PMsec: PUF-Based Energy-Efficient Authentication of Devices in the Internet of Medical Things (IoMT)

Venkata P. Yanambaka
College of Science and Engineering
Central Michigan University, USA.
Email: yanam1v@cmich.edu

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

Elias Kougianos
Electical Engineering
University of North Texas, USA.
Email: elias.kougianos@unt.edu

Deepak Puthal
School of Computing
Newcastle University
Email: Deepak.Puthal@newcastle.ac.uk

Laavanya Rachakonda
Computer Science and Engineering
University of North Texas, USA.
Email: rl0286@unt.edu

***Abstract*—This is an extended abstract for Research Demo Session based on our published article [1]. One of the major vulnerabilities of the Internet of Medical Things (IoMT) devices is identity spoofing. As a solution, a device authentication protocol is presented in this paper which authenticates the devices in the network without storing the information in the memory. Physical Unclonable Functions (PUFs) are used for giving a unique identity to each device present in the network and for being authenticated when transmitting the data to the server.**

I. Introduction

The healthcare industry is rapidly taking advantage of technological advancements. The market for smart healthcare systems is ever growing [2], [3]. Currently, off the shelf components have communication capabilities which make them ideal for developing IoMT applications. Patient data can be remotely collected and delivered to the doctor for further diagnosis and, in some cases, a possible treatment. But that makes them vulnerable to various attacks, one of them being identity spoofing or impersonation attacks [1].

Fig. 1 shows various threats on consumer electronic systems. IoMT devices such as an insulin pump can be configured remotely through remote control. An attacker can impersonate the remote control and send a malicious configuration to the device turning it into a potential threat to the consumer, where in some cases, it becomes lethal [4]. This paper presents a device authentication protocol for a network of IoMT devices which can increase the security of the system thereby making the network resistant to such attacks.

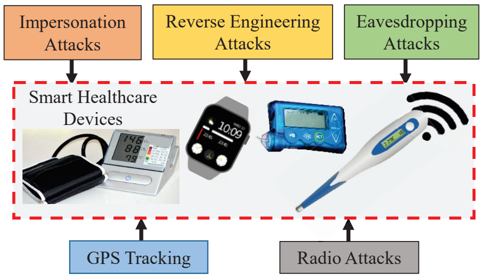


Fig. 1: Attacks on Consumer Electronic Systems.

II. PMsec: PUF Based Device Authentication

Physical Unclonable Functions (PUFs) are used for generating cryptographic keys [1]. A PUF uses the manufacturing variations that are introduced into an Integrated Circuit (IC) during its fabrication. The variations are unpredictable, uncontrollable, unavoidable and natural [5]. Hence the keys that are generated using the PUF module are also naturally random and are unique to the respective PUF module. Different PUF architectures were proposed by researchers around the world for integration into different environments. A Hybrid Oscillator Arbiter PUF proposed in [5] is used for PMsec, the PUF based device authentication protocol. Fig. 2 shows the overall concept of the PUF based security in an Edge Computing Paradigm.

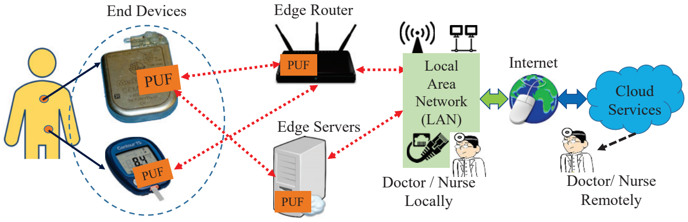


Fig. 2: Proposed PUF Based Security in Edge Computing Paradigm of IoMT.

In the PMsec approach, every device in the network will have a PUF module embedded in it. They are responsible for generating unique identities for the IoMT devices and the servers that are present in the network. The device authentication protocol involves two phases, the enrollment phase and the authentication phase.

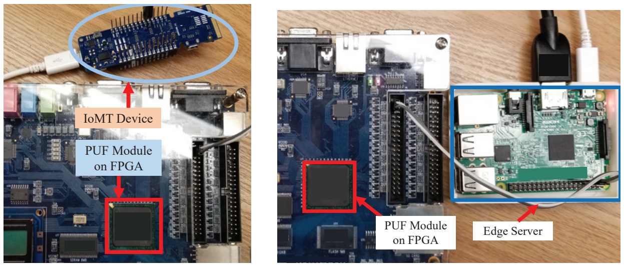
A. Enrollment and Authentication Phase

The Enrollment phase of the protocol occurs when a new device has to be introduced into the network. During this phase, the PUF module in the end device will be accessed by the server and the keys are securely enrolled. Initially, a challenge input $C1$ is given to the PUF module at the server and a response $R1$ is generated. This response ($R1$) is given as a challenge input to the PUF module at the end device and the response from it, $R2$ is generated. $R2$ is then transmitted to the PUF module at the server and given as a challenge input for a second time. Once the response $R3$ is generated, a hash of it is computed, $X = H(R3)$. This hash X and challenge input $C1$ are stored in a secure database. This process is repeated and the respective challenge input and the hashes are stored in the database for authenticating at a later time period.

Once the enrollment phase is complete, the device can be securely authenticated following similar steps during the enrollment phase. During authentication, the challenge $C1$ and the respective X from the secure database are collected. The challenge input is given as PUF input at the server and the process is followed to generate the hash, X' for the device in question. If the hash matches X, stored in the database, the device is authenticated.

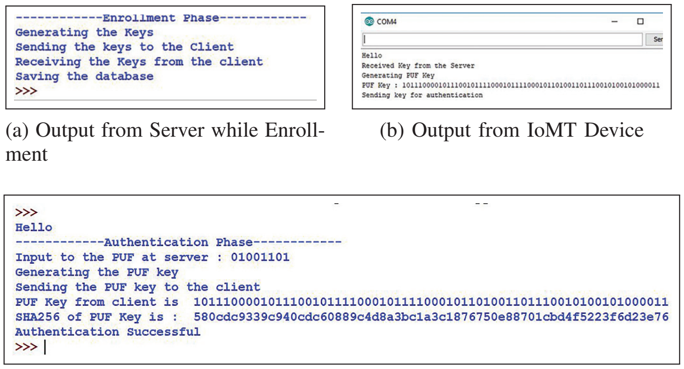
III. Implementation of PMsec

Fig. 3 shows the experimental setup for the prototype of PMsec. The PUF module was developed on an FPGA. The single board computer was the server and the microcontroller was the end device. The single board computer was the low power device and capable of performing the basic cryptographic functions, such as hash, which are necessary for the PMsec protocol. The microcontroller is connected to the FPGA for the keys generated by the PUF module. Fig. 4 shows the outputs from the single board computer and the microcontroller during the enrollment and authentication phases.



(a) IoMT Device with PUF (b) Edge Server with PUF

Fig. 3: Validation of PMSec in a Consumer Electronics Environment [1].



```
------------Enrollment Phase------------
Generating the Keys
Sending the keys to the Client
Receiving the Keys from the client
Saving the database
>>>
```

(a) Output from Server while Enrollment

```
Hello
Received Key from the Server
Generating PUF Key
PUF Key : 1011100001011100101111000101111000101101001101110010100101000011
Sending key for authentication
```

(b) Output from IoMT Device

```
>>>
Hello
------------Authentication Phase------------
Input to the PUF at server : 01001101
Generating the PUF key
Sending the PUF key to the client
PUF Key from client is  1011100001011100101111000101111000101101001101110010100101000011
SHA256 of PUF Key is :  580cdc9339c940cdc60889c4d8a3bc1a3c1876750e88701cbd4f5223f6d23e76
Authentication Successful
>>> |
```

(c) Output from Server during Authentication

Fig. 4: Validation of the Proposed Authentication Scheme [1].

The results obtained from prototyping the board are tabulated in Table I. The time taken for authenticating the device is 1.5 sec and the error rate is 10%. The overall power consumption of the system can be reduced by integrating more power efficient PUF designs into the protocols. With the device or the server side PUF module in hand, performing various attacks on the system will be challenging. As no information regarding the device is directly stored on the server database, this adds an extra layer of security to the environment.

TABLE I: Characterization of the Proposed PMsec [1]

Parameters	**Specific Values**
Server	Single Board Computer
End Device	32-bit Microcontroller based development board
Key generation time at Server	800 ms
Key generation time at IoMT Device	800 ms
Time for Authentication of Device	1.2 sec - 1.5 sec
Error Rate	10 %

IV. Conclusions

This paper presents a PUF based device authentication protocol capable of authenticating devices without demanding high processing power from the end devices. This protocol can be used irrespective of the communication protocol between the end device and the server. No information regarding the end device is directly stored on the server, which adds an extra layer of security for the environment.

Acknowledgment

This is an extended abstract for a demo at the Research Demo Session of iSES 2019 based on our article [1].

This material is based upon work supported by the National Science Foundation under Grant Nos. OAC-1924112. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] 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, Aug 2019.

[2] L. Rachakonda, P. Sundaravadivel, S. P. Mohanty, E. Kougianos, and M. Ganapathiraju, “A Smart Sensor for Stress Level Detection in IoMT,” in *Proceedings of the 4th IEEE International Symposium on Smart Electronic Systems (iSES)*, December 2018, pp. 141–145.

[3] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco, “RFID Technology for IoT-Based Personal Healthcare in Smart Spaces,” *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 144–152, April 2014.

[4] C. Li, A. Raghunathan, and N. K. Jha, “Hijacking an Insulin Pump: Security Attacks and Defenses for a Diabetes Therapy System,” in *Proc. IEEE Int. Conf. e-Health Networking, App. and Serv.*, June 2011, pp. 150–156.

[5] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, “Novel FinFET based Physical Unclonable Functions for Efficient Security in Internet of Things,” in *Proc. IEEE Int. Symp. Nanoelect. Inf. Sys. (iNIS)*, 2016, pp. 172–177.