Secure-iGLU: A Secure Device for Noninvasive Glucose Measurement and Automatic Insulin Delivery in IoMT Framework

Amit M. Joshi
Electronics & Commu. Engineering
MNIT, Jaipur, India.
Email: amjoshi.ece@mnit.ac.in

Prateek Jain
Electronics & Commu. Engineering
MNIT, Jaipur, India.
Email: prtk.ieju@gmail.com

Saraju P. Mohanty
Computer Science and Engineering
University of North Texas, USA.
Email: saraju.mohanty@unt.edu

***Abstract*—The growth of healthcare technologies has made a great impact on human life for the last few years. Various innovations in implantable and wearable medical devices improve the quality of life. Internet-of-Medical-Things (IoMT) based smart healthcare with continuous sensing, connectivity, and automatic medication is the latest trend. With the growth of technologies and connectivity, the security of these devices is a growing concern. The security of medical devices is important as the security compromise may lead to critical situations. This paper explores the security aspect of the IoMT system with a non-invasive glucose monitoring device integrated with an insulin delivery system (called iGLU) as a specific example. We call this secure system as Secure-iGLU. The paper presents a Hardware-Assisted Security (HAS) paradigm using Physical Unclonable Function (PUF) to design Secure-iGLU. PUF is a useful primitive to generate fingerprint of the hardware, and it has a great potential to mitigate the security problem of iGLU. The simulation results confirm the security of our Secure-iGLU using PUF in IoMT with safe insulin delivery system.**

***Index Terms*—Smart Healthcare, Continuous Glucose Measurement, Automatic Insulin Delivery, CPS Security, Physical Unclonable Function (PUF), Hardware-Assisted Security (HAS), Security-by-Design (SbD)**

I. Introduction

An estimated 463 million adults worldwide have diabetes and addressing their quality of life through smart healthcare technologies can have significant social impact [1]. Diabetes occurs when the body of a person finds the difficulty to balance glucose level during various prandial states [2]. The main cause of the diabetes is deficiency of insulin level in the body against the generated glucose. The diabetes control may lead to the reduction of blood pressure and other cardiovascular disease. Thus, we focus on noninvasive glucose level monitoring and insulin delivery system.

The healthcare has evolved from traditional to telemedicine, connected-health (cHealth), e-health, mobile-health (mHealth), to smart health (sHealth) [3]. The demand for remote healthcare is getting important than ever as evident from the situations in the hospitals during the (COVID-19) outbreak [4]. Smart healthcare built using Internet-Medical-Things (IoMT) is a key component in smart cities which can provide better and advanced medical facilities to the patients [5]. Present Internet of Medical Things (IoMT) based solution for smart healthcare encourages hospitals to ameliorate the care quality with focusing on overall expenses reduction. Smart healthcare provides many advantages which are called 7Ps including personalized care and participatory care [3]. Overall, smart healthcare is evolving with the help of healthcare Cyber-Physical System (H-CPS) that integrates IoMT, electronic health record (EHR) which is essentially e-health, and artificial intelligence (AI) obtained from sensor data and/or EHR [6].

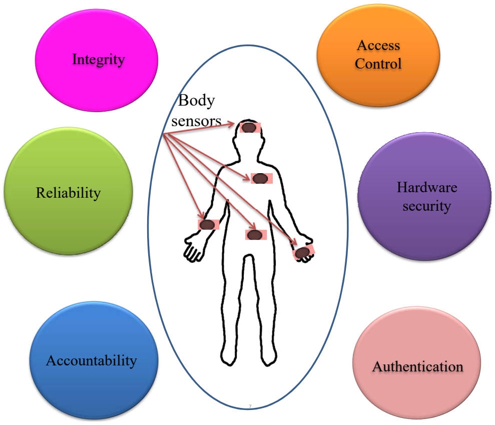


Fig. 1: Secure Body Area Network System.

Diabetes can be measured using non-invasive approach with wearable NIR sensors from the body. By using a non-invasive device iGLU for continuous blood glucose measurement, the patient can have a proper dose of insulin or other medications, and can control the blood glucose level during physical activities [7], [8]. In this process, the presence of diabetologist is necessary to provide the insulin doses when patient send data of blood glucose, plasma insulin and other glucose consumption parameters to provide precise treatment. There are different security vulnerabilities of body area network is shown in Fig. 1. The smart healthcare structure requires more security layers because of its connectivity with open network for the control of medical devices [9]. The security and privacy aspect of the IoMT based glucose-insulin control system has to play a vital role for reliable and efficient solution for diabetes control of the patient [10]. The proposed iGLU with insulin delivery mechanism is required to have secure and reliable insulin drug delivery mechanism which would be useful for hardware authentication of any node for the IoMT network.

Traditional cryptography schemes are not designed for IoMT security. Medical devices have constraints in terms of computational complexity, area, and power while continuously capturing various parameters such as, physiological and pharmacological parameters. It is required to design the security solution for medical device in IoMT framework where the access of such device is available in open environment, and the adversary may get the access to such devices [11]. The key of conventional cryptographic methods is stored in some non-volatile memory. The key is considered a secret and is out of the reach of adversary. The security is compromised when an unauthorized person gets access to the key. However, the basic principle of PUF concept is that hardware itself is memory where the random key is generated. It is vital to authenticate every potential medical devices (IoT nodes) in a IoMT framework where any security vulnerability may lead to the loss of patient's life. Therefore, there is a demand to develop a novel authentication mechanism which would be easily adapted to such low energy devices. Traditional cryptography methods are power hungry and sophisticated deeming them unsuitable for IoMT applications.

The rest of the paper is organized as follows. The security of the automatic glucose monitoring and control in IoMT have been discussed in Section II. The novel contribution of the paper has been summarized in Section III. The related works are discussed in Section IV. The results of the work are described in Section VI. Section VII presents conclusions and future directions.

II. Our Vision of Automatic Glucose Monitoring and Control in IoMT Framework - Secure iGLU

The secure framework of a insulin glucose control system is presented Fig. 2 [7], [8]. There are different levels of authentication for secure iGLU as follows: (1) The access control of the user by authentication for medical information of the patients stored data at the cloud. (2) Data encryption of the controller node for the device to the user from the channel. (3) The authentication of the hardware device (Glucometer, inlusin pump) for glucose insulin model. The paper provides hardware security solution through Physical Unclonable Function (PUF) for the medical devices of the network [12].

A Physical Unclonable Function (PUF) is mainly based on a physical system which is easier for evaluation (with the help of physical system) and is also unpredictable. It is a hardware primitive which can randomly extracts a secrete key (unique in nature) from a chip. Such generated key is helpful to authenticate the hardware module, and it is useful to identify the medical device (nodes) for the purpose of security in IoMT. Each hardware apparently has lots of process variations which are being introduced at the time of manufacturing process. It is impossible to clone two hardware by same design steps, with same packaging and manufacturing styles. Therefore a hardware module would increase its anti-cloning capability with help of PUF. PUF Security is based on the delays of wires and gates and quantum mechanical fluctuations. The characteristics of PUF are unique, reliable and unpredictable.

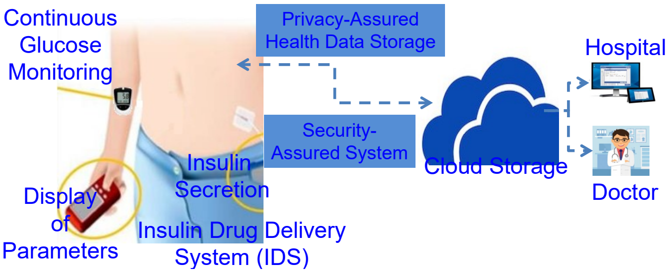

Continuous Glucose Monitoring
Privacy-Assured Health Data Storage
Hospital
Security-Assured System
Insulin Secretion
Cloud Storage
Doctor
Display of Parameters
Insulin Drug Delivery System (IDS)

Fig. 2: An Illustration of Secure iGLU for Noninvasive Glucose-Level Monitoring and Automatic Secure Insulin Delivery.

The PUF would be helpful to provide the hardware trust in IoMT framework. The secure iGLU is useful to create the environment where the glucose value is analysed properly of the diabetes patient. As per the measurement, the insulin dose is provided from insulin pump. The insulin drug delivery system defines the different parameters for glucose consumption for the accurate treatment of the remotely available diabetic patient. The data is mainly stored at the cloud server and it is to be analysed by diabetologist [13]. The diabetologist would take the decision of the insulin dose for the patent in terms of the amount and the time it should be taken. The diabetes patients would be provided automatic insulin treatment through remote location. The security of the insulin pump is very important because it would provide automatic injection of insulin. The malfunctioning of the pump would be harmful to the patient even cause the life of the patent if the insulin not being controlled properly or mishandled by any interpreter. The facility of security and reliability of the system would be helpful in smart healthcare system for diabetes control.

III. Novel Contributions of the Current Paper

The past few years have observed rapid growth in the cyber security threat for wearable and wireless medical devices. In 2015, FDA published article for cyber security risk and emphasized about security vulnerabilities of Hospira drug infusion pumps [14]. In 2016, Johnson & Johnson also issued warning regarding threats in the implantable product oneTouch insulin pump [15]. The communication between controlling node and medical device has also raised concern in smart healthcare. There is an increasing demand for the efficient security solution to remote operated medical devices. There is a growing requirement to build up robust methods to have secure devices and to maintain quality clinical practices. The paper covers the device authentication mechanism for the hardware security of our non-invasive glucose measurement device iGLU and the insulin delivery pump for the secure IoMT network.

In order to have secure solution for insulin doses, **a novel secure device for glucose measurement and automated insulin deliver system through IoMT (Secure-iGLU)** is presented in the paper. The propose secure IoMT is useful for instant diagnose and treatment of diabetic patients through proper dose control. The proposed secure device authentication protocol using PUF overcomes the limitations of traditional cryptographic techniques and has novel features as the following:

- Low-cost solution to authenticate the medical device for trusted hardware in IoMT.
- The secure way of communication among the devices using light weight protocol.
- Low power and area overhead protocol for hardware security in tiny nodes of IoMT.

IV. Related Prior Research Work

The security of the implantable and wearable medical devices (IWMDs) along with its secure communication is the area of concern from last decade. A comprehensive discussion of security for IoT has been presented in [9]. However, IoT security solutions are not directly applicable to IoMT. The security in IoMT has has energy constraints issues due to lack of computation resources and battery life [16]. Thus, a paradigm called "Hardware-assisted security (HAS)" is defined which is security provided by hardware for: (1) information being processed, (2) hardware itself, (3) overall system. HAS is subset of Security-by-Design or Secure-by-Design (SbD) which relies on integrating security right in the design phase of an system, rather than retrofitting [17]. This is most applicable for IoMT based smart healthcare devices. We discussed a selected security works for smart healthcare or IoMT in rest of this Section.

Wazid, et al. [18] presented three layer authentication between user and Implantable Medical Devices (IMD). They developed new user authentication approach where remote user and controller node can establish the authentication through the key for future communication. It included pairwise security mechanism from controller node to IMD.

Yasqoob, et al. [19] proposed risk assessment framework known as Integrated Safety, Security, and Privacy (ISSP) to evaluate the various levels of risk associated with medical devices and their control. It provided the systematic technique to calculate the risk and safety measurement for the medical devices in a network. Moreover, the framework was also able to provide privacy related risk for medical equipment manufacturers that do not comply Health Insurance Portability and Accountability Act (HIPAA) regulations.

Li, et al. [20] discussed security vulnerabilities of glucose monitoring and insulin secretion model. The paper showed passive and active attacks which could compromise the safety and privacy of the patent through reverse engineering. They proposed two possible solutions as remedy of the secure healthcare system with rolling-code cryptographic protocols and body coupled communications.

Bu, et al. [21] designed secure wireless communication channel which was able to protect IMDs against various attacks. They introduced low power and secure authentication protocol for third party access to medical devices through secure admission mechanism. The method was also able to detect the man in middle attack while secure communication between device and authorized person.

Yanambaka, et al. [22] developed device authentication method using PUF for IoMT network. The hybrid oscillator based Arbiter PUF was used to have enhanced robustness against the attacks. The solution was low power with not much extra overhead of area and required least memory for storage of the key.

The current work on Secure-iGLU presents the hardware security using PUF for the devices in the IoMT network. The paper has presented lightweight security module without addition burden of area and power. The solution would provide the secure and reliable process of glucose insulin model for diabetes control of the patient through IoMT.

V. Our Proposed Secure iGLU

This Section discusses the vision of proposed Secure-iGLU. It discusses algorithms proposed for its enrolment when an user first time uses it as well as authentication algorithm when later device communicates with the Secure-iGLU.

A. *Secure-iGLU Architecture*

The main components of secure iGLU are non invasive glucose measurement device (iGLU), insulin pump, controller node and central server. All these components are connected through IoMT network. In order to enable secure communication in IoT network, it is required to authenticate each device of the IoMT through reliable protocol. PUF provides the hardware trust, or device authentication to identify the medical device. The responses of each devices are recorded through challenges. Subsequently, the Challenge Response Pairs (CRPs) are stored at Edge-Datacenter (EDC) at the doctor or a central cloud server in large hospital. EDC and cloud datacenters are options when an user gets Secure-iGLU from a doctor. On the other hand, if an user gets Secure-iGLU individually and wants to activate and use, then cloud datacenter is the preferred option. These CRPs would be helpful later on to validate each node of the network. The architecture of the Secure-iGLU is illustrated in Fig. 3.

PUF provides disordered physical system where challenges (C_i) produce the corresponding response R_i where (C_i, R_i) tuples are generated for device authentication. PUF is designed in such a way that the responses depend on individual physical disorder of the hardware. Therefore, PUF response is function of challenge as well as physical disorder of each device. Hence, challenge-response pair would vary among different hardware for the same PUF. One CRP is not adequate to verify the identity of a chip. Therefore many CRPs are considered for the authentication purpose. Arbiter PUF is one of the silicon

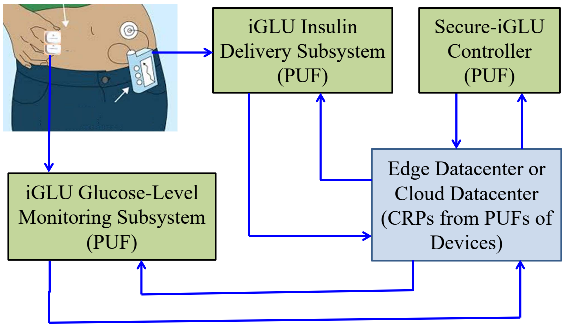

iGLU Insulin Delivery Subsystem (PUF)
Secure-iGLU Controller (PUF)
Edge Datacenter or Cloud Datacenter (CRPs from PUFs of Devices)
iGLU Glucose-Level Monitoring Subsystem (PUF)

Fig. 3: An Illustration of our Proposed Secure-iGLU with Hardware-Assisted Security using PUF.

type PUFs where a different response is generated for each device because of variability of the manufacturing. The main advantage of silicon PUF is that it would be able to capture the intrinsic variation of digital circuit which were established during the fabrication process at on-chip itself [23]. Arbiter PUF is useful PUF primitive and is considered in this work. The overall procedure is shown in Fig. 4. The path difference is being created for every challenge of the circuit which are excited at the same time. The comparison is made from the generated responses to result a value of 0 or 1 through the delays of path of the arbiter. There could be n such responses using same circuit with the duplication of n times, or with total n challenges. The PUF can be used as an unclonable key which would help as lock with database of challenge-response pairs. In order to open the lock, the key is required to have predefined response for many such types of challenges.

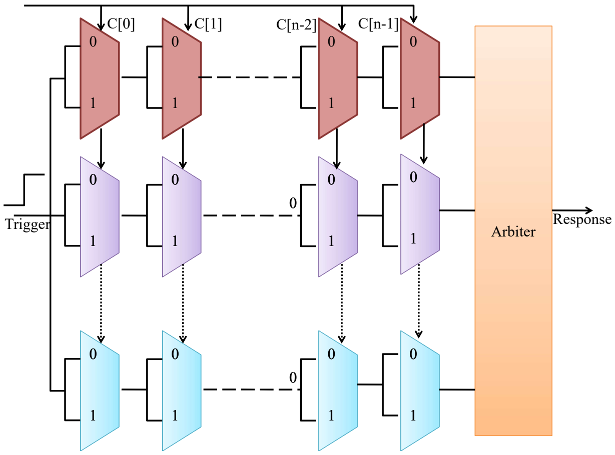


Fig. 4: Topology of an Arbiter based PUF.

B. PUF based iGLU Device Security

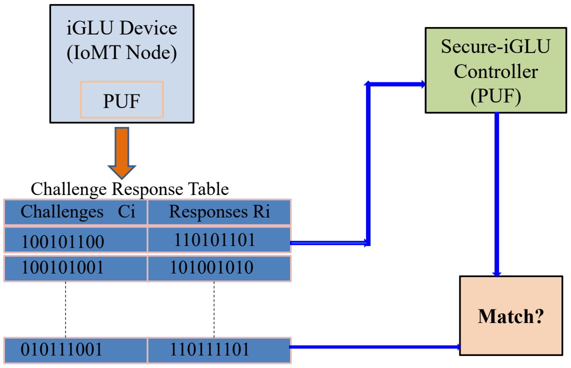
The device authentication protocol is developed to have a secure identification of a hardware for the claimed identity. The objective is to design a low-cost and lightweight authentication mechanism with the help of PUF. The proposed PUF based authentication comprises of mainly two phases: (a) Enrolment Phase and b) Authentication Phase.

1) PUF based Enrollment in Secure-iGLU: For Enrollment Phase, the challenges have been applied to PUF and their corresponding responses are collected in safe and secure environment at 25°C. It has been understand that Challenge Response Pairs (CRP) of the every device are stored at the Edge-Datacenter (EDC). These CRP pairs would be applicable for the hardware authentication for a trusted party, who has the ownership of the medical device. The steps of enrollment when Secure-iGLU is first time bought by an individual or installed with by a doctor is shown in Algorithm 1.

Algorithm 1 Enrollment Phase in Secure-iGLU.

```
for i=1 to K, where K is the number of devices do
Device sends request to the Edge-Datacenter (EDC) for the enrolment
EDC receives the request & assign unique ID to the device and shares same ID with the device
    EDC → $C_i$ to the device for the further process
Device receives $C_i$ and generates
    $R_i$ = PUF($C_i$)
For every randomly generated $C_i$ and corresponding $R_i$ collected by server
EDC stores CRPs table for the devices authentication in further phase.
end for
```

2) PUF based Authentication in Secure-iGLU: For the authentication phase, the response corresponding to the specific challenge is always matched with response at the Edge-Datacenter (EDC) for the same challenge in order to verify the device. Each medical device is labelled with its unique ID which is eventually being assigned to every hardware of the IoMT network. The authentication phase is defined in Fig. 5. The security is enhanced by sending challenge in some encryption format to the device. The steps of authentication is presented as Algorithm 2.



Challenges Ci	Responses Ri
100101100	110101101
100101001	101001010
010111001	110111101

Fig. 5: Illustration of Authentication in Secure-iGLU.

For thorough validation, we applied hundreds of challenges to PUF of Secure-iGLU in order to verify the authenticity of the device. Every time, the output responses are compared with stored responses. If the response bits are matched with the stored response bits then authentication process continues N number of times otherwise it would stop immediately with unauthenticated device. The values of N defines total

Algorithm 2 The Proposed Algorithm for Authentication in Secure-iGLU.

```
for i=1 to N do
  Edge-Datacenter (EDC) generate random number generator R.
  EDC is required to send
      $E \leftarrow R$ xor $ID$
  Here, ID is unique ID of each device.
  The device would receive the E and extract R using ID.
  EDC has to send again
      $E^{'} \leftarrow R$ xor $C_i$
  where $C_i$= Challenges
  Device now receives $E^{'}$ and it would extract $C_i$ with the help of R.
  Now device generates its own response $R_i^{'}$, and device would send
      $E^{''} \leftarrow R$ xor $R_i^{'}$
  This time EDC would extracts $R_i^{'}$ from the received $E^{''}$ using R.
  Now, the EDC will compare $R_i^{'}$ with stored $R_i$ in the database.
      if $R_i^{'}$ = $R_i$ then
  the process of the authentication is continued
  else
  the device is unauthenticated and process stops here
      end if
  end for
```

challenges which are to be sent from server to devices and it also depends on total number of the devices in the network.

It is to be noted that most of PUFs are vulnerable towards machine learning (ML) attacks and Arbiter PUF would also fail to provide the resilience against attacks such as artificial neural network and various regression models [24]. However, the proposed method has used initial encryption techniques where challenges are not sent in original form but they sent through hash of the device ID in order to improve the robustness against such types of attacks.

VI. Experimental Results

The performance of the proposed secure iGLU is measured with qualitative parameters such as Uniqueness, Uniformity, Reliability and Bit Aliasing and are shown in Table I along with details of the experiment setup. For the experimental purpose, the performance of arbiter PUF has been evaluated on total forty FPGA boards whereas twenty boards of Xilinx Nexys 4 DDR boards (XC7A100T-1CSG324C) and twenty boards of Xilinx Basys 4 boards (XC7A100T-1CSG324C). The Block RAM is used for storing the Challenge Response pairs (CRPs). The responses for various challenges are collected for each board. The design of PUF is implemented on both FPGA boards and testing is done at 25°C. The hardware-software co-interface is designed to verify the results and constraints are also applied through TCL and MATLAB scripts.

The responses of arbiter PUF are recorded using Integrated Logic Analyzer of Xilinx. The arbiter PUF is required to have a symmetric routing. The manual routing concept is applied for the specific placement of PUF block on FPGA. Using XDC macro the length of the routing and placement of design on FPGA board and slice number is fixed by putting constraint in XDC file during implementation. Hence when arbiter PUF is implemented, there is no change in routing length occurs that affects the responses. A total of 256 challenges are applied and 256 responses are obtained for every chip. The inter chip-Hamming Distance is observed around 0.45.

TABLE I: Experimental Analysis of Secure iGLU.

PUF Implementation - Field Programmable Gate Array - Device Family Nexys 4 DDR and Basys (Artix 7)

Parameters	**64 Stages Arbiter(%)**	**256 Stages Arbiter(%)**
Uniqueness	45	42
Uniformity	58	60
Bit Aliasing	52	53
Reliability (25°C)	97	95

Reliability metric is an indicator of the responses from the PUF under different operating conditions. The reliability is calculated to evaluate the variation of PUF responses under various environmental conditions. The reliability is measured with intra-chip hamming distance that shows mainly as the response bits are flipped at environmental variation. Table II shows the reliability of 256-bit Arbiter PUF at different temperatures.

The uniqueness is very important parameter which ensures that the responses of the two devices are not same while same challenges are applied. The uniqueness is similar as inter-chip hamming distance. Total 20 FPGAs are considered to compute the inter-chip hamming distance. PUF is able to generate a random signature from a digital circuit. Moreover, the circuit has some device manufacturing variations those are uncontrolled and always prone to environmental noise. Therefore, the performance of arbiter PUF may vary, which could result in the random flipping of bits.

TABLE II: Reliability of Arbiter PUF in iGLU.

Temperature	**Intra HD**	**Reliability**
15°C	0.42	93.8
20°C	0.43	94.2
25°C	0.45	95
30°C	0.43	92.5

Table III shows the comparison of the proposed work with previous similar work for IoMT framework. These works use a variety of security mechanisms and hence a fair comparison is difficult. The results show that the proposed work focuses on hardware security of medical devices for insulin drug delivery system for secure iGLU.

VII. Conclusions and Future Research

This paper described a secure iGLU with automatic diabetes control mechanism for insulin secretion, where continuous glucose monitoring is performed with IoMT framework. This secure iGLU proposes an efficient insulin drug delivery system. The proposed method is useful to provide hardware security of the medical devices of IoMT framework and it has been implemented and verified on 28 nm-technology Xilinx FPGA boards. Total 40 FPGA boards of two family (Nexys 4 DDR and Basys) are considered to measure the

TABLE III: Related Work for Security of Medical Devices.

Previous Work	**Technologies**	**Applications**	**Details**
Li, et al. (2011) [20]	Rolling Code	Medical devices of IoMT	Insulin pump
Abdmeziem, et al. (2014) [25]	Key management	Tiny sensor nodes	Authentication and strong encryption
Gong, et al. (2015) [26]	Light weight scheme; DES	Data transmission	Encryption for small IoT nodes
Li, et al. (2016) [27]	Authentication method	Emergency for medical systems using mobile	Confidentiality of medical record
Hu, et al. (2017) [28]	Cloud computing	Physiological data collection of elder people	Minimum usage of medical resource
Yanambaka, et al. (2019) [22]	PUF based Authentication	Device Security	Edge Computing
Proposed Work (Secure-iGLU)	PUF based Authentication	Medical devices of IoMT	Hardware security iGLU with insulin drug delivery

response bits. The performance results reveal that proposed device authentication protocol is suited for hardware security for medical devices of secure iGLU.

In future, we would focus on other security aspects of iGLU such as user authentication and cloud security. Future research will involve security protocols tolerant to ML attacks. The reliability of the system could be improved by incorporating error correction mechanism. We will work on real-time wearable glucose measurement device to provide secure and reliable glucose monitoring of the human body.

References

[1] I. D. Federation, "IDF Diabetes Atlas - Diabetes is rising worldwide... and is set to rise even further," 2019, last Accessed on 21 March 2020. [Online]. Available: https://diabetesatlas.org/en/sections/worldwide-toll-of-diabetes.html

[2] H. Yin, B. Mukadam, X. Dai, and N. Jha, "DiabDeep: Pervasive Diabetes Diagnosis based on Wearable Medical Sensors and Efficient Neural Networks," *IEEE Transactions on Emerging Topics in Computing*, no. 10.1109/TETC.2019.2958946, pp. 1–1, 2019.

[3] H. Zhu, C. K. Wu, C. H. KOO, Y. T. Tsang, Y. Liu, H. R. Chi, and K. Tsang, "Smart Healthcare in the Era of Internet-of-Things," *IEEE Consumer Electronics Magazine*, vol. 8, no. 5, pp. 26–30, Sep 2019.

[4] A. K. Tripathy, A. G. Mohapatra, S. P. Mohanty, E. Kougianos, A. M. Joshi, and G. Das, "EasyBand: A Wearable for Safety-Aware Mobility during Pandemic Outbreak," *IEEE Consumer Electronics Magazine*, no. 10.1109/MCE.2020.2992034, pp. 1–1, 2020.

[5] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything you wanted to know about smart cities: The Internet of things is the backbone," *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60–70, July 2016.

[6] M. Ghamari, B. Janko, R. Sherratt, W. Harwin, R. Piechockic, and C. Soltanpur, "A Survey on Wireless Body Area Networks for eHealthcare Systems in Residential Environments," *MDPI Sensors*, vol. 16, no. 6, p. 831, Jun 2016.

[7] P. Jain, A. M. Joshi, and S. P. Mohanty, "iGLU: An Intelligent Device for Accurate Non-Invasive Blood Glucose-Level Monitoring in Smart Healthcare," *IEEE Consumer Electronics Magazine*, vol. 9, no. 1, p. Accepted, January 2020.

[8] P. Jain, A. M. Joshi, N. Agrawal, and S. P. Mohanty, "iGLU 2.0: A New Non-invasive, Accurate Serum Glucometer for Smart Healthcare," *arXiv Electrical Engineering and Systems Science*, vol. abs/2001.09182, 2020. [Online]. Available: http://arxiv.org/abs/2001.09182

[9] A. Mosenia and N. K. Jha, "A Comprehensive Study of Security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, Oct 2017.

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

[11] R. AlTawy and A. M. Youssef, "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices," *IEEE Access*, vol. 4, pp. 959–979, 2016.

[12] A. Jain and A. M. Joshi, "Device Authentication in IoT using Reconfigurable PUF," in *Proc. 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM)*, 2019, pp. 1–4.

[13] P. Jain, S. Pancholi, and A. M. Joshi, "An IoMT Based Non-Invasive Precise Blood Glucose Measurement System," in *Pro. IEEE International Symposium on Smart Electronic Systems (iSES)*, 2019, pp. 111–116.

[14] U. Food and D. Administration, "Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication," *Silver Spring, Maryland (www. fda. gov/MedicalDevices/Safety/AlertsandNotices/ucm456815. htm)*, 2015.

[15] J. Finkle, "J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking," Reuters, 2016.

[16] S. P. Mohanty, "Security and Energy Trade-Offs in Smart City Cyber-Physical Systems," 2019, last Accessed on 21 March 2020. [Online]. Available: http://www.smohanty.org/Publications_Conferences/2019/Mohanty_ISC2-2019_Keynote-Abstract_Smart-City-CPS-Security.pdf

[17] S. P. Mohanty, "Security and Privacy by Design is Key in the Internet of Everything (IoE) Era," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 4–5, March 2020.

[18] M. Wazid, A. K. Das, N. Kumar, M. Conti, and A. V. Vasilakos, "A novel authentication and key agreement scheme for implantable medical devices deployment," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 4, pp. 1299–1309, 2017.

[19] T. Yasqoob, H. Abbas, and N. Shafqat, "Integrated Security, Safety, and Privacy Risk Assessment Framework for Medical Devices," *IEEE Journal of Biomedical and Health Informatics*, no. 10.1109/JBHI.2019.2952906, 2019.

[20] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *Proc. IEEE 13th International Conference on e-Health Networking, Applications and Services*, 2011, pp. 150–156.

[21] L. Bu, M. G. Karpovsky, and M. A. Kinsy, "Bulwark: Securing implantable medical devices communication channels," *Computers & Security*, vol. 86, pp. 498–511, 2019.

[22] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, and D. Puthal, "PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, 2019.

[23] Q. Wang and G. Qu, "A Silicon PUF Based Entropy Pump," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 3, pp. 402–414, 2018.

[24] J. Delvaux, "Machine-Learning Attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUFFSMs," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2043–2058, 2019.

[25] M. R. Abdmeziem and D. Tandjaoui, "A cooperative end to end key management scheme for e-health applications in the context of internet of things," in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2014, pp. 35–46.

[26] T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, "A medical healthcare system for privacy protection based on IoT," in *Proc. Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP)*, 2015, pp. 217–222.

[27] C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *Journal of Medical Systems*, vol. 40, no. 5, p. 117, 2016.

[28] J.-X. Hu, C.-L. Chen, C.-L. Fan, and K.-h. Wang, "An Intelligent and Secure Health Monitoring Scheme using IoT Sensor based on Cloud Computing," *Journal of Sensors*, vol. 2017, no. 10.1155/2017/3734764, p. 3734764, 2017.