PMsec: Physical Unclonable Function-Based Robust and Lightweight Authentication in the Internet of Medical Things

Venkata P. Yanambaka, *Member*, IEEE, Saraju P. Mohanty, *Senior Member*, IEEE, Elias Kougianos, *Senior Member*, IEEE, and Deepak Puthal, *Member*, IEEE

***Abstract*—Various commercial off-the-shelf components are available for the development of communication-enabled consumer electronics devices. This opens new doors to attackers who can take advantage of various vulnerabilities to attack the entire network and compromise the integrity of the s environment. If a malicious device enters the en the attacker gains access to the server or transmits to the server or cloud, the entire network can b To avoid such cases, this paper presents a device scheme which uses Physical Unclonable Functio is suitable for Internet-of-Medical-Things (IoM advantage of this authentication scheme is that n to the IoMT devices are stored in server memory. to authenticate the devices completely was 1.2 se Hybrid Oscillator Arbiter Physical Unclonable Fun for validation of the proposed authentication sch PUF module used during experimental validatio of keys that could be potentially used for the protocol from each design is approximately 240. authentication scheme increases the robustness while being lightweight to be deployed in variou supports scalability.**

***Index Terms*—Smart Homes, Smart Healthcar Medical-Things (IoMT), Wearable CE, IoT Sec Unclonanle Function (PUF)**

I. Introduction

Consumer Electronic (CE) devices are becoming more capable of performing complex tasks with ease compared to their predecessors. This has become a reality with the introduction of the Internet of Things (IoT). With the technological advancements and the development of high performance, low power devices, implementing an IoT environment is simple and easy [1–3]. The IoT finds applications in various domains including but not limited to Smart Home, Smart Healthcare, Military and Industrial [3–6].

Smart healthcare devices have great demand and market [7, 8]. Fig. 1 shows some applications and span of the Internet of Medical Things (IoMT). Various parameters pertaining to the health of a person can be collected automatically and transmitted to the cloud for post processing with the help of IoMT devices. All the IoMT devices are connected to the network by various methods wired or wireless which gives them communication capabilities and in many cases makes them mobile [9].

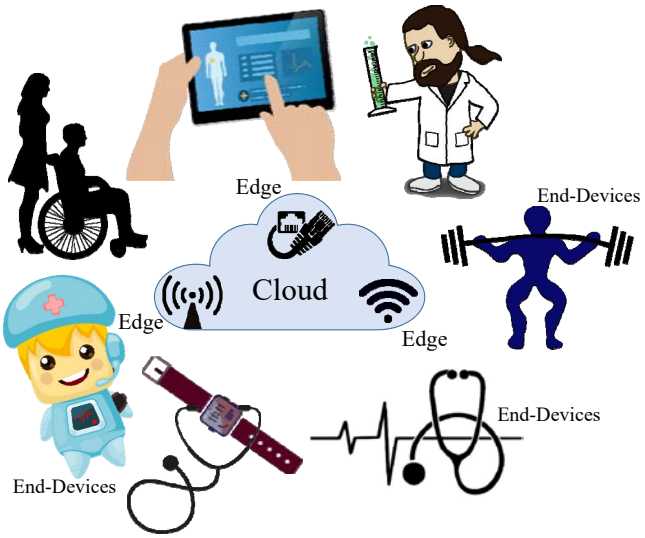


Fig. 1: The Internet of Medical Things (IoMT).

IoMT devices need to perform various tasks and must last longer without the change of a power source or a battery. This makes it difficult to implement various security measures including the implementation of cryptographic techniques [10, 11]. With various IoT devices connected to the network, most of them are vulnerable to various kinds of attacks [12–14]. Cloud services are used for the storage of data and the post processing. In the case of a Smart Healthcare, the devices are monitoring the health of patients and various parameters [15]. The collected data are used for the diagnosis of the patient. In some cases, the Smart Healthcare devices can be used for administering necessary drugs to the patient, for example, insulin. If such devices are attacked and the adversary gains control over the system, the patient could potentially come into danger. This paper presents a device authentication scheme, "PMsec" which defeats such attacks and helps maintain the integrity of the system. Physical Unclonable Functions (PUFs) are used for the design of PMsec. PUFs are used for generating cryptographic keys with the help of hardware, which reduces the demands on the processor.

V. P. Yanambaka is with the School of Engineering and Technology, Central Michigan University, E-mail: yanam1v@cmich.edu.

S. P. Mohanty is with the Department of Computer Science and Engineering, University of North Texas, E-mail: saraju.mohanty@unt.edu.

E. Kougianos is with the Department of Engineering Technology, University of North Texas, E-mail: elias.kougianos@unt.edu.

D. Puthal is with the School of Computing, Newcastle University, Email: Deepak.Puthal@newcastle.ac.uk.

The rest of the paper is organized as follows: Section II presents an overview of how smart consumer electronics are targeted by attackers and related research presenting solutions for attacks. Section III presents the novel contributions of the paper. Section V presents the design of Hybrid Oscillator Arbiter PUF. Section VI presents the implementation details. Conclusion and future research are presented in Section VII.

II. Security in Smart Healthcare Consumer Electronics - An Overview

A. Security Threats

There have been developments in Smart Healthcare technologies which help users keep track of their health. These devices also comprise of various Consumer Electronic devices, as shown in Fig. 2 and are connected in the context of IoMT. The communications capability of the CE devices (including wrist watch, and blood pressure monitor) is becoming a serious concern due to security vulnerabilities. For example, there have been successful attacks on insulin pumps which compromises the health and safety of their user [10, 17]. Wireless communication channels, often lacking the necessary cryptographic protection, are becoming a target of attackers. Initially, the adversary monitors the packets transmitted between the medical devices on the patient and the controller. Using the data gained, the adversary will be capable of reverse engineering the data and obtain the PIN of the controller and the device itself. This allows the adversary to impersonate the controller and send signals to the medical device and attack the patient. Fig. 2 presents several different possible scenarios of attacks [10, 19, 20].

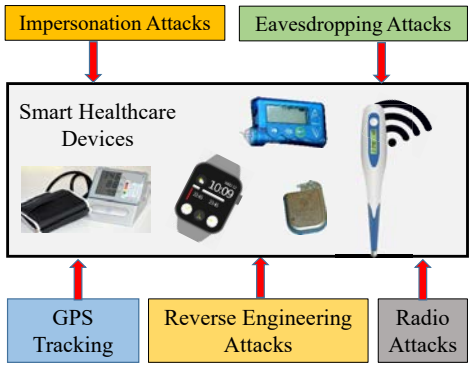


Fig. 2: Attacks on Consumer Electronic Systems.

Security threats against different devices connected to the network are not new. Fig. 3 shows some of the security threats and vulnerabilities that are possible on a smart consumer electronic device, in the IoMT context in particular.

When it comes to the IoT, the number of devices connected to the network can potentially reach trillions. The devices that are connected to the IoT network or present in the environment are of different types, categories and are made of different architectures manufactured or fabricated by different manufacturers. This presents a challenge for security, which increases the number and varieties of vulnerabilities in the entire environment. The IoT also must be protected against

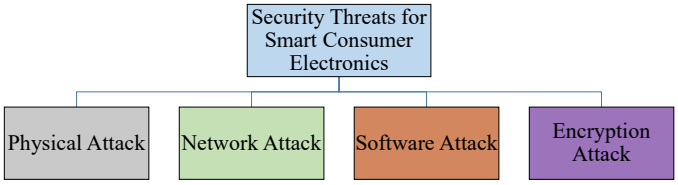


Fig. 3: Different forms of threats against smart CE [12].

hardware based vulnerabilities such as side channel attacks [21]. There have been many solutions that are proposed for IoT security [22, 23], but when consumer electronic devices are exposed to various threats, this can throw an entire household into chaos causing many issues.

B. Related Prior Research

Securing the wireless communication between IoMT devices requires implementation of cryptographic protocols. There are various architectures and protocols that are capable of providing security against various integrity vulnerabilities and threats which stop unauthorized access of the devices. Symmetric and asymmetric protocols can be implemented which can restrict access to the device and stop an attacker from gaining control over the system. Eavesdropping attacks can also be mitigated with such protocols. But if the patient data is encrypted, there is a chance that this becomes a hindrance during an emergency. When a medical representative has to access the device data, cryptographic implementations might restrict access which may risk patient life [10, 12]. As a solution, a universal access key can be provided to authorized medical representatives dealing with emergencies. But this defeats the fundamental reason for having cryptographic protocols in place, where attackers can use various methods to gain access to the key and tamper with the IoMT device. These can safeguard against remote attacks but the systems are vulnerable to close range attacks. An adversary can gain access to the key by shining ultraviolet light on the patient. The electrocardiography signals that originate from the patient are used to extract the key from the device. But a physical contact with the patient is sufficient to gain access to the key and extract it. Various home automation devices are also vulnerable to different attacks like radio attacks and impersonating attacks [20].

One other issue with IoMT devices is that they often rely on a proprietary protocol for securing the system and the communication channel [17]. With proprietary protocols in place, no extra cryptographic schemes are employed, which leaves the communication channels between the devices and the controllers vulnerable as discussed in the previous section.

This paper presents a device authentication scheme which can provide security against such attacks. PMsec uses Physical Unclonable Functions (PUFs) which generate the cryptographic keys used for authentication of the signals coming to the device. With the implementation of PUFs, the attackers can be stopped to a large extent and device security can be reprogrammed if deemed necessary. Research has been extensively done on various architectures of PUFs, such as

TABLE I: Contemporary Security Works in the Consumer Electronics Literature

Works	Security Protocol	Feature	Vulnerabilities
Amin, et al. 2017 [16]	Software agent enabled biometric security algorithm	Uses mutual authentication and a protocol with key negotiation.	Difficult to retrieve the data in case of emergencies.
Khan, et al. 2018 [17]	Various outdated security protocols	When the IoT devices are outdated, their security protocols also become old.	Potential entry points for attackers.
Bae, et al. 2018 [18]	Partial fingerprint matching authentication protocol	Uses partial fingerprints of the user for authentication	Adversary can gain access if he is near the user.
This work	**PMsec**	Authorization scheme is presented for increased robustness	No known security threats.

SRAM [24], Ring Oscillator [25], Multiplexer [26, 27] and Memristor. There are various designs of PUF based authentication mechanisms that are proposed for deployment in the IoT environment [28, 29]. Device authentication is of high priority in the IoT. There are many instances of attacks on an IoT network which involves malicious devices in the network compromising the security [30]. With the introduction of PUF modules in such cases, the need for storage is reduced significantly. Table I provides a comparative view of this work and other recently published works in IoT security.

III. Novel Contributions of the Current Paper

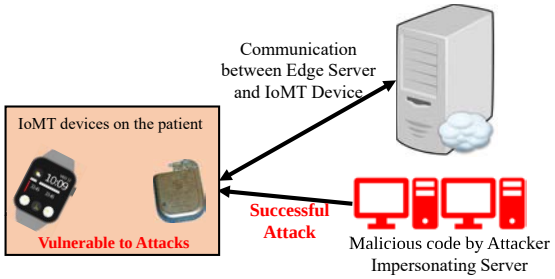
A. Problem Formulation

IoMT devices are capable of collecting patient data and transmitting them to the doctor for a diagnosis. An adversary will be able to take advantage of various vulnerabilities to attack the IoMT devices, as shown in Fig. 4. Some IoMT devices can be configured using remote control or a proprietary controller designed by the manufacturer. The remote control can be impersonated by the attacker to send malicious instructions to the IoMT device. The data from some IoMT devices is transferred to an edge server for processing. In such cases, reverse engineering attacks and radio attacks are performed by the attacker to gain access to the data and impersonate the edge server and gain unauthorized access to the IoMT device.

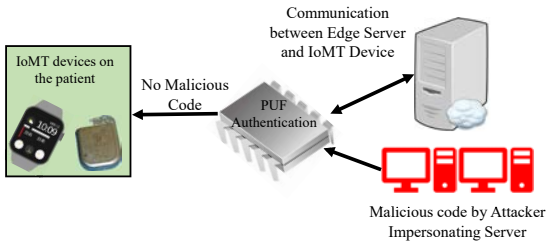
B. Proposed Solution

This paper presents a novel device authentication scheme, PMsec which is capable of authenticating the device before any data are read from it. One of the main concerns for IoMT devices is their processing power and storage. Most IoMT devices have low processing power which makes them incapable of running intensive cryptographic applications. Hence the novel PUF-based authentication scheme, PMsec is presented.

The current design is capable of authenticating devices without any load on the processor. This makes it suitable for various environments including medical devices. By integrating a low power PUF architecture, the power consumption of the entire system can be reduced to a minimum which is a basic necessity of any IoT device. With the implementation of PUFs in the authentication mechanism, the keys are not stored in memory which also reduces the memory requirements of the system. The key can be generated with the appropriate input to the PUF module whenever necessary.



(a) Threat Model



(b) Solution with PUF

Fig. 4: Threat Model and PUF Solution for IoMT Devices.

In addition to PMsec, experimental validation is also presented in this paper which uses a single board computer as an edge server and an IoT board as the IoMT device to demonstrate and validate the proposed scheme. The PUF module is implemented on an FPGA and is connected to the edge server and the IoMT device for the authentication process.

IV. PMsec: The Proposed PUF Based Device Authentication Scheme for the IoMT

This section presents the proposed PMsec model. A scenario where the data is exchanged between an IoMT client and a server, and the client transmits the data to an edge server, is examined. There are two stages in the authentication scheme, the enrollment phase and the authentication phase. When a device is initially introduced into the network, it undergoes enrollment, and once the device is enrolled in the server, it can be deployed in the application. During the authentication phase, the device is checked for authenticity and the data is received from the client. The proposed authentication scheme is suitable for various scenarios and IoMT applications where data needs to be transmitted between two different devices and

is not restricted by the communication protocol that is used between the two devices. This section presents the two phases of the authentication scheme.

A. PUF based Security Paradigm in Edge Computing

The proposed security paradigm is as shown in Fig. 5. As shown in the figure, the end devices are consumer electronic health care devices, which are present on the patient. They are connected to the edge routers, edge servers and gateways, depending on the requirements. The doctor will be able to access the data through a local area network and data from edge devices will be sent to the cloud services through the Internet. Edge device such as the edge server, edge router and the gateway are embedded with a PUF module and so are the end devices.

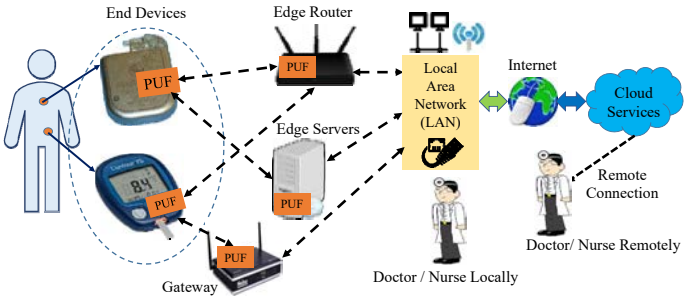


Fig. 5: Proposed PUF Based Security in Edge Computing Paradigm of IoMT.

B. Proposed PUF Based Enrollment Phase

When a new device needs to be added to the network, the IoMT device and the server go through the enrollment phase. A PUF module is embedded into every device that is added to the network. It is assumed that the input challenges are secure, satisfy the required characteristics of the PUF, and are available during the enrollment phase. The required characteristics of a PUF are discussed in Section V.

The enrollment phase process of the authentication scheme is shown in Fig. 6. There are PUF modules in both the server and the IoMT device. Initially, a challenge is chosen to be given as an input to the PUF module at the server. Let this input be "Challenge 1 (C1)". For this input, a response is obtained which is considered "Response 1 (R1)", as shown in Fig. 6. The process of generating responses from challenges in the PUF is denoted by $\rangle\rangle$. C1 and R1 are obtained at the PUF module in the server. After response 1 is generated, it needs to be checked if it satisfies the properties for the PUF module that is present in the IoMT device.

The R1 obtained is then transmitted to the IoMT device. At the IoMT device, this becomes the challenge input for the PUF module. The input is represented as "Challenge" as shown in Fig. 6. For the "Challenge (C)', the "Response (R)" is obtained at the IoMT device, i.e. C$\rangle\rangle$R. This acts as a unique fingerprint for the IoMT device because of the characteristics of PUFs.

This Response from the IoMT device is then transmitted to the server where it is given as challenge to the PUF

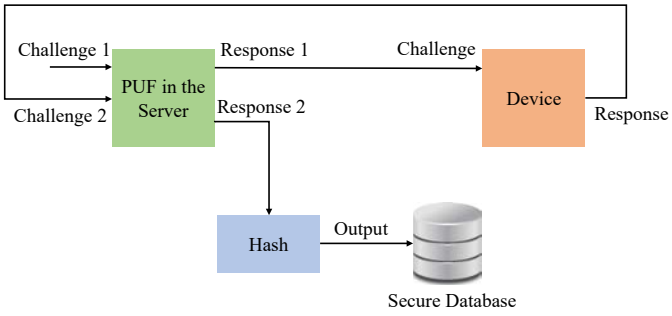


Fig. 6: Enrollment Phase.

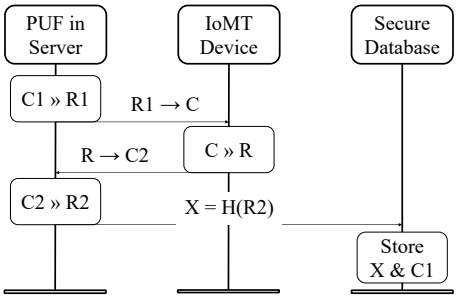


Fig. 7: Device Registration procedure.

module. The challenge is represented as "Challenge 2 (C2)" in Fig. 6. This challenge will result in an output represented as "Response 2 (R2)", i.e. C2$\rangle\rangle$R2. After obtaining R2, a hash of it is computed, such as $X = H(R2)$. The final hash output and the initial challenge (C1) are stored in a database. The process is repeated for multiple keys in the form of challenges and the corresponding hash values are generated. The control flow of the enrollment and registration phase is shown in Figure 7.

This authentication scheme does not store the data pertaining to the IoMT device in the server. This gives an advantage if the server is compromised and an attacker directly gains access to the database. The devices will be authenticated only when the response generated at the IoMT device passes through the PUF module at the server and the hash of R2 matches that from the database.

C. Proposed PUF Based Authentication Phase

Once the device is enrolled in the server, the IoMT device can be authenticated at any time to check its credibility.

Fig. 8 shows the authentication phase of the scheme. As shown in the figure, when the device needs to be authenticated, the database is checked and input challenge (C1) is given to the PUF module at the server. A response is collected from the PUF module, Response 1 ($R1'$). This is sent to the client device which has to be authenticated. $R1'$ becomes the challenge input to the PUF module at the client device. A response is collected from the PUF module and then sent to the server for further processing and authentication as in the enrollment phase. This ensures that there will be no challenge input generation at the client. Then the response becomes a challenge input to the PUF module at the server. This ensures that the data that is coming from the client are not

directly stored in memory or are not directly used for further processing. The response from the PUF is sent to the hash function and the hash is calculated as ($X' = H(R2')$). This is compared to the hash value that is stored in the database (X). If X and X' are same, the device is authentic and if they do not match, the device is malicious. The authentication phase is shown as a flow diagram in Fig. 9. A complete procedure for enrollment, authentication and key exchange is presented in Algorithm 1.

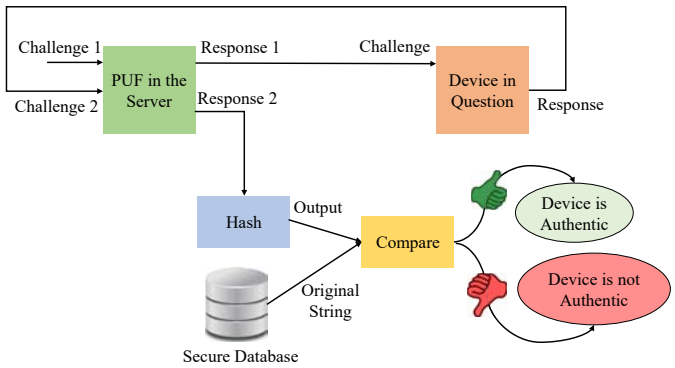


Fig. 8: Authentication Phase.

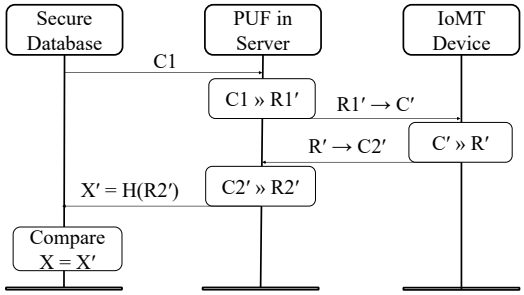


Fig. 9: Authentication Verification.

V. Hybrid Oscillator Arbiter Physical Unclonable Function

A PUF utilizes the manufacturing variations that occur during the fabrication process of an integrated circuit. During the fabrication process, due to the steps involved, variations are introduced into the devices which makes them differ from each other. No two devices on a single wafer look the same, which makes them provide different outputs. This variability is taken as an advantage by the PUF to generate cryptographic keys. These variations that are introduced in the devices are unpredictable, uncontrollable, unavoidable and natural. Hence, the output cryptographic keys from the PUF devices are also naturally random. The input to a PUF is called "Challenge" and the output from a PUF is called "Response". In the current design of PUF, the challenge and the response are in binary. The input output-pair of the PUF is called a Challenge-Response Pair (CRP) and is used for authentication of the device.

The variations that occur during the fabrication process are not uniform or are not the same for different wafers. For the same challenge input different PUF modules provide different responses. This makes the PUF response a fingerprint of that specific IC. The keys are generated without the need for any processing power from the main processor of the device. This makes the entire system lightweight and highly secure. Also the keys are not stored in the memory of the devices which makes them resistant to various side channel attacks. The keys can be generated when necessary depending on the cryptographic protocol implemented or the authentication mechanism used. This also reduces the memory necessary for the implementation of this authentication scheme in the context of the IoMT.

The number of input-output pairs from a single PUF module can be exponentially high depending on the design and architecture of the PUF. The core components of the PUF module determine the robustness of the design. Based on the challenge response pairs that a PUF module can generate, they are divided into three categories: (1) Strong PUF, (2) Weak PUF, and (3) Controlled PUF.

A strong PUF is capable of generating an exponentially high number of CRPs. With the high number of CRPs from the module, the chances of a successful attack can be reduced substantially. A weak PUF is capable of generating a low number of CRPs. In some cases, the CRPs from a weak PUF can be as low as one. In such cases, the PUF module needs to be safeguarded from side channel attacks. In a controlled PUF, the challenge and the response are processed before getting to and from the PUF module. The challenge is preprocessed and the response is postprocessed. This ensures that the PUF module is resistant to various side channel and power analysis attacks and increases the robustness of the design.

Algorithm 1: Secure Authentication Process

Inputs : Challenge 1 to PUF in Server (PUF-S) in *Phase-1* and to Secure database (SDB) in *Phase-2*.

Phase-1 (Enrollment)
PUF-S → IoMTD {R1, i.e. C}
C1 ⟩⟩ R1
PUF-S ← IoMTD {R1 i.e. C2}
C ⟩⟩ R
PUF-S → SDB {X}
X=H(R2)
Phase-2 (Authentication)
SDB → PUF-S {C1}
C1 ⟩⟩ R1′
PUF-S → IoMTD {R1′ i.e. C′}
C′ ⟩⟩ R′
PUF-S ← IoMTD {R′ i.e. C2′}
C2′ ⟩⟩ R2′
PUF-S → SDB {X′}
X′=H(R2′)
if *(X=X′)* **then**
  Authenticated
else
  Malicious found

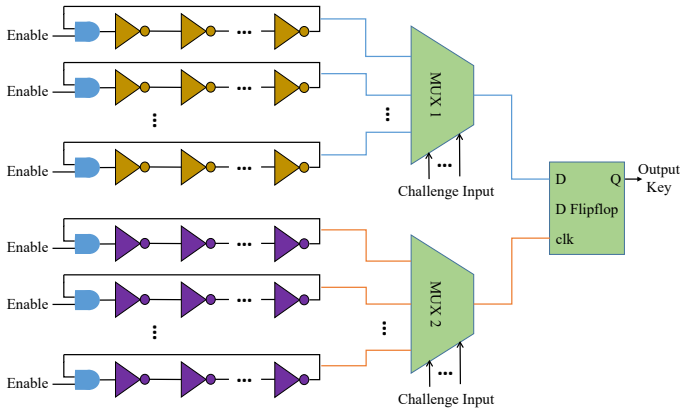


Fig. 10: Design of Hybrid Oscillator Arbiter PUF.

Fig. 10 shows the design of a Hybrid Oscillator Arbiter PUF. Ring Oscillators (ROs) are the core component in the Hybrid Oscillator Arbiter PUF module. This design of PUF is a Power Optimized Hybrid Oscillator Arbiter PUF. Details of its design are presented in [31]. The power consumption of this PUF is significantly lower compared to a Speed Optimized design of the Hybrid Oscillator Arbiter PUF. The Power Optimized design is more suited for IoMT applications. The Speed Optimized design can be used in applications like smart cars where processing power and latency are of highest importance compared to the power consumption of the device.

As discussed previously, the PUF modules take advantage of the manufacturing variations that occur during the fabrication of the IC. As shown in Fig. 10, there are two sets of ring oscillators in the design, which are differentiated by color. Each ring oscillator is connected to two multiplexers MUX1 or MUX2. These multiplexers are responsible for selecting the ring oscillators and feed them to the flipflop. The challenge input that is given to the PUF module is given to the select lines of the multiplexers. Using the challenge bit, ring oscillators are selected in various permutations.

In the current design, to generate a 128-bit output response, 256 ring oscillators are necessary which can be divided into two sets. The multiplexers select the oscillator based on the challenge bit and feed it to the D-flipflop clock and input ports. Based on the signal value at the inputs, the output of the D-flipflop is determined. Due to the variations, with a new challenge input given to the PUF module, the output of the D-flipflop changes giving a cryptographic key unique to the device.

VI. Proof-of-Concept Implementation of the Proposed PMsec

This section presents the theoretical validation and experimental evaluation of PMsec. The experimental setup uses an IoT device and an Edge server where both have PUf modules for authentication.

A. Theoretical Validation

The proposed PUF based authentication scheme is combining the concepts of hardware and cryptographic systems. The elements of bit strings are random variables and Hamming distances between different strings will result in a binomial distribution. Hence as a common measure, the Hamming distance is calculated between the keys that are generated by different PUF modules [32]. Along with PUF properties, a secure database is considered for IoMT device authentication which stores the hash value to avoid any kind of information theft [33].

In the enrollment phase (Fig. 5 and Algorithm 1), the server with PUF and the IoT device follow two rounds of challenge-response phases and subsequently the secure database stores the hash value of the final response (H(R2)). In the authentication phase (Fig. 9 and Algorithm 1), the IoMT device is initialized, and sends challenge (C1) to the server. The server finds the response by combining information from the IoMT device to send the hash value to the secure database ($C1\rangle\rangle R1' \rightarrow C'\ \rangle\rangle$ R $' \rightarrow$ X′=H(R2′)). The secure database matches the stored hash value with the received hash value to authenticate the device (X=X′). Due to the PUF, multicount challenge-response, and hash storage, a malicious device cannot be authenticated.

B. Experimental Setup

In the current implementation of the authentication mechanism, a 32-bit microcontroller-based development board with communication capabilities was used as the client which collects the data and transmits to the edge server. Both the edge server and the IoT board are equipped with PUF modules. Hybrid Oscillator Arbiter PUF modules are implemented on an FPGA and the keys are generated for the implementation. Edge server 2 was used as a server and an IoT board was used for the implementation of a client. An FPGA development board is used for the implementation of PUFs.

Fig. 11a and Fig. 11b show the IoT board and edge server connected to the FPGA. Both boards collect the PUF keys from the FPGA through the General Purpose IO (GPIO) Pins on the board. The PUF modules have multiplexers which take the challenge input given to the PUF module as the select lines. Based on the challenge input given to the PUF modules, the oscillators are selected. Two pins are used for the communication between the FPGA and the boards that need the key. One gives the input to the FPGA and through the other pin, the IoT board or edge server collects the data that is coming from the FPGA.

For the two different boards, IoT Board and Edge Server, the PUF modules are given different ring oscillators on the FPGA. Two implementations of PUF design, one with a 5 stage ring oscillator and the other with 7 stage ring oscillators were chosen for differentiation. This ensures that both boards are using different modules of the PUF and are generating different keys from each other. The integrity of the keys generated by the PUF modules can be estimated using their Hamming distance. Initially, the keys are generated by the PUF modules by giving them the inputs. Then the Hamming distance is calculated for the output keys generated. The ideal Hamming distance for the keys to be used is 50%. Fig. 12a shows the Hamming distance between the keys that are

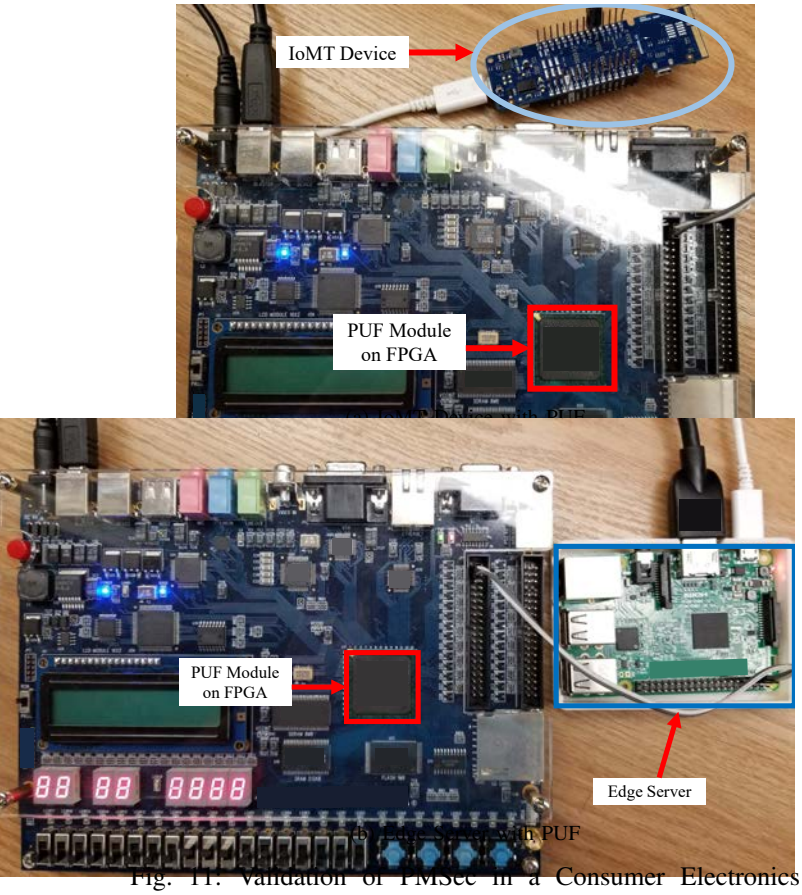
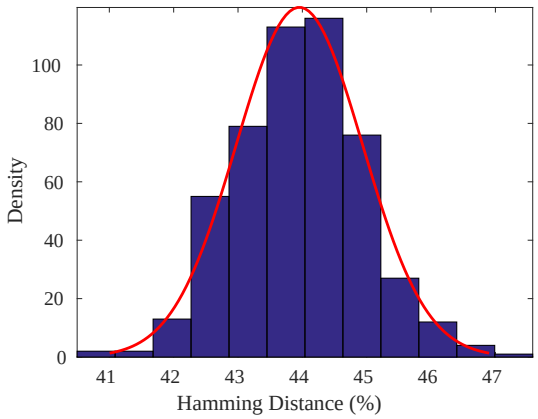
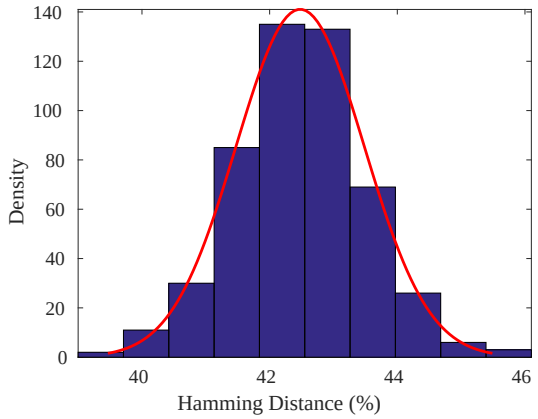


Fig. 11: Validation of PMSec in a Consumer Electronics environment.



(a) Hamming Distance of PUF with 7 Stage Ring Oscillator



(b) Hamming Distance of PUF with 5 Stage Ring Oscillator

Fig. 12: Physical Unclonable Function Validation.

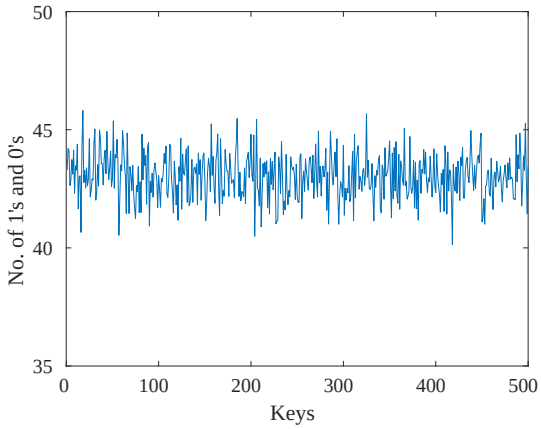


Fig. 13: Randomness of PUF Keys.

generated by the PUF modules with 7 stage ring oscillators for different inputs. The mean in the plot is around 44% and varies between 40% and 47%. These are close to the ideal values and hence can be used for the authentication of the devices. Fig. 12b shows the Hamming distance between the keys generated by the PUF module with 5 stage ring oscillators as core components. The mean Hamming distance is 43% and varies between 39% and 46%.

After the keys are generated and the Hamming distance is calculated, the output keys are evaluated for randomness. Randomness of a PUF is the property where the keys generated will contain equal number of 0's and 1's. This ensures that the output key is not vulnerable to certain types of machine learning attacks or predictabilities. The ideal randomness of the PUF key should be 50%. In the keys generated, the number of 1's that are present in the keys is checked and is plotted. Fig. 13 shows the randomness of different output keys generated by the PUF modules where the mean value is 44%.

C. Validation of the Proposed Scheme

Table II shows the different parameters of the Hybrid Oscillator Arbiter PUF. Table III shows the characterization table of the entire system. The number of keys generated is different for each PUF design. Between the server and the IoMT device, 7-stage and 5-stage ring oscillators were selected. The number of keys that has the optimum Hamming distance are 200 and 240 respectively. The number of keys that can be potentially generated can be much higher using the current design but the optimum Hamming distance of ≈50% should also be taken into consideration. 64-bit keys were generated from the PUF modules. The time taken to completely authenticate the device is 1.2 sec to 1.5 sec and the error rate for the authentication scheme in the prototype is 10%. To the best knowledge of the authors, this is the first paper presenting a PUF based device authentication scheme for the IoMT. Hence a direct comparison with other works

was not possible for the parameters presented in Table III and Table IV.

D. Authentication

After the keys are checked for security, the PUF modules are deployed for the authentication scheme. The edge server is connected to the FPGA and the PUF module is invoked to collect the keys. During the enrollment phase of the environment, the keys generated are sent to the IoT board. The IoT board will give the inputs to the PUF modules and send back the outputs of the PUF modules. These are again used as an input to the PUF module at the edge server. Once a final key is generated, the hash of the output is calculated. For every key that is generated at the server and the client, the hash is calculated and is stored in the memory. Fig. 14a shows the process of the enrollment phase. Python is used for implementation at the edge server.

After the enrollment phase, the IoT board, in this case the IoT device, is ready for deployment in the network. When the authenticity of the device is questioned, the authentication scheme is run again which makes sure the network is not compromised. Fig. 14c shows the authentication scheme at the edge server and Fig. 14b shows the authentication scheme at the IoT board. As shown in the figure, the edge server is given an input which generates the PUF key and sends it to the IoT board. As shown in Fig. 14b, the IoT board will get the key from the edge server. Then this is given as input to the PUF module at the client, the IoT board, and then the output is sent back for authentication. At the edge server, the output is received and the PUF key for that input is generated and the hash is calculated. If the database and the generated hash match, the device can be said to be authentic. If there is no match between them, the device will be considered malicious.

E. False Positives and False Negatives

When the devices are enrolled into the network, multiple input keys are selected for challenge inputs for the PUF module. This helps in developing multiple signatures for a single IoMT device. When a database is built with multiple PUF keys and hash outputs, validating the devices that are already in the network becomes simpler. The scenario where false positives and false negatives occur during the authentication process is also considered. A false positive is the case where a device that is being authenticated is malicious but the system authenticates the device. A false negative is the scenario where the device being authenticated is authentic but the system considers it malicious.

For the issue of false positive devices, multiple attempts will be made to authenticate the device. In the experimental setup, 3 keys from the database are selected and given as challenge inputs. If the final hash generated at the output does not match with the one stored in the database, the device is not granted access to store data or transmit the data. Access is granted upon successful authentication. Hence the response generated at the IoMT device PUF module is given as input to the PUF module at the edge server again as a solution to this issue. A PUF module output depends on the input value and if the input changes, the output of the PUF module will also change. A similar situation can be considered for the issue of false negatives. If the majority of the input challenges are authentic, the process is repeated again to account for the problem of errors during transmission.

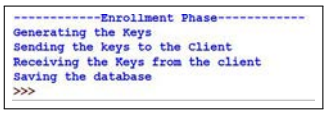
F. Analysis of Overhead on the Host CE Device

Any new addition to the existing circuitry will add an overhead. A PUF is one such design which is added to existing consumer electronics devices. In the case of the IoMT, power consumption and battery life are of highest priority. Any new addition to the device should not increase the power consumption significantly resulting in frequent battery changes.

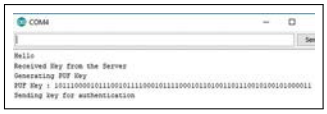
The design of PUF used for prototyping the authentication scheme is a Power Optimized Hybrid Oscillator Arbiter PUF. This design has been validated with state of the art technology in [31] and [34]. The PUF design was validated with 32nm FinFETs and Dopingless Junctionless FETs and power consumption was presented. The overhead added by the PUF design to the consumer electronic devices is significantly low. Table II shows the characterization of the Power Optimized Hybrid Oscillator Arbiter PUF used for prototyping PMsec. As presented in the table, the Hybrid Oscillator Arbiter PUF consumes significantly less power reducing the power overhead.

TABLE II: Characterization of the Hybrid Oscillator Arbiter PUF

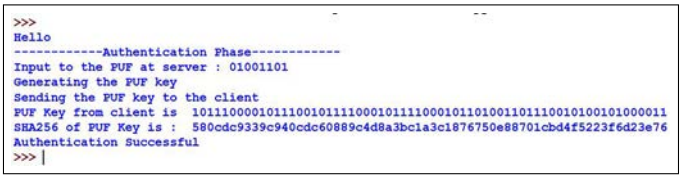
Parameter	FinFET	DLFET
Technology	32nm FinFET	15nm DLFET
Architecture	Ring Oscillator	Ring Oscillator
Oscillation Frequency	450 MHz	565 MHz
Uniqueness	50.9 %	48
Reliability	0.85 %	1.7 %
Average Power	285.5 μW	121.3 μW
Time to generate the key	150 ns	150 ns



(a) Output from Server while Enrollment



(b) Output from IoMT Device



(c) Output from Server during Authentication

Fig. 14: Validation of the Proposed Authentication Scheme.

TABLE III: Characterization of the Hybrid Oscillator Arbiter PUF

Server	Single Board Computer	
Client	32-bit Microcontroller Board	
PUF Implementation	Field-Programmable Gate Array (FPGA)	
Parameters	**7-Stage Ring Oscillator Based PUF**	**5-Stage Ring Oscillator Based PUF**
No. of Ring Oscillators	512	512
No. of keys generated	500	500
Hamming Distance	44 %	43 %
Randomness	44 %	44 %
No. of keys with optimal Hamming distance	200	240
Length of keys generated	64 bits	64 bits
Mean Frequency of Oscillations	450 MHz	495 MHz

TABLE IV: Characterization of the Proposed PMsec

Parameters	**Specific Values**
Server	Single Board Computer
IoMT Device	32-bit Microcontroller based development board
Time to Generate the Key at Server	800 ms
Time to Generate the Key at IoMT Device	800 ms
Time to Authenticate the Device	1.2 sec - 1.5 sec
Error Rate	10 %

VII. Conclusion and Future Research

In the modern era of connected devices, security is one of the major concerns. With so many devices connected to the network, the number of vulnerabilities that they open to an adversary is very large. In the case of the IoT, along with the software vulnerabilities, there are also many hardware vulnerabilities that can be taken advantage of by the attacker to gain access to the network. This paper presents a device authentication scheme which uses PUFs to authenticate the devices present in the network. One of the advantages of this scheme is that the device information is not stored in the memory of the server. Every device will have a PUF module which can be used for authentication but the challenge and response from the client PUF modules is not stored in the server memory. This can help in cases where the server is compromised and the device information will not be leaked to the adversary. As a future research, a client side authentication scheme can be developed to ensure that the client can authenticate the messages that are received from the server.

References

[1] M. Shahzad and M. P. Singh, "Continuous Authentication and Authorization for the Internet of Things," *IEEE Internet Comput.*, vol. 21, no. 2, pp. 86–90, Mar 2017.

[2] B. Ahlgren, M. Hidell, and E. C. H. Ngai, "Internet of Things for Smart Cities: Interoperability and Open Data," *IEEE Internet Comput.*, vol. 20, no. 6, pp. 52–56, Nov 2016.

[3] W. Chang, L. Chen, and Y. Chiou, "Design and Implementation of a Drowsiness-Fatigue-Detection System Based on Wearable Smart Glasses to Increase Road Safety," *IEEE Trans. Consum. Electron.*, pp. 1–1, 2018.

[4] J. Han, C. Choi, W. Park, I. Lee, and S. Kim, "Smart home energy management system including renewable energy based on ZigBee and PLC," *IEEE Trans. Consum. Electron.*, vol. 60, no. 2, pp. 198–202, May 2014.

[5] A. R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta, and M. Alikarar, "A Smart Home Energy Management System Using IoT and Big Data Analytics Approach," *IEEE Trans. Consum. Electron.*, vol. 63, no. 4, pp. 426–434, November 2017.

[6] T. Lee, B. M. Lee, and W. Noh, "Hierarchical Cloud Computing Architecture for Context-Aware IoT Services," *IEEE Trans. Consum. Electron.*, vol. 64, no. 2, pp. 222–230, May 2018.

[7] L. Rachakonda, P. Sundaravadivel, S. P. Mohanty, E. Kougianos, and M. Ganapathiraju, "A Smart Sensor for Stress Level Detection in IoMT," in *Proc. IEEE Int. Conf. Smart Elect. Sys. (iSES)*, December 2018.

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

[9] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. K. Ganapathiraju, "Everything You Wanted to Know about Smart Health Care: Evaluating the Different Technologies and Components of the Internet of Things for Better Health," *IEEE Consum. Electron. Mag.*, vol. 7, no. 1, pp. 18–28, Jan 2018.

[10] 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.

[11] M. Zhang, A. Raghunathan, and N. K. Jha, "MedMon: Securing Medical Devices Through Wireless Monitoring and Anomaly Detection," *IEEE Trans. Biomed. Circuits Syst.*, vol. 7, no. 6, pp. 871–881, Dec 2013.

[12] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *Proc. Int. Conf. IoT in Social, Mob., Analy. and Cloud (I-SMAC)*, Feb 2017, pp. 32–37.

[13] D. Yin, L. Zhang, and K. Yang, "A DDoS Attack Detection and Mitigation With Software-Defined Internet of Things Framework," *IEEE Access*, vol. 6, pp. 24 694–24 705, 2018.

[14] D. Puthal, S. P. Mohanty, S. A. Bhavake, G. Morgan, and R. Ranjan, "Fog Computing Security Challenges and Future Directions [Energy and Security]," *IEEE Consum. Electron. Mag.*, vol. 8, no. 3, pp. 92–96, 2019.

[15] A. Strielkina, D. Uzun, and V. Kharchenko, "Modelling of Healthcare IoT Using the Queueing Theory," in *Proc. IEEE Int. Conf. Intel. Data Acqui. and Adv. Compu. Syst.: Tech. and App. (IDAACS)*, vol. 2, 2017, pp. 849–852.

[16] R. Amin, R. S. Sherratt, D. Giri, S. H. Islam, and M. K. Khan, "A Software Agent Enabled Biometric Security Algorithm for Secure file Access in Consumer Storage Devices," *IEEE Trans. Consum. Electron.*, vol. 63, no. 1, pp. 53–61, February 2017.

[17] W. Z. Khan, M. Y. Aalsalem, and M. K. Khan, "Communal Acts of IoT Consumers: A Potential Threat to Security & Privacy," *IEEE Trans. Consum. Electron.*, pp. 1–1, 2018.

[18] G. Bae, H. Lee, S. Son, D. Hwang, and J. Kim, "Secure and Robust User Authentication Using Partial Fingerprint Matching," in *Proc. IEEE Int. Conf. Cons. Elect.*, Jan 2018, pp. 1–6.

[19] D. Pauli, 2016, last Accessed : 11/20/2018. [Online]. Available: https://www.theregister.co.uk/2016/12/01/

[20] T. Kim, H. Lee, and Y. Chung, "Advanced Universal Remote Controller for Home Automation and Security," *IEEE Trans. Consum. Electron.*, vol. 56, no. 4, pp. 2537–2542, November 2010.

[21] M. Tang, M. Luo, J. Zhou, Z. Yang, Z. Guo, F. Yan, and L. Liu, "Side-Channel Attacks in a Real Scenario," *Tsinghua Sci. and Tech.*, vol. 23, no. 5, pp. 586–598, Oct 2018.

[22] P. L. R. Chze and K. S. Leong, "A Secure Multi-Hop Routing for IoT Communication," in *Proc. IEEE World Forum. IoT (WF-IoT)*, March 2014, pp. 428–432.

[23] M. Singh, A. Singh, and S. Kim, "Blockchain: A Game Changer for Securing IoT Data," in *Proc. IEEE World Forum. IoT (WF-IoT)*, Feb 2018, pp. 51–55.

[24] W. Liu, Z. Lu, H. Liu, R. Min, Z. Zeng, and Z. Liu, "A Novel Security Key Generation Method for SRAM PUF Based on Fourier Analysis," *IEEE Access*, vol. 6, pp. 49 576–49 587, 2018.

[25] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "An Aging-Resistant RO-PUF for Reliable Key Generation," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 3, pp. 335–348, July 2016.

[26] Y. Gao, H. Ma, S. F. Al-Sarawi, D. Abbott, and D. C. Ranasinghe, "PUF-FSM: A Controlled Strong PUF," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 5, pp. 1104–1108, May 2018.

[27] D. P. Sahoo, D. Mukhopadhyay, R. S. Chakraborty, and P. H. Nguyen, "A Multiplexer-Based Arbiter PUF Composition with Enhanced Reliability and Security," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 403–417, March 2018.

[28] M. A. Muhal, X. Luo, Z. Mahmood, and A. Ullah, "Physical Unclonable Function Based Authentication Scheme for Smart Devices in Internet of Things," in *Proc. IEEE Int. Conf. Smart IoT*, Aug 2018, pp. 160–165.

[29] S. W. Jung and S. Jung, "HRP: A HMAC-Based RFID Mutual Authentication Protocol Using PUF," in *Proc. Int. Conf. Info. Networking (ICOIN)*, 2013, pp. 578–582.

[30] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[31] 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.

[32] C. Böhm and M. Hofer, *Physical Unclonable Functions in Theory and Practice*. Springer Science & Business Media, 2012.

[33] A. Nanda, P. Nanda, X. He, D. Puthal, and A. Jamdagni, "A Novel Hybrid Authentication Model for Geo Location Oriented Routing in Dynamic Wireless Mesh Networks," in *Proc. Hawaii Int. Conf. Syst. Sciences (HICSS)*, 2018, pp. 5532–5541.

[34] V. P. Yanambaka, S. P. Mohanty, E. Kougianos, P. Sundaravadivel, and J. Singh, "Dopingless Transistor Based Hybrid Oscillator Arbiter Physical Unclonable Function," in *Proc. IEEE-CS Int. Symp. VLSI*, 2017, pp. 609–614.

Venkata P. Yanambaka (M'19) received the Bachelor of Technology degree in electronics and communications from the JNTU, India, in 2014. He defended his Ph.D. at the System Electronic Systems Laboratory (SESL) at the Department of Computer Science and Engineering, University of North Texas. He is currently an Assistant Professor at the School of Engineering and Technology, Central Michigan University. My research interests are in Security in Internet of Things (IoT), Energy-Efficient Circuits and Systems, and Application-Specific Systems Design. He has authored of a 12 research articles which include multiple journals/transactions articles.

Saraju P. Mohanty (SM'08) obtained a Bachelors degree with Honors in Electrical Engineering from the Orissa University of Agriculture and Technology (OUAT), Bhubaneswar, 1995. His Masters degree in Systems Science and Automation is from the the Indian Institute of Science (IISc), Bangalore, in 1999. He obtained a Ph.D. in Computer Science and Engineering (CSE) in 2003, from the University of South Florida (USF), Tampa. He is a Professor at the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by National Science Foundations, Semiconductor Research Corporation, US Air Force, IUSSTF, and Mission Innovation. He has authored 300 research articles, 4 books, and invented 4 US patents. His Google Scholar h-index is 31 and i10-index is 110. He has received 9 best paper awards. He has delivered 8 keynote talks at various International Conferences. He received IEEE-CS-TCVLSI Distinguished Leadership Award in 2018 for services to the IEEE, and to the VLSI research community. He was the recipient of 2016 PROSE Award for best Textbook in Physical Sciences & Mathematics category from the Association of American Publishers for his Mixed-Signal System Design book published by McGraw-Hill in 2015. He is the Editor-in-Chief of the IEEE Consumer Electronics Magazine.

Elias Kougianos (SM'07) received a BSEE from the University of Patras, Greece in 1985 and an MSEE in 1987, an MS in Physics in 1988 and a Ph.D. in EE in 1997, all from Lousiana State University. From 1988 through 1997 he was with Texas Instruments, Inc., in Houston and Dallas, TX. In 1997 he joined Avant! Corp. (now Synopsys) in Phoenix, AZ as a Senior Applications engineer and in 2001 he joined Cadence Design Systems, Inc., in Dallas, TX as a Senior Architect in Analog/Mixed-Signal Custom IC design. He has been at UNT since 2004. He is a Professor in the Department of Engineering Technology, at the University of North Texas (UNT), Denton, TX. His research interests are in the area of Analog/Mixed-Signal/RF IC design and simulation and in the development of VLSI architectures for multimedia applications. He is an author of over 120 peer-reviewed journal and conference publications.

Deepak Puthal (M'16) received the Ph.D. degree in computer science from the University of Technology Sydney (UTS), Australia. He is currently a Lecturer at School of Computing, Newcastle University, Newcastle upon Tyne, UK. He is an author/co-author of more than 100 peer-reviewed publications in international conferences and journals, including ACM and IEEE transactions. His research interests include cyber security, Internet of Things, distributed computing, and edge/fog computing. He has been a Program Chair and a Program Committee member in several IEEE and ACM sponsored conferences. He was a recipient of the 2017 IEEE Distinguished Doctoral Dissertation Award from the IEEE Computer Society and STC on Smart Computing. He served as a Co-Guest Editor of several reputed journals, including Concurrency and Computation: Practice and Experience, Wireless Communications and Mobile Computing, and Information Systems Frontier. He is an Associate Editor of the IEEE Transactions on Big Data, and IEEE Consumer Electronics Magazine.