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

Amit M. Joshi[1], Prateek Jain[2] and Saraju P. Mohanty[3]

Malaviya National Institute of Technology, Jaipur, India. [1,2]

University of North Texas, Denton, TX , USA.[3]

Email: amjoshi.ece@mnit.ac.in[1], prtk.ieju@gmail.com [2], saraju.mohanty@unt.edu[3]

Outline of the Talk

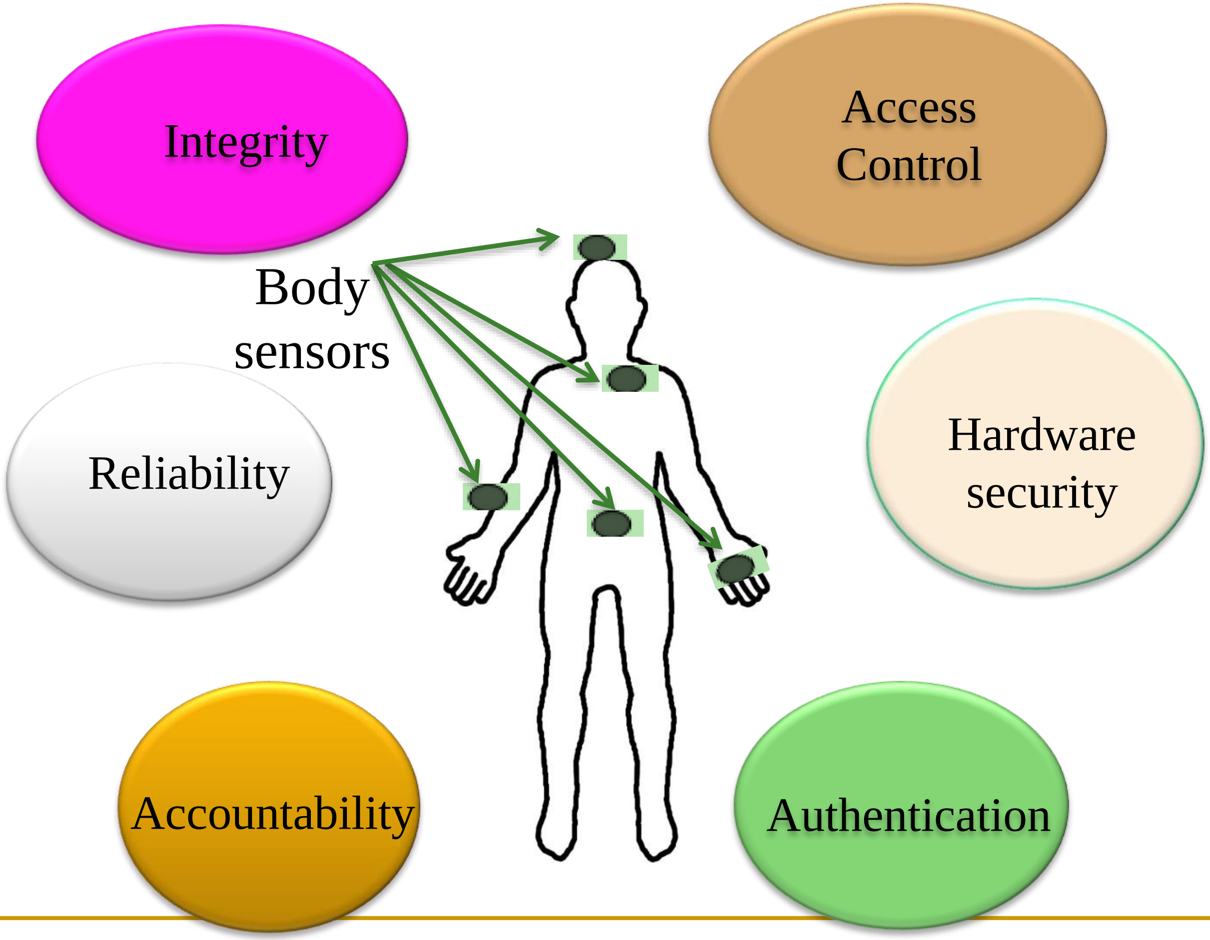
- Introduction
- Role of Security in Medical Devices
- Secure iGLU for automatic Glucose Control
- Hardware Security using PUF
- Related Work
- Proposed Secure iGLU
- Proposed Automatic Glucose Control model
- Simulation and Results
- Conclusions and Future Research

Motivation for Diabetes Control

- Around 463 million adults worldwide have diabetes and addressing their quality of life through smart healthcare technologies can have significant social impact.
- Diabetes occurs when the body of a person finds the difficulty to balance glucose level during various prandial states
- The diabetes control may lead to the reduction of blood pressure and other cardiovascular disease
- 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
- The smart healthcare structure requires more security layers because of its connectivity with open network for the control of medical devices

Secure Body Area Network

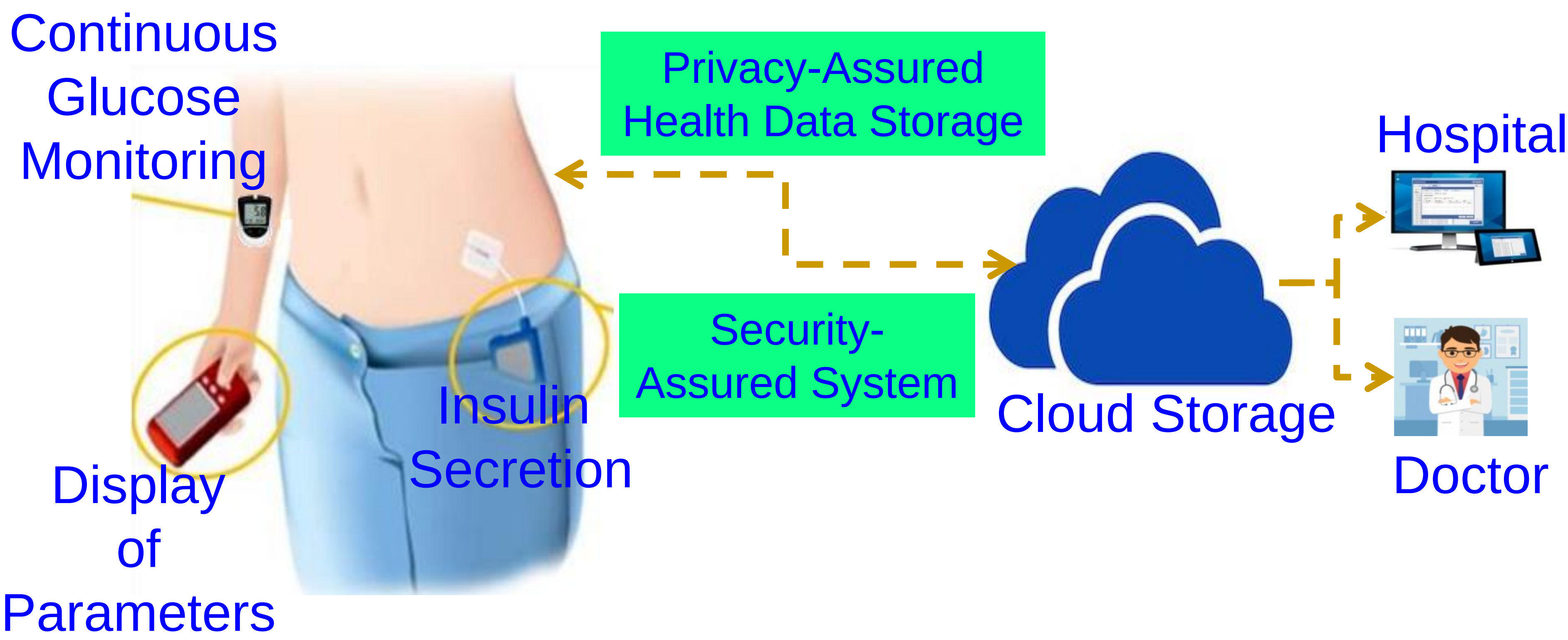
- There are different security vulnerabilities of body area network



Role of Security for Medical Devices

- 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 parameter
- The key of conventional cryptographic methods is stored in some non-volatile memory and 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

Secure iGLU for Automatic Glucose Control



Hardware Security using PUF

- 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.
- 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.
- It is helpful to authenticate the medical device (nodes) for the purpose of security in IoMT

Secure Glucose Monitoring in IoMT Framework

- PUF would 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

Novel Contribution of the Paper

- A novel secure device for glucose measurement and automated insulin deliver system through IoMT (Secure-iGLU) is presented in the paper
- The proposed secure device authentication protocol using PUF overcomes the limitations of traditional cryptographic techniques
- 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.

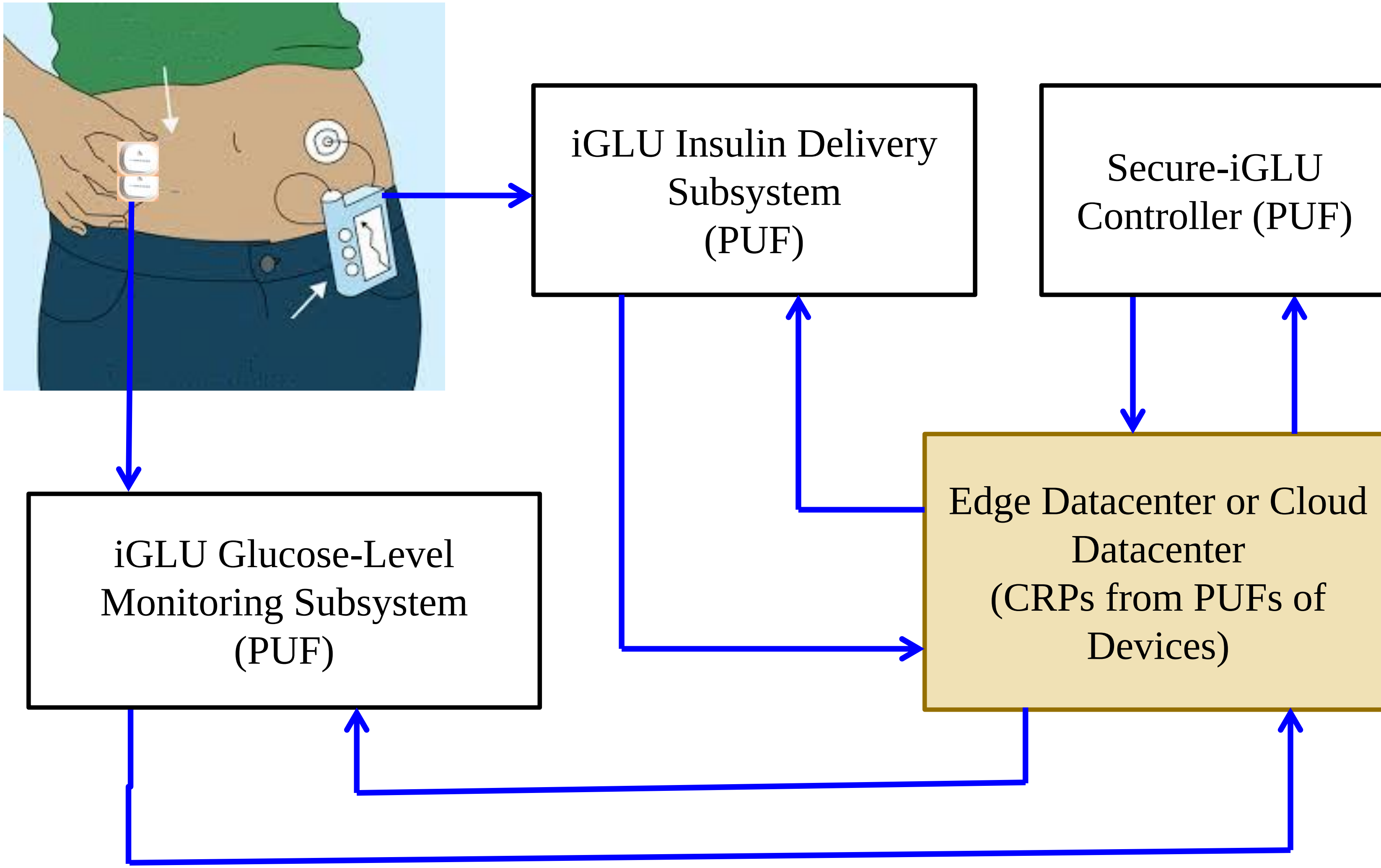
Related Prior Research Work

- Hardware-assisted security (HAS) are for: (1) information being processed, (2) hardware itself, (3) overall system. HAS is subset of Security-by-Design or Secure-byDesign (SbD) which relies on integrating security right in the design phase of an system, rather than retrofitting [17].
- 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

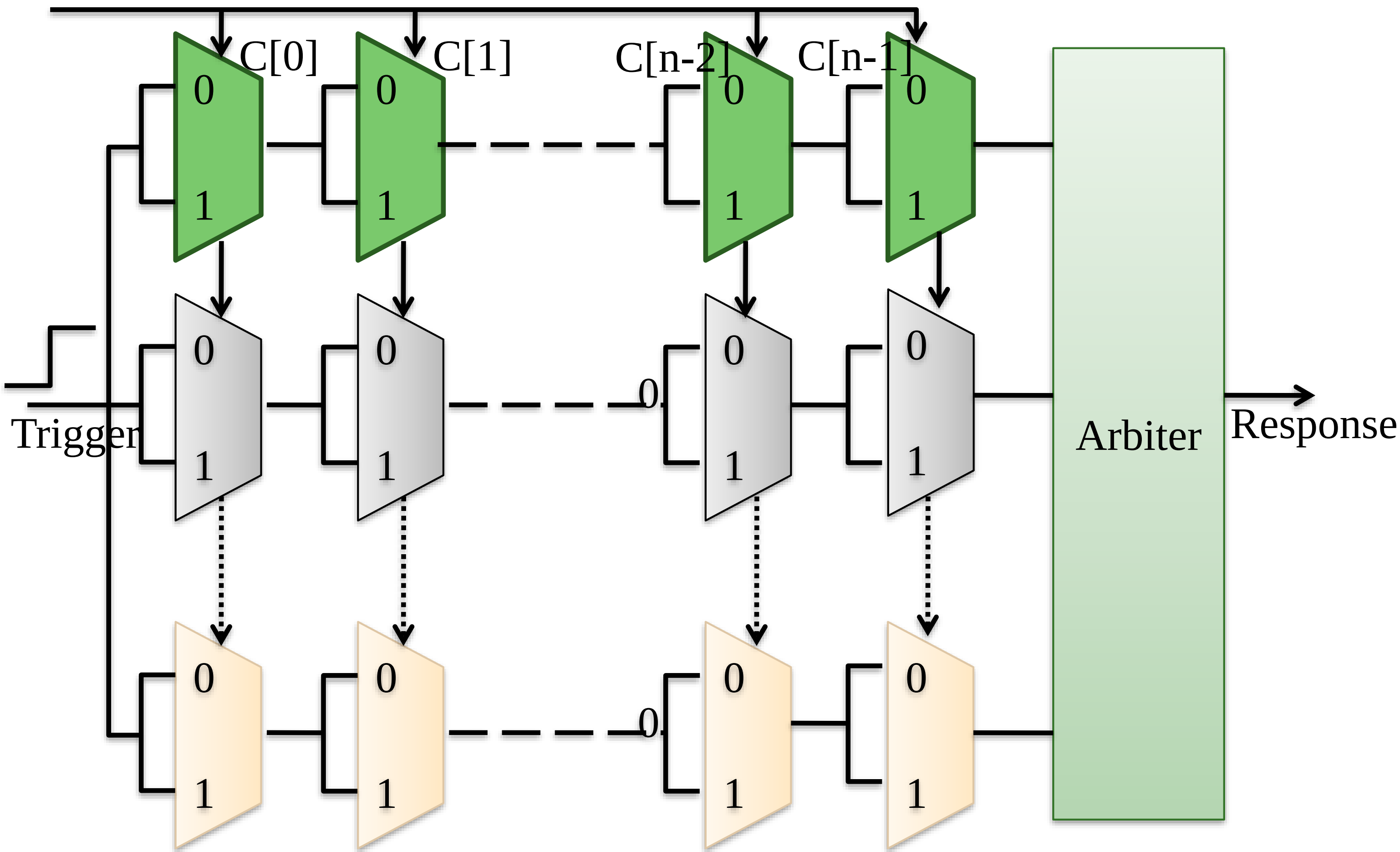
Related Prior Research Work

- 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.

Proposed Secure iGLU



Arbiter PUF for Secure iGLU

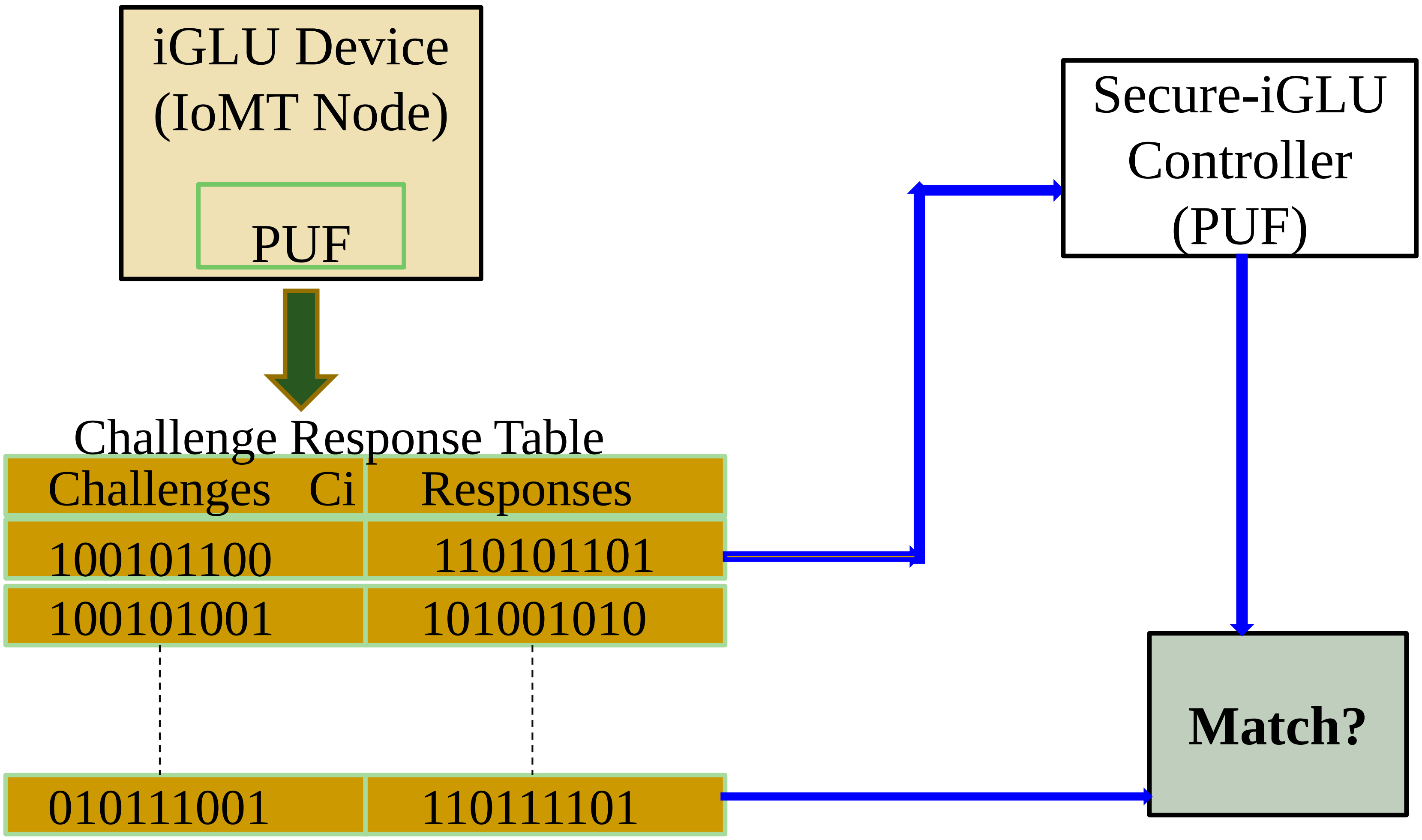


PUF based iGLU Security

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 $\rightarrow C_i$ 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

Authentication Mechanism in Secure iGLU



Authentication Phase of Secure iGLU

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

Experimental results

- The performance of the proposed secure iGLU is measured with qualitative parameters such as Uniqueness, Uniformity, Reliability and Bit Aliasing.
- 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 *degree* C. The hardware-software co-interface is designed to verify the results and constraints are also applied through TCL and MATLAB scripts.

Performance Evaluation of Secure iGLU

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

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

Comparison with Related Work

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

Conclusion

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

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/2001.0918

References

[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 CyberPhysical 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 onsumer 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 HealthInformatics, vol. 22, no. 4, pp. 1299–1309, 2017

References

[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 PUF–FSMs,” 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

Thank You !!!