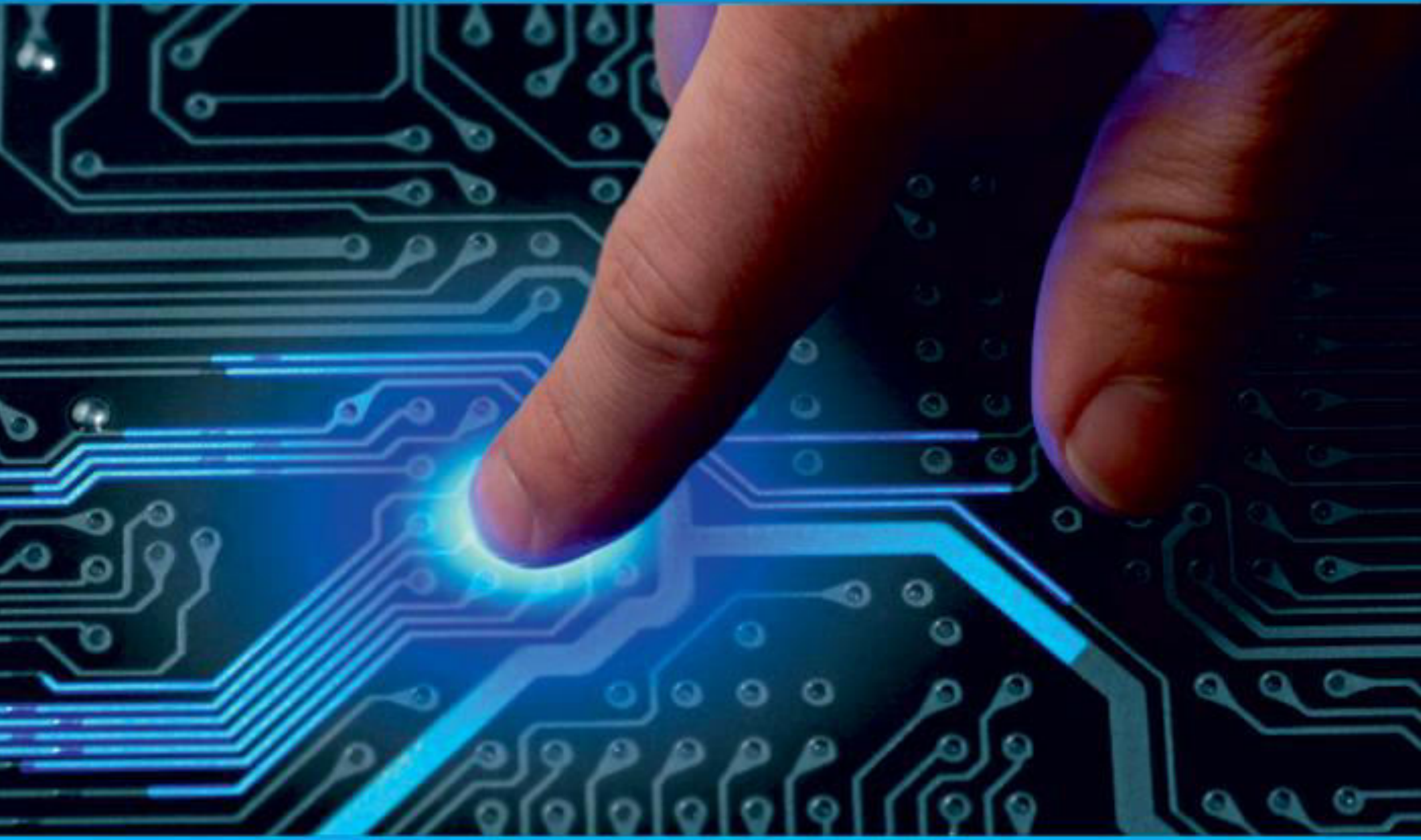
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 11, November 2024

ISSN
INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.625

9940 572 462 6381 907 438 ijircce@gmail.com www.ijircce.com

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Enhancing Trust in FPGA Supply Chains Through a Zero Trust Framework Utilizing Blockchain and ROPUF

Koti Ankith, Navya Beri

Students, Department of Electronics and Communication Engineering, GMR Institute of Technology, Rajam, A.P. India

ABSTRACT: The increasing adoption of field-programmable gate arrays (FPGAs) across various industries has highlighted some serious vulnerabilities in their supply chains, especially because of the involvement of untrusted parties. This paper addresses key security concerns like intellectual property theft, counterfeiting, and bitstream tampering, all of which can compromise the reliability of FPGAs and endanger users. To enhance trust and integrity in the FPGA supply chain, NIST has introduced a new zero trust framework that utilizes blockchain technology alongside ring oscillator physical unclonable functions (ROPUFs). Our architectural framework is based on zero trust principles laid out by the National Institute of Standards and Technology. We carried out an in-depth case study simulating a typical FPGA supply chain, which included all relevant stakeholders, using the Ganache framework from the Truffle suite. The experiments were conducted on Artix 7 Xilinx FPGAs installed on Nexys 4 Digilent boards. We evaluated how effective our zero trust framework is by analyzing different attack scenarios, showing its potential to reduce security threats. This research is a groundbreaking attempt to apply zero trust principles to safeguard the FPGA supply chain by integrating blockchain and hardware-based security measures.

KEYWORDS: Blockchain technology, field programmable gate arrays, hardware security, ring oscillator physical unclonable functions, zero trust architecture.

I.INTRODUCTION

Field-Programmable Gate Arrays (FPGAs) are a vital component for most industries, especially given the fact that they offer post-manufacturing time reconfigurability so as to have user-specific designs. The same advantage presents considerable security risks with regards to the intricate supply chain of the FPGA systems. Offshoring fabrication in FPGAs exposes a system to a potential threat such as intellectual property theft, hardware Trojans, and counterfeiting due to dependence on foundries.

Recent issues regarding counterfeit or resold FPGAs are becoming notorious for causing inconsistent performance and serious security threats for the owners. The U.S. government has initiated executive orders involving the resilience of supply chain improvement, which also involves initiating a zero-trust model to better cybersecurity. Never trust, always verify defines the zero-trust approach, wherein each access should be verified and never rely on a source or party whose identity or credibility has yet to be established.

The architecture here is a novel zero-trust structure in integrating blockchain with Physical Unclonable Functions (PUFs) that addresses insider threats and vulnerabilities in the semiconductor supply chain. Blockchain is a decentralized database that securely documents transactions between all stakeholders, while PUFs generate unique challenge-response pairs to enhance security for each chip.

The proposed framework should be able to enhance security and trustworthiness within the FPGA ecosystem by preventing unauthorized access or breaches. The research further will explore existing literature on zero-trust principles, blockchain technology, and PUFs before detailing the proposed architecture and strategies for implementation.

1. Zero Trust

Introduced by Forrester Research in 2010, Zero Trust is a cybersecurity model that necessitates ongoing validation of every request for access from all users, users devices, and applications, as well as every server or service within the network because no intrinsic trust in the user or any network exists, with every incoming or outgoing entity's access request validated before the access is granted. Zero Trust architecture leads to micro-segmentation of networks, thereby enhancing the protection of resources and minimizing the vulnerabilities within today's digital environments. In this way, strict controls over access and continuous monitoring provide better security for the organizations against sophisticated cyber threats. Generally, Zero Trust significantly enhances the security posture since it understands that trust should never be assumed and always verified.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

A. Zero Trust Principles

The Zero Trust security model is founded on a few critical principles designed to enhance the safety of organizations. The heart of it is "Never Trust, Always Verify," meaning no entity is trusted by default, even those located inside or outside the network. Each access request needs to be fully authenticated and authorized before access is given to any system or application.

Another fundamental principle is Minimum Privilege Access, which limits user and device access to only what is necessary for their roles. This reduces the damage that can be done in case of a breach. Micro-Segmentation further enhances security by dividing networks into smaller, isolated zones, thereby containing breaches and limiting lateral movement within the network.

Continuous monitoring and validation of user activities is the most important element in the Zero Trust model. Constantly, organizations must measure trust levels in evolving risks. Another aspect of it is Strong Identity Verification with methodologies like Multi-Factor Authentication that ensure access to sensitive resources is strictly granted only to the authorized users.

Data protection is also a priority and is focused on protecting data at rest and in motion through encryption. The principle of Assume Breach is to encourage organizations to act as if breaches are inevitable, which would prompt proactive monitoring and response strategies.

Collectively, these principles strengthen an organization's security posture by eliminating implicit trust and ensuring strict access controls based on verified identities and contextual factors. This all-rounded approach is directed at eliminating the risks posed by unauthorized access and cyber threats.

B. Zero Trust Access Model

The Zero Trust model is a principle that assumes all entities trying to connect to a network, whether it be users, devices, or applications, are untrusted by default, regardless of their location. It recognizes that threats can be both internal and external, hence eliminating the reliance on traditional trust based on proximity or past verification. To maintain security, every access request must undergo rigorous verification, ensuring that only authenticated and authorized entities can access sensitive resources, thereby significantly reducing the risk of unauthorized access and potential breaches.

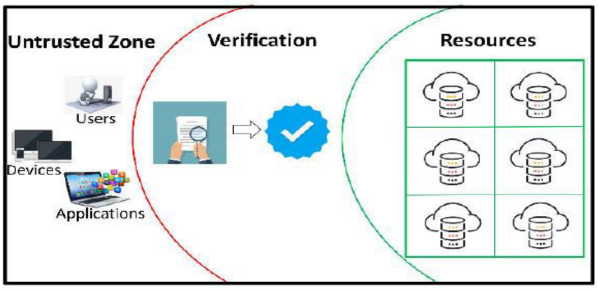


Figure 1: A zero trust access model [1].

The Zero Trust model emphasizes strict access control to protected resources, represented by lock icons, ensuring that only those who have successfully passed the verification process can gain entry. This principle reinforces the philosophy of "never trust, always verify," as every access request is meticulously scrutinized to uphold security across the network, thereby helping organizations safeguard their data and infrastructure against emerging threats.

C. Tenets of Zero Trust

Policies within the FPGA supply chain for implementing a zero trust architecture are based on NIST guidelines and will be focused on authorization and verification. Formulated policies regarding access control and authentication will enhance security and integrity in the supply chain ecosystem.

i. Data and computation are treated as resources.

ii. Information is secured regardless of its location.

iii. Access is granted on a per-session basis.

iv. Access decisions are based on dynamic policies.

v. Devices and assets must be maintained in a secure state.

vi. Strict enforcement of authentication and authorization.

vii. Continuous collection of information to enhance security.

The above tenets are applied to the FPGA supply chain in this work.

Implementing the zero trust framework within an organization's model can bring better cybersecurity posture, with each and every access request chipped away at to protect the integrity and security of the organization's networks.

II.BLOCKCHAIN TECHNOLOGY

Blockchain technology is a decentralized digital ledger that records transactions across an association of computers, ensuring the safety and transparency of data. By chaining these groups of transactions into blocks, this method constructs a chronological chain that it is almost impossible to manipulate or alter without the agreement of network participants. This system allows for secure peer-to-peer interactions without intermediaries because it provides a tamper-proof record of transactions. Thus, users have greater control over their data and transactions. This leads to trust among participants while minimizing the risks associated with unauthorized access and manipulation.

A. The Blockchain Structure

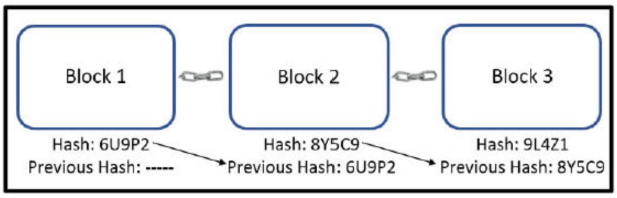


Figure 2: The blockchain structure [1].

The genesis block, Block 1, has a hash of '6U9P2' and refers to no previous hash; it is the starting block of the blockchain. The following blocks are Block 2 with a hash of '8X5C9' (previous hash '6U9P2') and Block 3 with a hash of '9L4Z1'(previoushash'8X5C9'), among others, which are chained in sequence.

A blockchain structure is made up of interlinked blocks, each containing several key components. Hash is a unique identifier for the block's data, generated through cryptographic hashing, while Previous Hash links the current block to its predecessor, forming a secure chain. The Transaction Data holds the actual data, typically a set of transactions relevant to the blockchain's application. Moreover, each block holds a Timestamp showing when it was actually created and a Nonce - a number used in mining a valid hash that satisfies network conditions of difficulty. Last, the Merkle Root symbolizes all transactions in the block that are computed by recursively hashing together pairs of transaction hashes, until a single hash value is obtained.

B. Process of Blockchain Technology

Blockchain technology operates through a straightforward process designed to ensure secure and transparent transactions. It begins with Transaction Creation, where a user or device initiates a transaction containing essential information such as sender and recipient addresses and asset amounts. Next, Transaction Verification occurs, where network participants validate the transaction's legitimacy and the sender's permissions before it can be added to the blockchain. A Consensus Mechanism is then applied to agree on the validity of the transaction, avoiding double-spending and ensuring that all nodes have a consistent view of the blockchain.

Once validated, the transaction will be combined along with other pending transactions into a Block, such as having its unique hashing of the prior block, meaning that once completed, then it will join the pre-existing blockchain by consensus: the new block is, therefore, finalized and thus cannot be amended. That updated blockchain gets distributed between all nodes, thereby increasing participants' transparency and trust. If applicable, Smart Contracts are run automatically when predefined conditions are met, allowing for automated processes without intermediaries. This constant monitoring for abnormalities ensures that blockchain provides a safe method for recording transactions in a decentralized manner while still maintaining integrity and trust within different applications, such as cryptocurrencies and supply chain management.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

C. Smart Contracts of Blockchain Technology

Smart contracts are self-executing agreements on a blockchain that automate processes, enhance trust through transparency, and ensure security while minimizing transaction costs and errors. In a Private Blockchain, these contracts create a secure environment for approved participants, allowing sensitive transactions involving assets like intellectual property cores to occur only among authorized entities, thereby reducing risks from unauthorized access.

III.PHYSICAL UNCLONABLE FUNCTIONS (PUFS)

A Physical Unclonable Function (PUF) is a hardware security primitive that generates unique digital outputs, known as responses, based on the inherent characteristics of a device. PUFs produce these unique responses for a given input, or challenge, while maintaining the secrecy of their relationship. This means that even when the same challenge is presented to different devices, the responses generated are distinct and specific to each device.

A. Representation of the relation between challenges (input),physical unclonable functions (PUFs), and responses (output).

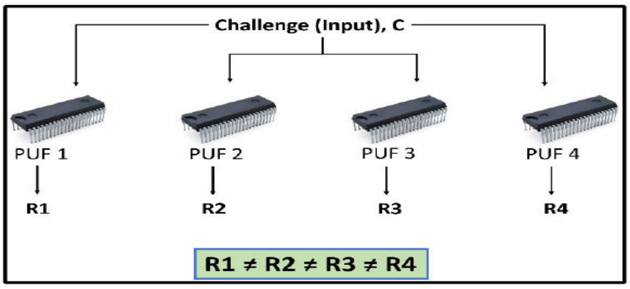


Figure 3: Presentation of relation between challenges and responses

The concept of Physically Unclonable Functions (PUFs). It shows four PUFs labelled PUF 1, PUF 2, PUF 3, and PUF 4, each connected to a unique resistor (R1, R2, R3, and R4). The label “Challenge (Input), C” indicates that the same input is applied to all four PUFs. The mathematical statement “R1 ≠ R2 ≠ R3 ≠ R4” highlights that each resistor has a different resistance value, making each PUF unique.

PUFs are useful in cryptography and secure communications because their unique responses are harder to duplicate or clone, which enhances security.

B. Ring Oscillator PUF (ROPUF)

The Ring Oscillator Physical Unclonable Function, or ROPUF for short, is a PUF based on delay generated by an odd number of inverters, using innate process variations in transistors and environmental conditions that can produce Challenge-Response Pairs for authentication purposes. The ROPUFS are very useful as they produce unique identifiers impossible to reproduce or predict on the FPGAs, giving them good resistance against counterfeiting and cloning. The generated CRPs can be securely stored on a blockchain, making easy verification and authentication throughout the supply chain. This integration enhances the security of FPGA devices by ensuring that each unit responds uniquely to challenges, thus safeguarding against unauthorized access and manipulation.

Structure: The ROPUF circuit consists of n identical ROs (denoted asRO_1 to RO_n) that produce oscillator frequencies inside a delay loop.

Frequency Generation: Due to the inherent manufacturing variations, each RO will produce different frequencies and, hence, different outputs when pairs of ROs are compared.

Challenge-Response Mechanism: A pair of multiplexers employs the PUF challenge to select frequency pairs to enable comparison of two frequencies f_a and f_b .

Response Generation :

The response bit r_{ab} is generated through a simple comparison method

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

This equation shows that if the frequency f_a is more than the frequency f_b, then, it sets the response bit into 1, otherwise to 0. This method ensures that for the same challenge, every device outputs a different response depending on its inherent properties.

C. Methodology for Implementing XOR-Inverter Based Ring Oscillator PUF (ROPUF) in FPGA Applications

In designing the Ring Oscillator Physical Unclonable Function, several key components that interwork to produce distinct outputs in authentication are required. Among these are a 1 by N Demultiplexer, an N by 1 Multiplexer, a Challenge Generator, a 16-bit Binary Counter, a Reference Counter, and a Timing Controller. A 10-bit challenge is created from the clock 50 MHz and driven through N-by-1 Multiplexer, to enable choosing one of the N SCROs that has somewhat distinct frequency, based on variations from process. The result out from selected SCRO drives it through the 16-bit binary counter to count cycles for given length, managed by Timing Controller. This process provides that every challenge applied must result in a different response (C1) according to the selected SCRO and challenge input, exploiting intrinsic manufacturing variations toward the generation of secure CRPs for use in hardware security applications. Unique frequencies generated by the ROPUF enable reliable authentication methods, thus protecting against clones or counterfeit devices.

D. Performance Metrics of the Implemented ROPUF

The performance of the ROPUF is evaluated using several key metrics:

Uniformity:

$$\text{Uniformity}_k = \frac{1}{n}\sum_{i=1}^{n} r_{i,j} \times 100\%$$

Uniformity Measures The uniformity ratio of 0's and 1's in response bits It should be approximately 50% for an ideal PUF. It could be calculated by using the following formula.

Uniqueness:

Uniqueness tests the ability of a PUF to produce distinct results at different devices or in the same device, on different locations. It is calculated by finding the Hamming distance between response bits across different chips:

$$\text{Uniqueness}_k = \frac{2}{k(k-1)}\sum_{i=1}^{k(k-1)}\sum_{j=i+1}^{k} \text{HD}(\text{Ri}, \text{R}_j)/\text{N}^{*}100\%$$

Bit Aliasing:

Bit aliasing estimates the bias of a response bit across different devices and is represented as:

$$(\text{bit - aliasing})_l = \frac{1}{k}\sum_{i=1k} r_{i,l} \times 100\%$$

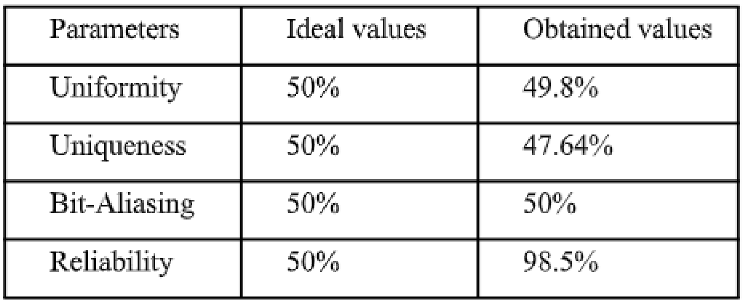
Reliability:

Reliability measures how consistently a PUF reproduces response bits under varying conditions.

It is computed using:

$$\text{Reliability}_k = 1 - \frac{1}{K.T.L}\sum_{k=1}^{K}\sum_{t=1}^{T}\sum_{l=1}^{L} r_{n,k,l} \otimes r_{n,k,t,l}$$

Table 1: Performance metrics of the ROPUF [1].



Parameters	Ideal values	Obtained values
Uniformity	50%	49.8%
Uniqueness	50%	47.64%
Bit-Aliasing	50%	50%
Reliability	50%	98.5%

All parameters are calculated according to the given equations, and the obtained results are presented in Table. For the designed ROPUF, the bit-aliasing, uniformity, and uniqueness metrics were reached as 50%, 49.8%, and 47.64%, respectively, close to the ideal goal of 50% mentioned in Moreover, the achieved reliability is 98.5%.

IV. PROPOSED ZERO TRUST ARCHITECTURE (ZTA)

Adopting the guidelines from NIST to secure the supply chain is crucial when implementing zero trust architecture. This involves using blockchain as a system for user authorization and PUF for authentication of FPGAs, while blockchain's traceability and immutability features enhance security, tracking all transactions and identifying any unauthorized change.

The Zero Trust Architecture (ZTA) policies for an FPGA supply chain follow NIST guidelines, emphasizing strict authorization and verification processes. These principles ensure that every user and device trying to access network resources is thoroughly authenticated, reducing the risk of unauthorized access. Key Zero Trust tenets include "Never Trust, Always Verify," meaning no entity is trusted by default, and "Least Privilege Access," where users and devices are granted only the minimum level of access necessary. Other tenets focus on continuous monitoring and validation of trust at all stages of interaction within the network. By implementing these principles, organizations can significantly enhance security in the FPGA supply chain, ensuring only authorized devices and users can interact with sensitive resources. The tenets aim to create a secure and trustworthy environment throughout the lifecycle of FPGA systems.

A. The Blockchain Support

The development of smart contracts is necessary for fulfilling the full potential of blockchain technology in enhancing the FPGA supply chain zero trust framework. These contracts A blockchain-enabled MFA application is implemented in the proposed research to ensure user authorization and verification. The application is meant to enhance security by recording all authentication actions to build trust among users, devices, and applications.

B. The ROPUF Supplement

The enhancement of the zero trust architecture comes from the implementation of ring oscillator PUFs together with blockchain technology, which acts as a Root-of-Trust (RoT) for chips in the FPGA supply chain, generating unique challenge and response pairs to authenticate and verify FPGAs.

V. INTEGRATION OF ZERO TRUST ARCHITECTURE(ZTA), BLOCKCHAIN TECHNOLOGY, PHYSICAL UNCLONABLE FUNCTION (PUF)

A Zero Trust Architecture (ZTA), blockchain technology, and Ring Oscillator Physical Unclonable Functions (ROPUs) together form a robust security framework for the FPGA supply chain, addressing risks like counterfeiting and tampering. Trusted participants, including manufacturers, distributors, and end-users, are authenticated through a blockchain-based identity management system, ensuring that only authorized entities can access sensitive data. The blockchain acts as an immutable ledger, recording all transactions and interactions for full transparency and accountability. ROPUFs create unique identifiers for each FPGA, stored securely on the blockchain, enabling real-time verification of device authenticity at every supply chain stage.

As the FPGA moves through manufacturing, distribution, and deployment, each transaction is logged, quickly detecting any tampering or counterfeit attempts. Blockchain smart contracts automate compliance checks and trigger actions when specific conditions are met, such as alerting stakeholders if an FPGA's authenticity is compromised. End-users can verify device integrity by comparing the FPGA's unique PUF response with the blockchain record, ensuring only legitimate devices are in use. This integrated approach enhances security, reduces risks, and strengthens the integrity of the entire FPGA supply chain.

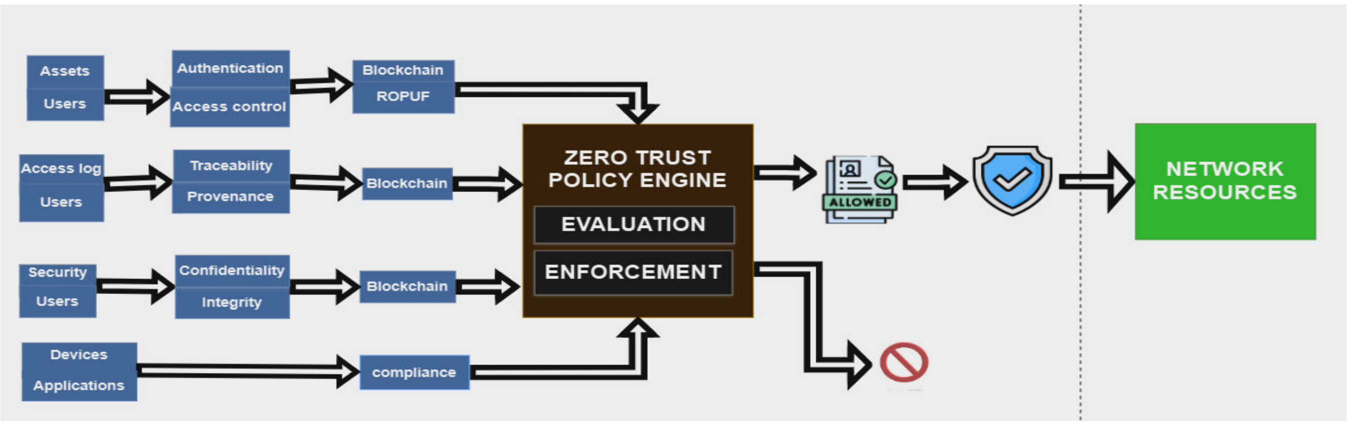
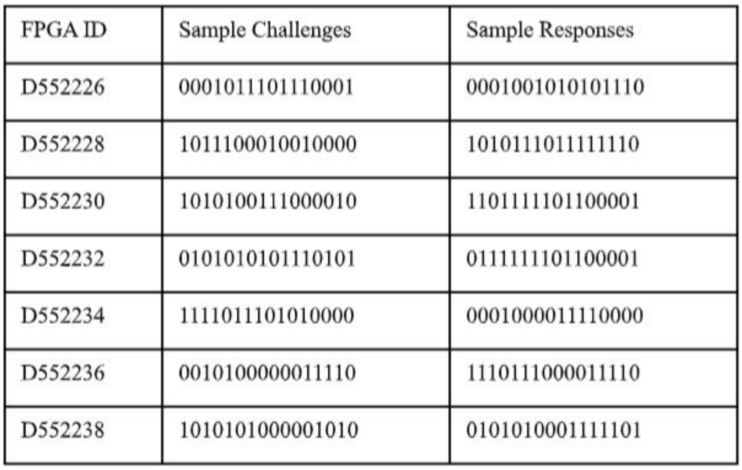


Figure 4: Proposed zero trust architecture for field programmable gate array supply chain security [1].

I.Case Study: Pseudocodes And Simulation

The case study presents a framework that harmonizes blockchain technology and PUFs to enhance security in the FPGA supply chain. Empirical testing was conducted on Xilinx Artix 7 FPGAs mounted on a Nexys 4 Digilent board, utilizing the Ganache framework, which is designed for Ethereum distributed applications. Ganache provides a safer environment for the development and testing of decentralized applications with features such as an interface that comes with preloaded accounts for transaction management. In its design phase, it focused on making policies, components, and implementations needed and includes a blockchain network, creating smart contracts, and includes ROPUFS and challenge-response pairs generation that is used to authenticate access. The ROPUF was generated CRPs using an Agilent 16801A logic analyzer. A sample of CRPs from a dataset of 30,000 was tabulated for later authentication and validation.

Table 4**:** Tabular form of CRPs sample from a data set [1].



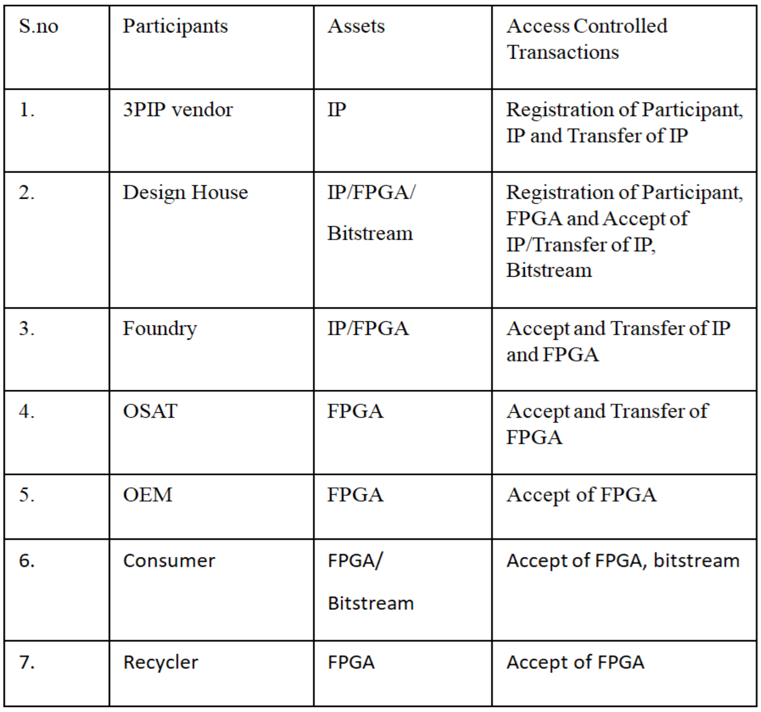
FPGA ID	Sample Challenges	Sample Responses
D552226	0001011101110001	0001001010101110
D552228	1011100010010000	1010111011111110
D552230	1010100111000010	1101111101100001
D552232	0101010101110101	0111111101100001
D552234	1111011101010000	0001000011110000
D552236	0010100000011110	1110111000011110
D552238	1010101000001010	0101010001111101

The experiment established a blockchain network centered around the FPGA supply chain, which consists of participants, assets, and transactions. In this context, assets include intellectual property (IP), bitstream files, and the

FPGAs themselves. Ownership of these assets is transferred among participants through various transactions such as registration, transfer, and acceptance.

The application developed ensures the managing of all the transactions made within the network of an FPGA supply chain using smart contracts, thus providing role-based access control along with a mechanism for a multi-factor authentication that could further provide a high security. First registered user to the blockchain is a 3PIP vendor who, rather than forwarding the IP cores to the design house directly uploads it securely on Inter Planetary File System, also abbreviated as IPFS. After uploading, these IP cores are registered on the blockchain, and it allows the vendor to initiate asset transfer by calling the transferIP() function of the smart contract. This ensures that only authorized participants can access and retrieve the IP cores from IPFS, maintaining a secure transaction environment.

Table 5**:** Tabular form of blockchain network [1].



S.no	Participants	Assets	Access Controlled Transactions
1.	3PIP vendor	IP	Registration of Participant, IP and Transfer of IP
2.	Design House	IP/FPGA/ Bitstream	Registration of Participant, FPGA and Accept of IP/Transfer of IP, Bitstream
3.	Foundry	IP/FPGA	Accept and Transfer of IP and FPGA
4.	OSAT	FPGA	Accept and Transfer of FPGA
5.	OEM	FPGA	Accept of FPGA
6.	Consumer	FPGA/ Bitstream	Accept of FPGA, bitstream
7.	Recycler	FPGA	Accept of FPGA

A. Pseudocode Explanation

The following pseudocode depicts some of the core functionalities implemented within the framework:

Pseudocode 1: Function Modifier

```
contract zeroTrustFPGA {
  address authorizedParticipantAddress;
  // Modifier to validate participant
  modifier onlyAuthorizedParticipant() {
    require(
      msg.sender == authorizedParticipantAddress,
      "Only Authorized Participant can perform this Operation."
    );
    ;
  }
```

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

```
}
```

This access control function modifier ensures that only verified users can perform specific operations on the FPGA supply chain network. It prevents unauthorized activities through strict access control that only designated users are capable of accessing such sensitive functions before executing critical operations.

Pseudocode 2: Event Function

```
contract zeroTrustFPGA {
  // Event to trigger an action
  event transferInitiated(address currentOwner, address newOwner);
  // Function to initiate transfer of an asset
  function transferOwnership() {
    // Code to execute transfer of ownership of an asset
    emit transferInitiated(currentOwner, newOwner);
  }
}
```

This event function triggers actions upon asset transfers within the blockchain network. That means, by emitting an event when ownership is transferred, it would allow other components in the system to react accordingly—such as notifying stakeholders or logging actions—ensuring that access is granted only after these specified events are performed successfully.

Pseudocode 3: IC Validation using PUFs

```
contract zeroTrustIC {
  // Function to validate IC
  functionvalidateIC(challenges,responses) onlyCurrentOwner() {
    if (challenges && responses == stored CRPs) {
      return true;
    } else {
      return false;
    }
  }
}
```

This validation mechanism relies on CRPs generated from ROPUFs to authenticate devices at any stage of the supply chain, thus guaranteeing security against counterfeit or tampered devices by confirming that challenges and responses match the stored CRPs.

VI.CONCLUSION

The paper introduces a zero-trust architecture for the FPGA supply chain that seeks to remove blind trust by authenticating every individual and device that accesses its resources. It further talks about how blockchain features are supporting the principles of a zero-trust architecture and the role of modifier, event functions in smart contracts, traceability, and immutability. Moreover, in the responses provided by the Ring Oscillator Physical Unclonable Functions, it helps in improving resistance to security attacks in this system. The pioneering hybridization of these technologies serves not only to enhance confidence and security in FPGA supply chains but also identifies existing vulnerabilities and tests robustness against numerous security threats. The study sets a precedent for potential future applications in comparable spaces, noting that implementing blockchain and ROPUF under a Zero Trust architecture effectively safeguards against hostile agents operating against critical supply chains.

VII.Future Scope

Further work on the proposed Zero Trust architecture will be to expand its attack surface of blockchain and smart contracts, identifying any weaknesses that malicious actors could potentially exploit. Plans are afoot to extend this framework to ASIC supply chains so that it can be further applied and have an increased impact in securing different kinds of supply chains and in adaptation of the architecture for ASIC environments. The researchers will determine the framework's potential effects on the overall performance of the supply chain by balancing comprehensive security measures with operational efficiency so that the increased security does not compromise effectiveness. This approach develops a more robust and flexible Zero Trust architecture that is adaptive to new threats and different applications, thus setting an example for future implementations in similar domains.

References

[1] Kulkarni, Akshay, Noor Ahmad Hazari, and Mohammed Niamat. "A Zero Trust-based framework employed by Blockchain Technology and Ring Oscillator Physical Unclonable Functions for security of Field Programmable Gate Array Supply Chain." IEEE Access (2024)

[2] A. Stern, H. Wang, F. Rahman, F. Farahmandi, and M. Tehranipoor, "ACED-IT: Assuring Confidential Electronic Design Against Insider Threats in a Zero-Trust Environment," IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 41, no. 10, pp. 3202–3215, Oct. 2022. DOI: 10.1109/TCAD.2021.3127864.

[3] T. Zhang, F. Rahman, M. Tehranipoor, and F. Farahmandi, "FPGAchain: Enabling Holistic Protection of FPGA Supply Chain with Blockchain Technology," IEEE Design & Test, vol. 40, no. 2, pp. 127–136, Apr. 2023. DOI: 10.1109/MDAT.2022.3213998.

[4] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," Proceedings of the IEEE, vol. 102, no. 8, pp. 1126–1141, Aug. 2014. DOI: 10.1109/JPROC.2014.2320516.

[5] N. A. Hazari, A. Oun, and M. Niamat, "Machine Learning Vulnerability Analysis of FPGA-Based Ring Oscillator PUFs and Countermeasures," ACM Journal on Emerging Technologies in Computing Systems, vol. 17, no. 3, pp. 1–20, Jul. 2021. DOI: 10.1145/3445978.

[6] U. Guin, K. Huang, D. DiMase, J.M Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain,\" Proc. IEEE, vol. 102, no. 8, pp. 1207–1228, Aug. 2014.doi: 10/1109/JPROC/2014/2332291.

[7] X.Xu et al., "Electronics supply chain integrity enabled by blockchain," ACM Transactions on Design Automation of Electronic Systems vol24 no3 pp1-25 May2019; doi:10/1145/3315571.

[8] Z.A.Collier and J.Sarkis "The zero trust supply chain: Managing supply chain risk in the absence of trust," International Journal of Production Research vol59 no11 pp3430-3445 Feb2021; doi:10/1080/00207543/2021/1884311.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING