Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 3, December 2021, pp. 1392∼1398
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i3.pp1392-1398

Proof of concept for lightweight PUF-based authentication protocol using NodeMCU ESP8266

Mohd Syafiq Mispan[1], Aiman Zakwan Jidin[2], Muhammad Raihaan Kamaruddin[3], Haslinah Mohd Nasir[4]
[1,2]Micro and Nano Electronics (MiNE), Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
[3]Machine Learning and Signal Processing (MLSP), Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
[4]Advance Sensors and Embedded Controls System (ASECs), Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
[1,2,3,4]Centre for Telecommunication Research and Innovation (CeTRI), Universiti Teknikal Malaysia Melaka, Melaka, Malaysia
[1,2,3,4]Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Article Info

Article history:

Received Jul 22, 2021
Revised Sep 28, 2021
Accepted Oct 5, 2021

Keywords:

Authentication
NodeMCU ESP8266
Physical unclonable function
Wireless sensor network

ABSTRACT

Wireless sensor node is the foundation for building the next generation of ubiquitous networks or the so-called internet of things (IoT). Each node is equipped with sensing, computing devices, and a radio transceiver. Each node is connected to other nodes via a wireless sensor network (WSN). Examples of WSN applications include health care monitoring, and industrial monitoring. These applications process sensitive data, which if disclosed, may lead to unwanted implications. Therefore, it is crucial to provide fundamental security services such as identification and authentication in WSN. Nevertheless, providing this security on WSN imposes a significant challenge as each node in WSN has a limited area and energy consumption. Therefore, in this study, we provide a proof of concept of a lightweight authentication protocol by using physical unclonable function (PUF) technology for resource-constrained wireless sensor nodes. The authentication protocol has been implemented on NodeMCU ESP8266 devices. A server-client protocol configuration has been used to verify the functionality of the authentication protocol. Our findings indicate that the protocol used approximately 7% of flash memory and 48% of static random-access memory (SRAM) in the sensor node during the authentication process. Hence, the proposed scheme is suitable to be used for resource-constrained IoT devices such as WSN.

Corresponding Author:

Mohd Syafiq Mispan
Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik
Universiti Teknikal Malaysia Melaka
Melaka, Malaysia
Email: syafiq.mispan@utem.edu.my

1. INTRODUCTION

Building a trusted and secure internet of things (IoT) solution is crucial especially for applications that process sensitive and user-specific data. Providing the aforementioned solution is exacerbated with the stringent requirement of power and area in resource-constrained IoT devices such as sensor nodes in wireless sensor networks (WSN). WSN consists of hundreds of thousands of sensor nodes used to sense the data and the main location (i.e., base station or sink) where the sensed data can be observed and analyzed. The sensor nodes can communicate among themselves and to the base station for transferring the sensed data. Therefore,

the identification and authentication process must exist to ensure secure node-to-node and node-to-base station communications.

Physical unclonable function (PUF) is a promising hardware fingerprinting technology that can be used in identification and authentication application [1]. PUF exploits the intrinsic process variations during integrated circuit (IC) fabrication to generate a device-specific response [2]. When a set of binary bit-stream known as the challenge is applied onto the PUF, a corresponding unique and random binary output known as the response is generated. The challenge and response generation is also known as the mapping of challenge-response pair (CRP) [3]. The device-specific response generated from a particular PUF can be used to uniquely distinguish a sensor node from a group of similar nodes. As building a PUF requires no special fabrication process and consumes considerably low gate counts, therefore, PUF is seen to be a promising identification and authentication technology for resource-constrained sensor nodes such as WSN applications.

Hence, in this paper, we provide a proof-of-concept of a lightweight PUF-based authentication protocol targeted for resource-constrained sensor nodes. In this study, 32-bit Arbiter-PUF is used as a PUF building block. The main contributions of this work are highlighted below:

1) We design the Arbiter-PUF using an artificial neural network (ANN) on the NodeMCU ESP8266 device which acts as a sensor node.
2) We develop a proof-of-concept for a lightweight PUF-based authentication protocol. The protocol is implemented on NodeMCU ESP8266 devices and verified using server-client configuration.

The rest of the paper is organized as follows. Section 2 describes the background related to this work. Section 3 describes the method to construct the proof of concept of the lightweight authentication protocol based on server-client configuration. The verification of the authentication protocol and the memory utilization are discussed in section 4. Finally, the conclusion is drawn in section 5.

2. RELATED WORK

Several techniques have been proposed in the past aiming for lightweight authentication schemes [4]-[9]. Yilmaz *et al.* [4] proposed a PUF-based IoT authentication protocol combined with Rivest cipher 5 (RC5) encryption technique implemented on Zolertia Zoul devices. A similar scope of work has been presented in [10], combined with the hash function. However, the device name/type for the implementation of the authentication protocol was never revealed. Elsewhere, the PUF-based authentication without explicit CRPs in the verifier database is proposed in [11]. A combination of PUF, identity-based encryption (IBE), and hash function were used to strengthen the proposed technique. Furthermore, the application of PUF technology in building the authentication protocol is expanded into the medical fields as proposed in [12] and [13] for internet-of-medical-things (IoMT) applications.

In another study, Gope *et al.*, [14], [15] proposed the PUF-based authentication protocol for real-time data access in industrial wireless sensor networks. The authentication scheme for field-programmable gate array (FPGA) application is proposed in [16]. The proposed technique eliminates the requirement of the enormous CRPs database in the verifier by using the double PUF authentication model. Elsewhere, a non-PUF-based lightweight authentication protocol of resource-constrained IoT devices is proposed in [17]. A combination of RC5 and elliptic curve cryptography (ECC) was used to implement the proposed protocol. All of the above studies mainly focused on the lightweight PUF-based authentication implementation on Zolertia Zoul and FPGA as IoT devices. In our study, we focus on building the lightweight PUF-based authentication scheme targeted for WSN applications using NodeMCU ESP8266 devices.

3. METHODOLOGY

In this section, the methodology used to develop the authentication protocol, building the PUF model, the verification of the authentication protocol, and the attacker threat model are described.

3.1. Authentication protocol

The authentication protocol described in [18], [19] is used as a proof-of-concept for a lightweight authentication scheme in our study. The authentication protocol consists of two phases which are enrollment and authentication. In the enrollment phase, a new PUF-based device (i.e., sensor node) is registered in the verifier's database, DB with the following steps:

1) Device identifier, ID for node j is entered into the DB_j.

2) The verifier sends a set of challenge $C = \{C_1, C_2, \ldots, C_k\}$ to node j and node j returns the corresponding response $R = \{R_1, R_2, \ldots, R_k\}$ to the verifier, sequentially. Further, $CRP_1, CRP_2, \ldots, CRP_k$ are stored in the DB.

In the authentication phase, the node j is deployed in the field and requested for authentication (i.e., i-th authentication) as illustrated in Figure 1. Node j sends its $ID^{'}$ to the verifier and the verifier finds the match ID in the DB. If the match ID is found, a challenge C_i is retrieved from the DB and sends to node j. Node j computes the response $R_i^{'}$ based on its PUF model and sends the $R_i^{'}$ to the verifier. The verifier retrieves R_i from the DB and compares against the $R_i^{'}$. If both matches, then node j is authenticated as a genuine device, otherwise the verifier detects node j as a fake device. Note that the CRP_i is only used once for the i-th authentication process. The subsequent CRP that is available in the DB will be used for the next authentication process to avoid a man-in-the-middle attack.

Verifier		**Node** j
$DB_j = \langle ID, CRP_1, CRP_2, \ldots, CRP_k \rangle$	$\xleftarrow{ID^{'}}$	**Send** $ID^{'}$
if $ID^{'} = ID$ **then**		
$C_i \in \{0,1\}^n;\ i \leq k;$	$\xrightarrow{C_i}$	$R_i^{'} = PUFmodel(C_i)$
else Rejected		
if $R_i = R_i^{'}$,	$\xleftarrow{R_i^{'}}$	**Send** $R_i^{'}$
then Succeeded; **else Rejected**		

Figure 1. Authentication protocol

3.2. Protocol verification and attacker threat model

The authentication protocol is verified using a server-client configuration implemented on NodeMCU ESP8266 devices which have specifications of 4MB of flash memory and 64kB of static random-access memory (SRAM) [4]. One device acts as a server (i.e., verifier or base station), and another device acts as a client (i.e., sensor node). All the required information such as ID and CRP for sensor node j are registered in the verifier's DB. The communication between the verifier and node j as depicted in Figure 1 is developed using the SimpleESPNowConnection library function.

Assuming that the adversary can eavesdrop on the communication between the verifier and node j, and successfully obtained the node's ID. Next, the adversary has to use the guessed CRPs data set and initiated the authentication process using previously obtained ID. To test this condition, another PUF model is built on NodeMCU ESP8266 with guessed CRPs data set and this node is defined as node $j^{'}$ (i.e., fake node). The authentication protocol between the verifier and node $j^{'}$ is performed and the analysis is discussed in section 4.

3.3. PUF model generation

In our study, the 32-bit Arbiter-PUF architecture which has been proposed in [20], [21] is used as a PUF in the sensor node. As mentioned in section 1, PUF is a hardware fingerprinting technology. Hence, the Arbiter-PUF needs to be implemented from the hardware layer (i.e., logic circuit). Nevertheless, it is impossible to build the hardware of Arbiter-PUF on microcontroller devices [22]. Hence, as a proof of concept to the authentication protocol, a supervised machine learning technique called artificial neural network (ANN) is used to model the Arbiter-PUF on NodeMCU ESP8266 device. A feed-forward network with multilayer perceptron and the resilient back-propagation algorithm has been chosen to construct our ANN as they offer the ability to solve non-linear problems and fast convergence time [23], [24].

The modeling of 32-bit Arbiter-PUF using ANN consists of two phases which are the training and testing phase. A set of CRPs is required as an input to train and test the ANN. Following the method in [25], a total of 32000 CRPs were measured to model the 32-bit Arbiter-PUF using ANN. Based on the measured CRPs, ANN successfully model the 32-bit Arbiter-PUF with a very high prediction accuracy of about 99%. The model of 32-bit Arbiter-PUF which is represented by the weightage and bias parameters of ANN is stored in NodeMCU ESP8266 memory. The Arbiter-PUF model in this device represents node j.

4. SIMULATION RESULTS AND ANALYSIS

In this section, the relevant simulation and analysis are discussed based on the described methodology in section 3. The estimation of memory usage is also discussed in this section.

4.1. PUF-based authentication

The authentication protocol as described in Figure 1 is evaluated using three NodeMCU ESP8266 devices which act as the verifier, node j, and node $j^{'}$ (i.e., fake device). Three communication ports were used which are COM10 for verifier, COM4 for node j, and COM5 for node $j^{'}$. Figure 2 illustrates the verifier status when no authentication request from the sensor nodes.

When the sensor node j is requested for authentication (i.e., node j is defined as device '0' in the program code), node j sends its ID to the verifier and the verifier matches the received ID with the one that stored in the DB. Figure 3 depicts the status of Online Client (status=1) and Paired Client (status=1) indicating that the authentication has been requested by the device '0'. The authentication status of the device '0' at this stage remains UNKNWON.

Once the match ID is found, the verifier sends ten of 32-bit challenges to the node j, and node j returns 10-bit of response to the verifier. The verifier compares the received response against the response in the DB. Figure 4 shows that the received response is matched with the response in the DB. Therefore, node j is a genuine device. When the fake device or node $j^{'}$ is requested for authentication with the guessed CRPs, the verifier failed to authenticate node $j^{'}$ as the CRPs are not exist in the DB. Hence, the verifier returns 'Device is Fake' status as illustrated in Figure 5.

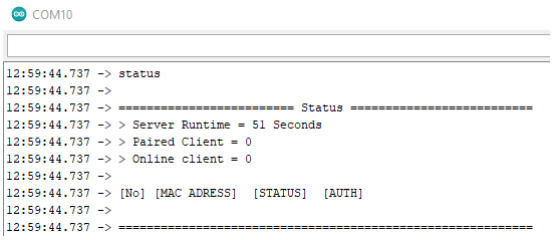

Figure 2. No authentication request

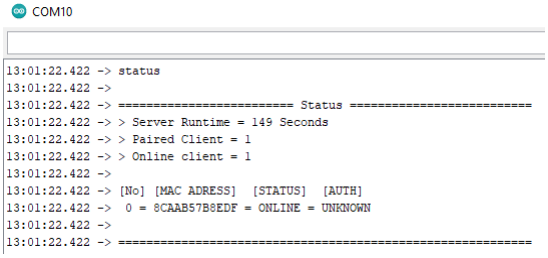

Figure 3. Device '0' or node j requested for an authentication

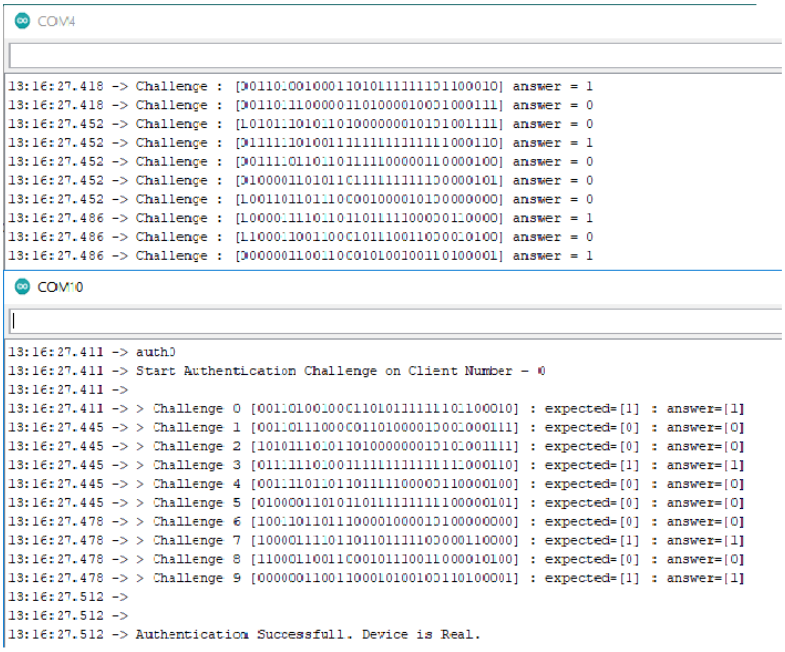

Figure 4. Authentication process between the verifier and device '0' or node j

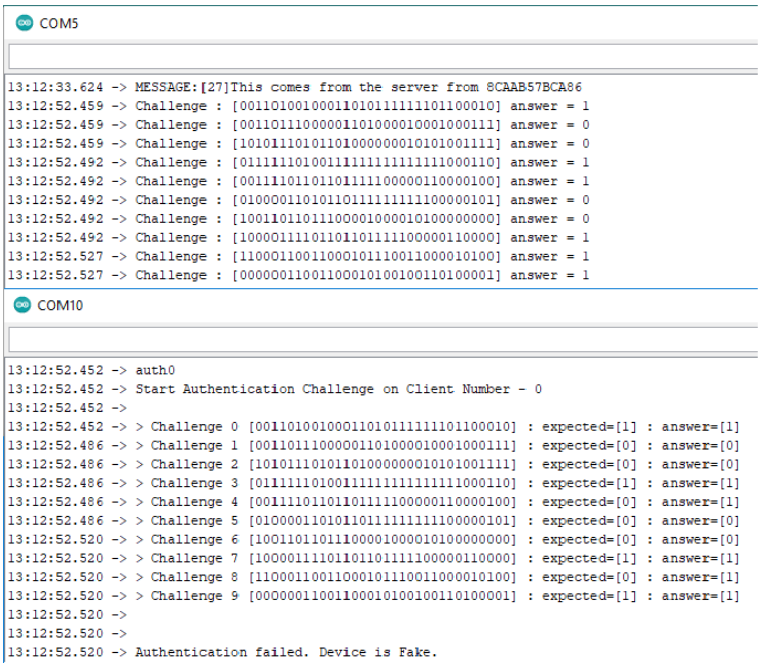

Figure 5. Authentication process between the verifier and device '0′' or node j'

4.2. Estimation of memory usage

The memory usage during the authentication process has been evaluated and summarized in Table 1. For a server configuration, a total of 277681 bytes for code and 5200 bytes for data were occupied on the flash memory (7.1% of flash memory consumption), and 32208 bytes of space was occupied on the SRAM (50.3% of SRAM consumption). Meanwhile, for a client configuration, a total of 278273 bytes for code and 3984 bytes for data were occupied on the flash memory (7.1% of flash memory consumption). In addition, 30640 bytes of SRAM were utilized to configure a client or sensor node (47.9% of SRAM consumption). Note that in this study, only one CRP has been registered in the server's DB to verify the server-client authentication protocol. In practice, the DB should consist enormous number of CRPs for the authentication process since the same CRP cannot be reused to avoid a man-in-the-middle attack. Therefore, the server needs a huge memory space to store the CRPs. This causes no issue as typically the server is resource-rich devices.

Table 1. Memory usage of the proposed authentication protocol based on server-client configuration

in Byte	.text	.data	.bss	Flash	SRAM	Total
Server (Verifier)	277681	5200	27008	282881	32208	309889
Client (Node)	278273	3984	26656	282257	30640	308913

5. CONCLUSION

Identification and authentication are the fundamental security processes in building the "trust" in secured-computing IoT devices. WSN is an example of an IoT application that requires such fundamental security. All the nodes which include the base station in WSN must be authenticated before the data transmission to ensure no loss of privacy which can be potentially caused by the man-in-the-middle attack. Nevertheless, providing the identification and authentication protocol for WSN applications is challenging due to the limited resources in sensor nodes. PUF is seen as a promising identification and authentication technology for WSN applications as it consumes low area overhead and power consumption. In this study, we have provide the proof of concept of a lightweight PUF-based authentication protocol for resources-constrained sensor nodes in WSN. The authentication protocol has been implemented on NodeMCU ESP8266 devices and verified using server-client configuration. Our finding shows that the sensor node which contains the PUF building block can be identified and authenticated as a genuine device using the CRPs database stored in the verifier (i.e., base station). Meanwhile, the sensor node which using the guessed CRPs is successfully authenticated as a fake

device since its CRPs are not registered in the verifier's database. Moreover, based on our analysis, the sensor node only consumes approximately 7% of flash memory and 48% of SRAM during the authentication process.

ACKNOWLEDGEMENT

The authors would like to thank Universiti Teknikal Malaysia Melaka and the Ministry of Higher Education Malaysia for the financial funding under Grant No. FRGS/1/2020/TK0/UTEM/02/56 for completing this project.

REFERENCES

[1] J. H. L. Teo, N. A. N. Hashim, A. Ghazali, and F. A. Hamid, "Ring oscillator physically unclonable function using sequential ring oscillator pairs for more challenge-response-pairs," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 13, no. 3, pp. 892-901, 2019, doi: 10.11591/ijeecs.v13.i3.pp892-901.

[2] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *ACM Conference on Computer and Communications Security*, 2002, pp. 148-160, doi: 10.1145/586110.586132.

[3] M. S. Mispan, H. Sarkawi, A. Z. Jidin, R. H. Ramlee, and H. M. Nasir, "Design and implementation of multiplexed and obfuscated physical unclonable function," *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 9, no. 1, pp. 91-100, 2021, doi: 10.52549/ijeei.v9i1.2664.

[4] Y. Yilmaz, S. R. Gunn, and B. Halak, "Lightweight PUF-based authentication protocol for IoT devices," in *2018 IEEE 3rd International Verification and Security Workshop (IVSW)*, 2018, pp. 38-43, doi: 10.1109/IVSW.2018.8494884.

[5] Y. Yilmaz, V.-h. Do, and B. Halak, "ARMOR: An anti-counterfeit security mechanism for low cost radio frequency identification systems," in *IEEE Transactions on Emerging Topics in Computing*, 2020, doi: 10.1109/TETC.2020.2964435.

[6] U. Guin, A. Singh, M. Alam, J. Canedo, and A. Skjellum, "A secure low-cost edge device authentication scheme for the internet of things," *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*, 2018, pp. 85-90, doi: 10.1109/VLSID.2018.42.

[7] F. Farha, H. Ning, K. Ali, L. Chen, and C. Nugent, "SRAM-PUF based entities authentication scheme for resource-constrained Iot devices," in *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5904-5913, 1 April1, 2021, doi: 10.1109/JIOT.2020.3032518.

[8] M. Barbareschi, A. De Benedictis, E. La Montagna, A. Mazzeo, and N. Mazzocca, "PUF-enabled authentication-as-a-service in Fog-IoT systems," in *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, 2019, pp. 58-63, doi: 10.1109/WETICE.2019.00020.

[9] S. Li, T. Zhang, B. Yu, and K. He, "A provably secure and practical PUF-based end-to-end mutual authentication and key exchange protocol for IoT," in *IEEE Sensors Journal*, ol. 21, no. 4, pp. 5487-5501, Feb. 15, 2021, doi: 10.1109/JSEN.2020.3028872.

[10] M. A. Muhal, X. Luo, Z. Mahmood, and A. Ullah, "Physical unclonable function based authentication scheme for smart devices in Internet of Things," in *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, 2018, pp. 160-165, doi: 10.1109/SmartIoT.2018.00037.

[11] U. Chatterjee *et al*., "Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 3, pp. 424-437, 1 May-June 2019, doi: 10.1109/TDSC.2018.2832201.

[12] 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, doi: 10.1109/TCE.2019.2926192.

[13] X. Tan, J. Zhang, Y. Zhang, Z. Qin, Y. Ding, and X. Wang, "A PUF-Based and cloud-assisted lightweight authentication for multi-hop body area network," *Tsinghua Science and Technology*, vol. 26, no. 1, pp. 36-47, Feb. 2021, doi: 10.26599/TST.2019.9010048.

[14] P. Gope and B. Sikdar, "Lightweight and privacy-preserving two-factor authentication scheme for IoT devices," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 580-589, Feb. 2019, doi: 10.1109/JIOT.2018.2846299.

[15] P. Gope, A. K. Das, N. Kumar, and Y. Cheng, "Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 9, pp. 4957-4968, Sept. 2019, doi: 10.1109/TII.2019.2895030.

[16] J. Long, W. Liang, K. C. Li, D. Zhang, M. Tang, and H. Luo, "PUF-based anonymous authentication scheme for hardware devices and IPs in edge computing environment," *IEEE Access*, vol. 7, pp. 124785-124796, 2019, doi: 10.1109/ACCESS.2019.2925106.

[17] Y. Yilmaz and B. Halak, "A two-flights mutual authentication for energy-constrained IoT devices," in *2019 IEEE 4th International Verification and Security Workshop (IVSW)*, 2019, pp. 31-36, doi: 10.1109/IVSW.2019.8854438.

[18] G. E. Suh and S. Devadas, "Physical Unclonable Functions for device authentication and secret key generation," in *2007 44th ACM/IEEE Design Automation Conference*, 2007, pp. 9-14.
[19] J. Delvaux, R. Peeters, D. Gu, and I. Verbauwhede, "A survey on lightweight entity authentication with strong PUFs," *ACM Computing Surveys*, vol. 48, no. 2, pp. 1-42, 2015, doi: 10.1145/2818186.
[20] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas, "Extracting secret keys from integrated circuits," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 13, no. 10, pp. 1200-1205, Oct. 2005, doi: 10.1109/TVLSI.2005.859470.
[21] J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "A technique to build a secret key in integrated circuits for identification and authentication applications," in *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No.04CH37525)*, 2004, pp. 176-179, doi: 10.1109/VLSIC.2004.1346548.
[22] T. Sutikno, H. S. Purnama, A. Pamungkas, A. Fadlil, I. M. Alsofyani, and M. H. Jopri, "Internet of things-based photovoltaics parameter monitoring system using NodeMCU ESP8266," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 6, pp. 5578-5587, 2021, doi: 10.11591/ijece.v11i6.pp5578-5587.
[23] J. Heaton, *Introduction to Neural Networks for Java, 2nd Edition*, 2nd ed. Heaton Research, Inc., 2008.
[24] G. Hospodar, R. Maes, and I. Verbauwhede, "Machine learning attacks on 65nm Arbiter PUFs: Accurate modeling poses strict bounds on usability," in *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, 2012, pp. 37-42, doi: 10.1109/WIFS.2012.6412622.
[25] M. S. Mispan, H. Su, M. Zwolinski, and B. Halak, "Cost-Efficient Designs for Modeling Attacks Resistant PUFs," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2018, pp. 467-472, doi: 10.23919/DATE.2018.8342054.

BIOGRAPHIES OF AUTHORS

Mohd Syafiq Mispan received B.Eng Electrical (Electronics) and M.Eng Electrical (Computer and Microelectronic System) from Universiti Teknologi Malaysia, Malaysia in 2007 and 2010 respectively. He had experienced working in semiconductor industries from 2007 until 2014 before pursuing his Ph.D. degree. He obtained his Ph.D. degree in Electronics and Electrical Engineering from University of Southampton, United Kingdom in 2018. He is currently a senior lecturer in Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik, Universiti Teknikal Malaysia Melaka. His current research interests include hardware security, CMOS reliability, VLSI design, and Electronic Systems Design.

Aiman Zakwan Jidin obtained his M.Eng in Electronic and Microelectronic System Engineering from ESIEE Engineering Paris France in 2011. He has 2 years of working experience in designing digital IC and digital system in FPGA at Altera Corporation Malaysia, before joining Universiti Teknikal Malaysia Melaka as lecturer and researcher, in Electronics and Computer Engineering. His research interests include FPGA Design and Digital System Design.

Muhammad Raihaan Kamaruddin received the B.Eng (Electronics and Computer Systems) and M.Eng (Electronics and Information Science) degrees from Takushoku University, Japan, He is working toward the PhD degree in Electronics and Computer Engineering with the Universiti Teknikal Malaysia Melaka (UTeM). His PhD is on the Implementation of bio-inspired robotic navigation system using stochastic computing. He has working experience as lecturer in Universiti Teknikal Malaysia Melaka (UTeM) for 10 years (2010-present). His research interest includes machine learning, robotic and stochastic computing.

Haslinah Mohd Nasir received her Bachelor Degree in Electrical-Electronic Engineering (2008) from Universiti Teknologi Malaysia (UTM), MSc (2016) and PhD (2019) in Electronic Engineering from Universiti Teknikal Malaysia Melaka (UTeM). She had 5 years (2008-2013) experience working in industry and currently a lecturer in UTeM. Her research interest includes microelectronics, artificial intelligence and biomedical.