A PUF-based Approach for Sustainable Cybersecurity in Smart Agriculture

Venkata K. V. V. Bathalapalli
Comp. Science & Engineering
University of North Texas.
VenkatakarthikvishnuvardBathalapalli@my.unt.edu

Saraju P. Mohanty
Comp. Science & Engineering
University of North Texas.
saraju.mohanty@unt.edu

Elias Kougianos
Electrical Engineering
University of North Texas.
elias.kougianos@unt.edu

Venkata P. Yanambaka
College of Science & Engineering
Central Michigan University.
yanam1v@cmich.edu

Babu K. Baniya
Computer Science & Digital Technologies
Grambling State University.
baniyab@gram.edu

Bibhudutta Rout
Dept. of Physics
University of North Texas.
bibhudutta.rout@unt.edu

2021 19th OITS International Conference on Information Technology (OCIT) | 978-1-6654-1664-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/OCIT53463.2021.00080

***Abstract*—The simplicity, low cost, and scalability of Internet of Things (IoT) devices have led researchers to study their applications in a wide range of areas such as Healthcare, Transportation, and Agriculture. IoT devices help farmers to monitor the conditions in a field. These are connected to edge devices for real-time analysis. The edge servers send commands to actuators in the farm directly, without human intervention. At the same time, security vulnerabilities are a big concern, concomitant with the increasing utilization of IoT devices. If the duplication of an IoT device occurs and attackers gain access to the system, then the integrity of the entire ecosystem will be at stake, regardless of the application domain. This paper presents a Physical Unclonable Function (PUF) based hardware security primitive for the authentication of Internet of Agro-Things (IoAT) devices. The proposed security scheme has been prototyped with a testbed evaluation. An arbiter PUF module has been used for the validation of the proposed scheme. The PUF based security primitive is lightweight, scalable, and robust as it mainly depends on inherent manufacturing variations, thereby ensuring no chance for the duplication of IoT devices.**

***Index Terms*—Smart Agriculture, Internet of Things (IoT), Internet of Agro-Things (IoAT), Cybersecurity, Physical Unclonable Function (PUF), Arbiter PUF**

I. Introduction

Smart Agriculture is the use of information and communication technologies to enhance the productivity in farming [1], [2]. The utilization of the IoT is useful in the areas of “Fertigation” which is the process of monitoring remotely the usage of fertilizers, pesticides, and other soil products and analyzing the soil moisture values, thereby playing an important role in determining soil quality [3]. Water resource management is another important aspect of Smart Agriculture where water resources are monitored remotely and where proper analysis can be carried out by farmers and decision making can be done based on the information from sensors in the field [3]. Agriculture is the main occupation of the people in almost all *emerging* economies. This sector is the source of income for almost 70% of the population in developing countries but is contributing only up to 18% to 19% of the Gross Domestic Product (GDP) [4]. As global population growth is at an unprecedented rate, productivity in agriculture also needs to be increased in accordance with the population growth. Various applications of the IoT in agriculture are shown in Fig. 1.

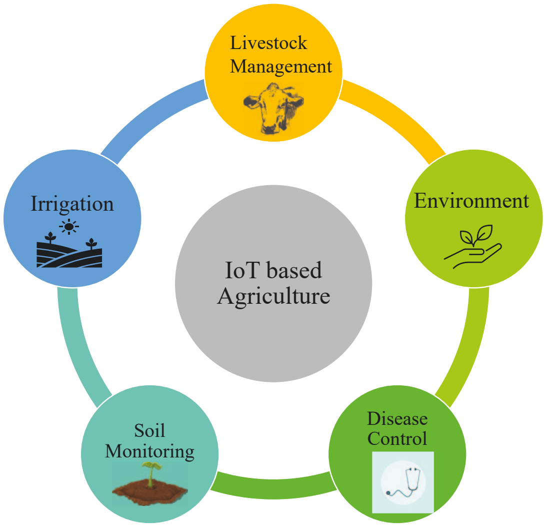


Fig. 1: IoT Applications in Agriculture

In Smart Agriculture various sensors in the field, such as soil moisture sensors, and sensors embedded inside the cattle to monitor their health are responsible for collecting the data and sending it to the edge for real-time analysis and decision making using the Internet [5], [6].

The rest of the paper is organized in the following manner: Section II presents the security issues and related research in Smart Agriculture. Section III presents the novel contributions of the current paper. Section IV presents the proposed PUF

978-1-6654-1664-1/21/$31.00 ©2021 IEEE
DOI 10.1109/OCIT53463.2021.00080

based security protocol. Section V presents the design of the Arbiter PUF. Section VI outlines the implementation details and Section VII presents the conclusions and directions for future research.

II. Related Research on Security in Smart Agriculture

Existing device authentication schemes heavily rely on public key cryptography which increases the computational load on the processor. The U.S.Department of Homeland and Security report on security issues in Agriculture highlights the importance of data security, confidentiality, and integrity in agriculture [5]. Cloud and edge computing schemes have become the backbone for IoT applications in Smart Farming due to their information processing capabilities. A cloud-based scheme effectively analyzes the data in a more accurate way while an edge computing paradigm is a subsidiary of the cloud, as information processing is done near the farm, where data generation takes place [7]. Data security and privacy have become a serious concern among the farming community. Though smart agriculture involves processing non-personal data, linking it to a particular identity becomes a cause of concern. For instance, linking livestock data to farmer and crop insurance details linked with the farmer's personal identity becomes a potential point of entry for an adversary to affect the whole farm security ecosystem [5]. An increasing number of IoAT devices also brings forth the problem of scalability and information security. Hence Big data, Blockchain, and Artificial intelligence are gaining prominence for effective decision making and processing of huge information data sets from IoAT devices [8]. Various IoT sensors and their applications in Smart Agriculture are presented in Table I.

TABLE I: IoT Devices in Agriculture

Sensor	Operations
pH Sensor	It measures the amount of nutritional contents in the soil to asses the soil health for irrigation [9].
Humidity Sensor	It measures the humidity level in air which directly or indirectly affects the process of photosynthesis and growth of plant leaf [10].
Soil Moisture Sensor	Monitors the water content in the soil [11].
Gas Sensor	It measures the amount of Toxic gases in the greenhouse and live stock [12].

A. Security Threats in Smart Agriculture

In a Smart Farm, many IoT devices are connected to the Internet. These devices are vulnerable to various types of attacks and when a malicious node is injected into the system by an attacker, the whole farm security is jeopardized [13].

The edge server sends commands to the on-field actuators. If the attacker is able to observe the flow of data from on-field sensor, like soil moisture, humidity, and temperature data to the edge and cloud, then an adversary can gain access to the data, impersonate the server, and can take control of the system thereby sending malicious commands to the on-field actuators to perform operations that could affect productivity.

In reverse engineering attacks, an adversary analyzes the core components of the process to gain access to the system or network [14]. This allows the attacker to learn the vulnerabilities of the devices. Once the attacker gains access to the device and its vulnerabilities, the attacker can tamper with the device and reintroduce it to the IoT environment for more damage [14]. An attacker can also intercept or, in some cases, modify the data that is being transmitted in the network. Such attacks are called Man-in-the-Middle attacks. Sometimes, an unauthorized user can gain access to the data or the network. In such Access Attacks, an attacker can access data and steal it [15]. An attacker can access the IP address of a device transmitting the data and spoof it to perform a spoofing attack [16].

B. Solutions for Threats in Smart Agriculture

In general, Smart Agriculture relies on a Peer-to-Peer (P2P) network paradigm. Such networks rely on device authentication mechanisms for communication and data transfer. But these algorithms add additional strain on the already resource constrained devices [17]. Many authentication protocols were proposed for security threats and vulnerabilities [18] where an algorithm that uses session keys and public keys for expedited encryption and decryption process is presented. A summary of security aspects in Smart Agriculture is given in Table II. There are also many Blockchain based solutions in Smart Agriculture. The blockchain can help in maintaining data integrity and security during the storage of collected data. Blockchain-based applications in Smart Farming are predominantly used for production and inventory management [17]. Such solutions cannot be used for resource constrained devices such as IoT for device authentication unless a lightweight authentication mechanism is available. Many such solutions exist but implementing them becomes a challenge.

III. Novel Contributions of the Current Paper

A. Problem Addressed in the Current Paper

Malicious IoT devices on the farm could affect the integrity of the system. A person can intentionally place a fake node in place of a legitimate node or sensor which performs operations that could ultimately affect the farm productivity by sending wrong data to the cloud where decision making is done based on the data from devices on field. As there is no security protocol to check the legitimacy of the devices, node replication could not be identified. A malicious actuator in irrigation could flood the field or not release water to the field. In the absence of a proper authentication mechanism, a soil moisture sensor can capture values and sends the data to the edge server. Depending on the moisture data, the edge server sends commands to the actuators in the field to activate sprinklers to increase the moisture level of the field. If, for instance, the soil moisture sensor is replaced by a false node which sends inaccurate data to the edge server, the server sends wrong commands to the actuators depending on the

TABLE II: Security protocols for Smart Agriculture in the Literature

Works	Objective	Features	Drawbacks
Threats to Precision Agriculture [5]	Uncovers major security vulnerabilities in Smart Agriculture.	Defines Precision Agriculture and security practices.	Fails to distinguish between threats in CPS and threats in precision agriculture
Enhanced Secure Device Authentication Algorithm in P2P-based Smart Farm System [5]	Enhanced peer to peer communications in smart farms using cryptography.	A protocol for encryption and decryption to facilitate authentication	No implementation and analysis of the protocol on testbed
Remote Farm Security [19]	Implementation of Machine learning techniques for videos during Farm surveillance	Real time analysis and decision making	Scalability
Cyber Security in Food distribution sector [5]	uncovers major security issues in Agri Food system	outlines the need for data security in AgriFood sector by explaining the increase of data usage	No security protocols proposed
Smart agriculture Cyber Security issues [3]	Outlines security issues and challenges in Smart Agriculture	Highlights the security issues and challenges including agro-terrorism, ransomware and other cyber threats	No test bed evaluation and results
Cyberbiosecurity [20]	Defines cyberbioeconomy and its security issues	Highlights how the infrastructure and data issues affect the agro economy	No proposal of a feasible solution

data from the falsified node. The field is then either over flooded or under flooded. This can cause great damage to the whole agriculture ecosystem. Fake or malicious nodes in Smart Agriculture could be a huge problem. An overview of the IoAT is represented schematically in Fig. 2.

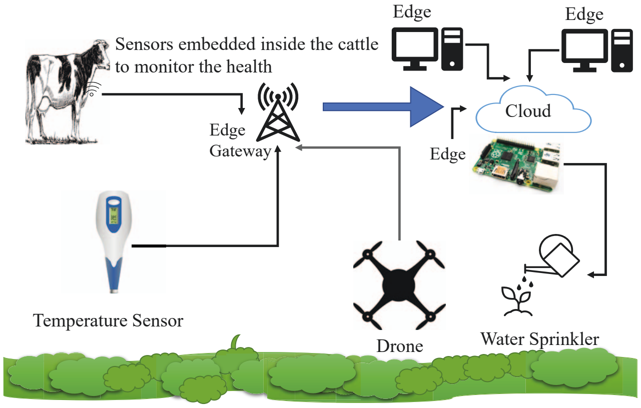


Fig. 2: Internet of Agro-Things

PUF based security scheme is simple, doesn't require much computation, and best, makes use of the device characteristics to create a unique defined fingerprint thereby preventing the duplication of sensors on field by authentication using hardware without storing the keys in memory [5].

B. Solutions Proposed in the Current Paper

As IoAT devices are resource constrained, complex security mechanisms are inappropriate to implement, hence PUF based security can be used to address these issues [13]. IoT devices with PUF module embedded inside the device can be authenticated without requiring large power and memory. As the PUF modules are unique for each device, there will be no chances for duplication. Hence credibility is ensured using PUF based security scheme in IoAT devices.

C. Novelty and Significance of the Proposed Solution

IoT devices are authenticated using the uniqueness of inherent micro manufacturing variations of a chip. A PUF based security protocol is proposed to address the gaps in security pertaining to an IoT sensor. A PUF based low power architecture ensures minimal consumption of power [13]. The existing research has mostly been focusing on data security while in this paper we propose a protocol to addresses device security which is lightweight and robust. Edge computing is used to process the data which is critical and time constrained. In some applications, it is preferred over cloud computing due to low latency and the edge server can easily be deployed in remote areas because it doesn't require connectivity to a central server.

IV. The Proposed PUF based Authentication scheme in Smart Agriculture

This section presents the proposed PUF based security Protocol. A scheme is developed where data exchange takes place between the IoAT devices, which are smart consumer electronic devices, and edge servers for real-time data analysis and decision making. This scheme involves two stages: Device enrollment and Authentication. Initially, the client and server are connected to the same PUF module. Two different challenges are sent to both the server and client which are connected to the same PUF module, one for the client and one for the server. The two output response keys from Server and Client are XOR ed and the resultant output is then given as the challenge input to the server. A hash is computed on the resultant response output from the server and the hash value along with initial challenges are stored in a secure database. During the authentication phase hash is computed at the server using the above steps and device authenticity is checked by comparing the computed hash value and stored hash value in the secure database [13]. If the obtained hash value is equal to the stored hash value, then the device is considered as authentic.

A. Proposed Security Protocol in Edge Computing Platforms

The client devices are smart sensors on the farm which collect data for analysis, processing, and decision making. They can be connected to servers either wired or wireless. The end devices will enroll using PUF keys generated so any duplication of end devices will be immediately identified during authentication as the enrollment is done only once initially. The farmer will be able to access the data from devices using the Internet for analysis. Temperature, humidity, and pH values collected by end devices in the farm are sent to the edge for real-time analysis. After proper analysis, commands are sent to the actuators on the ground. Analysis of obtained information is done and commands are given to actuators like sprinkler to water the farm for a specified time. Edge devices are equipped with the PUF module just like IoAT smart consumer electronic devices. The process of device enrollment is shown in Fig. 3 and IoAT enrollment and authentication processes are explained in Algorithm 1 and Sec. IV-B.

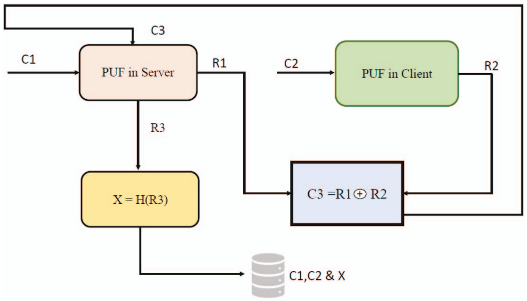


Fig. 3: Device Enrollment Process

B. IoAT Device Enrollment Process

In this phase, the IoAT device enrolls itself with its unique fingerprint. Initially the IoAT device and server with the same PUF module are given two separate challenges which are $C1$ and $C2$, and responses $R1$ and $R2$ are obtained from the client and server. The two responses $R1$ and $R2$ are XORed and the output is given as the second challenge input to the server. Finally a hash is computed on the output response $R3$ from the server. The hash output X along with challenges $C1$ and $C2$ are stored in a secure Database during this enrollment process.

C. IoAT Device Authentication Process

During the Authentication phase, Responses $R1^{'}$ and $R2^{'}$ from the server and client obtained are XOR ed and finally $C3^{'}$, which is the XOR ed output is given as the challenge input to the server and response $R3^{'}$ is obtained. Finally a hash is computed on the final response $R3^{'}$ from server and obtained hash $X^{'}$ and initially stored hash X in the secure data base are compared. If X and $X^{'}$ match, then the IoAT device is authentic, otherwise the device is considered as illegitimate. Fig. 4 represents the authentication phase of the proposed security scheme.

Algorithm 1 Enrollment and Authentication of IoAT Devices

```
The Challenges $C1$ and $C2$ are given to the Server and Client PUF module.
$C1\rightarrow$ SERVER, $C2\rightarrow$CLIENT
Perform XOR operation on the Responses.
$R1 \oplus R2$
Assign the XOR output to the Challenge $C3$
$C3 = R1 \oplus R2$
Challenge $C3$ is given to the Server and hash computation is performed on the obtained final response $R3$.
$X = H(R3)$
During Authentication $R1'$ and $R2'$ are obtained using challenges $C1$ and $C2$ stored in database and the XOR ed output is assigned to Challenge $C3$.
$C3' = R1' \oplus R2'$
Response $R3'$ is obtained from the server using $C3'$ as challenge input and hash is computed.
$X' = H(R3')$
if $X == X'$ then
    Device is Authentic.
else if $X$ !== $X'$ then
    Device is not Authentic.
end if
```

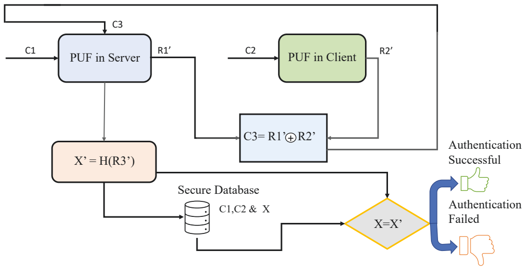


Fig. 4: IoAT Device Authentication Process

V. Arbiter PUF

A PUF is a hardware security primitive which utilizes the uniqueness of variations in manufacturing of an electronic device to create a fingerprint exclusively for the device [21]. An arbiter PUF in this work is designed with large combinational logic blocks based on the structure of an Field Programmable Gate Array (FPGA). The design of an Arbiter PUF is shown in Fig. 5.

The Arbiter PUF is most widely used in applications in control and management. Many systems use a combination of an arbiter PUF with cryptography embedded in the chip. It is a physical entity incorporated in a structure. Fig. 6a and Fig. 6b show the Hamming distance and reliability of the keys generated using the Arbiter PUF module.

VI. Experimental Results

During the enrollment phase, the server and client send challenge inputs to the PUF module and collects the response outputs. The client, which is also connected to the same PUF, sends a different challenge input to the PUF module and

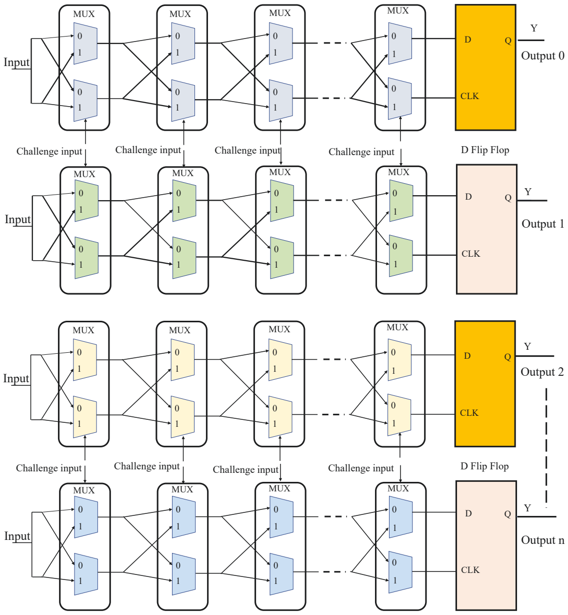
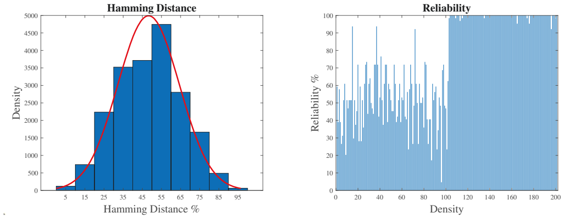


Fig. 5: Arbiter PUF

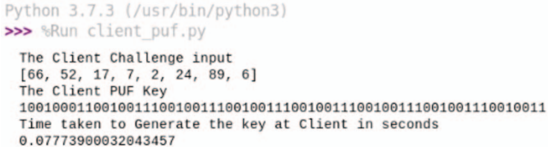


(a) Hamming Distance.

(b) Reliability.

Fig. 6: Arbiter PUF Metrics

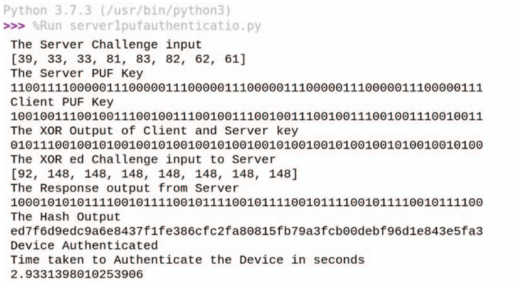
collects the output key. The output at the client during the enrollment phase is shown in Fig. 7.



```
Python 3.7.3 (/usr/bin/python3)
>>> %Run client_puf.py
 The Client Challenge input
 [66, 52, 17, 7, 2, 24, 89, 6]
 The Client PUF Key
 1001000110010011100100111001001110010011100100111001001110010011
 Time taken to Generate the key at Client in seconds
 0.07773900032043457
```

Fig. 7: Output from Client during Enrollment

The total time taken to generate the key at client is 0.07 seconds. The collected output key is sent to the server through UDP and the server with the initially obtained key and the received key performs an XOR operation and creates a new key. The XORed output is given as challenge input to PUF module connected to the server. A hash operation is performed on the obtained response output key from the server and the hash is stored in a secure database. During the authentication phase the same sequence of operations is performed at both ends and the collected PUF keys from client and server are XORed and the output is then given as challenge input to the server, and the hash is computed on the output key from the server. The obtained hash is compared with the stored hash in the secure database and if both hashes match, then the device is authenticated. The output at server during the authentication is shown in Fig. 8.



```
Python 3.7.3 (/usr/bin/python3)
>>> %Run server1pufauthenticatio.py
 The Server Challenge input
 [39, 33, 33, 81, 83, 82, 62, 61]
 The Server PUF Key
 1100111100000111000001110000011100000111000001110000011100000111
 Client PUF Key
 1001001110010011100100111001001110010011100100111001001110010011
 The XOR Output of Client and Server key
 0101110010010100100101001001010010010100100101001001010010010100
 The XOR ed Challenge input to Server
 [92, 148, 148, 148, 148, 148, 148, 148]
 The Response output from Server
 1000101010111100101111001011110010111100101111001011110010111100
 The Hash Output
 ed7f6d9edc9a6e8437f1fe386cfc2fa80815fb79a3fcb00debf96d1e843e5fa3
 Device Authenticated
 Time taken to Authenticate the Device in seconds
 2.9331398010253906
```

Fig. 8: Output from Server during Authentication

The proposed scheme is robust as $R2$ generated at the client is sent to the server and unique challenge input $C3$ is generated using the two PUF keys $R1$ from the server and $R2$ from the client. Even if one key is compromised the hash value of obtained $R3$ from the server will change. In this way both client's and server's legitimacy is brought into confidence during authentication. The purpose of using the XOR operation is to create a unique key so as to improve the robustness of the proposed security protocol. The time taken to authenticate the device is 0.16 to 2.93 seconds and the power consumption by a Single Board Computer is 3.2 Watts. The parameters of the proposed security scheme are given in Table III.

TABLE III: Characterization of the Proposed Security Scheme.

Parameters	Values
Server	Single Board Computer
Client	Single Board Computer
PUF Implementation	Field-Programmable Gate Array
Hamming Distance	48%
Randomness	41.7%
Time taken to generate the key at Client	0.07 seconds
Time taken to generate the key at Server	0.07 seconds
Time taken to Authenticate the Device	0.16 to 2.93 seconds
Power consumption of Server/Client	3.2 Watts

A Single Board Computer (a Raspberry Pi) is used as the server and the client and PUF module are built on a Digilent Basys 3 Xilinx FPGA. The baud rate is 9600 for establishing serial communication between PC and FPGA. The Server and Client are connected to FPGA Pmod connector by shorting TX and RX pins on raspberry pi with the TX and RX pins on FPGA. The minimal power consumption of the Raspberry pi substantiates the robustness of the proposed security scheme. The experimental setup is shown in Fig. 9. The original Client and Server PUF keys are not used during the final hash computation and are not exposed. Hence more security is ensured through the security protocol.

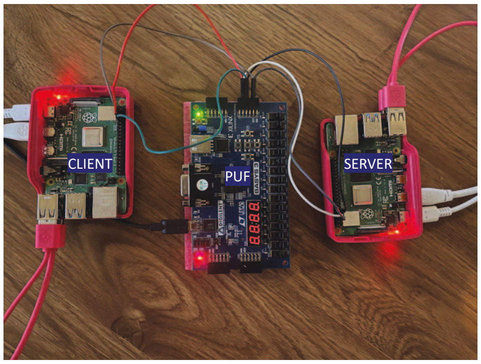


Fig. 9: Experimental Setup.

VII. Conclusion and Future Research

Smart Agriculture cybersecurity issues have now become a focal point for the research community. As IoT device utilization is being extended to agriculture, security vulnerabilities of IoT devices are becoming bottlenecks for Smart Agriculture practices. This paper presents a robust security protocol to address the security issues pertaining to authenticity of IoT devices. Each device is equipped with a PUF module that can be used for authentication. Client challenge and response keys are not stored in server memory. Even if the attacker is able to observe the flow of data, the adversary may not be able to get access because in the server a unique key is generated using an XOR operation with both client and server PUF keys. Hence both client and server are involved in the authentication process which brings more security to the system. We envision working on the concept of Security by Design (SbD) and Privacy by Design (PbD) in IoT which is essential for the growing smart Farming sector.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant number HBCU-EiR-2101181. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] V. Udutalapally, S. P. Mohanty, V. Pallagani, and V. Khandelwal, “sCrop: A novel device for sustainable automatic disease prediction, crop selection, and irrigation in Internet-of-Agro-Things for smart agriculture,” *IEEE Sensors Journal*, vol. 21, no. 16, pp. 17 525–17 538, Aug 2020.

[2] P. K. Tripathy, A. K. Tripathy, A. Agarwal, and S. P. Mohanty, “MyGreen: An IoT-Enabled Smart Greenhouse for Sustainable Agriculture,” *IEEE Consumer Electronics Magazine*, vol. 10, no. 4, pp. 57–62, July 2021.

[3] L. Barreto and A. Amaral, “Smart farming: Cyber security challenges,” in *Proc. International Conference on Intelligent Systems*, 2018.

[4] S. Verma, R. Gala, S. Madhavan, S. Burkule, S. Chauhan, and C. Prakash, “An internet of things (IoT) architecture for smart agriculture,” in *Proc. Fourth International Conference on Computing Communication Control and Automation*, 2018.

[5] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, “Security and privacy in smart farming: Challenges and opportunities,” *IEEE Access*, vol. 8, pp. 34 564–34 584, 2020.

[6] N. Nhamo and D. Chikoye, “Smart agriculture,” in *Smart Technologies for Sustainable Smallholder Agriculture*. Elsevier, 2017, pp. 1–20.

[7] M. S. Farooq, S. Riaz, A. Abid, K. Abid, and M. A. Naeem, “A survey on the role of IoT in agriculture for the implementation of smart farming,” *IEEE Access*, vol. 7, pp. 156 237–156 271, 2019.

[8] S. Wolfert, L. Ge, C. Verdouw, and M.-J. Bogaardt, “Big data in smart farming – a review,” *Agricultural Systems*, vol. 153, pp. 69–80, may 2017.

[9] A.-J. Garcia-Sanchez, F. Garcia-Sanchez, and J. Garcia-Haro, “Wireless sensor network deployment for integrating video-surveillance and data-monitoring in precision agriculture over distributed crops,” *Computers and Electronics in Agriculture*, vol. 75, no. 2, pp. 288–303, feb 2011.

[10] S. Balaji, K. Nathani, and R. Santhakumar, “IoT technology, applications and challenges: A contemporary survey,” *Wireless Personal Communications*, vol. 108, no. 1, pp. 363–388, apr 2019.

[11] C. Brewster, I. Roussaki, N. Kalatzis, K. Doolin, and K. Ellis, “IoT in agriculture: Designing a europe-wide large-scale pilot,” *IEEE Communications Magazine*, vol. 55, no. 9, pp. 26–33, 2017.

[12] V. Bapat, P. Kale, V. Shinde, N. Deshpande, and A. Shaligram, “WSN application for crop protection to divert animal intrusions in the agricultural land,” *Computers and Electronics in Agriculture*, vol. 133, pp. 88–96, feb 2017.

[13] 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.

[14] Liang, Xingwei and Kim, Yoohwan, “A Survey on Security Attacks and Solutions in the IoT Network,” in *Proc. 11th IEEE Annual Computing and Communication Workshop and Conference (CCWC)*, 2021, pp. 0853–0859.

[15] B. Chen, J. Wan, A. Celesti, D. Li, H. Abbas, and Q. Zhang, “Edge computing in iot-based manufacturing,” *IEEE Communications Magazine*, vol. 56, no. 9, pp. 103–109, 2018.

[16] P. K. Sharma, M.-Y. Chen, and J. H. Park, “A software defined fog node based distributed blockchain cloud architecture for IoT,” *IEEE Access*, vol. 6, pp. 115–124, 2018.

[17] M. Gupta, M. Abdelsalam, S. Khorsandroo, and S. Mittal, “Security and privacy in smart farming: Challenges and opportunities,” *IEEE Access*, vol. 8, pp. 34 564–34 584, 2020.

[18] Chae, Cheol-Joo and Cho, Han-Jin, “Enhanced Secure Device Authentication Algorithm in P2P-Based Smart Farm System,” *Peer-to-Peer Networking and Applications*, vol. 11, no. 6, pp. 1230–1239, 2018.

[19] D. D. Abuan, A. C. Abad, J. B. L. Jr, and E. P. Dadios, “Security systems for remote farm,” *Journal of Automation and Control Engineering*, vol. 2, no. 2, pp. 115–118, 2014.

[20] S. E. Duncan, R. Reinhard, R. C. Williams, F. Ramsey, W. Thomason, K. Lee, N. Dudek, S. Mostaghimi, E. Colbert, and R. Murch, “Cyberbiosecurity: A new perspective on protecting U.S. food and agricultural system,” *Frontiers in Bioengineering and Biotechnology*, vol. 7, Mar 2019.

[21] S. Joshi, S. P. Mohanty, and E. Kougianos, “Everything you wanted to know about PUFs,” *IEEE Potentials*, vol. 36, no. 6, pp. 38–46, nov 2017.