Blockchain-Enabled Whitelisting Mechanisms for Enhancing Security in 3D ICs

Gaines Odom
Auburn University
Auburn, Alabama, USA
gaines.odom@auburn.edu

Hardhik Mohanty
University of Southern California
Los Angeles, California, USA
hmohanty@usc.edu

Ujjwal Guin
Auburn University
Auburn, Alabama, USA
ujjwal.guin@auburn.edu

Bhaskar Krishnamachari
University of Southern California
Los Angeles, California, USA
bkrishna@usc.com

ABSTRACT

The globalization of the semiconductor supply chain has paved the way for a rapid enhancement in the research and development, and the production of electronic devices. The exponential growth in manufacturing, design, and distribution has given rise to a complex ecosystem where the risk of counterfeit or Trojan-inserted integrated circuits (ICs) becomes significant. As emerging technologies continue to reshape the landscape of the electronics supply chain, addressing the challenges and risks posed by these developments becomes increasingly crucial. The challenge of ensuring security for 2.D/3D ICs, composed of multiple chiplets manufactured globally, is exacerbated by the lack of trust among entities in the semiconductor supply chain. The chiplets that are fabricated at an untrusted location can be tampered with, resulting in the insertion of malicious circuits that may leak secret information to an adversary. This paper presents a conceptual approach that limits the communication capability of an untrusted chiplet using a whitelisting technique inspired by security measures deployed in traditional networks. We also propose to use a logger to capture any communication rule violation that occurs during die-to-die communications across different chiplets. The logger state can be further uploaded to an immutable blockchain ledger for forensics purposes if an attack is identified.

CCS CONCEPTS

• **Security and privacy → Malicious design modifications**; **Hardware-based security protocols**; **Information flow control**.

KEYWORDS

Whitelisting, blockchain, traceability, provenance, IP piracy, tampering

ACM Reference Format:
Gaines Odom, Hardhik Mohanty, Ujjwal Guin, and Bhaskar Krishnamachari. 2024. Blockchain-Enabled Whitelisting Mechanisms for Enhancing Security in 3D ICs. In *Great Lakes Symposium on VLSI 2024 (GLSVLSI '24), June 12–14, 2024, Clearwater, FL, USA.* GLSVLSI, Knoxville, TN, USA, 6 pages. https://doi.org/10.1145/3649476.3660368

1 INTRODUCTION

The globalization of the semiconductor supply chain brings rapid research and development (R&D) of chip fabrication and design, as well as swift adoption of the latest technology node. System-on-chip (SoC) has evolved in the past decades to combine different intellectual properties (IPs) into one design layout, and thus, a single die with multiple functions in one chip. However, the intensive computation workload in today's high-performance computers (HPC), data centers, cloud computing, and machine learning applications demands innovations beyond the current state-of-the-art SoC status quo. Driven by the need to further reduce latency and power consumption, increase throughput, and a better yield in IC fabrication, heterogeneous integration (HI) and 2.5D/3D packaging emerge as the new technological solution. This allows the horizontal and vertical stacking of multiple dies in a single package/chip, analogous to a system of mini-chips than the monolithic IC in SoC [16, 19]. It is actively being researched and developed by multiple entities in the supply chain, e.g., TSMC 3DFabric^{TM} a 3D silicon stacking and advanced packaging technologies [15], and Samsung 3D-TSV (12 layers) DRAM Chip [13]. A ubiquitous interconnect, e.g., Universal chiplet interconnect express (UCIe) [18] and open high-bandwidth interface (OpenHBI) [12], at the package level to cover die-to-die (D2D) communication has been developed.

Unfortunately, the same globalization of the semiconductor supply chain opens the door for various threats to US critical infrastructures, where they are targeted by untrusted electronic products, counterfeit ICs, and devices with hardware Trojans [8, 17]. These threats originated from malicious third-party IP vendors, untrusted manufacturing facilities, and rogue distributors, including pirated and maliciously modified IPs, cloned and recycled ICs, *etc.* Bloomberg reported in 2018 and 2021 that the groundbreaking hardware hack with an extra tiny chip, covertly placed on board, can breach sensitive data from US companies [2, 3]. Although the published hack targeted pre-HI hardware, it is possible that an adversary can still execute similar hacks by incorporating malicious die(s) inside 2.5D/3D packages. When the hardware is compromised due to hardware Trojans in the chip or malicious chiplets, existing

GLSVLSI '24, June 12–14, 2024, Clearwater, FL, USA

ACM ISBN 979-8-4007-0605-9/24/06…$15.00
https://doi.org/10.1145/3649476.3660368

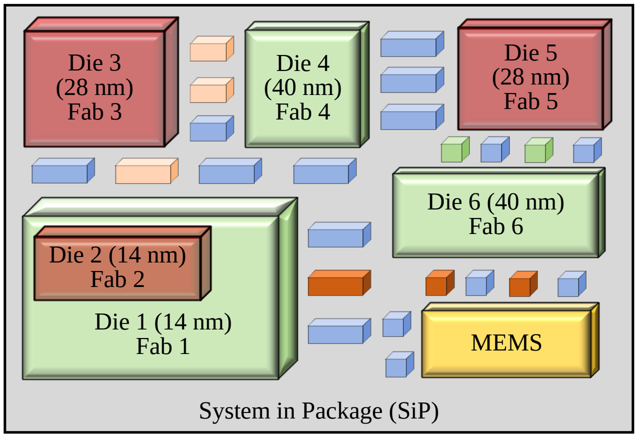

Figure 1: An abstract representation of heterogeneous integration where multiple chiplets are assembled in a SiP.

and additional software attacks can be mounted for malicious purposes. When hardware is not authentic (compromised or cloned), the firmware and software running on it can be exploited by the attacker – easily bypassing the existing security measures implemented at the software level as the entry point to gain access to the device and/or system.

Figure 1 shows a typical system-in-package (SiP) architecture that integrates multiple dies within a single package, such as combining a 2.5D and a 3D stacked die into one unit. One chip can consist of several dies varying in process node, function, and manufacturing origin stacked and incorporated into the same package. As such, a significant concern exists regarding chiplets manufactured overseas, which may have (possibly unbeknownst to its IP holder) been tampered with hardware Trojan circuitry. In Figure 1, chiplets 1, 4, and 6 are assumed to be trusted, and chiplets 2, 3 and 5 are assumed to be untrusted. If data transmission remains unrestricted, chiplets 2, 3, and 5 pose a threat to the overall chip. A Trojan in one die could potentially compromise sensitive data or disrupt services anywhere within the die's permitted transmission network. Without run-time attack detection and protection, a malicious die can have unrestricted access to critical systems and data, making it imperative to secure against unnecessary communications.

Given the nascent nature of 2.5D/3D ICs, there is a noticeable gap in prior research in this domain. While researchers have proposed solutions to enhance the security of these ICs against hardware Trojans [11, 21], they often fall short in addressing the runtime threats these chips face once deployed in the field. Despite decades of dedicated research, the challenge of detecting hardware Trojans persists [10, 20]. In contrast to the conventional Trojan detection methods, our approach aims to proactively curb malicious activities through the implementation of a whitelisting strategy.

The contributions of this paper are summarized as follows:

- *Whitelisting:* We believe we are the first to propose whitelisting to allow trusted chiplets to communicate outside of their communication domain. By adopting a whitelist-based approach, our solution exclusively permits authorized communications, acting as a robust barrier against any unsanctioned communication attempts originating from untrusted chiplets and directed beyond chip boundaries.
- *Designing an on-chip logger:* The proposed on-chip logger serves as a vigilant recorder, capturing any deviations or breaches that may transpire during the chiplets' communication. It is imperative to deploy this logger within a trusted chiplet, such as the network IO responsible for external communications. This strategic placement ensures that the logger remains immune to manipulation by untrusted chiplets, safeguarding the integrity of logged entries. By designating a trusted enclave for the logger, we fortify its role as an impartial and secure observer, enhancing the overall reliability and accountability of the logging mechanism.
- *Integration of blockchain:* Our proposed approach involves leveraging a permissioned blockchain ledger to systematically and permanently document the state of the on-chip logger at regular intervals. This blockchain-based ledger serves as an immutable record, enhancing the traceability and transparency of the logger's activity over time. In the event of identifying a potential attack, this ledger proves instrumental for conducting in-depth analyses. Detailed insights can be gleaned by referring to the recorded logger states, enabling a comprehensive understanding of the nature and extent of any detected security breach or malicious activity. This integration of blockchain technology elevates the resilience and forensic capabilities of our proposed logging system, ensuring a robust response to security incidents.

The rest of the paper is organized as follows: In Section 2, we present a general overview of the proposed architecture, including whitelisting, the use of an on-chip logger, and an external blockchain ledger for security. We presented the implementation details in Section 3. Finally, we conclude the paper in Section 4.

2 PROPOSED ARCHITECTURE

The proposed architecture relies on allowing authorized communication for a chiplet. Figure 2 shows the overall architecture of enabling security for 3D ICs. First, we advocate creating a suitable firewall on-chip to filter and limit the data that is sent from a given chip in and out of that chip. Firewalls are a cornerstone of network security mechanisms and play a critical role in managing traffic flows between distinct networks, ensuring that unauthorized messages do not transgress from one network to another. They achieve this by employing rule-based configurations, primarily using two primary filtering techniques: blacklists and whitelists. Typically, blacklists are lists of IP addresses, domains, or specific protocols deemed untrustworthy or harmful, thereby preventing any inbound or outbound traffic associated with these entities [6]. On the contrary, whitelists operate on the principle of "deny all, except" by only allowing specified, trusted entities to send or receive messages, effectively blocking all others by default. By combining both methods, firewalls can offer a comprehensive, layered protection mechanism against a variety of threats, from malicious attacks to unsolicited traffic [14].

The physical layer (PHY) of the router, typically resides in the chiplet, uses a protocol stack, e.g., widely accepted UCIe [18], that receives flits from the link layer. The header flit, the first flit to start a D2D communication, holds information about this packet's route, such as the source and destination addresses, and sets up the routing behavior for all subsequent flits. We propose to implement the whitelist on the network I/O on the path to the chip-to-chip

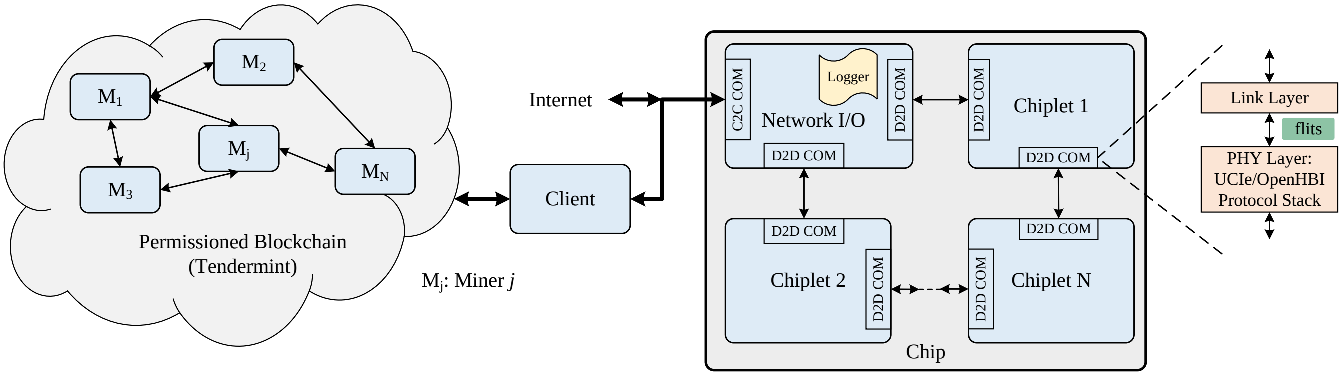

Figure 2: An abstract view of the proposed solution for securing 3D ICs.

communication. The whitelist is implemented as a set of allowed source-destination pairs. Only messages from white-listed sources (typically, these would correspond to chiplets from trusted sources) being sent to the corresponding white-listed destinations (these would need to be determined in an application-specific manner) will be allowed out of the chip. We further propose to add an on-chip logger to the network I/O. Any time there is a message that fails the white-list (i.e., sent with an unauthorized source-destination pair in the header), it generates an entry in the logger. We assume the logger has sufficient memory resources to store some number of messages that failed the white-list. The logger may have a local counter that is used to help with time-stamping. In case more messages are logged than one can fit in the logger, the additional messages may either overwrite older messages (i.e., implementing a type of circular buffer) or drop the newer messages.

Each entry in the whitelist specifies a unique combination of source chiplet address and destination chiplet address, ensuring that only verified and intended communications traverse the network. There is a tradeoff in the size of the white-list – the larger that it is, the higher the chance that some unauthorized activity takes place, as it effectively increases the attack surface for an adversary. However, a whitelist that is too short might be too restrictive and negatively affect legitimate uses of the hardware. The management of this whitelist will need to be embedded within the network's administrative framework, likely situated in a centralized security module within the chiplet architecture. This module will allow an authorized administrator to update the whitelist, incorporating changes based on ongoing security assessments and alterations in network or hardware configuration. The updates might be automated through scripts that process security updates or manually through network administrators' inputs.

We propose to use blockchain technology to capture the state of an on-chip logger at regular intervals. The traceability of the logger states for a chip can be ensured using a unique one-time programmable device ID, commonly known as an electronic chip ID or ECID [9]. One can use the same blockchain infrastructure for device traceability as well so that we can track the parts with their design, manufacturing, and distribution information [7, 22]. We envision the blockchain used to be a permissioned blockchain customized for this use case (for example, using Tendermint [4] or Hyperledger Fabric [1]), although it may also be of interest to explore the possibility of developing the system as a privacy-sensitive smart contract on a suitably capable public blockchain. Note that the rate at which logger-generated messages are sent to blockchain is relatively small compared to the capacity of the blockchain protocol. Compression or lossy admission-control approaches could be used to reduce the offered load to the blockchain if needed.

A lightweight blockchain client would run on the system, taking the data from the logger and publishing it securely over the Internet, possibly through a secure virtual private network, to one or more of the peer-to-peer servers that act as the blockchain's validator nodes. Each transaction posted to the chain would follow a consistent message format that also contains a global time-stamp, so that logger messages from different chiplets or chips can be correlated as needed for forensics. Data from multiple logger events may be batched, either as a fixed number of events or once per specified interval, into a single transaction. In future-proofing the blockchain-based system, emphasis is placed on scalability, adaptability to new technologies, and integration of advanced cryptographic methods. The architecture is modular, allowing easy updates to accommodate new blockchain protocols and encryption algorithms, ensuring resilience against evolving security threats. This adaptability is crucial for managing increasing data volumes from loggers without sacrificing performance. The cost-benefit analysis reveals that while initial investments include software development, infrastructure deployment, and human resources to manage the system, the long-term benefits—enhanced security, traceability, compliance, and reduced risks of counterfeit chips justify these costs. Over time, the system's contribution to operational efficiency and reduced security risks is expected to outweigh the initial setup expenses, making it a sustainable solution for secure on-chip communications.

The secure and effective functioning of the on-chip logger involves a multi-step process. Firstly, the messages generated by the on-chip logger must undergo digital signing using a private key associated with the chip. Ensuring the utmost security of the system necessitates careful handling of the secret key, limiting its accessibility exclusively to the trusted network I/O module. Robust measures must be in place to prevent any unauthorized access from other modules within the system. To fortify the confidentiality of the secret key, it should be securely programmed into a tamper-proof memory, impervious to manipulation or unauthorized retrieval.

This tamper-proof memory serves as an additional layer of protection against potential security breaches. Simultaneously, storing the secret key in non-volatile memory ensures its persistence even in the absence of power, enhancing reliability and facilitating seamless retrieval when necessary. By implementing these dual layers of security measures, we establish a robust foundation for safeguarding the confidentiality of the secret key, contributing significantly to the overall integrity and resilience of the system. Following this, the digitally signed messages are transmitted over the internet to one or more servers associated with the relevant blockchain.

Ensuring that the messages from the on-chip logger reach the blockchain will require careful hardware design. We propose incorporating a dedicated network interface card of the overall architecture. This specialized component plays a dual role, serving as a hardware blockchain client while effectively managing the digital signature process. Operating seamlessly as a liaison between the on-chip logger and the blockchain servers, this dedicated card ensures a swift and secure exchange of digitally signed messages over the network. Moreover, this card can effectively handle the reception of messages from trusted loggers dispersed across various chips within the system. This strategic feature not only streamlines communication but also enhances the system's ability to gather data from multiple sources within the network. By providing this dual functionality, this card acts as a centralized hub for managing blockchain interactions and facilitating efficient communication between the on-chip loggers and the broader blockchain network. One can also use a local system (such as a laptop/desktop) that runs either a server node on the blockchain or has a secure client that can communicate with one or more server nodes on the blockchain. The data from the logger will be read by software running in a trusted manner and used to generate a message that is digitally signed and submitted to the blockchain from the local node.

The overall whitelisting and validation process can be summarized as follows:

● *Step 1: Violation Occurance:* A violation occurs within a network inside of a chip consisting of many chiplets as shown in Figure 2. Specifically, when a chiplet *i* tries to transmit a packet beyond the chip boundaries, utilizing an invalid source-destination pair, the system detects a breach. The communication protocol stipulates that only whitelisted chiplets are authorized to engage in external communications. However, chiplet *i* lacks such permissions, possibly attributable to factors such as being manufactured in an untrusted environment. Consequently, this attempt is deemed a violation of the established network policies.

● *Step 2: Violation Logging:* In the event of a violation, it becomes imperative to capture the occurrence, even if the chiplet's attempt to communicate externally proves unsuccessful, for subsequent forensic analysis. Our proposed methodology involves recording crucial details, including the chiplet ID, destination address, and timestamp associated with the violation. Subsequently, this information is digitally signed using the chip's secret key, and the resulting signature is securely stored alongside the aforementioned data. Note that access to the logger state is restricted solely to authorized entities, ensuring confidentiality. Moreover, stringent controls are imposed on updates to prevent any malicious attempt to delete or manipulate records of the violation by potential adversaries.

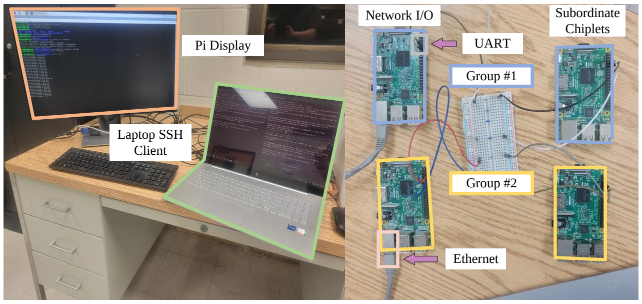

Figure 3: Experimental Setup for implementing whitelisting, where Raspberry Pis are modeled as chiplets.

● *Step 3: Logger State Collection:* The desktop/server orchestrating the blockchain client maintains regular communication intervals with a chip, executing periodic exchanges (e.g., every ten or fifteen minutes). A compact buffer is incorporated within the chip to store the logger state temporarily. In the event that the buffer reaches full capacity, a proactive mechanism is implemented. The chip autonomously triggers a request to the server, prompting the upload of the logger state.

● *Step 4: Overall Logger States Collection:* Despite the inherent diversity in resources and functionality among the various chips within the network—considering complex systems like smart grids—it is crucial to highlight that they share a common infrastructure. This infrastructure comprises multiple chiplets and a logger, as depicted in Figure 2, facilitating seamless chip-to-chip communications. All loggers in the network - every logger on every chip - will record their states in a similar fashion at the time interval mentioned in *Step 3*. Note that all logger entries are digitally signed.

● *Step 5: Blockchain Entry:* The desktop or server hosting the blockchain client aggregates all the digitally signed transaction logs it has acquired from different chips. This consolidated set of logs is then appended to the blockchain, ensuring a tamper-proof record of the transactions. Once they are in the blockchain ledger, this data becomes a valuable resource for future forensics, enabling the retrospective analysis and verification of communication events and potential security breaches within the system.

3 IMPLEMENTATION DETAILS

To demonstrate the effectiveness of our proposed approach, we have implemented the whitelisting strategy on a network of 2 groups of Raspberry Pi 3 devices acting as chiplets. The Pi 3s comprising one SiP equivalent are connected physically by UART, and the Pi 3s acting as Network I/O chiplets are additionally connected outwardly by Ethernet, shown in Figure 3. Communications between chiplet models are conducted by in-house C programs. We opted to utilize a UART-based communication environment. UART facilitates straightforward serial communication, which is ideal for debugging and iterative testing without the overhead associated with setting up a UCIe environment. While UCIe is quickly becoming a widely adopted chiplet communication interface, offering efficiency, scalability, multi-protocol support (PCIe, CXL), and standardization for multi-chip architectures [18], leveraging UART allowed us to focus on prototyping and validation, ensuring a successful proof-of-concept.

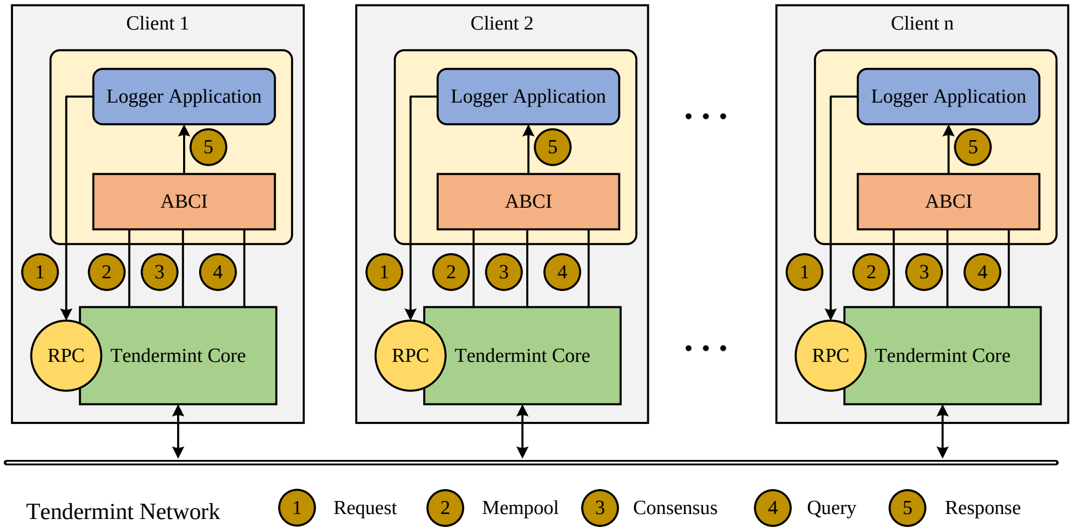

Figure 4: Tendermint implementation for logging runtime violations occurring during an attack.

The communication protocol among Pis operates as follows: messages transmitted from chiplets undergo deserialization and conversion into flattened messages. Subsequently, the messages undergo validation, where the header flits, containing the origin and destination information, are compared against a predefined whitelist. This whitelist comprises paired source and destination addresses, specifying allowed communications. If a message satisfies the whitelist criteria, it proceeds to the designated Network I/O interface for Ethernet. There, it undergoes reserialization before transmission over the wired Ethernet connection.

Figure 4 demonstrates the overall blockchain framework that enables the detection of run-time attacks originating from untrusted chiplets. Tendermint is a blockchain software for securely and consistently replicating an application on multiple machines [4]. At its core, it is a Byzantine Fault Tolerant (BFT) state machine replication, and it can be used to create and manage a blockchain network. It is designed for flexibility and modularity by its Tendermint Core consensus mechanism and Application Blockchain Interface (ABCI). The ABCI facilitates communication between the blockchain and the application's operational logic. This modularity is crucial in the context of global adoption, as it allows the application to process specific transactions related to security events without interfering with the underlying blockchain dynamics. Clients play a pivotal role in the blockchain framework. They are responsible for several key functions and act as a bridge between the on-chip loggers situated within a chip's network I/O module and the blockchain. In particular, they collect, verify, and package the logged data from the chiplets, which include detailed records of communication activities and security policy violations. Once this data is prepared, the client then securely transmits it to the blockchain network for validation and recording. Clients ensure that the data adheres to the expected format and contains valid signatures before it's sent to the Tendermint network.

The secure recording process of logs begins with the collection of data from on-chip loggers positioned within the network I/O module of a chip. This logger is tasked with collecting logs from various chiplets integrated within the chip. It records instances of unauthorized communication attempts or breaches against the established whitelisting policy. The logger captures essential data such as the source and destination of the attempted communication, the timestamp of the event, and the type of policy violation. Each chip contributes to this security measure by appending its digital signature to the log data it generates, ensuring authenticity and integrity. This signed log data is securely encrypted by the logger and then transmitted to the client. The client, in turn, is responsible for relaying this data to the Tendermint blockchain network, where it undergoes further processing and is finally integrated into the blockchain ledger.

The integration of Tendermint Core with the application logic responsible for processing and verifying data from the on-chip logger is facilitated through three critical components: consensus, mempool, and query. The mempool in Tendermint acts as a temporary buffer for transactions before they are processed by the consensus engine. Our security application allows the system to efficiently manage and prioritize the influx of valid logging data from the on-chip logger, ensuring that the blockchain can handle high volumes of violation data without any bottleneck scenario. Next, Tendermint's consensus mechanism ensures that all transactions representing logged security events from the on-chip logger are validated and agreed upon by all participating validator nodes in the network before being committed to the blockchain ledger. This BFT consensus mechanism is pivotal for maintaining the integrity and tamper-resistance of the ledger, ensuring that only verified events are recorded. Through ABCI, the application logic can query the blockchain state, enabling real-time monitoring and forensic analysis of the logged security events. This capability is crucial for identifying patterns of unauthorized communication attempts across chiplets, facilitating timely interventions, and enhancing the overall security of 2.5D/3D ICs. The Tendermint Core provides the foundational blockchain functionality, including the consensus engine, networking, and blockchain state management. Our security system leverages this Tendermint core to ensure a secure, consistent, and tamper-evident ledger of chiplet communication events that violate the whitelist policy.

Transactions originating from the on-chip loggers are encoded into a JSON format, providing a standardized and suitable medium for encapsulating the metadata associated with each blockchain transaction. The JSON-formatted data is then converted into a byte representation and subsequently encoded as a hexadecimal string. This hexadecimal encoding serves as a blockchain-compatible format facilitating the digital signing of the transaction. Digital signatures are appended to the transactions using private keys that are securely managed and stored within the chip infrastructure. Upon successful encoding and digital signing, the transactions are submitted to the blockchain network via an HTTP request to the Tendermint node's Remote Procedure Calls (RPC) interface [5]. This submission leverages the unique transaction format and incorporates the hexadecimal-encoded data as a parameter in the request URL, ensuring that the transaction is appropriately broadcasted to the network for consensus processing. Once a transaction is received for processing, it undergoes a decoding step where the hexadecimal-encoded data is converted back into its original JSON format before being admitted into the blockchain. This preliminary decoding is essential for validating and processing the transaction through the consensus mechanism. Upon successful validation, the transaction is added to the blockchain, becoming a permanent and immutable record within the ledger. This procedure is critical for the forensic analysis and audit of security events within the 2.5D/3D IC ecosystem. The immutable nature of these records ensures that stakeholders can reliably query and examine historical data, providing invaluable insights into unauthorized communications and potential security breaches. This streamlined process of decoding followed by blockchain integration ensures the utility of the security framework in monitoring and safeguarding communications across multiple chiplets within and between chips.

4 CONCLUSION

Ensuring security in 2.5D/3D ICs encounters significant challenges due to the inherent lack of trust among entities within the semiconductor supply chain. The fabrication of chiplets at untrusted locations introduces the potential for tampering, leading to the insertion of malicious circuits capable of compromising the confidentiality of sensitive information. This paper introduced a novel conceptual approach aimed at mitigating these risks by constraining the communication capabilities of untrusted chiplets. We implemented the proposed whitelisting approach using Raspberry Pis and Tendermint blockchain framework. Additionally, our strategy involves the deployment of a logger to monitor and capture any violations of communication rules during chiplet-to-chiplet interactions in 2.5D/3D ICs. In the event of a detected breach, the logger's state can be securely uploaded to an immutable blockchain ledger, providing a robust forensic trail for further analysis and identification of potential attacks.

In the future, we plan to explore various types of violations and perform an in-depth analysis of the threats while considering the dynamic risk profile. Moreover, we will work on refining our framework's scalability by enhancing the logger efficiency and conducting thorough analyses on resource requirements, including memory, processing power, and energy consumption, across various network topologies and chiplet configurations. Additionally, as adversarial entities become more and more capable, the whitelisting approach proposed here may be insufficient for preventing more sophisticated threats, and an advanced whitelisting implementation needs to be developed.

ACKNOWLEDGMENTS

This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-23-1-0312. Any opinions, findings, and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Air Force.

REFERENCES

[1] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference*. 1–15.

[2] Bloomberg. 2018. The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies.

[3] Bloomberg. 2021. The Long Hack: How China Exploited a U.S. Tech Supplier.

[4] Ethan Buchman. 2016. *Tendermint: Byzantine fault tolerance in the age of blockchains*. Ph. D. Dissertation. University of Guelph.

[5] Daniel Cason, Enrique Fynn, Nenad Milosevic, Zarko Milosevic, Ethan Buchman, and Fernando Pedone. 2021. The design, architecture and performance of the tendermint blockchain network. In *2021 40th International Symposium on Reliable Distributed Systems (SRDS)*. IEEE, 23–33.

[6] W. R. Cheswick, S. M. Bellovin, and A. D. Rubin. 2003. *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Professional.

[7] Pinchen Cui, Julie Dixon, Ujjwal Guin, and Daniel DiMase. 2019. A blockchain-based framework for supply chain provenance. *IEEE Access* 7 (2019), 157113–157125.

[8] Ujjwal Guin, Ke Huang, Daniel DiMase, John M Carulli, Mohammad Tehranipoor, and Yiorgos Makris. 2014. Counterfeit Integrated Circuits: A Rising Threat in the Global Semiconductor Supply Chain. *Proc. IEEE* 102, 8 (2014), 1207–1228.

[9] IEEE. [n. d.]. ECID - Electronic Chip ID. https://grouper.ieee.org/groups/1149/1/ECID_Electronic_Chip_ID.html

[10] Ayush Jain, Ziqi Zhou, and Ujjwal Guin. 2021. Survey of Recent Developments for Hardware Trojan Detection. In *IEEE International Symposium on Circuits and Systems (ISCAS)*. 1–5.

[11] Siroos Madani, Mohammad R Madani, Indira Kalyan Dutta, Yamini Joshi, and Magdy Bayoumi. 2018. A hardware obfuscation technique for manufacturing a secure 3D IC. In *IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 318–323.

[12] Open Compute Project. 2021. OpenHBI Specification Version 1.0. https://www.opencompute.org/documents/odsa-openhbi-v1-0-spec-rc-final-1-pdf

[13] Samsung Electronics. 2019. Samsung Electronics Develops Industry's First 12-Layer 3D-TSV Chip Packaging Technology.

[14] W. Stallings and L. Brown. 2017. *Computer Security: Principles and Practice*. Pearson.

[15] Taiwan Semiconductor Manufacturing Company. [n. d.]. TSMC 3DFabric. https://3dfabric.tsmc.com

[16] Taiwan Semiconductor Manufacturing Company. 2020. Introducing TSMC 3DFabric: TSMC's Family of 3D Silicon Stacking, Advanced Packaging Technologies and Services. https://www.tsmc.com/english/news-events/blog-article-20200803

[17] M. Tehranipoor, U. Guin, and D. Forte. 2015. *Counterfeit Integrated Circuits: Detection and Avoidance*. Springer International Publishing.

[18] Universal Chiplet Interconnect Express. [n. d.]. UCIe. https://www.uciexpress.org/

[19] Nidish Vashistha, Md Latifur Rahman, Md Saad Ul Haque, Azim Uddin, Md Sami Ul Islam Sami, Amit Mazumder Shuo, Paul Calzada, Farimah Farahmandi, Navid Asadizanjani, Fahim Rahman, and Mark Tehranipoor. 2022. ToSHI-Towards Secure Heterogeneous Integration: Security Risks, Threat Assessment, and Assurance. *Cryptology ePrint Archive* (2022).

[20] Kan Xiao, Domenic Forte, Yier Jin, Ramesh Karri, Swarup Bhunia, and Mohammad Tehranipoor. 2016. Hardware trojans: Lessons learned after one decade of research. *ACM Transactions on Design Automation of Electronic Systems (TODAES)* 22, 1 (2016), 1–23.

[21] Y. Xie, C. Bao, C. Serafy, T. Lu, A. Srivastava, and M. Tehranipoor. 2016. Security and Vulnerability Implications of 3D ICs. *IEEE Transactions on Multi-Scale Computing Systems, vol. 2* (2016), 108–122.

[22] Yadi Zhong, Amaar Ebrahim, Ujjwal Guin, and Vivek Menon. 2023. A Modular Blockchain Framework for Enabling Supply Chain Provenance. In *IEEE Physical Assurance and Inspection of Electronics (PAINE)*. 1–7.