into the pattern and can be easily be detected. However, the main purpose of the PIPAC scheme is to simply detect the abnormal dosage infusion and not to suggest any remedial measures. In this paper, we propose a Fingerprint based Insulin Pump security (FIPsec) scheme which applies the fingerprint based authentication technique to control the direct access to the pump. With this scheme, users who want to change the parameter settings in the pump have to be authenticated first by using the patient's finger biometrics. Any attacker who wants to configure the pump maliciously will be blocked from accessing it effectively. These configurations include changing basal rates and bolus dosage settings in the pump. This authentication requirement also protects information privacy of the data stored in the pump as only legitimate users can pass the fingerprint authentication, and retrieve and read information. The contributions of the paper are summarized below:

- We analyze the security design challenges for the IPS and present the design of the FIPsec scheme in Section II. Through the use of this scheme, any access to the insulin pump must first undergo a verification process which involves the use of the patient's finger.
- We propose an improved cancelable Delaunay triangle-based fingerprint matching algorithm to implement the FIPsec scheme in Section III. This matching algorithm is designed to protect the biometric template stored in the pump, resist against nonlinear fingerprint distortion and conserve pump resources.
- We conduct extensive experiments to evaluate the performance of the proposed fingerprint matching algorithm in Section IV. Results show that the improvement to the algorithm by reducing the size of query features does not affect the overall matching performance, and at the same time it helps to conserve the resources in the pump remarkably.

Section V analyzes the security performance of the FIPsec scheme while Section VI discusses related research progress in this area. The final section summarizes our research with concluding remarks.

II. FIPSEC SCHEME DESIGN

This section analyzes the security design challenges for the IPS and then presents the design of the FIPsec scheme which can support the fingerprint based IPS security solutions.

A. THREAT MODELING

Threat modeling is the prerequisite for designing a security scheme. Generally the threats facing an IPS can be categorized into two main classes:

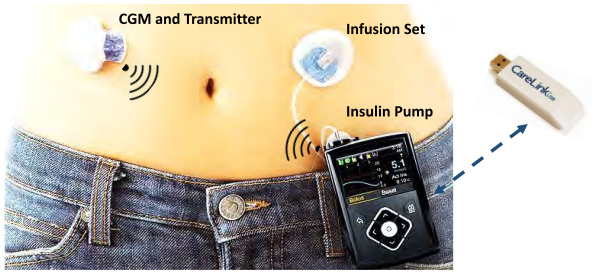

FIGURE 1. An insulin pump system (IPS) which is composed of a continuous glucose monitor (CGM), an insulin pump and an infusion set.

1) PASSIVE EAVESDROPPERS

A passive eavesdropper wiretaps the wireless channel in an insulin pump system and captures sensitive information of the patient which may contain the patient's ID, contact number, glucose levels, etc. As shown in Fig. 1, real-time glucose readings could be leaked from the wireless channel between the continuous glucose monitor and the pump. Meanwhile, eavesdroppers could obtain the patient's personal information

and pump configurations from the wireless channel between the pump and the external USB device.

2) ACTIVE ADVERSARIES

Active adversaries have capabilities to launch attacks on the IPS actively. They can obtain the patient's personal information by having access to the pump directly. This access may even allow the adversaries to make malicious changes to the pump settings, leading to overdosage or underdosage of insulin injection to the patient. Both overdosage and underdosage of insulin injection are lethal to the patient.

The active adversaries are more harmful to the patient than passive eavesdroppers. The FIPsec scheme proposed in this paper has the capability to control access to the pump so that the active attacks which target at changing injection settings in the pump are to be blocked from accessing it. Meanwhile, a fingerprint authentication system is vulnerable to presentation attacks where an artificial replica of the user's fingerprint can be used to spoof the system. This type of attacks can be countered by using various liveness detection methods. However, considering the restriction of resources in the pump, the liveness detection function is not adopted in our FIPsec scheme design.

B. SECURITY DESIGN CHALLENGES

There are three major components in an insulin pump system: a CGM, an insulin pump and an infusion set, as shown in Fig. 1. The function of each component and how they mutually interact are described below.

- *CGM and transmitter:* The CGM measures the glucose levels on a continual basis via an indwelling subcutaneous sensor. It then transmits the glucose data wirelessly to the insulin pump unit via a transmitter.
- *Insulin pump:* The insulin pump has a reservoir which stores insulin. Depending on the patient's current glucose levels, the required dosage of insulin is infused into the patient's body. It receives and displays near-continuous glucose readings from the CGM.
- *Wireless link:* The wireless link between the CGM and the insulin pump is responsible for transmitting the glucose values from the CGM to the pump.
- *USB device:* An extra USB device (e.g., the CareLink USB from the Medtronic Inc.) is used to configure the pump settings. A doctor uses a computer and the USB to upload the settings to the pump wirelessly.

The pump delivers insulin in two modes: *basal rate* and *bolus dose*. With the basal rate, the pump delivers a small amount of insulin continuously. Meanwhile, when the patient is going to have meals or needs to correct high blood glucose levels, a bolus dose of insulin can be configured by the patient and injected into his/her body.

Compared to traditional information technology systems, there are significant challenges in the IPS security design which stem from its life-saving medical application requirements, limited resources for wireless communications and user-friendly interface and operations [11], [12], each of which is discussed below.

- *Medical applications:* The security design for the IPS has to achieve a trade-off between security and medical safety. Any security scheme for the IPS should not hinder its medical applications, such as delivering the precise dose of insulin to a patient's body in a timely manner. If a password is applied to control the access to the insulin pump, then remembering and entering the password is required whenever the patient wants to change his/her insulin pump settings. Using the password is not convenient and remembering it would be very challenging and cumbersome, especially for elderly patients or someone with mental issues.
- *Limited resources:* The IPS has limited resources in the CGM and the pump itself. There is a transmitter in the CGM to send the glucose readings to the pump wirelessly. Ideally, confidentiality and integrity could be achieved if the glucose data could be encrypted and its message digest be calculated and appended to the message before transmission. However, these additional security mechanisms will place an unacceptably heavy burden on the tiny CGM module and thus are not viable from a practical perspective. The insulin pump is also an embedded system and powered by a battery. So, any security scheme designed to run on the pump should be energy efficient.
- *Usability:* A basic requirement for a medical device such as the IPS is that any proposed security mechanism to safeguard it must be easy to operate with and must work in a correct, safe and timely manner with no room for errors. Many strong and robust security solutions that require the usage of complicated passwords/operations are not viable in this scenario.

In summary, the IPS has unique characteristics, e.g., tiny and wireless devices, live-saving applications, extremely limited resources and special usability requirements, which pose great challenges to its security design. The security issues of the IPS need to be addressed urgently since any data tampering by adversaries could be life-threatening with a fatal consequence to the patients.

C. FIPSEC SCHEME DESIGN

In order to address these design challenges, in this section, we propose a Fingerprint based Insulin Pump security (FIPsec) scheme. This FIPsec hardware needs a fingerprint scanning sensor with a corresponding fingerprint processing algorithm to be added to the existing IPS hardware. Similar to most of the other fingerprint design schemes popularly used in mobile phones, this fingerprint scanner could be integrated with the round button on the surface of the pump (in Fig. 1) or by using a separate chip processing the fingerprint.

The FIPsec scheme applies a fingerprint-based authentication technique to control the access to the insulin pump. Different fingerprint matching approaches can be adopted in the authentication process, such as image correlation [13], [14],

phase matching [15], skeleton matching [16] and minutiae matching [17]. Because of successful use records in forensic examinations and storage efficiency in embedded computing systems, minutiae representation-based matching has become the most widely used one [17] and is also chosen in our FIPsec scheme. The scheme includes two phases: the enrollment phase and the authentication phase, which are detailed below.

- In the *enrollment phase*, the patient's fingerprint template is registered in the IPS for use in the authentication phase. A good quality fingerprint image is captured by using a fingerprint scanning sensor and then is used to extract minutiae points. Fingerprint minutiae, including ridge endings and ridge bifurcations, are the major features of a fingerprint image. The minutiae are later used to construct a template with refined discriminatory features/structures. This template is stored in the memory of the pump. The enrollment process is performed initially when an IPS is being configured for use for each patient. It can be processed once and used in the IPS until the end of the IPS lifetime.
- In the *authentication phase*, fingerprint query is generated and compared against the template stored in the pump. A matching score is calculated to determine the similarity level between the query and the template. If the score is larger than a pre-defined threshold, the authentication is deemed to be successful and the access to the pump is granted. Otherwise, the access request is rejected. In this phase, the patient's fingerprint image is captured and processed by using the same processing algorithm as the one being used in the enrollment phase.

When applying the FIPsec scheme, functions and components that need to be added to an existing insulin pump include (a) a fingerprint scanner, (b) a fingerprint image processing and minutiae extraction function, (c) a fingerprint feature representation and cancelable transformation function, (d) a fingerprint matching function to compare the query against the template and (e) a fingerprint template stored in the memory of the insulin pump.

Two fingers from each patient can be registered in his/her IPS profile: one as the primary and the other as the secondary. If the primary one cannot be used for authentication because of some reasons (e.g., hurt, burnt), the patient can use his/her secondary finger to access the insulin pump.

With the FIPsec scheme, whenever the critical settings of the insulin pump is to be changed, e.g., increasing or reducing the basal insulin or configuring the bolus dose of insulin, it requires the patient to authenticate to the pump by using the prescribed fingerprint authentication procedure.

III. FINGERPRINT AUTHENTICATION ALGORITHM

The FIPsec scheme could be implemented by using various fingerprint authentication algorithms. Some of these algorithms have a high level matching performance. For instance, the state-of-the-art Minutia Cylinder-Code (MCC)-based algorithm can achieve an equal error rate of below 2% on FVC2006 DB2 [18]. However, the construction of a local structure (a cylinder) is complex and consumes significant amount of resources. Considering that the insulin pump is a wireless mobile system with limited resources, a triangle-based feature representation is selected in the scheme design where features are constructed from minutiae triplets [19], [20]. In this section, a Delaunay triangulation process is applied to triangulate the minutiae on a fingerprint as it has capabilities to tackle nonlinear fingerprint image distortion and missing or spurious minutiae influences. A cancelable feature is added into the scheme in order to protect the fingerprint template stored in the IPS which can be revoked if it is disclosed by adversaries.

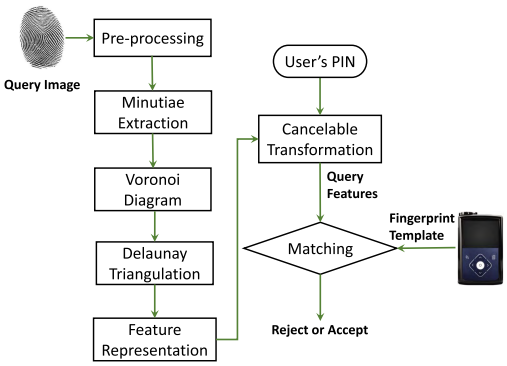

FIGURE 2. The fingerprint verification algorithm using cancelable Delaunay triangulation based feature representations. User's PIN is used to generate cancelable fingerprint templates for use.

A. FINGERPRINT VERIFICATION PROCESS

The Delaunay triangulation based fingerprint verification method is shown in Fig. 2, with each step described below:

- *Delaunay triangle-based feature representation:* This step in Fig. 2 includes processes of image preprocessing, minutiae extraction, Voronoi partitioning, Delaunay triangulation and feature representation. After this step, the fingerprint image is represented as triangle features which are suitable for the automatic matching process.
- *Cancelable transformation:* This step transforms triangle features to generate cancelable fingerprint templates by using one-way transformation function in the feature domain. The cancelable fingerprint template is used to protect the patient's biometrics which are stored in the medical device. With the cancelable transformation, if the fingerprint template is compromised, a new template can be generated by using a new transformation function.
- *Fingerprint matching:* The matching step compares query features against the template features in the IPS to decide whether the access to the IPS is allowed or not.

In the processes, the query image is the fingerprint measured every time before the verification takes place. The user's PIN is a secret key that is used to transform the fingerprint features

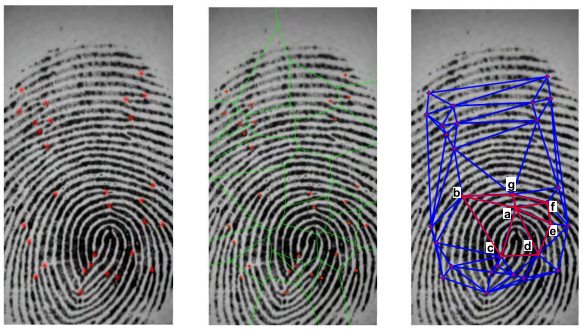

FIGURE 3. The process of Delaunay triangulation. (a) A fingerprint image with detected minutia points. (b) A Voronoi diagram which partitions the plane into cells. (c) Delaunay triangulation of the minutiae.

in order to generate cancelable features. Each of these steps are detailed in the following sections.

B. DELAUNAY TRIANGULATION-BASED MATCHING

1) MINUTIAE DELAUNAY TRIANGULATION

Assume there is a fingerprint image, FI, in $\mathbb{R}^2$ with a set of minutiae points $M = \{m_i\}_{i=1}^n$, as shown in Fig. 3 (a). For $\forall m_i \in M$ the Voronoi cell $V_M(i)$ of m_i can be denoted by,

$$V_M(i) := \{\, q \in \mathbb{R}^2 |\, d(q, m_i) \leq d(q, p) \quad \text{for } \forall p \in M\} \quad (1)$$

$d(.)$ is the Euclidean distance between two points in $\mathbb{R}^2$. $d(q, m_i) \leq d(q, p)$ represents that, for any point q in a Voronoi cell $V_M(i)$, the Euclidean distance to the its center, $d(q, m_i)$, is not greater than its distance to any other minutiae p in M. The Euclidean distance between a point $q(q_x, q_y)$ and a minutia, e.g., the minutia $m_i(m_{ix}, m_{iy})$, can be calculated as

$$\begin{aligned} d(q, m_i) &= \|q - m_i\| \\ &= \sqrt{(p_x - m_{ix})^2 + (p_y - m_{iy})^2} \end{aligned} \quad (2)$$

The Voronoi Diagram $VD(M)$ of the minutiae set $M = \{m_i\}_{i=1}^n$ in $\mathbb{R}^2$ is the subdivision of the plane induced by the Voronoi cells $V_M(i)$ for $i = 1, 2, \ldots, n$ (as shown in Fig. 3 (b)). The set of vertices are denoted by $VV(M)$, the set of edges by $VE(M)$ and the set of regions by $VR(M)$. If no four points in M are co-circular, then for every vertex $v \in VV(M)$, v is the common intersection of exactly three edges from $VE(M)$ and is the incident to exactly three regions from $VR(M)$. v is also the center of a circle $C(v)$ which goes through exactly three minutiae in M and $C(v) \cap M = \emptyset$.

A triangulation of a finite minutiae set $M = \{m_i\}_{i=1}^n$ in $\mathbb{R}^2$ is defined as a collection τ of triangles which satisfy conditions that:

$$\begin{cases} conv(M) = \bigcup_{T \in \tau} T \\ M = \bigcup_{T \in \tau} V(T) \\ T_i \cap T_j = V(T_i, T_j), E(T_i, T_j), or\ \emptyset \\ \qquad\qquad \text{for } \forall T_i, T_j \in \tau, i \neq j \end{cases} \quad (3)$$

where $conv(M)$ is the convex hull of the minutiae set M. T is a triangle in the collection τ with its vertices denoted by $V(T)$ and edges by $E(T)$. The triangulation of convex hull M is the straight-line dual of the Voronoi Diagram, $VD(M)$, which is constructed by connecting any two minutiae points in the neighboring Voronoi cell by a straight line (shown in Fig. 3 (c)). This is a Delaunay triangulation of M, denoted by τ_{DT}, which will be unique if no three points from M are collinear and no four points from M are cocircular. τ_{DT} satisfies the empty circumcircle criterion, that is, there is no minutia in the interior of the circumcircle of every triangle in τ_{DT}. Compared to other triangulations of the minutiae set M, the Delaunay triangulation maximizes the smallest interior angle of triangles. If the smallest angle of a triangulation, τ, is denoted by $\gamma(\tau)$, then $\gamma(\tau) \leq \gamma(\tau_{DT})$.

2) FINGERPRINT FEATURE REPRESENTATION AND MATCHING

A local structure in the fingerprint image is defined as a convex hull which consists of all triangles with a minutiae as the common vertex, denoted by,

$$LS(m_i) = \bigcup T(m_i), \quad \forall m_i \in M \quad (4)$$

where $LS(m_i)$ is the local structure at the minutia m_i and $T(m_i)$ is a triangle with m_i as its vertex. Features of the fingerprint image with the minutiae set M can be represented as a collection ψ of local structures, denoted by

$$\psi = \bigcup_{i=1,\ldots,n} LS(m_i), \quad m_i \in M \quad (5)$$

For $LS(m_i)$, a Cartesian coordinate system is defined to describe coordinates of triangle features, with its origin located at m_i and its x axis aligned with the orientation of the minutiae m_i. Fig. 3 (c) shows a local structure $LS(a)$ with the minutia a as the common vertex. Features from the triangle $\triangle abc$ which are used to represent the triangle are described below:

- l_{ao}: the distance between the vertex a and the incircle center o.
- α_{cax}: the angle between the x axis and the edge ac measured in the anti clockwise direction.
- α_{bax} is the angle between the x axis and the edge ab measured in the anti clockwise direction.
- β_{bc}: the orientation difference between the minutiae b and c.

So, features obtained from the triangle $\triangle abc$ can be denoted by $f_{\triangle abc} = (l_{ao}, \alpha_{cax}, \alpha_{bax}, \beta_{bc})$. Features for the local structure $LS(a)$ can be denoted by $F(a) = \{f_{\triangle abc}, f_{\triangle acd}, f_{\triangle ade}, f_{\triangle aef}, f_{\triangle afg}, f_{\triangle agb}\}$. Thus, the fingerprint image can be represented by features of these local structures, denoted by

$$F(FI) = \bigcup_{i=1,\ldots,n} F(m_i), \quad m_i \in M \quad (6)$$

where $F(m_i)$ is features of the local structure $LS(m_i)$ and $F(FI)$ represents the features of the fingerprint FI.

A cancelable transformation is performed on the features in order to protect the original fingerprint template.

Ratha *et al.* [21] initiated three different methods to generate cancelable fingerprint templates: Cartesian, polar and functional transformations. In order to improve system security and performance, Wang *et al.* [22], [23] proposed a few new cancelable transformation methods, such as the partial Hadamard transform based approach [22] and the approach based on zoned minutia pairs and partial discrete Fourier transform (P-DFT) [23]. Based on the P-DFT method, Yang *et al.* [24] proposed an enhanced partial discrete Fourier transform (EP-DFT) based non-invertible transformation algorithm which achieves a better security performance. Kho *et al.* [25] proposed a cancelable design based on Partial Local Structure (PLS) descriptor and Permutated Randomized Non-Negative Least Square (PR-NNLS) which has the capability to resist against matching performance deterioration after transformation. In this paper, a polar transformation, proposed by Ahmad et al. [26], is adopted to transform the template.

A polar coordinate space can be divided into several polar sectors, with L levels and S angles. The polar transformation changes the sector positions of the fingerprint template features $F(FI)$, including the angle and the length of each Delaunay triangle. If the transformation matrix for the angle and the length features are M_s and M_l, respectively, then the polar transformation process is denoted by,

$$\begin{cases} T_s = S + M_s \\ T_l = L + M_l \end{cases} \tag{7}$$

For instance, if $S = 4, L = 1$ and $M_s = [1, 1, -1, -3]$, the polar transformation through the matrix M_s is:

$$\begin{aligned} T_s &= S + M_s \\ &= [1, 2, 3, 4] + [1, 1, -1, -3] \\ &= [2, 3, 2, 1] \end{aligned} \tag{8}$$

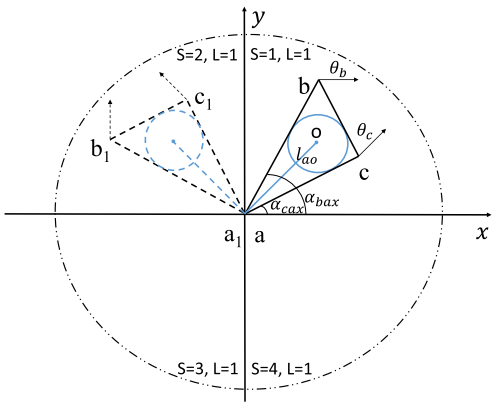

FIGURE 4. Fingerprint feature representation with cancelable transformation. Features from $\triangle abc$ include α_{cax}, α_{bax}, l_{ao}, θ_b and θ_c. A polar transformation method transforms features in $\triangle abc$ to those in $\triangle a_1\ b_1\ c_1$.

Fig. 4 shows that the $\triangle abc$ in Sector 1 (S = 1) is transformed to $\triangle a_1\ b_1\ c_1$ in Sector 2 (S = 2). Obviously, this mapping is a many-to-one process. After the transformation, original features in both Sector 1 and 3 are mapped to the sector 2. Therefore, it is impossible for an adversary to obtain the original template by inverting the transformed features, even if the adversary knows the transformation matrices and the transformed features. The combination of M_s and M_l is used as the user's PIN, that is, a secret key, to generate cancelable fingerprint templates. If the template data is compromised, a new template can be generated and stored in the IPS by simply using different matrics of M_s and M_l.

The matching process is performed based on the transformed triangle features. For the triangle $\triangle abc$, its transformed features can be denoted by $f_{\triangle a_1\ b_1\ c_1} = (l_{a_1\ o_1}, \alpha_{c_1\ a_1\ x_1}, \alpha_{b_1\ a_1\ x_1}, \beta_{b_1\ c_1})$. These feature values are then quantized for the matching purpose. Suppose there is a fingerprint template with a set of minutiae $M^T = \{m_i\}_{i=1}^{n^T}$ with features of a local structure denoted by $F^T(m_i)$, and a query with a set of minutiae $M^Q = \{m_j\}_{j=1}^{n^Q}$ with features of a local structure denoted by $F^Q(m_j)$. If these two local structures match one another, their local triangle features should be the same. If there are n_{ij} matched triangles between $F^T(m_i)$ and $F^Q(m_j)$, then the similarity between them is defined by:

$$S_{ij} = \frac{n_{ij} \times n_{ij}}{n^T \times n^Q} \tag{9}$$

These two local structures, $F^T(m_i)$ and $F^Q(m_j)$, are considered to be matching one another if the similarity score, S_{ij}, is larger than a pre-defined threshold, th_{ij}. By comparing all local structures between the template and the query, the number of matched local structures, n_{TQ}, is calculated. If n_{TQ} is equal to or larger than a pre-defined threshold, th_{TQ}, the query image is considered as matching with the template stored in the insulin pump. In this case, the fingerprint-based authentication is successful and the access to the insulin pump is permitted. Otherwise, the access to the insulin pump is considered as malicious and is to be rejected.

C. MATCHING ALGORITHM IMPROVEMENT

As a wearable device, an insulin pump has very limited resources in terms of computations, power and storage. In order to conserve these resources, we propose to improve the fingerprint matching algorithm by reducing the size of features. The overheads that are introduced by a matching algorithm are mainly determined by the number of features in the template and the query fingerprint, denoted by,

$$O = g(n^T, n^Q) \tag{10}$$

where O represents the overheads due to computations and power usage, and g is a positive correlation function. n^T and n^Q are the number of local structures in the template and the query. Here the reduction of the template size is not recommended due to following reasons: a) the template is captured and processed before it is embedded into the pump; b) using the whole template can ensure a high matching accuracy of the algorithm. The steps in the improved query generation process is outlined below:

1) The IPS with a fingerprint scanner captures the patient's finger tip image, FI^Q, and detects the corresponding minutiae points, M^Q. Thereafter, it deploys the cancelable Delaunay Triangulation algorithm to create local structures associated with each minutia, $LS^Q(m_i)$, in order to generate query features, $F^Q(m_i)$, where $m_i \in M^Q$.
2) The IPS then obtains the central point of the query image by calculating the mean of x-axis and y-axis values respectively of the minutiae in M^Q, denoted by $C = mean(\{x_{m_i}\}, \{y_{m_i}\})$ where x_{m_i}, y_{m_i} are coordinate values of minutiae, and $mean(.)$ is a function to calculate the mean value.
3) It then proceeds to select a subset from M^Q with n_s minutiae which are spatially closest to the center C, denoted by $M_s^Q = \{m_{s_1}, m_{s_2}, \ldots, m_{s_{n_s}}\}$. The Euclidean distance between a minutia, $m = \{x_m, y_m\}$, and the query image center, C, is calculated to determine which minutiae lie closest to the center, denoted by $d(m, C) = \sqrt{(x_m - x_c)^2 + (y_m - y_c)^2}$.
4) The query features are selected from $F^Q(m_i)$, where $m_i \in M_s^Q$, denoted by F_s^Q. This query feature sub-set is then used for the matching purpose.

According to the local structure construction in Section III, each LS contains information of the minutiae which are surrounding the center minutia of LS. So, the query F_s^Q represents minutiae more than M_s^Q. This guarantees the improved matching algorithm to have reduced false acceptance rate.

IV. EXPERIMENTAL ANALYSIS

In this section, the proposed cancelable Delaunay triangle-based fingerprint matching algorithm is tested in order to evaluate its overall performance in securing the insulin pump system. The influence of the cancelable polar transformation is also investigated in the experiments.

The publicly available fingerprint databases from the FVC2002 DB1 and FVC2002 DB2 are used in the experiments [27]. Each database has 800 gray-level fingerprint images. They are captured from 100 different fingers with 8 images of each finger captured. Minutiae points from each image are extracted by using the Verifinger 4.0 software tool from the Neurotechnology [28]. The FVC2002 test protocol [29] is adopted in the experiments.

Since the fingerprint image contains pixel information, the quantization step for l_{ao} is set as 20 pixels. The quantization steps for the angles α_{cax}, α_{bax} and β_{bc} are defined as $\frac{5\pi}{36}$. The division angles and levels in the polar space are chosen to be $S = 8$ and $L = 3$. The similarity threshold, th_{ij}, is defined as 0.25.

The performance of the proposed cancelable Delaunay triangle-based algorithm is evaluated by using the following parameters:

1) *False Rejection Rate (FRR):* the ratio of failed authentication attempts to the total number of attempts when a genuine finger is used in each attempt.
2) *False Acceptance Rate (FAR):* the ratio of successful authentication attempts to the total attempts when a falsified fingerprint is applied in each attempt. This falsified fingerprint could be from a different person's finger or a counterfeited fingerprint image.
3) *Equal Error Rate (EER):* the error rate when the FRR equals the FAR. The optimal system performance could be achieved when both rates are equal.
4) *Genuine Acceptance Rate (GAR):* the ratio of successful genuine attempts to the total genuine attempts. GAR equals 1-FRR.

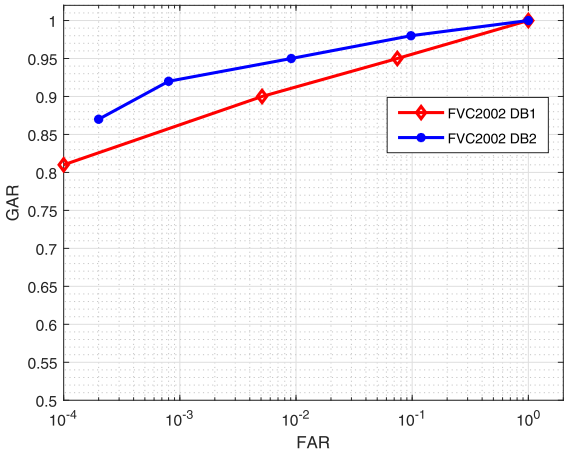

FIGURE 5. Experimental results of the fingerprint matching algorithm which includes the cancelable transformation process. The fingerprint databases, FVC2002 DB1 and DB2, are used in the experiment.

Matching with cancelable transformation: The performance of the fingerprint matching algorithm with cancelable transformations is evaluated using both FVC2002 DB1 and DB2 databases, with the results shown in Fig. 5. All the features used in the experiment are extracted from Delaunay triangles which are processed by the polar transformation before the matching process. We can see from Fig. 5 that the proposed cancelable fingerprint matching algorithm can achieve a high GAR while keeping the FAR at low level. The EER performance is 5.88% on DB1 and 3.90% on DB2.

Matching without cancelable transformation: The influence of cancelable transformation on the fingerprint matching performance is investigated. Two individual experiments are run on each fingerprint database. In each experiment, we compare the matching performance of the algorithm which has the process of cancelable transformation with the algorithm which does not. The results from experiments on FVC2002 DB1 are shown in Fig. 6 and those on FVC2002 DB2 shown in Fig. 7. Their EER results are presented in Table 1.

We can see from the results that, after the cancelable transformation, the matching performance of the algorithm slightly declines, with the EER on DB1 increasing from 5.38% up to 5.88% and the EER on DB2 from 2.69% up to 3.90%. This is because the many-to-one polar mapping may cause collision. As a result, some triangles in the print

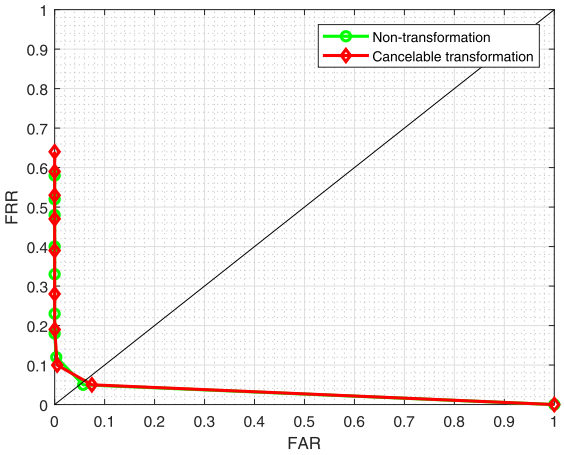

FIGURE 6. The comparison of matching performances on FVC2002 DB1 between the algorithm which does not include the cancelable transformation process and the one which has the cancelable transformation process.

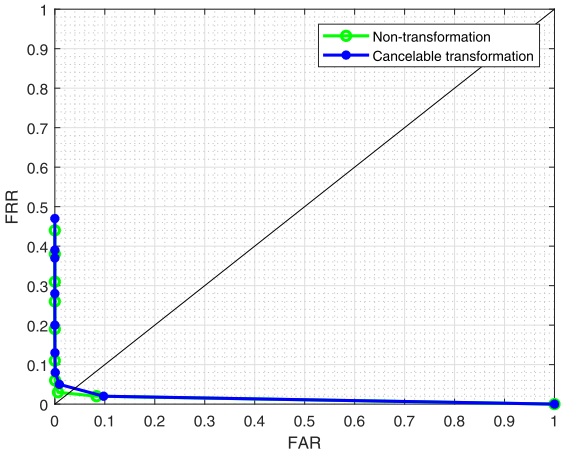

FIGURE 7. The comparison of matching performances on FVC2002 DB2 between the algorithm which does not include the cancelable transformation process and the one which has the cancelable transformation process.

TABLE 1. EER experimental results on both the FVC2002 DB1 and DB2 fingerprint databases.

	FVC2002 DB1	FVC2002 DB2
Cancelable	5.88%	3.90%
Non-Transformation	5.38%	2.69%

not do not match after non-invertible transformation. However, with the cancelable fingerprint matching algorithm, the overall EER can still be maintained at around 5%, which is within the acceptable limits. Therefore, the proposed matching algorithm is efficient and can be a viable option to protect the insulin pump from malicious access from active adversaries.

In order to test the performance of the improved fingerprint matching algorithm, query features associated with n_s minutiae which are closest to the fingerprint center are selected. In the experiments, n_s is chosen from 18 to 40, as shown in column 1 in Table 2 and Table 3. In the table, Half Total Error

TABLE 2. Experimental results of improved Cancelable Delaunay triangulation algorithm on FVC2002 DB1.

Number of Query LS	FRR	FAR	HTER
40	5.00%	7.14%	6.07%
37	5.00%	6.87%	5.93%
35	5.00%	6.76%	5.88%
32	6.00%	6.29%	6.15%
30	6.00%	6.00%	6.00%
27	6.00%	5.27%	**5.64%**
25	8.00%	4.73%	6.36%
23	8.00%	4.30%	6.15%
20	11.00%	3.36%	7.18%
18	16.00%	2.81%	9.40%

TABLE 3. Experimental results of improved Cancelable Delaunay triangulation algorithm on FVC2002 DB2.

Number of Query LS	FRR	FAR	HTER
40	3.00%	7.92%	5.46%
37	3.00%	7.45%	5.23%
35	4.00%	7.19%	5.60%
32	4.00%	6.41%	5.21%
30	4.00%	5.88%	4.94%
27	5.00%	4.94%	4.97%
25	5.00%	4.65%	4.82%
23	5.00%	4.27%	**4.64%**
20	7.00%	3.76%	5.38%
18	7.00%	3.55%	5.27%

Rate (HTER), which is the mean value of FRR and FAR, is used to assess the overall performance of the algorithm. We can see from Table 2 that when the number of selected local structures in query decreases, the FRR performance goes down while the FAR goes up. It reaches the best HTER when $n_s = 27$. In comparison to the algorithm that uses 40 local structures in its query, in our proposed approach, the size of the query features is reduced by 32.5%. Similarly, in Table 3 the HTER is the smallest when $n_s = 23$. Compared to the query which uses 40 local structures, the size of the query is decreased by 42.5%. We can therefore safely conclude that it will not affect the overall matching performance by reducing the size of query features. However, it can help conserve resources in the pump and improve the energy efficiency of the IPS.

V. SECURITY ANALYSIS

The current range of insulin pump products do not have support for any rigorous authentication mechanism that can moderate and control the access to the pump. So, by sending a malicious request to the pump, adversaries can retrieve private information of the patient or even change therapy related settings in the pump. These settings decide the dosage of insulin that will be infused into the patient's body. Both, an overdose or an underdose of insulin, can cause harmful or even lethal consequences to the patient. However, with the proposed FIPsec scheme, any user who wants to perform operations on the pump has to be first authenticated by using the patient's finger. It becomes intuitively clear when a malicious entity who tries to unlock the pump with

TABLE 4. Comparison of fingerprint authentication algorithms for securing an insulin pump.

Fingerprint authentication algorithms	Key points if applied to secure an insulin pump
Minutia Cylinder-Code (MCC) (Cappelli et al. [18])	1) Feature representation is achieved by associating a local structure (called a cylinder) to each minutia. 2) It is the state-of-the-art and can achieve an EER of below 2% on FVC2006 DB2. 3) Generating a binary sequence from each cylinder requires computations of sigmoid functions, euclidean distances and other complex math functions.
Fixed-length binary strings for feature representation (Jin et al. [30])	1) Generation of fixed-length representation requires two steps: Polar Grid-based Three-tuple Quantization (PGTQ) and Kernel-based Fixed-Length Transformation(KFLT). 2) PGTQ generates an alignment-free feature representation by using polar coordinate-based transformation. 3) KFLT uses a symmetric and positive definite kernel function to transform the PGTQ feature representation to a fixed-length real-valued representation.
Pair-polar coordinate-based feature representation (Ahmad et al. [26])	1) For each minutia, generate pair-polar coordinate vectors which has relative information of that minutia to others. 2) A cancelable template is produced by performing a polar transformation. 3) The EER of the cancelable fingerprint matching can achieve 6% on FVC2002DB2 and 9% on FVC2002DB1.
CNN and deep learning-based fingerprint verification (Lin and Kumar [31])	1) The verification algorithm is built upon multi-Siamese convolutional neural networks and deep learning technologies. 2) A large volume of training dataset is required to train the verification algorithm. 3) The training and tests were performed on an Intel i5-2500 3.3GHz CPU with NVIDIA 980Ti GPU.
Finger texture verification based on deep learning (Omar et al. [32])	1) The biometric trait used is the finger texture which is the area between the upper phalanx and the lower knuckle of the finger. 2) The verification algorithm relies on the multi-layered deep learning technology, including a convolution layer, a rectified linear unit layer, a pooling layer, etc.

the patient's fingertip can be easily detected by the patient. Since the adversary cannot pass the authentication process, its communication request to the pump will be blocked, which in turn protects the pump from both privacy breach and adverse dosage attacks.

In the FIPsec scheme, the fingerprint matching algorithm has the property of cancelability. So, an adversary cannot reveal the patient's fingerprint if the biometric template in the pump is disclosed. A new template can be generated by using a different transformation matrix and saved in the pump for authentication. Hence, the patient's original fingerprint template will be protected. Furthermore, the proposed Delaunay triangle based matching algorithm can achieve around 5% EER, which is viable in the real application scenario, since the insulin pump has to be always worn on the patient's body and can be constantly monitored by the patient. If an adversary wants to launch a brute-force attack on the pump by continually using a forged fingerprint, it will be easily detected by the patient. Therefore, the use of the fingerprint based authentication scheme can protect the pump effectively by blocking malicious operations from adversaries on the pump with lethal consequences.

VI. RELATED WORK

Wireless connections in insulin pump systems have triggered cyber security concerns [7], [33]–[37]. These issues can not only result in breaches of privacy of the patients, but also have a potential to risk the patient's life by delivering a lethal dose of insulin to the patient. Therefore, the cyber security issues have to be resolved before the next generation automated IPS products coming out [38]. This section compares recently proposed fingerprint authentication algorithms and analyzes related work on the IPS security.

A. FINGERPRINT AUTHENTICATION

The design of a security scheme for the IPS needs to achieve a trade-off between the security performance and the resource constraints in the device, since the insulin pump is a wireless mobile medical device with very limited resources. In this paper, we proposed to apply an improved cancelable Delaunay triangle-based fingerprint matching algorithm to control access to the pump. Table 4 lists some of the recent proposed fingerprint verification algorithms and highlights the key points if they are applied to secure an IPS, including the state-of-the-art Minutia Cylinder-Code (MCC) based algorithm [18] and the convolutional neural networks (CNNs) and deep learning based fingerprint verification algorithm [31]. This section will compare the fingerprint authentication algorithm designed for the IPS with each one in the table.

The MCC-based fingerprint verification algorithm is the state-of-the-art and can achieve an EER of less than 2% on FVC2006 DB2. The construction of local structures (cylinders) includes processes of projecting minutiae into cells in the cylinder and calculating a numerical value of each cell based on accumulated contributions from its neighboring minutiae. It requires mathematical computations of sigmoid functions, euclidean distances, Gaussian functions and others, and therefore is more complex than the construction of triangle local structures in the FIPsec scheme. Considering that the insulin pump has very limited resources most of which have to be reserved for medical applications,

TABLE 5. Recent research results on the insulin pump system security.

Research areas	Related work	Key techniques/discoveries
IPS vulnerabilities	Blues [8] Li [39] et al. Radcliffe [40]	1) Breach patient's privacy by eavesdropping 2) Send malicious commands to IPS by active adversaries 3) Inject lethal dose of insulin, resulting in hyperglycemia or hypoglycemia
IPS security solution design	Hei et al. [6], [41] Marin et al. [42] Ahmad et al. [43] Zhao et al. [44]	1) Patient infusion pattern based access control scheme (PIPAC) 2) Apply AES-128 for encryption and authentication 3) Use deep learning and gesture recognition 4) Use a visible light channel for PIN/key transmission
IPS forensics	Benedict [45] et al. Nathan et al. [46] Rahman et al. [47]	1) Presented a homicide case of injecting lethal doses via the IPS 2) Detect bowel sounds of the patient for forensic analysis 3) Use a forensically ready system to record medical incidents

the MCC-based algorithm is not viable here. In the fingerprint verification algorithm proposed by Jin *et al.* [30], two steps are required to generate fixed-length binary strings to represent minutiae features: Polar Grid-based Three-tuple Quantization (PGTQ) and Kernel-based Fixed-Length Transformation(KFLT). The first step (PGTQ) already generates alignment-free feature representation. However, compared with the MCC, it requires one more step, that is, KFLT, to generate fixed-length binary strings from the alignment-free feature representations. So, this algorithm is not viable to be applied on the IPS due to the computation complexity concern in the fingerprint local structure process.

Ahmad *et al.* [26] proposed to use pair-polar coordinate vectors to represent the fingerprint minutiae features. For a fingerprint template with a minutiae set $M = \{m_i\}_{i=1}^{n}$, each local structure associated to a minutia has $(n-1)$ vectors and each vector contains three features, including angles and distances. However, in our proposed algorithm, each local structure (a Delaunay triangle) is denoted by one vector with only four feature elements in the vector, for instance, $f_{\triangle abc} = (l_{ao}, \alpha_{cax}, \alpha_{bax}, \beta_{bc})$ for $\triangle abc$ in Fig. 4. So, features used to represent each local structure in [26] are more than that in our proposed algorithm, resulting in more resource consumption in the pump. Furthermore, its matching performance (EER of 6% on FVC2002 DB2 and 9% on DB1) is not as good as our proposed algorithm which can achieve EER of 3.90% on DB2 and 5.88% on DB1, respectively.

Lin and Kumar [31] proposed a novel fingerprint verification algorithm built upon convolutional neural networks and deep learning technologies. This algorithm does not require the construction of local structures to represent the fingerprint. Nonetheless, the computation of CNNs and deep learning algorithms is heavy and thus is not suitable for wireless medical devices. Authors used Intel i5-2500 3.3GHz CPU and NVIDIA 980Ti GPU to perform training and testing of the algorithm in [31]. Omar *et al.* [32] proposed to use finger textures (FTs) for the verification purpose. The biometric trait used is the FT which is the area located between the upper phalanx and the lower knuckle of the finger, which is not convenient for biometric capture in practice compared with the fingerprint based biometric algorithm. Meanwhile, the deep learning technologies are used in [32], making the computation load of the algorithm heavy for the wireless insulin pump.

B. IPS SECURITY

Recent IPS security research can be categorized into three types: IPS vulnerabilities test and demonstration, IPS security solution proposal and design, and IPS forensics, as shown in Table 5. The summary and analysis of research in each category is presented below:

1) *IPS vulnerabilities:* Recent research demonstrates that the IPS could be attacked by using Universal Software Radio Peripheral (USRP) [39] or a customized software and antenna [8]. Both eavesdropping and active attacks can be launched by the adversaries. The experiments showed that the privacy of the patient could be breached by the eavesdroppers, e.g., the patient ID, medical history and therapeutic records. Furthermore, active adversaries can send malicious commands to control the pump and deliver lethal dose of insulin to the patient, which may lead to medical conditions such as hyperglycemia (high blood glucose) or hypoglycemia (low blood glucose).
2) *IPS security solution design:* Currently a few solutions have been proposed to secure the IPS. Hei *et al.* [6], [41] proposed a patient infusion pattern based access control scheme (PIPAC) which uses patient infusion patterns to detect abnormal infusion delivery in order to recover the safe infusion settings automatically according to the pump's logs. Its aim is to address two types of abnormal infusion attacks: abnormal bolus dosage attacks and abnormal basal rate attacks. Marin *et al.* [42] proposed a solution that made use of both the AES-128 in counter mode and the AES-128 as a message authentication code (MAC) to provide confidentiality and authentication as well. However, the AES algorithm cannot be applied to CGM since it is only a sensor coupled with a transmitter. Ahmad *et al.* [43] proposed to use a deep learning method to predict the dosage threshold and ask the patient to perform gestures if the insulin to be injected is higher than the threshold. A visible channel based access control scheme, proposed by Zhao *et al.* [44], can authenticate the doctor's USB by transmitting the PIN/key to the IPS via visible light signals.
3) *IPS forensics:* Forensic research for the IPS and medical devices in general is to keep records related to medical devices for post incident investigation.

Benedict *et al.* [45] presented a case of homicide in which the victim's insulin pump was used to inject lethal doses of etomidate and atracurium. Henry *et al.* [46] proposed to integrate a new sensor into the IPS in order to detect bowel sounds of the patient for forensic analysis. This forensic information can determine the cause of the event and whether it is due to security breaches to the IPS or not. Rahman *et al.* [47] proposed a forensically ready system which uses drones and surveillance cameras to record medical incidents and save them into a forensic server located in a hospital internal network.

In this paper, we have proposed a novel IPS security solution based on fingerprint authentication. It is lightweight in terms of resource consumption in the insulin pump as it does not require the pump to capture and process a real-time fingerprint in each and every authentication attempt. It does not rely on a key or password to be stored in every hospital. Any doctor can gain access to the pump by using the patient's finger directly. It also has a strong usability as the patient can just press his/her finger on a button on the IPS. So, it is very useful for elderly people, especially those with dementia.

VII. CONCLUSION

Current insulin pump products lack support for rigorous authentication mechanism to prevent malicious entities from accessing it, and this can lead to attacks that are harmful to the patients. Therefore, in this paper, we propose a Fingerprint based Insulin Pump security (FIPsec) scheme which employs a fingerprint authentication scheme to verify any access request to the pump. With this scheme, any unauthorized or malicious access to the pump will be instantly blocked. A cancelable Delaunay triangle-based fingerprint matching algorithm is presented to implement the scheme which has the capabilities to resist against fingerprint distortion or missing minutiae during the capturing process. In order to conserve resources in the insulin pump, the matching algorithm is further improved by reducing the size of query features. Experimental results show that this improvement does not influence the overall matching performance but it can help conserve the resources in the pump significantly.

REFERENCES

[1] S. Zavitsanou, A. Chakrabarty, E. Dassau, and F. J. Doyle, "Embedded control in wearable medical devices: Application to the artificial pancreas," *Processes*, vol. 4, no. 4, p. 35, 2016.

[2] B. H. McAdams and A. A. Rizvi, "An overview of insulin pumps and glucose sensors for the generalist," *J. Clinical Med.*, vol. 5, no. 1, p. 5, Jan. 2016.

[3] H. Rathore, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A review of security challenges, attacks and resolutions for wireless medical devices," in *Proc. 13th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2017, pp. 1495–1501.

[4] K. Saleem, B. Shahzad, M. A. Orgun, J. Al-Muhtadi, J. J. P. C. Rodrigues, and M. Zakariah,"Design and deployment challenges in immersive and wearable technologies," *Behav. Inf. Technol.*, vol. 36, no. 7, pp. 687–698, Jan. 2017.

[5] G. Fang, M. A. Orgun, R. Shankaran, E. Dutkiewicz, and G. Zheng, "Truthful channel sharing for self coexistence of overlapping medical body area networks," *PloS One*, vol. 11, no. 2, Feb. 2016, Art. no. e0148376.

[6] X. Hei, X. Du, S. Lin, I. Lee, and O. Sokolsky, "Patient infusion pattern based access control schemes for wireless insulin pump system," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 11, pp. 3108–3121, Nov. 2015.

[7] N. Paul, T. Kohno, and D. C. Klonoff, "A review of the security of insulin pump infusion systems," *J. Diabetes Sci. Technol.*, vol. 5, no. 6, pp. 1557–1562, Nov. 2011.

[8] S. Blues. (Oct. 2011). *Insulin Pump Hack Delivers Fatal Dosage Over the Air*. [Online]. Available: https://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack

[9] G. Zheng, W. Yang, C. Valli, L. Qiao, R. Shankaran, M. A. Orgun, and S. C. Mukhopadhyay, "Finger-to-heart(F2H): Authentication for wireless implantable medical devices," *IEEE J. Biomed. Health Inform.*, to be published.

[10] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, and W. H. Maisel, "Security and privacy for implantable medical devices," *IEEE Pervasive Comput.*, vol. 7, no. 1, pp. 30–39, Jan./Mar. 2008.

[11] L. Reverberi and D. Oswald, "Breaking (and fixing) a widely used continuous glucose monitoring system," in *Proc. 11th USENIX Conf. Offensive Technol.*, Berkeley, CA, USA, 2017, pp. 1–10.

[12] S. Kulaç, "Security belt for wireless implantable medical devices," *J. Med. Syst.*, vol. 41, no. 11, p. 172, Sep. 2017.

[13] K. Nandakumar and A. K. Jain, "Local correlation-based fingerprint matching," in *Proc. 4th Indian Conf. Comput. Vis., Graph. Image Process. (ICVGIP)*, Kolkata, India, Dec. 2004, pp. 503–508.

[14] A. M. Bazen, G. T. Verwaaijen, S. H. Gerez, L. P. Veelenturf, and B. J. Van Der Zwaag, "A correlation-based fingerprint verification system," in *Proc. Workshop Circuits, Syst. Signal Process.*, Nov. 2000, pp. 205–213.

[15] J. Feng and A. K. Jain, "Fingerprint reconstruction: From minutiae to phase," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 2, pp. 209–223, Feb. 2011.

[16] J. Feng, Z. Ouyang, and A. Cai, "Fingerprint matching using ridges," *Pattern Recognit.*, vol. 39, no. 11, pp. 2131–2140, 2006.

[17] A. K. Jain, J. Feng, and K. Nandakumar, "Fingerprint matching," *Computer*, vol. 43, no. 2, pp. 36–44, Feb. 2010.

[18] R. Cappelli, M. Ferrara, and D. Maltoni, "Minutia cylinder-code: A new representation and matching technique for fingerprint recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 32, no. 12, pp. 2128–2141, Dec. 2010.

[19] B. Bhanu and X. Tan, "Fingerprint indexing based on novel features of minutiae triplets," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 5, pp. 616–622, May 2003.

[20] M. A. Medina-Pérez, M. García-Borroto, A. E. Gutierrez-Rodríguez, and L. Altamirano-Robles, "Improving fingerprint verification using minutiae triplets," *Sensors*, vol. 12, no. 3, pp. 3418–3437, Mar. 2012.

[21] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, Apr. 2007.

[22] S. Wang, G. Deng, and J. Hu, "A partial hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognit.*, vol. 61, pp. 447–458, Jan. 2017.

[23] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," *Pattern Recognit.*, vol. 66, pp. 295–301, Jun. 2017.

[24] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, Jun. 2018.

[25] J. B. Kho, J. Kim, I.-J. Kim, and A. B. J. Teoh, "Cancelable fingerprint template design with randomized non-negative least squares," *Pattern Recognit.*, vol. 91, pp. 245–260, Jul. 2019.

[26] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," *Pattern Recognit.*, vol. 44, nos. 10–11, pp. 2555–2564, 2011.

[27] *FVC2002 Databases*. (2002). [Online]. Available: http://bias.csr.unibo.it/fvc2002/databases.asp

[28] NeuroTechnology. (2017). *Verifinger SDK*. Accessed: Apr. 2017, 10. [Online]. Available: http://www.neurotechnology.com/verifinger.html

[29] B S Laboratory, (2002). *Fingerprint Verification Competition-Performance Evaluation*. [Online]. Available: http://bias.csr.unibo.it/fvc2002/perfeval.asp

[30] Z. Jin, M.-H. Lim, A. B. J. Teoh, B.-M. Goi, and Y. H. Tay, "Generating fixed-length representation from minutiae using kernel methods for fingerprint authentication," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 46, no. 10, pp. 1415–1428, Oct. 2016.

[31] C. Lin and A. Kumar, "A CNN-based framework for comparison of contactless to contact-based fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 3, pp. 662–676, Mar. 2019.
[32] R. R. Omar, T. Han, S. A. M. Al-Sumaidaee, and T. Chen, "Deep finger texture learning for verifying people," *IET Biometrics*, vol. 8, no. 1, pp. 40–48, Jan. 2019.
[33] K. E. Britton and J. D. Britton-Colonnese, "Privacy and security issues surrounding the protection of data generated by continuous glucose monitors," *J. Diabetes Sci. Technol.*, vol. 11, no. 2, pp. 216–219, Mar. 2017.
[34] D. T. O'Keeffe, S. Maraka, A. Basu, P. Keith-Hynes, and Y. C. Kudva, "Cybersecurity in artificial pancreas experiments," *Diabetes Technol. Therapeutics*, vol. 17, no. 9, pp. 664–666, Aug. 2015.
[35] D. C. Klonoff, "Cybersecurity for connected diabetes devices," *J. Diabetes Sci. Technol.*, vol. 9, no. 5, pp. 1143–1147, Apr. 2015.
[36] N. Paul and T. Kohno, "Security risks, low-tech user interfaces, and implantable medical devices: A case study with insulin pump infusion systems," *Presented 3rd USENIX Workshop Health Secur. Privacy*, Bellevue, WA, USA, Aug. 2012, pp. 1–2.
[37] L. Wu, X. Du, M. Guizani, and A. Mohamed, "Access control schemes for implantable medical devices: A survey," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1272–1283, Oct. 2017.
[38] J. R. Castle, J. H. DeVries, and B. Kovatchev, "Future of automated insulin delivery systems," *Diabetes Technol. Therapeutics*, vol. 19, no. S3, p. S-67, Jun. 2017.
[39] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. 13th IEEE Int. Conf. e-Health Netw. Appl. Services*, Jun. 2011, pp. 150–156.
[40] J. Radcliffe, "Hacking medical devices for fun and insulin: Breaking the human SCADA system," in *Proc. Black Hat Conf. Presentation Slides*, Aug. 2011, pp. 1–13.
[41] X. Hei, X. Du, S. Lin, and I. Lee, "Pipac: Patient infusion pattern based access control scheme for wireless insulin pump system," in *Proc. INFOCOM*, Aug. 2013, pp. 3030–3038.
[42] E. Marin, D. Singelée, B. Yang, I. Verbauwhede, and B. Preneel, "On the feasibility of cryptography for a wireless insulin pump system," in *Proc. 6th ACM Conf. Data Appl. Secur. Privacy*, New York, NY, USA, Mar. 2016, pp. 113–120.
[43] U. Ahmad, H. Song, A. Bilal, S. Saleem, and A. Ullah, "Securing insulin pump system using deep learning and gesture recognition," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng.*, Aug. 2018, pp. 1716–1719.
[44] J. Zhao, K. Kong, X. Hei, Y. Tu, and X. Du, "A visible light channel based access control scheme for wireless insulin pump systems," in *Proc. IEEE Int. Conf. Commun.(ICC)*, May 2018, pp. 1–6.
[45] B. Benedict, R. Keyes, and F. C. Sauls, "The insulin pump as murder weapon: A case report," *Amer. J. Forensic Med. Pathol.*, vol. 25, no. 2, pp. 159–160, Jun. 2004.
[46] N. L. Henry, N. R. Paul, and N. McFarlane, "Using bowel sounds to create a forensically-aware insulin pump system," *Presented Workshop Health Inf. Technol.*, Washington, DC, USA, 2013, p. 8.
[47] A. F. A. Rahman, R. Ahmad, and S. N. Ramli, "Forensics readiness for Wireless Body Area Network (WBAN) system," in *Proc. 16th Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2014, pp. 177–180.

GUANGLOU ZHENG (S'13–M'17) received the B.Eng. and M.Eng. degrees from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2006 and 2009, respectively, and Ph.D. degree in computer science from Macquarie University, Sydney, NSW, Australia, in 2016. The title of his Ph.D. thesis is "securing wireless implantable medical devices using electrocardiogram signals."

He is currently a Postdoctoral Research Fellow with the Security Research Institute, Edith Cowan University, Perth, WA, Australia. He was a Telecommunication System Research and Development Engineer with Nanjing Zhongxing Software Company, Ltd., Nanjing. His research interests include wireless network security, medical system security, biometrics, IoT security, ECG signal processing, spacecraft orbit determination, GPS/GNSS, and precise navigation and positioning technologies.

WENCHENG YANG received the bachelor's degree from the Wuhan University of Technology, Wuhan, China, in 2006, the master's degree in computer science from Korea University, South Korea, in 2008, and the Ph.D. degree in computer science from the University of New South Wales, Australia, in 2015.

He is currently a Postdoctoral Researcher with the Security Research Institute (SRI), Edith Cowan University (ECU), Perth, WA, Australia. His research interests include biometric security and pattern recognition. He has published several high-quality papers on high ranking journals and conferences, e.g., IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, and *Pattern Recognition*.

CRAIG VALLI received the Diploma of Teaching from the Western Australian CAE, Perth, Australia, in 1985, and the Bachelor of Education, Master of Management (Information Systems), and Doctor of Information Technology degrees from Edith Cowan University, Perth, in 1990, 2000, and 2003, respectively. He has over 30 years' experience in the ICT Industry and consults to industry and government on cyber security and digital forensics issues. He is the Director of Edith Cowan University Security Research Institute and a Professor of Digital Forensics.

He has over 100 peer reviewed academic publications in cyber security and digital forensics. His main research and consultancy is focused on securing networks and critical infrastructures, detection of network borne threats and forensic analysis of cyber security incidents.

Mr. Craig is a Fellow of the Australian Computer Society, and the Director of the Australian Computer Society Centre of Expertise in Security at ECU. He is currently the Research Director of the Australian Cyber Security Research Institute, the Vice President of the High-Tech Crime Investigators Association (Australian Chapter) and a Member of the INTERPOL Cyber Crime Experts Group.

RAJAN SHANKARAN received the M.B.A. degree in management information systems from the Maastricht School of Management, Holland, in 1994, and the M.Comp., M.Sc. (Hons.), and Ph.D. degrees in computing from the University of Western Sydney, in 1996, 1999, and 2005, respectively.

He was a Lecturer with the University of Western Sydney. He is currently a Senior Lecturer with the Department of Computing, Macquarie University, where he is a member of the WiMED Research Center, Faculty of Science and Engineering. He is also a member of the Advanced Cyber Security Research Group, Department of Computing. His current research interests include network security and trust and key management in ad-hoc/sensor networks.

HAIDER ABBAS (SM'15) received the M.S. degree in engineering and management of information systems and the Ph.D. degree in information security from KTH, Sweden, in 2006 and 2010, respectively.

He is currently associated with the National University of Sciences and Technology, Pakistan, as an Associate Professor. He is the Cyber Security Professional, who took professional trainings and certifications from the Massachusetts Institute of Technology, USA, Stockholm University, Sweden, IBM, and EC-Council. He is also the Principal Advisor for several graduate and doctoral students with King Saud University, the National University of Sciences and Technology, Pakistan, and the Florida Institute of Technology, USA. He is an associate editor or on the editorial board of a number of international journals. He received many awards and several research grants for ICT related projects from various research-funding authorities from U.S., EU, KSA, and Pakistan.

GUANGHE ZHANG received the M.E. degree from Jiangxi Normal University, Nanchang, China, the Ph.D. degree from the Institute of Computing Technology, Chinese Academy of Sciences (CAS), China.

He is currently an Assistant Teaching Professor with Jiangxi Normal University. His current research interests include body sensor network security, biosignal processing, and development of software for education.

GENGFA FANG received the master's degree in telecommunications from Zhejiang University and the Ph.D. in wireless communications from the Institute of Computing Technology, Chinese Academy of Sciences, in 2002 and 2007, accordingly.

He is currently a Senior Lecturer with the University of Technology Sydney, Sydney, NSW, Australia. From 2007 to 2009, he was a Researcher with the Canberra Research Laboratory of National ICT Australia (NICTA) on WCDMA Femtocell Project. Since 2010, he was involving on Rural Broadband Access project at CSIRO as a Research Scientist. From 2009 to 2015, he was with the Department of Engineering Macquarie University. He has published over 100 papers, patents on embedded wireless network systems, MAC protocols, cross-layer design, wireless resource management, and allocation for 5G, IoT, and medical body area networks.

JUNAID CHAUDHRY received the Ph.D. degree in cyber security from Ajou University, South Korea. He obtained training with Harvard Business School, University of Amsterdam, and Kaspersky Research Laboratory in cyber hunting and training. He is currently a Cyber Security Faculty with the College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ, USA.

He has over 15 years of exciting experience in academia, industry, law-enforcement, and in corporate world in information and cyber security domain. He is a Practicing Engineer, a Member of High Technology Crime Investigation Association (HTCIA), Australian Computing Society, Australian Information Security Association, and frequently volunteers in promotion of science through public speaking, conference organisation, and by editing the scientific journals, i.e., IEEE Access, *Computer and Security* (Elsevier), the IEEE Internet Policy and IEEE Future Directions, and the board member of tech startups. He has authored three books and over 75 research papers. He received awards for his research achievements from Government of South Korea, Qatar, Pakistan, and Saudi Arabia.

LI QIAO received the B.Eng. and Ph.D. degrees from the Nanjing University of Aeronautics and Astronautics, China, in 2004 and 2011, respectively. She was a Visiting Ph.D. Student with the University of New South Wales (UNSW), Sydney, Australia, from 2008 to 2010.

She has been a Research Associate with UNSW since 2011, where she is currently with the Capability Systems Center, School of Engineering and Information Technology. Her current research interests include space system engineering, GNSS navigation, spacecraft attitude determination and control systems, space operations and optimal estimation, and filtering design.