IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 25 July 2024, accepted 20 August 2024, date of publication 26 August 2024, date of current version 5 September 2024.

*Digital Object Identifier 10.1109/ACCESS.2024.3449702*

RESEARCH ARTICLE

# ZEBRA: Zero Trust Architecture Employing Blockchain Technology and ROPUF for AMI Security

**FARIS ALSULAMI[1], (Member, IEEE), AKSHAY R. KULKARNI[2], (Member, IEEE), NOOR AHMAD HAZARI[3], AND MOHAMMED Y. NIAMAT[2], (Life Member, IEEE)**

[1]Department of Computer and Network Engineering, University of Jeddah, Jeddah 23890, Saudi Arabia
[2]Department of Electrical Engineering and Computer Science, The University of Toledo, Toledo, OH 43606, USA
[3]Department of Electrical Engineering, College of Charleston, Charleston, SC 29403, USA

Corresponding author: Faris Alsulami (fnalsulami@uj.edu.sa)

**ABSTRACT** Smart grid (SG) has evolved as a recent topic of discussion and research globally, due to the integration of communication and internet in its network. It facilitates the bidirectional flow of information and power making it vulnerable to attacks including denial of service, fault injection, man-in-the-middle, etc. An integral part of the SG, is the advanced metering infrastructure (AMI), which in turn embodies within itself a critical component of SG such as smart meter (SM), utility company (UC), etc. The AMI also exchanging data and electricity within itself, is a gold mine for adversaries. In addition, the smart meter, being a hardware entity, is susceptible to hardware oriented attacks. In this work, a novel authentication scheme, ZEBRA, for the AMI is proposed. ZEBRA utilizes a combination of Ring Oscillator Physical Unclonable Functions (ROPUFs) for authentication and blockchain for traceability in a Zero Trust Architecture (ZTA) to enhance the security of the AMI. The architecture entails a design that allows for the smart meters in the AMI network to be retrofitted with the new hardware and does not require any use of onboard memory. The authentication scheme, itself, is built to function using the Hamming code parity bits of the ROPUF's response, rather than the direct responses from the ROPUFs. This ensures a higher degree of difficulty towards a malicious actor attempting to hack the device. By combining ROPUFs and blockchain technology for ZTA a maximum security, real-time AMI authentication scheme is realized. The investigation aimed at satisfying the tenets of ZTA laid down by National Institute of Standard and Technology. ROPUF and blockchain have been used individually and together to realize these tenets for sucessful implementation of ZEBRA.

**INDEX TERMS** Advanced metering infrastructure, blockchain technology, hardware security, ring oscillator physical unclonable functions, zero trust architecture.

## I. INTRODUCTION

In efforts to modernize the electrical grid, the smart grid system has been proposed to update the traditional architecture. The smart grid utilizes a two-way communication between the entities in a network and enhances the computing power in order to improve the efficiency and reliability of the current system [1]. The two-way communication is a key characteristic of the smart grid (SG) and allows for all participants of the network to exchange information that is valued and trusted. The secure interaction of actors in a smart grid is shown in Fig. 1, reproduced from NISTIR [2].

At the core of this smart grid is the Advanced Metering Infrastructure (AMI), which consists of the Smart Meters (SMs), Data Collectors (DCs) and the data management systems running in the Utility Company (UC) which control all the communication and data exchange [3]. The AMI consists of different networking channels and systems that

The associate editor coordinating the review of this manuscript and approving it for publication was Liang-Bi Chen.

gather and analyze the data transmitted via smart grids. Moreover, various power service applications are attached to AMI to gather the relevant data from smart grids and meters. AMI plays an important role in the analysis and functions of smart grids [4].

Most of the equipment used in grids and energy distribution is made up of embedded systems. These systems have limited processing and computational power. The equipment and infrastructure required for smart grids are critical to the implementation of seamless communication and data analysis. As a result, security for these systems must be high to avoid any malicious attacks. Such attacks can potentially damage the infrastructure and distribution systems. As AMI is an integral and essential part of the smart grid; it is the most sought after attack target for adversaries. Manipulation through IoT attack, falsified data injection and system faults attacks are some of the possible attacks that can disrupt the normal functioning of the AMI [5]. These attacks may lead the smart grid to cause blackouts, imbalance in response-demand systems, incorrect load management, tripping and faults, and many more [6]. A large portion of known attacks on the AMI focus on exploiting the entities within the network. A masquerade attack is an example of an exploitation attack, in which an illegitimate user may attempt to gain greater privileges than they should have to perform unauthorized actions on devices in the AMI [7].

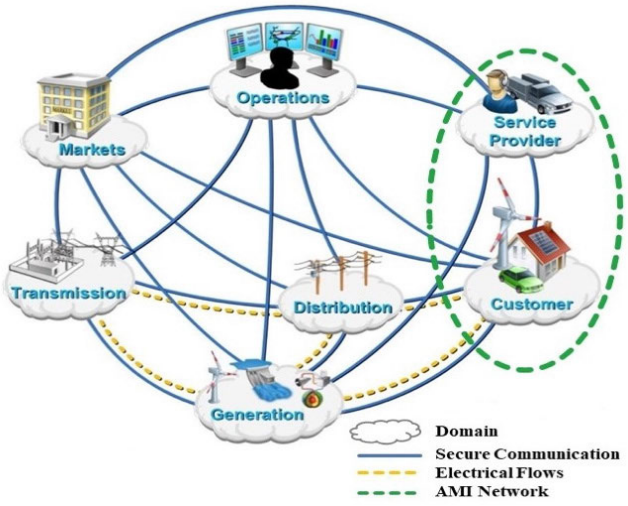


**FIGURE 1.** Smart grid network model [2].

Researchers are exploring various methods to enhance Advanced Metering Infrastructure (AMI) security. A lightweight solution for managing cryptographic keys in smart meter networks is proposed in [8], enabling secure key sharing and efficient private key updates using physical unclonable functions. In terms of data transmission security, a Concealed Based Security Scheme (CBSS) was introduced in [9] that reduces computational load and energy consumption while providing data authentication. Taking a network-centric approach, authors in [10] develop a secure smart metering platform based on the SCION network to address communication vulnerabilities. Investigation conducted in [11] focuses on the impact of increased data loads from grid edge devices and Distributed Energy Resources (DERs) on network performance, offering models to manage latency, packet loss, and congestion. Finally, authors in [12] address privacy concerns in the Electric Smart Grid (ESG), highlighting the effectiveness of Multi Authority Access Control (MAAC) in protecting sensitive data.

Another potent weapon is blockchain technology, which can be used to protect the AMI during authentication and to assess real-time energy consumption data. The real-time data is collected from smart meter that can provide the required useful information regarding the hardware. The collection of data is vital to ensure the security of smart meters. Another technique in security of AMI is physical unclonable functions (PUFs) which are used to protect hardware [13]. PUFs act as a fingerprint to any device that enhances the security of the device significantly [14].

The combination of PUFs and blockchain have been used in various domain including microelectronics supply chain [15]. The use of PUFs for verification along with blockchain technology can prevent the smart grid from providing falsified data and protect it from malware attacks [16]. The combination of these two technologies can prevent Trojans and malware from accessing sensitive data and solve security vulnerabilities. Moreover, these technologies can easily be integrated with smart meter and grid infrastructures. Modern systems and networking channels are more sophisticated and advanced with various applications. At the same time, these modern systems are more vulnerable to both physical and software attacks. The traditional system architecture is not enough to provide the required security from such attacks.

Therefore, the latest systems utilize zero trust architecture (ZTA) in networks to protect sensitive data from security breaches. Kindervag [17] first introduced ‘‘Zero Trust’’ in mid-2010 to tackle modern attacks in the information security domain. According to NIST SP 800-207 [18] ‘‘a cybersecurity plan that implements the concepts of zero trust and encompasses component relationships, workflow planning, and access policies is called a zero-trust architecture (ZTA)’’. The main advantages of ZTA are enhanced security and universal authentication for computational resources and relevant data.

Malicious attacks target the vulnerabilities in AMI infrastructure. Therefore, it is essential to provide AMI with the necessary tools and systems to protect sensitive data against adversaries that can cause significant damage to the smart grid and metering infrastructure. Many current methods of security [19], [20], [21], [22], [23], [24], [25], [26], as discussed and cited in Section II, do not defend against such attacks, as it is assumed that, since the user appears to be legitimate based on everything except intention, the user is trustworthy and can be given access to any information or

actions that are within their level of access. It is for this reason that this paper proposes a novel protocol for the verification of the AMI.

This protocol implements a zero trust architecture (ZTA) that is enabled by blockchain for monitoring and physical unclonable functions (PUFs) on field programmable gate arrays (FPGAs) for authentication. Due to PUFs' ability to replicate outputs unique to the device they are located on, such a protocol allows for the removal of the requirement for any entity that is not the utility company (UC) to have any secure nonvolatile memory to keep track of secret keys. The implementation of ZTA allows for the nullifying of many attacks that rely on access being maintained by a malicious actor and offers complete traceability of the transaction of any data that is sent between all devices in the network due to the blockchain.

The main contributions of this paper are as follows:

- Building a novel authentication protocol for securing AMI using zero trust architecture realized by blockchain and PUFs.
- Developing an ANN-based modeling attack resistant ROPUF with close to ideal performance metrics.
- Developing a blockchain system to ensure traceability and accountability between participants in the AMI.
- Developing an ANN-based modeling attack to test the security level of ROPUF.
- Calibrating the three concepts viz., ROPUF, blockchain and ZT to work in tandem for security of AMI.

## II. RELATED WORK

Many authentication schemes for the AMI have been used previously for key authentication, communication networks, smart meter, and data collection. Current technologies used for smart meter usually include cryptography that is based on electrically erasable memory programs or uses random access memory [19], [20], [21]. These techniques are, however, susceptible to malicious attacks.

These vulnerabilities have been significantly investigated and attempts for their countermeasures are presented and exclusively available in literature. Authors in [22], present an efficient security protocol for AMI communication, called Integrated Authentication and Confidentiality (IAC). However, the authentication here is done via an authentication server located at a local management office, which poses integrity and availability threats. Also, a server under attack, can leak the information stored, risking the AMI and SG. Another countermeasure is provided in [31], where the authors present a mutable AMI configuration technique for proactive defense.

The authors in [27] highlight limitations in traditional Access Control (AC) for securing Internet of Things (IoT) and Edge computing. A central server managing AC policies creates a single point of failure. Traditional AC also has difficulty scaling to manage complex policies in large and dynamic IoT networks. Additionally, resource limitations in some edge devices might make them incompatible with existing AC hardware requirements. Implementing blockchain for access control in the Internet of Things (IoT) holds promise, but there are hurdles to overcome. Choosing the right consensus mechanism for the blockchain depends on the specific network design and security threats, but all options involve trade-offs between the number of devices involved and the processing power needed. Existing research hasn't looked into large-scale deployments for managing device identities using blockchain because current solutions are too demanding for resource-constrained IoT devices. Even established platforms like Ethereum are impractical for IoT due to slow update times and the significant storage space they require [28], [29]. Despite these limitations, blockchain's potential for access control remains. Future research focused on developing lightweight consensus algorithms and storage strategies specifically designed for resource-limited devices is crucial for realizing this potential [28].

Further research in the security of AMI led to the implementation of PUFs in this area. The authentication scheme proposed by [13] and [24] use a PUF-based authentication method, meaning no data is stored on the vulnerable SMs. Such a technique is strong against the attacks on memory in AMI, but there is no mention of logging the transactions between entities which can be realized using blockchain technology. Authors in [25] propose an authentication process with the use of PUFs to securely transmit data from smart grids and prevent any future malware attacks. The work in [26] proposes a new privacy authentication scheme (PAC) for the smart grid that is based on PUFs. Experimental results suggest the high efficiency of this scheme; however, neither [25] nor [26] discuss internal breach and traceability within the system. To combat the traceability issue with the AMI, blockchain is considered to be a strong contender. There are numerous authentication schemes implemented using blockchain.

In [30] the researchers, put forward a security scheme using Rainbowchain. Rainbowchain uses dual chains using seven different authentication algorithms. The implementation of the Rainbowchain in this manner is to assist in the decision-making regarding access. Kim and Huh [31] propose a mutual authentication protocol using blockchain to act as the register authority of the network. However, this paper does not describe how the SMs, and UCs are meant to authenticate each other, and instead focuses on the registration of the entities within the blockchain. Additionally, implementation of blockchain in access control, especially in IoT and healthcare systems has been investigated by authors in [32], and [33]. In [32], authors introduce a novel system to provide the data sharing that integrates blockchain based access control system for IoT devices. Authors in [33] propose a trustworthy access control system that uses smart contracts to achieve greater security while sharing electronic health records among various patients and healthcare providers. However, in both these works, the device adversity has not been regarded.

The implementation of ZTA in this paradigm through the use of a digital twin is presented in [34]. In the paper, a dynamically aligned digital twin to reflect the state of the real-world network is proposed. The twin is then used as an enforcement agent for provided policies, however this design is applied broadly to the smart grid as a whole and focuses on the addition and removal of entities from the smart grid network. The security issues and networking problems have led the work in [35] to come up with a solution to employ the architecture that uses the zero-trust-based approach for authentication purposes, though not explicitly for the AMI. The stenographic overlay was used to induct the authentication tokens. Rose et al. [18] explained how the inclusion of ZTA improves the security structure for various systems. ZTA is proven to be more reliable to prevent any future malware attacks. The main drivers for the implementation of ZTA are explained in [36]. ZTA offers a better solution to enhance security and control at the device level.

## III. PRELIMINARY CONCEPTS

In this section, we introduce some concepts that are integral to understanding both the functional behaviors and the security of the proposed protocol.

### A. ADVANCED METERING INFRASTRUCTURE (AMI)

The AMI is one of the 4 subsystems of the smart grid. In the AMI, there are two primary goals: to establish communications with customers, and to provide timestamped information to the other 3 elements of the smart grid. The AMI uses a variety of technologies to achieve these goals, such as Meter Data Management Systems, communication networks, and SMs.

At the core of the AMI is a utility network through which the customers indirectly communicate with the UC. This begins with a Home Area Network that communicates to its own SM. The SM then communicates with a backhaul link that acts as a bridge to a Data Collector (DC). The DC is indirectly connected to the UC through a core backbone. For the purposes of this paper, this description of the utility network can be further abstracted to simply include the UC, DC, and SM, in which the DC acts as a middleman and aggregation point for the data, as seen in Fig. 2.

Given the complex nature of the AMI, the network is inherently vulnerable to attacks of many forms. Thus, there are 4 key factors that any proposed security protocol for the communication network must satisfy [37]:

1. **Confidentiality**– This refers to the privacy of the customers metrology and consumption data. In the case of an attack in any form, it is vital that the customers' data are not accessed. Access to this data is to only be given to authorized system, such that a malicious actor is never able to view the information.

2. **Integrity** – This is the network's ability to guarantee that data sent and received between any pairs of entities in the network is from the entity that is claimed and not from a malicious actor masquerading as an authorized entity. Therefore, an SM, DC, or the UC must be able to ignore any requests coming from unauthorized entities.


**FIGURE 2.** AMI network in smart grid [2].

3. **Availability**– While some data are not time-sensitive, it is expected for all data to be transferred in a timely manner. This is particularly the case for data that are taken at short intervals, which relay vital information regarding the health of components.

4. **Accountability**– Metadata regarding aspects of a message, such as a timestamp, must be kept so there is a level of traceability for vulnerabilities should an attack take place. This also means that, so long as both entities have shown themselves as authorized entities through the applied authorization protocol and the request is of a valid security level, communication from one entity to another should not be denied.

These factors are taken care by the blockchain, which is further discussed in Subsection C.

### B. PHYSICAL UNCLONABLE FUNCTIONS (PUFs)

A PUF is a physical, one-way function designed to take in a challenge Ci ∈ C input and output a response Ri ∈ R unique to that challenge. PUFs take advantage of hardware manufacturing variances to generate the response, which provides the advantage of the PUF being unique to a specific device and making it impossible for an identical copy to be made using the same design [38], [39]. An ideal PUF is expected to output a unique response for each unique challenge. PUFs offer the inherent advantage of not requiring any memory space, which can be vulnerable to a multitude of attacks.

#### 1) RING OSCILLATOR PUF (ROPUF)

The Ring Oscillator PUF, commonly known as ROPUF, is a type of delay based Physical Unclonable Function (PUF). The fundamental design of the ROPUF relies on delay loops created using an odd number of inverters [40]. In an ROPUF circuit, n- identical Ring Oscillators (ROs) ($RO_1$ *to* $RO_n$) are utilized to generate oscillator frequencies within a delay loop. These ROs exhibit unique oscillation behavior, producing distinct frequencies due to variations in

the manufacturing process [38], [39]. As a result, when pairs of ROs are mapped to different chip locations, they generate different frequencies, denoted as ($f_a$ *and* $f_b$). To select these frequency pairs, a pair of multiplexers is employed, with the PUF challenge serving as the select bits for the multiplexers. By quantitatively comparing these real-valued frequencies ($f_a$ *and* $f_b$) using a simple comparison method, a response bit ($r_{ab}$) is generated. The comparison method is as follows-

$$r_{ab} = \begin{cases} 1, & if\ f_a > f_b, \\ 0. & otherwise. \end{cases} \quad (1)$$

### 2) ARCHITECTURE OF IMPLEMENTED ROPUF

Various types of Physical Unclonable Functions (PUFs) have undergone analysis and been proposed for security applications in hardware. Among these, the Ring Oscillator PUF (ROPUF) has emerged as the most appropriate choice for FPGA-based applications because it does not require the mirror symmetry necessary for other variants of PUF [41]. In this investigation, we employ an XOR-inverter based Ring Oscillator PUF represented in Fig. 3, previously developed within our lab and published in [42]. This PUF produces challenge-response pairs (CRPs) with enhanced uniformity, uniqueness, randomness, bit aliasing, and reliability.

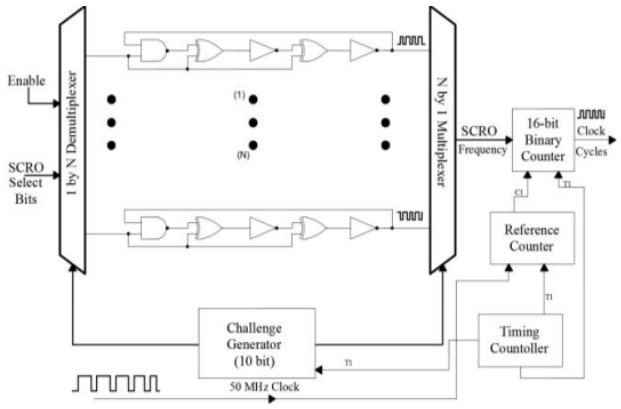


**FIGURE 3.** Representation of the implemented ROPUF [42].

The ROPUF design employed for this paper as depicted in Fig. 3 comprises NAND, XOR, and INV gates. The Artix-7 FPGA architecture features 2 slices per Configurable Logic Block (CLB), with each CLB containing 4 Look-Up Tables (LUTs). Five-stage oscillators are realized within 5 LUTs. To ensure consistent routing for the oscillators, 256 oscillators are positioned within the FPGA using hard macro configurations, as depicted in Fig. 4. Challenges for selecting the Ring Oscillators (ROs) are generated by a 10-bit challenge generator. Each RO is activated for 0.4 ms, followed by a 0.1 ms delay for transitioning to the next RO specified by the challenges. Subsequently, a frequency counter is enabled for 0.4 ms to capture the response from the ring oscillator.

### 3) PERFORMANCE METRICS OF THE IMPLEMENTED ROPUF

PUF metrics are a set of parameters that define the performance of different PUF designs [43]. The ROPUF produces an 'n' bit response for every 'n' bit challenge provided. The following subsection discusses the different performance metrics of the ROPUF including uniformity, uniqueness, bit aliasing, and reliability.

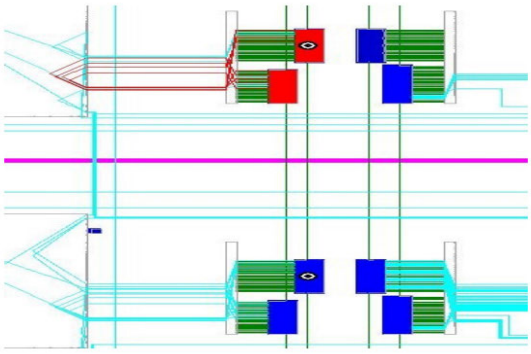

**FIGURE 4.** Hard Macro design of the ROPUF for fixed routing of oscillators [42].

- Uniformity: PUF uniformity approximates the consistence ratio of 0's and 1's in the response bits of a PUF [44]. For an ideal PUF the uniformity should be 50% [45]. Mathematically, it is represented as-

$$(Uniformity)_k = 1/n \sum_{i=1}^{n} r_i; X100\%$$

- Uniqueness: The uniqueness of a PUF is the ability of a PUF to generate different results in different locations of the same device or different devices [46]. For different RO PUF, we calculate inter-chip uniqueness by determining Hamming Distance of response bits corresponding to the challenges across all the chips. The uniqueness is calculated by –

$$Uniqueness = \underset{100\%}{2/\mathrm{k}(\mathrm{k}-1)} \sum_{i=1}^{k-1} \sum_{i=1+1}^{k} HD\,(R_i, R_i)\,/N^*$$

- Bit Aliasing: Bit aliasing estimates the bias of a response bit across different devices [47]. It can be represented as follows-

$$(bit - aliasing) = 1/\mathrm{k} \sum_{i=1}^{k} r_{ij} X100\%$$

- Reliability: Reliability measures the ability of a PUF to reproduce the response bit in different conditions [48]. The equation to compute it is given by-

$$\mathrm{Reliability} = 1 - 1/\mathrm{K.T.L}/\,\Gamma_{ik=1}^{K}\Gamma_{i=1}^{T} \sum_{I=1}^{L} r_{v,l} \otimes r_{nktj}$$

All the parameters have been calculated according to the equations mentioned and the results for them are tabulated in Table 1. The bit-aliasing, uniformity, and uniqueness for the implemented ROPUF are 50%, 49.8% and 47.64% which are close to the ideal value of 50% given in [45]. The reliability obtained is 98.5%.

### C. BLOCKCHAIN TECHNOLOGY

Blockchain is a distributed database and a peer-to-peer network that stores a registry of transactions [49]. In a blockchain, each block can be likened to a folder on a computer (node) that contains specific data [50]. The blockchain itself, comprises these interconnected subfolders. Blockchain is categorized into different types based on two factors: the type of ownership and the level of access granted to participants.

**TABLE 1. Performance metrics of the ROPUF.**

| Parameters | Ideal Values | Obtained Values |
|---|---|---|
| Uniformity | 50% | 49.8% |
| Uniqueness | 50% | 47.64% |
| Bit-Aliasing | 50% | 50% |
| Reliability | 100% | 98.5% |

- **Public Blockchain –** This type of blockchain is an open blockchain, where participation is unrestricted, and anyone can join the network at any time [51].
- **Private Blockchain –** This network is one where a single entity operates and runs the blockchain. In this type of blockchain, ownership is concentrated in the hands of one party, unlike the public blockchain. Consequently, it does not possess the full decentralization characteristic typically associated with blockchain networks [52].
- **Consortium Blockchain –** In this blockchain, multiple parties are granted permissioned control over the entire network, distinguishing it from the previously described types. This blockchain is characterized by a fair and transparent decision-making process, contributing to smooth operations. Additionally, it offers reduced costs and increased efficiency compared to other models [53].

For the purpose of this investigation, a consortium blockchain is utilized [54].

The smart contract plays a pivotal role in blockchain technology and is vital for establishing trust within the network. Despite its name, the smart contract does not have a legal context and is simply a computer program. The code of the smart contract is stored on the blockchain and is linked to a unique address [55]. In adherence to the terms defined by the smart contract, any updates made within the blockchain network are considered valid only when a majority of the involved parties reach an agreement or consensus. If a consensus is not achieved, the update is deemed invalid and consequently rejected.

In a blockchain, mathematical algorithms known as consensus algorithms are employed to verify transactions and establish trust among the participating parties [56]. Different consensus mechanisms are utilized by different blockchains, while for the purpose of this investigation, the proposed model utilizes the Proof-of-Authority (PoA) consensus mechanism [57]. The consensus algorithms are beyond the scope of this work, however interested readers can refer to [41], [48], [58], [59], and [60], detailed, in-depth information about them.

In the proposed model, all transactions taking place within the network are recorded in the blockchain, ensuring a transparent and immutable record of actions. This recording of transactions serves to track the sequence of events and maintain accountability within the network.

### D. ZERO TRUST

The term zero trust was first introduced in 2010 by the analyst firm Forrester Research to address modern attacks in the information security domain [57]. In the traditional security model, everything within the security boundaries is assumed to be trusted. However, with recent advances in technology, this assumption has become obsolete. Zero trust is a cybersecurity paradigm that concentrates on resource protection and acknowledges that trust cannot be blindly placed in anything but must be continually evaluated. It is centered on the belief that organizations should not automatically trust anything inside or outside their periphery. Instead, every access request and connection attempt should be verified before granting access. This leads to micro segmentation of the network which is the foundation of a zero trust network as illustrated in Fig. 5.

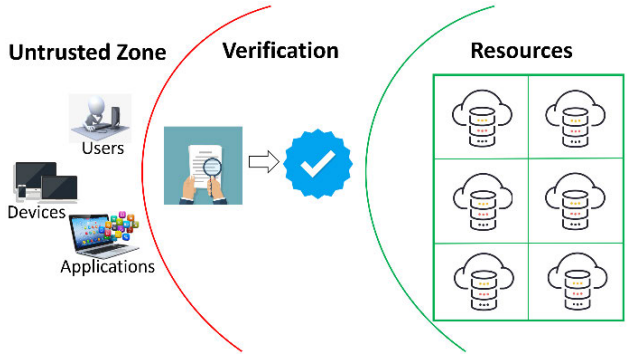


**FIGURE 5. A zero trust access model.**

In practice, the concept of zero trust entails that access to any resource within the network must adhere to predefined trust dimensions or parameters. Failure to meet these parameters should result in the denial or revocation of access to the specific resource [61]. Zero trust encompasses a set of concepts and ideas aimed at reducing uncertainty in enforcing precise, least-privilege, and per-request access decisions in information systems and services. This approach leads to the creation of a micro-segmented network [62].

Unlike the traditional access control mechanisms, zero trust does not base authorization on pre-defined conditions. Access to a network in the traditional manner is based on fine grained access control [63] such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), and Role based Access Control (RBAC) [64]. However, in a zero trust model, access is based on a critical concept "*never trust, but verify*." A traditional access control can be a part of zero

trust model, however every access needs to be verified, before entry is granted, even for pre-defined users and entities.

Based on this principle, the National Institute of Standards and Technology (NIST) has defined seven tenets that characterize zero trust in a special publication [18]. These tenets are as follows:

(i) Data and computation are considered as resources
(ii) Information is secured regardless of location
(iii) Access to resources on a per-session basis
(iv) Access is determined by a dynamic policy
(v) Device and assets are held in the most secure state possible
(vi) Authentication and authorization are strictly enforced
(vii) Collection of information on current state to improve security

These above tenets are satisfied in this work. Moreover, as part of this investigation, policies for access control and authentication have been formulated to enhance the security and integrity of the AMI ecosystem.

## IV. THREAT MODEL

Any AMI authentication scheme may face a multitude of potential security threats with a variety of objectives. However, all of these attacks aim to disrupt at least one of the key factors of the AMI's security. These attacks can be categorized based on the target layer of AMI: the data layer, the hardware layer, or the communication layer [65]. This paper attempts to secure the hardware layer, which subsequently aligns with the security of data and communication layer.

The data layer is focused on the storage and transfer of data, which are vulnerable to manipulation, insertion, and hijack attacks [66]. One threat is of a malicious actor manipulating the firmware of the SM (smart meter) or DC (data collector) that could modify data or limit the functionality of the device. Since this authentication model would require any file transfers to come from authenticated entities, meaning the SM or DC would never accept files from some unauthenticated entity. The limiting of such unauthorized file transfers, whether transferring to an AMI entity or taking data from an AMI entity, is at the core of the proposed model. Another possible attack in the data layer relates to internet protocol (IP) based systems, in which an actor may be able to spoof an IP, use a teardrop attack, or simply use a Denial of Service (DoS) attack to harm AMI functionality or steal data [67]. Again, due to the limiting of unauthorized communication, such attacks should not be possible since any communication would simply be denied.

In the hardware layer, one of the primary problems is the lack of onboard storage for the SM. This means that there may not be enough space for the chip to perform cryptographic calculations, and any storage added retroactively would increase the chip's vulnerability to physical and cyber-attacks. Both of these problems are solved by the proposed authentication scheme, as a PUF requires no onboard storage, meaning the SM is capable of using all of its storage for metering purposes. While PUFs may be vulnerable to machine learning attacks, this can be minimized depending on the PUF's design, such that the PUFs become resistant to such attacks [68]. It is also possible to launch these attacks against the DC, though since the DC is treated no different from an SM, there is no more risk for one than the other. There is also the possibility of malicious code being sent to an SM or DC, but this should not have any impact on the devices due to the authentication required. Lastly, many of the same problems are relevant in the communication layer, such as a malicious firmware update. Nevertheless, fears of a man-in-the-middle (MitM) attack can be avoided through the authentication mechanism and traced due to the implementation of blockchain in the scheme.

On top of attacks specific to these three layers, there are also more generalized attacks that may impact multiple layers. One possibility is an attacker inserting their own node to act as a DC, rerouting all traffic through itself so that it can manipulate the data before sending it onward. However, since someone at the UC firsts need to take note of each device's CPBPs and add them to a list in the UC before allowing any communication with a device, an attacker attempting to insert a new device into the AMI needs to have full access to the UC, itself, before doing so. There is also a possibility of an attacker masquerading as the UC, though this attack is dealt with, trivially due to the authentication scheme and is entirely traceable because of the implementation of the blockchain. Another attack may be if a user manages to bypass the entire authentication scheme due to poor implementation. While this certainly impacts the system, due to the blockchain, any such attack is entirely traceable, and it is very simple to discover all details on the attack and deal with it accordingly.

## V. PROPOSED ZEBRA ARCHITECTURE

To achieve a successful implementation of a zero trust architecture, it is essential to adhere to the tenets outlined by NIST, which establish a secure perimeter around the supply chain network. These tenets focus on access control, authorization, supervision, and overall security. For user authorization, blockchain technology is primarily utilized, leveraging its features such as transparency and decentralized control. PUFs, on the other hand, play a crucial role in authenticating the FPGAs within the network. Monitoring and security are addressed through the traceability and immutability features offered by blockchain. These features enable the recording and tracking of transactions, ensuring that any tampering attempts or unauthorized changes can be identified and prevented. The combination of these features in the proposed architecture helps establish a secure and trustworthy supply chain network.

### A. ZERO TRUST POLICIES

As mentioned in subsection D of Section III, the zero trust architecture incorporates micro-segmentation within

a network through authorization and verification policies. In this section, the policies necessary for the successful implementation of the zero trust architecture in the FPGA supply chain are discussed. These policies draw inspiration from the zero trust tenets defined by NIST [18]. The tenets are interpreted specifically for AMI domain and are presented in Table 2. The application of these tenets within the proposed research is discussed in detail, highlighting how they contribute to establishing a secure and trustworthy AMI network.

**TABLE 2. Zero trust tenets and their interpretation for AMI security.**

| Tenets | Interpretation |
|---|---|
| Data and computation are considered as resources | Disparate resource set |
| Information is secured regardless of location | Independent security |
| Access to resources on a per-session basis | Traceability |
| Access is determined by a dynamic policy | Provenance |
| Device and assets are held in the most secure state possible | Confidentiality |
| Authentication and authorization are strictly enforced | Integrity |
| Collection of information on current state to improve security | Persistent Evaluation |

### B. THE BLOCKCHAIN SUPPORT

The development of smart contracts plays a crucial role in providing the key features of blockchain technology [44]. These features, in combination with smart contracts, contribute to the successful fulfillment of the zero trust tenets, described in the subsection above, within the proposed work. Smart contracts enable the automation and enforcement of predefined rules and policies, ensuring transparency, accountability, and secure transactions within the FPGA supply chain network.

In order to ensure authorization and verification of users in the system, the proposed research implements a blockchain-enabled multi-factor authentication (MFA) application. It is important to note that the authors have used the MFA scheme presented in [45] and do not claim any credit for it. The multi-factor authentication application is integrated into the system to enhance security. By leveraging blockchain technology, trust is established in the users, devices, applications, and traffic within the network. This is achieved through the recording and storage of all authentication and verification actions in the blockchain, along with corresponding timestamps.

In addition to the users and FPGAs, this work also aims at securing the FPGA bitstream file from being tampered. An application of blockchain called Inter Planetary File Storage (IPFS) is utilized in this work to store the bitstream file [46]. IPFS is a blockchain based peer-to-peer file storage system, which allocates a unique hash for the stored file upon uploading [47]. This hash changes with every modified version of the uploaded file [46].

### C. THE ROPUF SUPPLEMENT

In conjunction with blockchain technology, the implementation and execution of the zero trust architecture are further reinforced by the utilization of ring oscillator physical unclonable functions. PUFs serve as a Root-of-Trust (RoT) for the chips involved in the FPGA supply chain, focusing primarily on ensuring their security. The challenge and response pairs generated by the PUFs play a crucial role in authenticating and verifying the FPGAs. By leveraging the unique characteristics provided by the PUFs, the authentication process enhances the overall security of the supply chain, mitigating potential risks and ensuring the integrity of the FPGAs.

### D. PROPOSED ZEBRA MODEL: IMPLEMENTATION

The individual roles of zero trust, blockchain, and ROPUFs in this research are elucidated in previous subsections. This subsection delves into the functioning of blockchain and ROPUFs to fulfill the requirements of the zero trust tenets. While Table 2 provides an interpretation of the zero trust tenets, their practical implementation in this work is described as follows:

***- Disparate resource set***: This involves the management of different resources and granting user access only after verification. To achieve this, a multi-factor authentication scheme is integrated into the system.

- ***Independent security implementation across all resources:*** This ensures that only authorized individuals have access to the resources they should have access to. It involves providing the least privilege access or role-based access. This is accomplished through the use of modifier and event functions in the smart contract.

***-Maintain traceability of access to all the resources:***

This involves maintaining a record and tracking of individuals who accessed the resources, along with the timestamp of their access and the actions they performed. This is accomplished through the traceability feature offered by the blockchain.

- ***Checking the provenance of the policy that determined the grant of access:*** This means that a record is maintained to track who accessed the resources, when they accessed them, and what actions they performed with the resources or the associated information. This level of tracking and accountability is enabled by the provenance feature provided by the blockchain.

- ***Preserve confidentiality:*** Critical information should be restricted to a specific set of participants and not accessible to others. The use of modifier functions in smart contracts helps in ensuring the confidentiality of such information, allowing access only to authorized participants.

***-Maintain integrity of the process:*** Ensuring that individuals are carrying out their designated tasks is achieved through the use of a shared ledger, which is immutable. Every action or transaction occurring in the network is recorded and

updated on the shared ledger, guaranteeing the integrity of the system.

***-Persistent evaluation:*** This involves the collection of information and conducting persistent and rapid analysis. Constant monitoring of blockchain performance enables continuous evaluation and analysis of the system.

**TABLE 3. Zero trust tenets and their implementation in ZEBRA.**

| Policies | Implementation | Feature utilized |
|---|---|---|
| Disparate resource set | Multifactor Authentication | Blockchain/ROPUF |
| Independent security | Modifier function of smart contract | Blockchain/ROPUF |
| Traceability | Traceability feature of blockchain | Blockchain |
| Provenance | Provenance check feature of blockchain | Blockchain |
| Confidentiality | Modifiers in smart contract | Blockchain |
| Integrity | Immutability feature of blockchain | Blockchain |
| Persistent Evaluation | Monitoring the blockchain | Blockchain |

All these policies have been formulated based on the principles laid down by NIST and are summarized in Table 3.

The proposed zero trust architecture for the AMI network, as depicted in Fig. 6, integrates various components and mechanisms to ensure authentication, access control, traceability, and security. The authentication and access control of the users is mainly done through the blockchain enabled MFA and FPGA (SM) is authenticated via CRPs obtained from ROPUF. The transactions performed in the network is updated on the shared blockchain ledger and hence are trackable and traceable. To maintain confidentiality and integrity of the assets, features offered by blockchain are utilized. Furthermore, this work enforces that all the devices used in the network are updated with latest security patches and all the computer codes are developed taking into consideration the concepts of secure coding, thus adhering to the ZT compliance. The zero trust policy engine evaluates and enforces all the policies formulated for the architecture. Upon enforcement of the protocols, access to the network resources is either allowed or blocked, depending upon the evaluation of the policies laid and their implementation. With these protocols in place, everything that enters the network to fetch access to the resources is verified and authenticated, with very less or no room for an untrusted element to enter the network.

While access control mechanisms are crucial for cloud data storage security and other applications, our work focuses on a different aspect of security within the context of Advanced Metering Infrastructure (AMI). We are particularly interested in strengthening the device, user, and ultimately network authentication through zero-trust access control. This approach inherently mitigates insider threats by not trusting any pre-authenticated user. Our work covers all the threat models presented in [69]. Implementation of ZEBRA blocks access to any user or intruder and does not grant power to any component to authorize access except for the policy enforcement and evaluation engine in Fig. 6. This focus on device authentication aligns well with the security needs of embedded environments commonly found in AMI systems.

## VI. CASE STUDY: SIMULATION

For the purpose of this investigation, a smart meter embedded with a Artix 7 Xilinx FPGAs mounted on a Nexys 4 Digilent board FPGA [13] is employed. This FPGA is implemented with ROPUF. The smart contracts developed have been tested on the Ganache framework provided by the Truffle suite [70]. Ganache is a personal blockchain designed for rapid development of Ethereum distributed applications. It offers both a UI and a CLI for development, deployment, and testing of dApps in a secure and deterministic environment. Ganache UI is a desktop application that supports Ethereum technology. It provides ten accounts, each with a hundred Ethers (for testing purposes only, not to be used in a real blockchain network), which can be used for transactions. These accounts allow for running tests, executing commands, and inspecting the blockchain state while controlling the operations on a personal Ethereum blockchain. All the transactions and commands in the investigation are acronymized and a list of abbreviations is provided in Table 4.

**TABLE 4. Abbreviations and their full forms.**

| Abbreviation | Full Form |
|---|---|
| **REQ** | Request |
| **AUTH** | Authenticate |
| **VER** | Verify |
| **CPBP** | Challenge Parity Bits Pair |
| **$C_i$** | Challenge (i) |
| **$PB_i$** | Parity Bits (i) |
| **ACK** | Acknowledge |

Firstly, the policies for the architecture are devised and the corresponding components required for their successful implementation are designed. These components include building a blockchain network developing a smart contract and implementing ROPUFs on the FPGA boards to produce CRPs for authentication. The ROPUF has been designed as discussed in subsection B of Section III and the CRPs are generated using an Agilent 16801A logic analyzer. These CRPs are stored in the blockchain for later authentication and validation.

The developed application, which facilitates all transactions within the AMI network, is blockchain-enabled. It incorporates smart contracts that provide role-based or least privilege access to users. The application also integrates a multi-factor authentication mechanism inspired by [71]. The smart contracts are not only responsible for access control but also for recording transactions within the network.

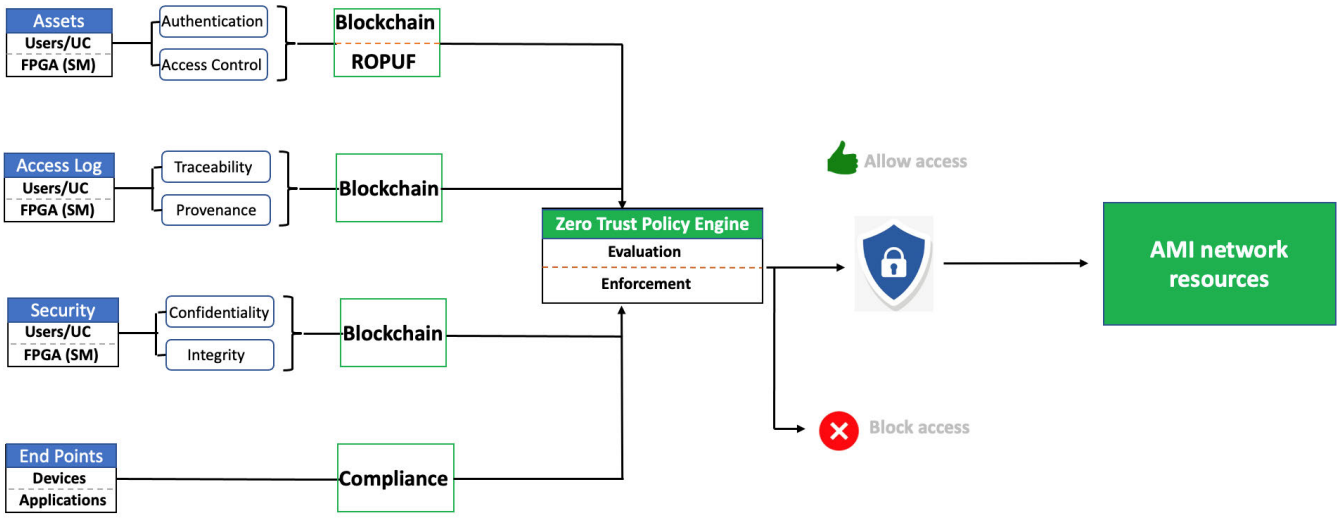


**FIGURE 6.** Proposed zero trust architecture, ZEBRA, for AMI network security.

There are three primary entities within the AMI: the UC, the SM, and the DC. In the AMI, all data collected from an SM must go through a series of other SMs until reaching a DC and finally being forwarded to the UC. Likewise, though the UC is never considered trusted by any of the SMs, the UC is to store the Hamming code parity bit pairs (CPBPs) that have been generated by each ROPUF depicted in Fig. 7. The UC is assigned this task since it has a much greater capacity for storage than a single SM. Furthermore, the UC is less vulnerable to physical attacks than the SMs since it is not in the field, and it is also less vulnerable to cyberattacks due to the firewall it should have in place. Nevertheless, this does mean that the security of the UC is of the utmost importance.

From a security standpoint, a DC should be treated as an SM by the UC in all aspects. It is proposed that every SM be retroactively outfitted with a ROPUF. These ROPUFs' CPBPs and their respective challenges are registered with the UC before being integrated into the network. It is therefore necessary that the set of challenges ($C_i$) for each ROPUF is provided by the manufacturer.

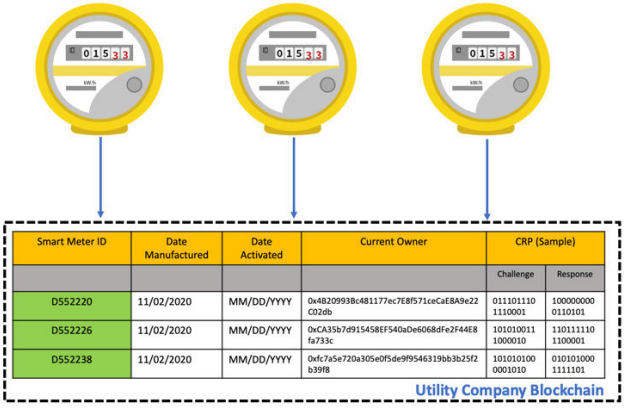


**FIGURE 7.** Smart meter registration with utility company.

The use of $PB_i$ over simply using $R_i$ as the authentication mechanism for $C_i$ is to improve the security of the system against attacks that aim to model the ROPUF from its responses. The advantage of using the CPBP rather than the challenge-response pairs is that an adversary would not be able to match a response to a specific challenge [72]. In the case that the UC is hacked it is possible to reconfigure the system. This is done by replacing the ROs, and therefore $R_i$ and $PB_i$.

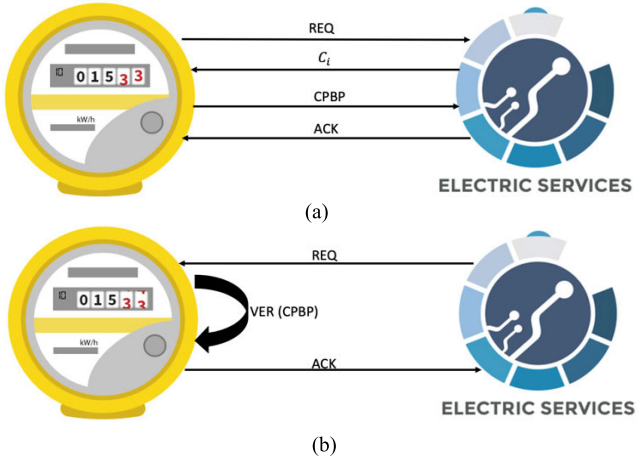


**FIGURE 8.** (a) Smart meters to utility company authentication. (b).Utility company to smart meter authentication.

In order to add an SM to the network, the new SM and its ROPUF's CPBPs are registered with the UC. It is important to note that this does not mean the UC is a "trusted party" as this would violate ZTA; instead, this is to provide the UC the ability to authenticate the entity it is communicating with and for the UC to authenticate itself to a secondary entity. Upon registration, the SM can be added to the network for initial authentication to begin. The initial authentication

verifies to the UC that the SM is legitimate. First, the SM sends a request to the UC, following which the UC responds with a challenge. The SM then generates the CPBP and sends it back to the UC. Upon receiving the SM's response, the UC will then acknowledge or not acknowledge the SM based on whether the response is consistent with what was given in the registration process. This process is shown in Fig. 8 (a). Upon acknowledgement, the SM authenticates the UC, as seen in Fig. 8 (b). This is done by the UC requesting high-level access to the SM. Included in this request is a challenge $C_i$ and CPBP $PB_i$. The SM then challenges itself with $C_i$ and verifies $PB_i$. The SM then either acknowledges or does not acknowledge the UC based on this verification. After acknowledgement is made, the connection is closed, and the SM calls a function on the blockchain which stores details of the transaction. This ensures the satisfaction of the ZTA tenets regarding the monitoring of the system and the collection of information regarding the network.

Due to the zero trust nature of the proposed model, authentication by both the UC and SM is required for each session. Upon a need to exchange data, the entities are to authenticate each other in a similar manner as when the SM was first added to the network. The process of mutual authentication is shown in Fig. 9. The UC must first authenticate the SM by sending a challenge to the SM and verifying the CPBP, then acknowledging or not acknowledging the SM based on whether the CPBP is consistent with what the known response should be. Likewise, the SM is to authenticate the UC in the same manner as when it was added to the network, though limiting the access of the UC only to the minimum level access required, in accordance with the tenets of zero-trust. The UC will post a request with the access needed and send a challenge $C_i$ and a CPBP $PB_i$ to the SM. The SM will then generate its own CPBP and compare it with $PB_i$. Based on this comparison, it will either acknowledge or not acknowledge the UC. After both the UC and SM have acknowledged each other, data can be exchanged. Once the exchange is complete, the connection is closed. After that point, authentication will be required again to exchange any more data. The SM then documents the exchange on the blockchain. This is the process of mutual authentication and data transfer between UC and SM as depicted in Fig. 9.

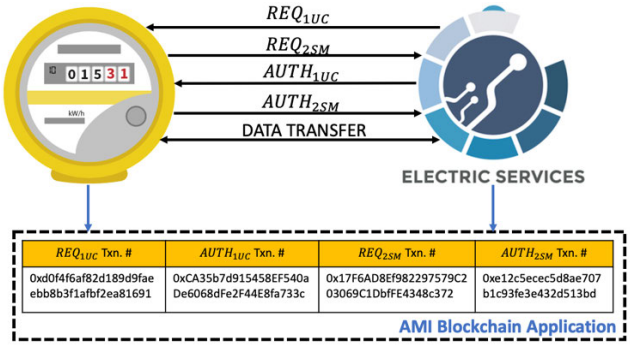


**FIGURE 9.** Mutual authentication and data transfer protocol.

The blockchain provides traceability and accountability within the system [73]. For successful implementation of the blockchain, smart contracts have been developed using Solidity and were used to perform the communication between the UC and SM and finally authenticate it. All the transactions are recorded on the distributed ledger with a timestamp, ensuring no wrongdoings within the AMI system as depicted in Fig. 10, which shows the 'request' transaction between the UC and SM.


**FIGURE 10.** Example of a blockchain transaction between UC and SM.

It is expected for the UC to act as a watchdog for the blockchain in the case that any requests are made from an unauthorized source. In the case that the UC recognizes a suspicious request for a blockchain entry, it should throw a warning. Physical investigation is then required of a party at the UC to find the reason behind the request and decide the correct course of action. Such a warning will be placed on the blockchain, so that any consistent suspicious requests from the same party or demonstrating some other pattern may be looked at. This is to further enhance the traceability and accountability of the system, thereby assisting in any future investigations, regardless of if past warnings have turned up little evidence.

It may be possible for a malicious actor to model a ROPUF using machine learning as described in [39]. However, in such a case they can predict the $R_i$ for a respective $C_i$. This would give them the ability to exchange data with a UC. Though this attack would eventually be caught due to the implementation of the blockchain, temporary damage may still be possible. To prevent such an attack, the authentication scheme instead uses the Hamming code parity bits $PB_i$. This scheme utilizes the (8,4) Hamming code, a linear error correcting code, as a one-way function to create a consistent output for the ROPUF and to make it impossible to model the ROPUF using machine learning [57]. While a hash function may also have the same effect of preventing machine learning attacks, if even a single bit of the $R_i$ suffers a bit-flip, the hash cannot be recovered. However, the use of the PBs allows for a predefined level of discrepancy, such that the authentication can still take place even under anomalous circumstances. Furthermore, the Hamming code algorithm is trivial and require very little computational power, meaning it is far more efficient than a hash, without any decrease in security. While it may be possible for an attacker to gather the $PB_i$ and $C_i$, that information becomes immediately useless since a new challenge is used for every session of communication.

**TABLE 5.** Authentication time for each security level defined by ANSI C12.22.

| Security Level | Ri (bits) | PBi (bits) | Ci (bits) | PBi Generation Time (ms) | PBi Transfer Time (ms) | Ci Transfer Time (ms) | Total PBi and Ci time (ms) | Blockchain Transaction Time (s) | Total Time (ms) |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 128 | 128 | 2048 | 76.8 | 0.094 | 1.505 | 76.801 | 50 | 126.801 |
| 2 | 256 | 256 | 4096 | 153.6 | 0.0188 | 3.010 | 153.603 | 50 | 203.603 |
| 3 | 512 | 512 | 8192 | 307.2 | 0.0376 | 6.020 | 307.206 | 50 | 357.206 |
| 4 | 1024 | 1024 | 16384 | 614.4 | 0.0753 | 12.041 | 614.412 | 50 | 664.412 |
| 5 | 2048 | 2048 | 32768 | 1228.8 | 0.1506 | 24.082 | 1228.824 | 50 | 1278.824 |

## VII. PROOF OF CONCEPT

This section discusses different aspects of the methodology including performance, storage requirements, and robustness.

As seen in Table 5, there are 3 elements of the PUF that must be analyzed to evaluate the time taken to generate the parity bits PBi and transfer the challenge bits Ci. Since the parity bits PBi are generated using the Hamming code function, the response Ri that is generated by the PUF is used as an input. While this does come with the advantage of being more secure and requiring less data to transfer, this also means the transferring of the calculation of the parity bits takes longer than simply using the response bits generated directly by the PUF. Nevertheless, the generation of the response bits and the calculation of the parity bits meets the requirements of the smart grid and can still be achieved in real-time. The number of bits used for the challenge Ci is 16 times (example: $16 \times 128 = 2048$) that of the response bits and, consequently, 16 times that of the parity bits. Since the transfer time of the challenge can be expected to scale linearly along with the number of bits in the challenge, the challenge typically takes 16 times as long to transfer, as seen in Table 3, which discusses the different levels of security defined by ANSI C12.22 [74]. Despite this increase in transfer time, it maintains real-time responses. Furthermore, the flat overhead created by implementing the blockchain, has no impact in the responsiveness of the communication, since this is done after the communication takes place.

As described in Section V, we use Ganache as our simulation environment. One notable feature of Ganache is the ability to customize the block mining time. Unlike the real-world Ethereum blockchain, where the time between two blocks is determined by network consensus, Ganache allows users to pre-define the block interval. The block mining time can be set within a range of 1 to 200 seconds. In the case study described, the accounts are assigned to different users within the network, and the blockchain system is tested and simulated accordingly. Simulations, for our case are conducted using block times of 60 seconds. In these 60 seconds of block interval, the number of transactions stored in each block is 19, with the number of blocks created for the entire case study being 17. For these values, the transactions per second (TPS) obtained are 0.017. With these numbers, one transaction takes place in 50 seconds, which is tabulated in Table 5.

The PUF implemented in this design is done so on an FPGA. This comes with the advantage of the PUF being easily reconfigurable. In the case of an attack, the PUF can simply be altered such that any predictive model is useless after reconfiguring. Furthermore, due to the volatile nature of the response bits generated by the PUF, it is difficult to launch an invasive attack on this aspect of the scheme, despite being in the most vulnerable of positions. Even in the case that the PUF on the FPGA is perfectly modeled, it would still be nearly impossible to fully infiltrate even a single SM without having complete access to that specific PUF's CPBPs. Assuming such an attack was able to succeed, it would still only give the malicious actor control of that single SM until the PUF is reconfigured.

Thus, the securing of the database containing all the challenges and their respective parity bits should be the highest priority. There are many obstacles any attacker would have to overcome before becoming a threat to the UC. While the database should inherently be more secure due to its firewall and physical location, attacks are theoretically possible. Fortunately, the system is reconfigurable such that any attacks may be rendered ineffective. Furthermore, due to the nature of the database, it is expected that it is easier to address problems in the case of a system failure, an attack, or some other fault.

The storage calculated in Table 6 is by assuming that level 1 security exchanges occur every 15 minutes, as this is the most frequent communications typically found, and that higher level security exchanges happen 5 times a day. However, the size of this changes based on the frequency of communications, such that the longer time between data exchanges, the less storage capacity required to authenticate over a similar period of time. If the devices exchange data every 15 minutes, there is a need of 35,064 CPBPs on average for each year. This means that one year of low-level authentications would take only 9.3 MB of storage. While this is low, as the storage is dependent upon the frequency of communications, it is possible to lower this even further by increasing the amount of time between communications. Assuming a 50-year lifespan of the AMI, one device will take a total of 1.187 GB of storage, as seen in Fig. 11. Thus, if the AMI contains a total of 2000 devices, the total storage required is only 2374.852 GB. However, this is also heavily impacted by communication frequency, and it may be realistic to half this by limiting communication frequency.

Nevertheless, even if the 15-minute period is maintained, the storage capacity is low for the entirety of the AMI's lifespan, meaning the protocol is efficient regarding storage requirements.

**TABLE 6. Data storage size for each authentication level.**

| CPBP authentication level | Year(s) | Data size (megabytes) |
|---|---|---|
| First | 1 | 9.257 |
| | 10 | 92.569 |
| | 20 | 185.138 |
| | 30 | 277.707 |
| | 40 | 370.276 |
| | 50 | 462.845 |
| Second | 50 | 48.213 |
| Third | 50 | 96.624 |
| Fourth | 50 | 193.248 |
| Fifth | 50 | 386.496 |

Note that this experiment, has been successfully implemented on Ganache in the research lab, and it can also be migrated on Ethereum Mainnet. However, deploying it and executing the transactions on the real network would cost real Ethers and hence was only tested on the test network and not on actual blockchain network. In addition, the authors understand the technical challenges anticipated to be encountered during the real-life deployment such as implementation, scalability etc. Solving these challenges while still keeping ZEBRA architecture efficient is future research investigation the authors intend to work on.

ZEBRA's implementation hurdles can be addressed through FPGA-based System-on-Chip (SoC) technology. SoCs integrate processing power, memory, and reconfigurable logic for ROPUFs onto a single chip, eliminating complex and expensive smart meter retrofits. This simplifies deployment and enhances scalability as SoCs can handle multiple ROPUFs and potentially some blockchain verification, reducing hardware requirements for new meter additions. Furthermore, SoCs offer improved security by incorporating features like secure boot and tamper detection, mitigating concerns associated with traditional hardware integration methods. By overcoming these limitations, FPGA-based SoCs pave the way for a more feasible and secure ZEBRA implementation in AMI systems.

In addition to the above challenges, we understand the implementation issues in fitting ZEBRA for different AMI environment. This work provides a high-level security framework for AMI. The ZEBRA framework will have to be tailored for different AMI settings, to suit the specifications of the particular AMI. In such scenario, ZEBRA will act as the basis on which the specific zero trust based AMI security framework is built.

## VIII. SECURITY THREAT EVALUATION

To test the ROPUF security level, an ANN-based modeling attack is used to model the ROPUF based on the challenges (Ci) and parity bits (PBi). The parity bits are derived from ROPUF responses ($R_i$) using (8,4) parity bit generation. The attack is performed based on the assumption that an adversary somehow manages to acquire a small set of Ci and PBi and tries to predict the parity bits for the remaining challenges. A sample of 10% of the available Ci and PBi is considered stolen. With this 10% of the data, ANN-based models have been trained using three different optimizations, namely, RMSprop, Adam, and Nadam.

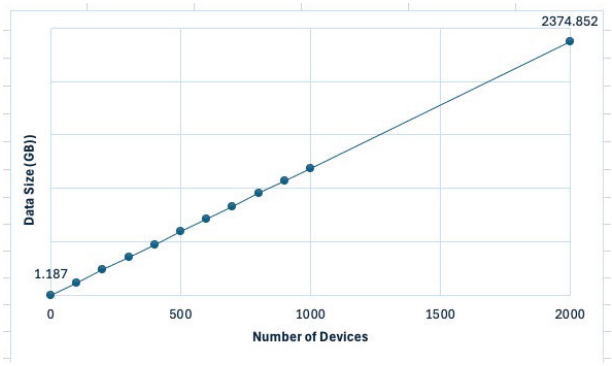


**FIGURE 11. Data storage size needed based on number of devices on the AMI.**

Fig. 12 shows the training and prediction accuracy for ANN-based modeling using RMSprop optimizer. Though the training accuracy reaches close to 100%, the prediction accuracy stays between 59-60.5%. The best accuracy is obtained for RMSprop optimization, which is 60.25%, showing that the Ci and PBi data cannot be used for predicting the remaining parity bits (PBi) from the remaining responses. This experiment justifies the use of ROPUF with PBi so that the AMI system is not harmed by modeling attacks on ROPUF.

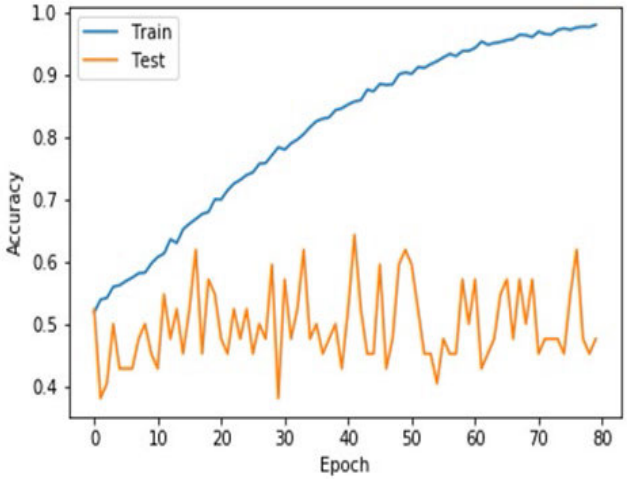


**FIGURE 12. Training and testing accuracy of (Ci, PBi ) for RMSprop optimization.**

**TABLE 7.** Comparison of zebra with previous literature on concepts implemented.

| Concepts/Previous Work | [13] | [16] | [26] | [34] | [35] | ZEBRA |
|---|---|---|---|---|---|---|
| Physically Unclonable Functions (PUFs) | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ |
| Blockchain Technology | ✘ | ✔ | ✘ | ✔ | ✘ | ✔ |
| Zero Trust Architecture | ✘ | ✘ | ✘ | ✘ | ✔ | ✔ |

While there are many papers attempting to secure the AMI, no prior literature proposes an authentication scheme that is fully traceable while simultaneously fulfilling the ZTA tenets. By creating a system that satisfies ZTA tenets, lateral movement can be entirely halted, and masquerade attacks are made much more difficult. Furthermore, the reconfigurability of the PUF and the usage of blockchain means that, even in the case of an attack, the damage can be quickly noticed, and the system can be reconfigured, limiting the damage and making it easier to take an action that may repair or even nullify the damage caused. While previous individual literatures may support pieces of these capabilities using one or two of the three concepts, this is the first work to satisfy ZT using other two concepts, and thus, combine the advantages that come with each. Table 7 shows the different elements incorporated into the various authentication and permission systems in previous literature compared with the proposed framework, ZEBRA.

Given the increasing sophistication of attacks and the cunning nature of threat actors, the blockchain ecosystem finds itself susceptible to various malicious activities, such as majority attacks or 51% attacks, back-running, front-running and sandwich attacks [75], [76], [77], [78]. Furthermore, smart contracts might also be susceptible to various attacks [79], [80]. It is important to recognize that in light of this vulnerability, our future research endeavors are primarily directed towards bolstering the security of the blockchain network.

## IX. CONCLUSION

A novel authentication scheme and network security measures are proposed in this work. Utilizing ROPUFs for the authentication and blockchain for traceability, the scheme ensures a system that fulfills the ZTA tenets and minimizes the impact of any unforeseen attacks on the AMI. The use of ROPUFs rather than typical cryptography limits the effectiveness of physical attacks and the use of Hamming code parity bits over the response bits limits the effectiveness of machine learning attacks. The authentication times for L1 and L2, the most common security levels, are 126.80 ms and 203.603 ms, respectively, satisfying the real-time requirements of such a system. In addition, due to the scheme's use of FPGAs, new design and technology can be retroactively fitted into current smart meters making them future proof.

Furthermore, through the implementation of blockchain technology, communications are fully traceable, allowing for ease in investigation and establishing the trustworthiness of the AMI network. Not only the proposed scheme satisfy the requirements of ZTA, but by making the transaction data on the blockchain available to all nodes, the data becomes immutable and secure.

## REFERENCES


[1] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.

[2] *The Smart Grid Interoperability Panel-Smart Grid Cybersecurity Committee, Guidelines for Smart Grid Cybersecurity*, document NISTIR 7628 Rev.1, Smart Grid Cybersecurity Committee, 2014.

[3] R. R. Mohassel, A. S. Fung, F. Mohammadi, and K. Raahemifar, "A survey on advanced metering infrastructure and its application in smart grids," in *Proc. IEEE 27th Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2014, pp. 1–8, doi: 10.1109/CCECE.2014.6901102.

[4] A. P. D. Nath, F. Amsaad, M. Choudhury, and M. Niamat, "Hardware-based novel authentication scheme for advanced metering infrastructure," in *Proc. IEEE Nat. Aerosp. Electron. Conf.*, Jul. 2016, pp. 364–371, doi: 10.1109/NAECON.2016.7856831.

[5] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094.

[6] B. M. R. Amin, S. Taghizadeh, M. S. Rahman, M. J. Hossain, V. Varadharajan, and Z. Chen, "Cyber attacks in smart grid—Dynamic impacts, analyses and recommendations," *IET Cyber-Physical Syst., Theory Appl.*, vol. 5, no. 4, pp. 321–329, Dec. 2020.

[7] Z. E. Mrabet, N. Kaabouch, H. E. Ghazi, and H. E. Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Electr. Eng.*, vol. 67, pp. 469–482, Apr. 2018.

[8] V. Seferian, R. Kanj, A. Chehab, and A. Kayssi, "Identity based key distribution framework for link layer security of AMI networks," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3166–3179, Jul. 2018, doi: 10.1109/TSG.2016.2628090.

[9] O. Kebotogetse, R. Samikannu, and A. Yahya, "A concealed based approach for secure transmission in advanced metering infrastructure," *IEEE Access*, vol. 10, pp. 84809–84817, 2022, doi: 10.1109/ACCESS.2022.3195240.

[10] T. John and D. Hausheer, "S3MP: A SCION based secure smart metering platform," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2021, pp. 944–949.

[11] C. Huang, C.-C. Sun, N. Duan, Y. Jiang, C. Applegate, P. D. Barnes, and E. Stewart, "Smart meter pinging and reading through AMI two-way communication networks to monitor grid edge devices and DERs," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 4144–4153, Sep. 2022, doi: 10.1109/TSG.2021.3133952.

[12] A. Triantafyllou, J. A. P. Jimenez, A. D. R. Torres, T. Lagkas, K. Rantos, and P. Sarigiannidis, "The challenges of privacy and access control as key perspectives for the future electric smart grid," *IEEE Open J. Commun. Soc.*, vol. 1, pp. 1934–1960, 2020, doi: 10.1109/OJCOMS.2020.3037517.

[13] M. Mustapa, M. Y. Niamat, A. P. Deb Nath, and M. Alam, "Hardware-oriented authentication for advanced metering infrastructure," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1261–1270, Mar. 2018, doi: 10.1109/TSG.2016.2582423.

[14] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th Annu. Conf. Design Autom.*, 2007, p. 9.
[15] A. Kulkarni, N. A. Hazari, and M. Niamat, "Ring oscillator PUF and blockchain: A way of securing post fabrication FPGA supply chain," in *Proc. IEEE 66th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2023, pp. 35–39, doi: 10.1109/MWSCAS57524.2023.10405953.
[16] S. Ghosh, U. Chatterjee, D. Chatterjee, R. Masburah, D. Mukhopadhyay, and S. Dey, "Demand manipulation attack resilient privacy aware smart grid using PUFs and blockchain," in *Applied Cryptography and Network Security Workshops*. Cham, Switzerland: Springer, 2021, pp. 252–275.
[17] J. Kindervag, "Build security into your network's DNA: The zero trust network architecture," *Forrester Res. Inc.*, vol. 1, pp. 1–27, Nov. 2010.
[18] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero-trust architecture," *NIST Special Publication 800*, vol. 207, pp. 1–59, Aug. 2020.
[19] F. N. Alsulami, "A comprehensive analysis of the environmental impact on ROPUFs employed in hardware security, and techniques for trojan detection," Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Univ. Toledo, Toledo, OH, USA, 2022.
[20] S.-H. Chang, T. William, W.-Z. Wu, B.-C. Cheng, H. Chen, and P.-H. Hsu, "Design of an authentication and key management system for a smart meter gateway in AMI," in *Proc. IEEE 6th Global Conf. Consum. Electron. (GCCE)*, Oct. 2017, pp. 1–2, doi: 10.1109/GCCE.2017.8229288.
[21] I. Parvez, M. Aghili, and A. Sarwat, "Key management and learning based two level data security for metering infrastructure of smart grid," 2017, *arXiv:1709.08505*.
[22] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, "A key management scheme for secure communications of advanced metering infrastructure in smart grid," *IEEE Trans. Ind. Electron.*, vol. 60, no. 10, pp. 4746–4756, Oct. 2013.
[23] Y. Yan, R. Q. Hu, S. K. Das, H. Sharif, and Y. Qian, "An efficient security protocol for advanced metering infrastructure in smart grid," *IEEE Netw.*, vol. 27, no. 4, pp. 64–71, Jul. 2013, doi: 10.1109/MNET.2013.6574667.
[24] M. Q. Ali, E. Al-Shaer, and Q. Duan, "Randomizing AMI configuration for proactive defense in smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2013, pp. 618–623, doi: 10.1109/SMARTGRIDCOMM.2013.6688027.
[25] M. Tahavori and F. Moazami, "Lightweight and secure PUF-based authenticated key agreement scheme for smart grid," *Peer-Peer Netw. Appl.*, vol. 13, no. 5, pp. 1616–1628, May 2020, doi: 10.1007/S12083-020-00911-8.
[26] P. Gope and B. Sikdar, "A privacy-aware reconfigurable authenticated key exchange scheme for secure communication in smart grids," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5335–5348, Nov. 2021, doi: 10.1109/TSG.2021.3106105.
[27] R. Asif, K. Ghanem, and J. Irvine, "Proof-of-PUF enabled blockchain: Concurrent data and device security for Internet-of-Energy," *Sensors*, vol. 21, no. 1, p. 28, 2021.
[28] R. C. Lunardi, R. A. Michelin, C. V. Neu, and A. F. Zorzo, "Distributed access control on IoT ledger-based architecture," in *Proc. IEEE/IFIP Netw. Oper. Manage. Symp.*, Apr. 2018, pp. 1–7, doi: 10.1109/NOMS.2018.8406154.
[29] M. M. Ahemd, M. A. Shah, and A. Wahid, "IoT security: A layered approach for attacks & defenses," in *Proc. Int. Conf. Commun. Technol.*, Apr. 2017, pp. 104–110, doi: 10.1109/COMTECH.2017.8065757.
[30] Y.-N. Cao, Y. Wang, Y. Ding, H. Zheng, Z. Guan, and H. Wang, "A PUF-based lightweight authenticated metering data collection scheme with privacy protection in smart grid," in *Proc. IEEE Intl. Conf. Parallel Distrib. Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw.*, Sep. 2021, pp. 876–883.
[31] S.-K. Kim and J.-H. Huh, "A study on the improvement of smart grid security performance and blockchain smart grid perspective," *Energies*, vol. 11, no. 8, p. 1973, Jul. 2018.
[32] P. Chinnasamy, B. Vinodhini, V. Praveena, C. Vinothini, and B. B. Sujitha, "Blockchain based access control and data sharing systems for smart devices," *J. Phys. Conf. Ser.*, vol. 1767, no. 1, Feb. 2021, Art. no. 012056.
[33] P. Chinnasamy, A. Albakri, M. Khan, A. A. Raja, A. Kiran, and J. C. Babu, "Smart contract-enabled secure sharing of health data for a mobile cloud-based E-health system," *Appl. Sci.*, vol. 13, no. 6, p. 3970, Mar. 2023.
[34] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and efficient mutual authentication protocol for smart grid under blockchain," *Peer-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2681–2693, Nov. 2020, doi: 10.1007/S12083-020-01020-2.
[35] G. P. Sellitto, H. Aranha, M. Masi, and T. Pavleska, "Enabling a zero trust architecture in smart grids through a digital twin," in *Proc. Dependable Comput.-EDCC 2021 Workshops*, 2021, pp. 73–81.
[36] C. DeCusatis, P. Liengtiraphan, A. Sager, and M. Pinelli, "Implementing zero trust cloud networks with transport access control and first packet authentication," in *Proc. IEEE Int. Conf. Smart Cloud*, Nov. 2016, pp. 5–10.
[37] B. Embrey, "The top three factors driving zero trust adoption," *Comput. Fraud Secur.*, vol. 2020, no. 9, pp. 13–15, Jan. 2020.
[38] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014, doi: 10.1109/JPROC.2014.2320516.
[39] N. A. Hazari, A. Oun, and M. Niamat, "Machine learning vulnerability analysis of FPGA-based ring oscillator PUFs and counter measures," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 17, no. 3, pp. 1–20, Jul. 2021, doi: 10.1145/3445978.
[40] M. Tehranipoor, H. Salmani, and X. Zhang, *Integrated Ciruit Authentication*. Cham, Switzerland: Springer, 2015.
[41] S. M. H. Bamakan, A. Motavali, and A. Babaei Bondarti, "A survey of blockchain consensus algorithms performance evaluation criteria," *Expert Syst. Appl.*, vol. 154, Sep. 2020, Art. no. 113385.
[42] N. A. Hazari, F. Alsulami, A. Oun, and M. Niamat, "Performance analysis of XOR-inverter based ring oscillator PUF for hardware security," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Jul. 2019, pp. 253–256.
[43] A. Wang, W. Tan, Y. Wen, and Y. Lao, "NoPUF: A novel PUF design framework toward modeling attack resistant PUFs," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 6, pp. 2508–2521, Jun. 2021, doi: 10.1109/TCSI.2021.3067319.
[44] Z. Zheng, S. Xie, H.-N. Dai, W. Chen, X. Chen, J. Weng, and M. Imran, "An overview on smart contracts: Challenges, advances and platforms," *Future Gener. Comput. Syst.*, vol. 105, pp. 475–491, Apr. 2020, doi: 10.1016/J.FUTURE.2019.12.019.
[45] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl.*, May 2009, pp. 641–644, doi: 10.1109/AICCSA.2009.5069395.
[46] R. Kumar and R. Tripathi, "Blockchain-based framework for data storage in peer-to-peer scheme using interplanetary file system," in *Handbook of Research on Blockchain Technology*. New York, NY, USA: Academic, 2020, pp. 35–59.
[47] J. Sun, X. Yao, S. Wang, and Y. Wu, "Blockchain-based secure storage and access scheme for electronic medical records in IPFS," *IEEE Access*, vol. 8, pp. 59389–59401, 2020, doi: 10.1109/ACCESS.2020.2982964.
[48] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *Proc. 41st Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2018, pp. 1545–1550, doi: 10.23919/MIPRO.2018.8400278.
[49] F. Amsaad, T. Hoque, and M. Niamat, "Analyzing the performance of a configurable ROPUF design controlled by programmable XOR gates," in *Proc. IEEE 58th Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2015, pp. 1–4, doi: 10.1109/MWSCAS.2015.7282135.
[50] S. Nakamoto. (2008). *Bitcoin: A peer-to-peer Electronic Cash System*. [Online]. Available: https://assets.pubpub.org/d8wct41f/31611263538139.pdf
[51] A. Kulkarni, N. A. Hazari, and M. Niamat, "A blockchain technology approach for the security and trust of the IC supply chain," in *Proc. IEEE Nat. Aerosp. Electron. Conf. (NAECON)*, Jul. 2019, pp. 249–252, doi: 10.1109/NAECON46414.2019.9058027.
[52] F. Irresberger, K. John, P. Mueller, and F. Saleh. (2021). *The Public Blockchain Ecosystem: An Empirical Analysis*. [Online]. Available: https://ssrn.com/abstract=3592849
[53] S. Pahlajani, A. Kshirsagar, and V. Pachghare, "Survey on private blockchain consensus algorithms," in *Proc. 1st Int. Conf. Innov. Inf. Commun. Technol. (ICIICT)*, Apr. 2019, pp. 1–6, doi: 10.1109/ICIICT1.2019.8741353.
[54] M. Du, Q. Chen, J. Chen, and X. Ma, "An optimized consortium blockchain for medical information sharing," *IEEE Trans. Eng. Manag.*, vol. 68, no. 6, pp. 1677–1689, Dec. 2021, doi: 10.1109/TEM.2020.2966832.
[55] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017, doi: 10.1109/TII.2017.2709784.

[56] N. Chaudhry and M. M. Yousaf, "Consensus algorithms in blockchain: Comparative analysis, challenges and opportunities," in *Proc. 12th Int. Conf. Open Source Syst. Technol. (ICOSST)*, Dec. 2018, pp. 54–63, doi: 10.1109/ICOSST.2018.8632190.

[57] S. Joshi, "Feasibility of proof of authority as a consensus protocol model," 2021, *arXiv:2109.02480*.

[58] M. Sadek Ferdous, M. Jabed Morshed Chowdhury, M. A. Hoque, and A. Colman, "Blockchain consensus algorithms: A survey," 2020, *arXiv:2001.07091*.

[59] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *Proc. IEEE Int. Conf. Syst. Man, Cybern. (SMC)*, Oct. 2017, pp. 2567–2572, doi: 10.1109/SMC.2017.8123011.

[60] X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms: Mechanism, design and applications," *Sci. China Inf. Sci.*, vol. 64, no. 2, pp. 1–26, Nov. 2020.

[61] J. Kindervag, "No more chewy centers: Introducing the zero trust model of information security," *Forrester Res. Inc.*, pp. 1–15, Sep. 2010.

[62] A. Kerman, O. Borchert, S. Rose, and A. Tan, "Implementing a zero trust architecture," in *Proc. MITRE Corp., Tech. Rep.*, Mar. 2020, pp. 1–20.

[63] P. Chinnasamy, P. Deepalakshmi, and K. Shankar, "An analysis of security access control on healthcare records in the cloud," in *Intelligent Data Security Solutions for E-Health Applications*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 113–130.

[64] J. Park and R. Sandhu, "Towards usage control models: Beyond traditional access control," in *Proc. 7th ACM Symp. Access control models Technol.*, Jun. 2002, pp. 57–64.

[65] R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, "Access control policy enforcement for zero-trust-networking," in *Proc. 29th Irish Signals Syst. Conf. (ISSC)*, Jun. 2018, pp. 1–6, doi: 10.1109/ISSC.2018.8585365.

[66] M. Shokry, A. I. Awad, M. K. Abd-Ellah, and A. A. M. Khalaf, "Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision," *Future Gener. Comput. Syst.*, vol. 136, pp. 358–377, Nov. 2022, doi: 10.1016/J.FUTURE.2022.06.013.

[67] L. Na, X. Xiaohui, M. Xiaoqin, M. Xiangfu, and Y. Peisen, "Fake data injection attack detection in AMI system using a hybrid method," in *Proc. IEEE Sustain. Power Energy Conf.*, Nanjing, China, Dec. 2021, pp. 2371–2376, doi: 10.1109/ISPEC53008.2021.9735875.

[68] K. Pedramnia and M. Rahmani, "Survey of DoS attacks on LTE infrastructure used in AMI system and countermeasures," in *Proc. Smart Grid Conf. (SGC)*, Sanandaj, Iran, Nov. 2018, pp. 1–6, doi: 10.1109/SGC.2018.8777832.

[69] P. Chinnasamy, P. Deepalakshmi, A. K. Dutta, J. You, and G. P. Joshi, "Ciphertext-policy attribute-based encryption for cloud storage: Toward data privacy and authentication in AI-enabled IoT system," *Mathematics*, vol. 10, no. 1, p. 68, Dec. 2021, doi: 10.3390/MATH10010068.

[70] (2023). *What is Ganache*. Accessed: Jun. 5, 2023. [Online]. Available: https://trufflesuite.com/docs/ganache/

[71] M. C. I. Putri, P. Sukarno, and A. A. Wardana, "Two factor authentication framework based on ethereum blockchain with dApp as token generation system instead of third-party on Web application," *Register, Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 6, no. 2, p. 74, Jun. 2020.

[72] F. Alsulami and M. Niamat, "Performance study of FPGA based and-inverter ring oscillator PUFs," in *Proc. IEEE Int. Conf. Electro Inf. Technol. (EIT)*, Jul. 2020, pp. 194–199, doi: 10.1109/EIT48999.2020.9208341.

[73] A. Kulkarni, H. Bhattarai, T. H. Syed, and M. Niamat, "Protecting hardware IP by employing non-fungible tokens (NFTs)," in *Proc. IEEE Nat. Aerosp. Electron. Conf.*, Aug. 2023, pp. 187–191, doi: 10.1109/NAECON58068.2023.10365737.

[74] *ANSI C12 Smart Grid Meter Package*. Accessed: Jun. 20, 2022. [Online]. Available: http://goo.gl/PQxkW

[75] C. Ye, G. Li, H. Cai, Y. Gu, and A. Fukuda, "Analysis of security in blockchain: Case study in 51%-attack detecting," in *Proc. 5th Int. Conf. Dependable Syst. Their Appl. (DSA)*, Sep. 2018, pp. 15–24, doi: 10.1109/DSA.2018.00015.

[76] S. Eskandari, S. Moosavi, and J. Clark, "SoK: Transparent dishonesty: Front-running attacks on blockchain," in *Financial Cryptography and Data Security*. Cham, Switzerland: Springer, 2020, pp. 170–189.

[77] L. Zhou, K. Qin, C. F. Torres, D. V. Le, and A. Gervais, "High-frequency trading on decentralized on-chain exchanges," in *Proc. IEEE Symp. Secur. Privacy (SP)*, San Francisco, CA, USA, May 2021, pp. 428–445, doi: 10.1109/SP40001.2021.00027.

[78] Y. Wang, P. Zuest, Y. Yao, Z. Lu, and R. Wattenhofer, "Impact and user perception of sandwich attacks in the DeFi ecosystem," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, Apr. 2022, pp. 1–15, doi: 10.1145/3491102.3517585.

[79] S. Sayeed, H. Marco-Gisbert, and T. Caira, "Smart contract: Attacks and protections," *IEEE Access*, vol. 8, pp. 24416–24427, 2020, doi: 10.1109/ACCESS.2020.2970495.

[80] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on Ethereum smart contracts (SoK)," in *Principles of Security and Trust*. Cham, Switzerland: Springer, 2017, pp. 164–186.

**FARIS ALSULAMI** (Member, IEEE) received the M.S. degree in electrical engineering and the Ph.D. degree in engineering from The University of Toledo, Toledo, OH, USA, in 2016 and 2022, respectively. He is currently working an Assistant Professor with the Department of Computer and Network Engineering, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia. His research interests include hardware-assisted security for trusted embedded systems, cybersecurity, computing systems, FPGA security, hardware Trojans, side-channel attacks (SCAs), smart grids, and advanced metering infrastructure (AMI).

**AKSHAY R. KULKARNI** (Member, IEEE) received the Bachelor of Engineering degree in electronics and telecommunication from the University of Mumbai, Mumbai, India, and the Ph.D. degree from The University of Toledo, OH, USA, in 2023, under the supervision of Dr. Mohammed Y. Niamat. Between his undergraduate degree and start of Ph.D., he acquired abundant industry experience working in India and New Zealand. He is currently working as a Postdoctoral Research Associate with the University of Florida. His research interests include hardware security with focus in semiconductor supply chain, hardware security primitives, FPGA security, fault injection, side channel assessment, silicon photonics security, blockchain and zero trust for assured and trusted semiconductors, battery security, and space electronics security.

**NOOR AHMAD HAZARI** received the B.Sc. degree in electrical and electronics engineering from Khulna University of Engineering and Technology (KUET), Khulna, Bangladesh, and the Ph.D. degree in electrical engineering from The University of Toledo, Toledo, OH, USA. He is currently working as an Assistant Professor with the Department of Electrical Engineering, College of Charleston, Charleston, SC, USA. His research interests include hardware security, FPGA design security, PUFs, machine learning, and blockchain technology for hardware security.

**MOHAMMED Y. NIAMAT** (Life Member, IEEE) received the bachelor's degree in electrical engineering from Aligarh Muslim University, Aligarh, India, the master's degree in electrical engineering from the University of Saskatchewan, Saskatoon, SK, Canada, and the Ph.D. degree from The University of Toledo, Toledo, OH, USA, in 1989. From 1996 to 1997, he was a Visiting Associate Professor at the Center for Reliable Computing, Stanford University. He is currently working as the Group Leader of the High-Performance Computing Research Group, Department of Electrical Engineering and Computer Science, The University of Toledo. He has supervised more than 50 graduate students, including Faris Alsulami, Akshay R. Kulkarni, and Noor Ahmad Hazari.