# Countering Botnet of Things using Blockchain-Based Authenticity Framework

**Pinchen Cui*** **and Ujjwal Guin†**
*Dept. of Computer Science and Software Engineering, Auburn University
†Dept. of Electrical and Computer Engineering, Auburn University

***Abstract*—The success and widespread use of Internet of Things (IoT) bring remarkable contributions and economic benefits in various fields. However, the increasing number of devices also raises security concerns. The prevalence of Botnet of Things (BoT) has been observed and it has been recently reported that the launched attacks affect multiple domains and have caused unacceptable losses. As majority of IoT devices are manufactured off-shore, ensuring their identity becomes one of the major challenges. Cloned devices, with backdoors for malicious purposes, can provide an undue advantage of the adversary to compromise a system even though proper security measures are in place. In this paper, we propose a novel blockchain-based framework to provide traceability of hardware. A unique identity for every IoT device is ensured using a physically unclonable function (PUF). The blockchain provides the verification of these devices by comparing these unique IDs. HyperLedger is selected to implement the blockchain-based framework, and its performance is being evaluated and analyzed.**

***Index Terms*—Internet of Things (IoT), Botnet, Physically Unclonable Functions (PUF), Hardware Security, Cloning, Blockchain, Device Identity**

## I. Introduction

Internet of Things (IoT) is one the most promising technologies which contributes to various fields and possesses a bright market prospect. It is reported that already $235 billions has been spent in the IoT market in 2017 and is predicted to grow to $520 billions in 2021 [1]. Those network enabled sensors and devices provide automation, convenience, and intelligence for a variety of services and operations. IoT technique is thus not only promising but also necessary. While the world observes the maturing of IoT, there is a dark side which needs to be considered as well. The large number of IoT devices are becoming new and vulnerable attack targets.

Most IoT devices are resource-constraint and are equipped with limited memory and computing resources, thus, the traditional security measures during the communication is not applicable or affordable in an IoT infrastructure [2], which incurs potential security risks. In addition, the manufacturing and distribution of IoT devices lack trust and regulation. The IoT supply chain is challenged by tampering, counterfeiting, and cloning [3]–[6]. As a result, an adversary could inject malicious codes into IoT devices via unprotected communication channel or utilize the backdoor in tampered or counterfeit devices to launch attacks.

One compromised IoT device seems to be negligible but the problem becomes severe when a cluster of compromised devices forms a malicious botnet, which is a network that consists of remote controlled "bot" devices. Botnets controlled by adversaries are always used as remote attack launch points. The IoT botnet based Distributed Denial of Service (DDoS) attack is an increasingly severe security problem. The first Mirai

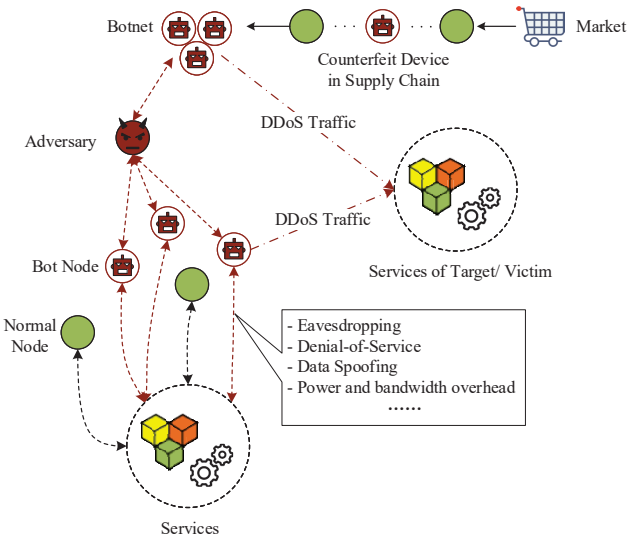


Figure 1: Threat model.

malware based IoT botnet DDoS attack launched in 2016 sent out 620 Gbps traffic to the victim and the later attack on service provider Dyn took down hundreds of web services for several hours (including Github, Twitter, Netflix, etc.) [7]. These DDoS attacks not only damaged the targeted services but also effected the IoT devices owners – the attack on Krebs costed the devices' owners approximately $320,000 on excess power and bandwidth consumption [8]. According to Nokia Threat Intelligence Report, 78% of malware activities in 2018 are driven by IoT botnets [9]. Even though there is no reported incidents of cloned botnets used by the adversaries, we believe that they could use these cloned devices for malicious purposes in the near future. Recently Bloomberg Businessweek reported that a tiny chip is being used to infiltrate 30 U.S. companies [10]. Therefore, the problem of Botnet of Things (BoT) must be prevented and solved.

Figure 1 describes the threat model where a botnel enters into a secure system through the untrusted supply chain. The cloned IoT devices in the supply chain may contain backdoor(s) or vulnerabilities that could be exploited by an adversary [5], [11], [12]. After the illegitimate devices have been purchased and deployed in IoT infrastructure, the adversary could transfer those devices into bots. As shown in the Figure 1, the nodes in color green stand for normal nodes, and the the nodes with a red bot inside represent the bot nodes. These bot nodes form a botnet which is remotely controlled by the adversary. This botnet can be used to launch DDoS attack onto a remote target/victim. Meanwhile, the botnet also threatens the services run by the

device owners. The bot nodes damage the local IoT infrastructure by performing eavesdropping, Denial-of-Service, data spoofing, and incurring additional power and bandwidth overhead.

### A. Contributions

This paper aims to provide a blockchain based solution against BoT by ensuring the authenticity of IoT devices in the supply chain. The proposed solution uses an SRAM based Physically Unclonable Function (PUF) [13], [14] to provide traceability and reliable identity for an IoT device. PUF uses inherently uncontrollable and unpredictable variations of the manufacturing process to produce random, unique, and unclonable bits. Since IoT edge devices have a small SRAM based memory and embedded processors, SRAM PUFs is an ideal option to generate device IDs with no additional cost or complexity.

We propose to use a permissioned blockchain to store the unique device identities (IDs) generated from the SRAM PUF. Blockchain is generally a distributed ledger system that provides additional security against tampering, more details are introduced in I-B. Once a IoT device ID is registered on the blockchain, the authenticity of IoT devices can be verified remotely and efficiently. Moreover, additional security information, such as firmware version and security updates, can be recorded and notified by the system as well. Therefore, distributors and device owners could use the framework to obtain all the needed security related information of the IoT devices. The major contributions of this paper summarized as follows:

- We propose a novel permissioned blockchain-based framework to provide authenticity for IoT devices. By using the SRAM PUF generated ID, an IoT device can be registered and protected by the proposed framework.
- We implement a prototype of proposed framework using the Hyperledger Fabric. We have also analyzed the performance of the prototype framework.
- We demonstrate how the proposed framework could counter the Botnet of Things problem, and also perform a security analysis of the framework.

### B. Blockchain and Related Works

The concept of blockchain was first introduced by Satoshi Nakamoto in the Bitcoin system, which was originally proposed to solve the double-spending problem [15]. Technically, blockchain is a peer-to-peer (P2P) [16] based distributed ledger system, which provides tamper-resist and transparent data and value exchange among untrusted entities without involving a third party. The key components of blockchain are transactions, blocks, and a consensus algorithm [17]. Notable consensus algorithms are Proof-of-Work (PoW) [15], Proof-of-Stake (PoS) [18], and Byzantine Fault Tolerant (BFT) [19]. Another crucial feature is the smart contract, which represents the scripts stored in blockchain. These scripts allow users to have general-purpose computations on the chain [20]. Smart contract is the enabler of data storage and data management in blockchain. Along with the prevalence and maturity of smart contract, blockchain could contribute to various application domains, such as voting systems, financial services, and supply chain management [21].

The properties and features of blockchain could contribute to the traceability, transparency, and reliability of the supply chain [22], [23]. Various blockchain based frameworks are proposed to refine the supply chain in the domains of agriculture, industry, and healthcare [11], [24]–[28]. However , there are still two issues which need to be taken into account: (i) ensuring the authenticity of parts circulating in supply chain requires a global unique and unclonable identity for each object. If the identity could be cloned and tampered with, then blockchain cannot not provide any additional security related to the authenticity of the identity. (ii) recording daily operations of supply chain on a public (permissionless) blockchain platform, such as Bitcoin and Ethereum, may cost a considerable transaction fee, and the intensive Proof-of-Work (PoW) mining also incurs additional resource overhead.

### C. Organization

The rest of the paper is organized as follows: we demonstrate the proposed blockchain-based framework in Section II. Section III describes the implementation of the framework. The performance evaluation of the framework is performed in Section IV. We provide a detailed analysis on proposed solution in Section V. Finally, we conclude the paper in Section VI.

## II. Proposed Blockchain-Based Framework

An IoT edge device can be identified using the fingerprint generated from an SRAM PUF. The ID generated from the PUF could be used as backbone of the authenticity framework, which is built upon a permissioned blockchain platform to eliminate the cost of transaction fees and overhead of PoW mining. A permissioned blockchain is formed by a group of known, verified, and trusted members in the supply chain. Hyperledger is a well-known permissioned blockchain platform with promised high efficiency. It excludes the transaction fee and uses non-resource intensive consensus algorithm [29].

The proposed IoT device authenticity framework is depicted in Figure 2. The procedures for registration, verification, and maintenance of security information are shown.

### A. Blockchain Service

This permissioned blockchain service can be created and maintained by either a group of authenticated IoT device manufacturers, or a trusted blockchain service provider. Note that, no matter how the blockchain is created, no one actually fully controls or owns the blockchain. As blockchain guarantees the decentralization, integrity, and transparency, even the creator of the blockchain service cannot modify the data with no traces.

Manufacturers are the participants of this authenticity framework, each of them needs to run one or multiple blockchain network nodes to perform blockchain operations. The underlying data storage and management capabilities of the service are provided by chaincode (smart contract) [29]. The chaincode needs to be installed on the nodes before it can be used. In addition, at least one of the nodes need to create and maintain an API, which is used by the off-chain users to query the data stored in blockchain.

### B. Registration of IoT Device

The procedure of storing IoT device identity into blockchain is described by the Step 1 and Step 2 in Figure 2. When a device identity needs to be stored into the blockchain, the manufacturer of the device needs to perform:

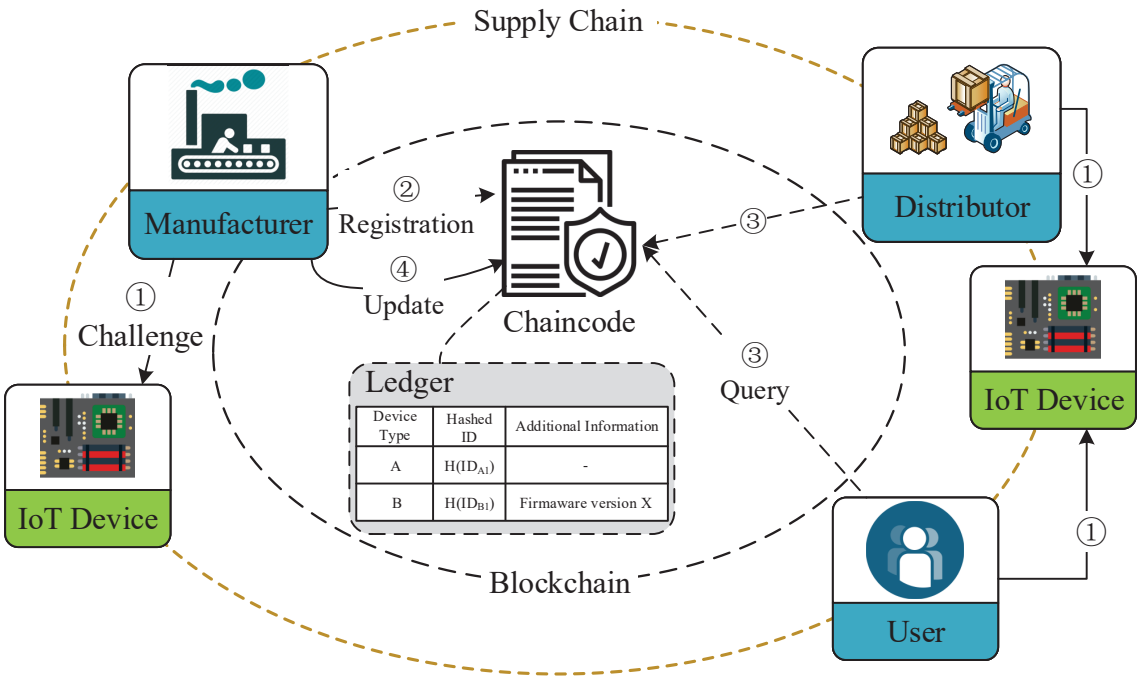


Figure 2: Proposed Blockchain based Authenticity Framework.

- *Step 1 - Challenge:* Sending a challenge to the PUF on this IoT device (e.g., Device $A_1$) to obtain its response. The response is the unique ID of this device (e.g., $ID_{A1}$)), and then the hash of this ID is computed (e.g., $HID_{A1}$).
- *Step 2 - Registration:* Sending out a transaction to invoke the chaincode (smart contract) in the blockchain with the data payload: device type and hashed device ID. Once the transaction is received and confirmed by the blockchain, an entry contains the device type and hashed device ID is created in the blockchain ledger for this device.

Depending on the implementation of the chaincode, specific manufacturers could only register certain device types. Available device types in the blockchain are maintained separately, which is introduced in Section III. Moreover, a manufacturer could register one or multiple devices in one transaction. Once a device is registered in blockchain, all the succeeding owners of this device in supply chain could easily and remotely verify its authenticity.

### C. Verification of IoT Device

In order to perform the verification of an IoT device, the owner of this device (distributor or user) needs to accomplish following operations:

- It is necessary to provide a challenge to the device (Step 1, which is demonstrated in Section II-B).
- *Step 3 - Query:* The verifier needs to send out a HTTP [30] query to the API of the blockchain with the hashed device ID as data payload. If this device is a legitimate device that has been registered in the framework, the query response contains corresponding entry data, thus the verification succeeds. If this device is an illegitimate device (e.g. counterfeit, tampered, or cloned), the API should return no response or an error response, thus the illegitimate device can be detected.

The query to the blockchain does not alter the data stored in blockchain, so there is no need for device owner to join blockchain network and maintain blockchain nodes. By using this framework, distributors and users could protect and authenticate their IoT devices without knowing detailed and advanced blockchain architecture and knowledge.

### D. Maintenance of Additional Security Information

The optional and additional security information of IoT devices could be uploaded into this framework as well. Although the authenticity is guaranteed by the framework, secure is not fully equivalent to legitimate. For example, a legitimate Huawei router may still have security flaws (CVE-2017-17215) [31]. It is the responsibility of the manufacturers to announce and notify the security updates to device owners. The maintenance of additional security information can be achieved by using Step 4 in Figure 2. Manufacturer of a specific type of device could send a transaction to update or upload additional security notes to this device type. Any query after the completed update would respond with entry data which includes additional security information. Depending on the implementation of chaincode, this information could be formed by several optional fields (e.g. Firmware version, product generations, vulnerability statistics, and etc.), or just contains plain sentences (strings). *Note that, a manufacturer could only update its corresponding device types, the operations are regulated by the blockchain policy profiles.*

## III. Implementation

We implemented a proof-of-concept prototype by using Hyperledger Fabric [32] and Hyperledger Composer [33]. Composer is a tool provided by Hyperledger community for generating Hyperledger blockchain network models, which is generally comprised of Assets, Participants, and Transactions. Assets are the data and

values stored in blockchain, they could be created and transferred by the participants. Participants are the actors and entities in this network, who can process and initiate transactions. Transactions are participants triggered actions that effect assets. The creation and alteration of assets and participants are carried out by transactions. These three basic elements are defined in a Composer network model file. Moreover, Composer defines and stores the chaincode (the smart contract in Hyperledger) in a logic script. This script mainly defines the transaction processing functions, those functions are triggered whenever a transaction is received.

In our network model, we define two assets (*Device* and *DeviceType*) to store the IoT device data entries. The data structure of the stored entries is described below.

```
Struct Device :
    address DeviceType;
    string DeviceID;
    address Manufacturer;
Struct DeviceType :
    string TypeName;
    //optional additional information fields
```

A device entry contains multiple attributes, such as device type, device ID, manufacturer, and additional security information. The device type is defined and limited by another asset type in the network model to ensure only specific device types could be registered. The $Manufacturer$ attribute contains an address (reference) of an existing participant. This means a device data entry is associated with a device type entry and a participant.

To register a device and create a device entry in the system, the manufacturer needs to send a transaction that includes the device type and device ID. This transaction is then received and processed by Hyperledger. Algorithm 1 describes the procedure of device registration. If the input device ID does not exist in blockchain, it will return an error. If this ID exists, then a new device asset is created and added into Hyperledger asset registry (registries are internally maintained by Hyperledger engine, and processing of asset creation transactions relies on built-in functions of Hyperledger).

**Algorithm 1:** Device Registration

**Input :** Device Type (T), Device ID (I)
**if** *Device ID I exists* **then**
    return
**end**
Set $Device.DeviceType = T$;
Set $Device.DeviceID = I$;
Set $Device.Manufacturer = CurrentParticipant$;
Add $Device$ into AssetRegistry;

The update and maintenance of the additional information attribute of device data entries is carried out by another transaction, therefore we need a different transaction processing function. Algorithm 2 demonstrates the processing function of information maintenance transactions. The Manufacturer could update the additional information of a particular device type. Since each of the device entry is associated with a device type asset, once the update is completed, all the device entries associated with this type are effected as well.

Verification of IoT devices relies on the query functions provided by Hyperledger Composer. By defining the functions in a query configuration file, one could query the data stored in Hyperledger. As shown in Algorithm 3, the underlying mechanism of query is in a SQL fashion. Retrieving both device data and device type data (that includes additional information) actually takes two queries, this can be achieved and customized in the exposed API.

**Algorithm 2:** Additional Information Update

**Input :** Device Type Name (N), Information Content (C)
**if** *Device Type T not exists* **then**
    return
**end**
Get $DeviceType$ with $TypeName = N$ from AssetRegistry;
Set $DeviceType.AdditionalInformation = C$;
Update $DeviceType$ in AssetRegistry;

**Algorithm 3:** Device Verification

**Input :** Hash of the device IDs, $HIDs$
$QueryResult$ = SELECT *namespace.authenticity.device* WHERE (*DeviceID = HID*);
Set $T = QueryResult.DeviceType$;
$QueryResult$ = SELECT *namespace.authenticity.DeviceType* WHERE (*DeviceType = T*) + $QueryResult$ ;
Print $QueryResult$

## IV. Performance Evaluation

We evaluated and tested our prototype framework using Hyperledger Caliper [34], an open source Hyperledger benchmark tool which supports performance measurement for multiple blockchains. An Ubuntu 16.04 virtual machine with 8GB RAM is used to setup the testing environment. We built the environment with Hyperledger Composer version 0.20 and Fabric version 1.2. We modified the basic-sample-network configuration file of Caliper benchmark to match our authenticity network design. The device registration and information update transactions are tested in a 3-organization-1-peer network (1 peer for each organization). This network is running with one orderer in "Solo" mode.

The performance is tested with different transaction rates and block sizes, the results of throughput, latency, memory usage, and CPU usage are depicted in Table I. Note that, changing the block size does not obviously effect CPU and memory usage, thus Table I only shows the result of using block size 10 (10 transactions per block). The CPU and memory usage of the peer nodes are calculated by average usages of 3 organization's peers. The results indicate that the memory usages of peer and orderer node are not significantly effected by the increasing transaction rate. On the other hand, CPU usage of peer nodes increases dramatically while transaction rate growing from 2 transaction per second (tps) to 8 tps, but the CPU usage maintains stable after 8 tps. For the throughput perspective, as shown in Figure 4, the throughput is peaked at 15.1 tps with using block size 30. Similarly, with increasing the transaction rate to 24 tps, the best latency performance is still achieved by using block size 30 (3.14s, see Figure 3).

According to the design of Hyperledger Fabric, it should have a high throughput that approximately reaches 3500 tps [29].

Table I: Performance Evaluation - Block Size 10

| Transaction Rate | Throughput | Latency | Memory (Avg. Peer) | CPU (Avg. Peer) | Memory (Avg. Orderer) | CPU (Avg. Orderer) |
|---|---|---|---|---|---|---|
| 2 tps | 2 tps | 0.48s | 259.8MB | 242.79% | 14.3MB | 47.89% |
| 4 tps | 4 tps | 0.41s | 264.2MB | 321.58% | 14.3MB | 66.0% |
| 8 tps | 7.8 tps | 0.54s | 267.8MB | 488.53% | 14.1MB | 109.45% |
| 12 tps | 10.8 tps | 1.37s | 271.9MB | 513.1% | 13.9MB | 99.57% |
| 16 tps | 11.9 tps | 2.60s | 259.6MB | 521.5% | 14.1MB | 100.47% |
| 24 tps | 12.6 tps | 3.91s | 243.4MB | 549.1% | 14.3MB | 99.51% |

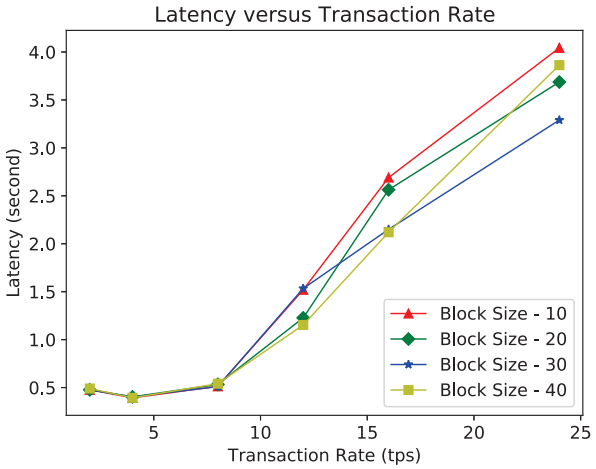


Figure 3: Latency versus Transaction Rate

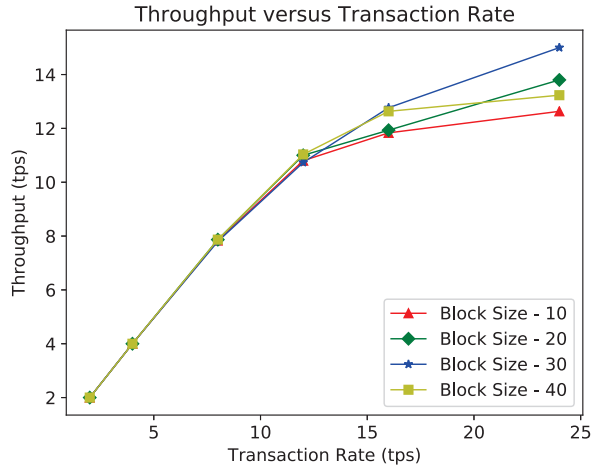


Figure 4: Throughput versus Transaction Rate

Hyperledger significantly outperforms other blockchains, for example, Bitcoin system can process around 7 transactions per second and Ethereum can process 20 transactions. The reason of our prototype has a throughput bottleneck at 15 tps is, our prototype is running with only one orderer with "Solo" mode. "Solo" mode is only used for experimental scenarios, and "Kafka" mode is for real world production environment. Therefore, we are planning to investigate and evaluate the performance of "Kafka" consensus with multiple orderers.

## V. Analysis and Discussion

### A. Concerns of Blockchain based Solutions

The necessity and feasibility of blockchain based solution seems to be arguable. The problems and concerns can be summarized to several categories [17], [35], [36]: Exposure of Data, Implementation Cost, and Performance Bottlenecks. However, our proposed framework does not fall into the questioned areas. The reasons are explained as follows:

1) *Exposure of Data:* The on-chain data privacy is still a challenging problem but the proposed framework dose not expose any sensitive data in blockchain. The stored hashed device IDs in the system are visible, but a known hashed ID does lead to any type of damage to this system or actual IoT devices as long as the ID is unique and hash function is secure. Therefore the known ID cannot be used for cloning).
2) *Implementation Cost:* The cost problems are referred to data redundancy and resource intensive computing. The drawbacks of storing unnecessary data and waste of storage space in blockchain system cannot be eliminated, because the decentralization of blockchain is built upon collaborative recording. However, our proposed framework only stores hashed IDs by default, the storage cost per data entry is extremely low. Moreover, Hyperledger does not use resource intensive consensus algorithm.
3) *Performance Bottleneck:* Throughput and latency bottlenecks severely constrain the use of blockchain systems. However, as mentioned in Section IV, Hyperledger is designed to have a higher performance threshold. One may ask whether 3500 tps is sufficient, however, the fact is Visa network only process around 1700 transactions per second [37]. For an specific application perspective, Hyperledger is efficient enough (although some scenarios may require high speed and high frequency of data transmission, the optimization of blockchain is out of the scope of this paper).

### B. Supply Chain Security and Botnet of Things

Recently, supply chain security problem is receiving increasing attention. The global cost of counterfeiting is at 1.8 trillion and increasing [38], and the hardware hack found by Bloomberg [39] warns people that the hardware is not always trustworthy. It is obvious that counterfeit and clone devices may incur infection of botnets. Verification of device authenticity is absolutely necessary, especially when the device is deployed in crucial infrastructure.

Our proposed framework could enhance supply chain security against potential botnet risk with minimum overhead. The implementation of PUF requires SRAM, which is generally present in all IoT devices. The verification procedure requires a query in the blockchain, it could be carried out at any

location and any time without direct interaction with original manufacturer or any third party.

### C. Security Beyond Supply Chain

Supply chain security and hardware security are not the only factors of botnet problem. Malware, firmware flaws, and various other potential threats need to be detected and solved. According to a research talk in HITBSecConf 2018 [40], backdoors exist in approximately 1%-2% of 8700 unique IoT products' firmware. Since IoT devices always have a long lifetime after their deployments, the firmware and services running on the devices need updates along with evolving security requirements.

Using blockchain to remotely verify and update the firmware and services on the embedded devices is promising and practical [41], [42]. The proposed framework could be used to integrate with other security solutions. Our framework provides a direct channel to the device owner, service provider, and manufacturers, which could help to solve other security problems beyond supply chain.

## VI. Conclusion

We presented a novel blockchain based framework to provide authenticity for IoT devices in the supply chain. This framework helps to protect against potential botnet threats. Once a device is registered in this framework, the future device owner could verify the authenticity with additional security information of this device in a remote and efficient manner. All the tampered, counterfeit and cloned devices will be detected by using this framework. We also implemented and evaluated this proposed framework using Hyperledger Fabric and Hyperledger Caliper.

## ACKNOWLEDGEMENT

This work was supported by the National Science Foundation under grant number CNS-1755733.

## References

[1] IoT Market Predicted To Double By 2021, Reaching $520B, https://www.forbes.com/sites/louiscolumbus/2018/08/16/iot-market-predicted-to-double-by-2021-reaching-520b/#c33643c1f948.

[2] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security Privacy*, Jan 2015.

[3] U. Guin, K. Huang, D. DiMase, J. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, pp. 1207–1228, 2014.

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

[5] M. M. Tehranipoor, U. Guin, and S. Bhunia, "Invasion of the hardware snatchers," *IEEE Spectrum*, vol. 54, no. 5, pp. 36–41, 2017.

[6] U. Guin, D. DiMase, and M. Tehranipoor, "Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead," *Journal of Electronic Testing*, vol. 30, no. 1, pp. 9–23, 2014.

[7] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, 2017.

[8] "Study: Attack on krebsonsecurity cost iot device owners $323k," https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot-device-owners-323k/.

[9] "78% of malware activity in 2018 driven by iot botnets, nokia finds," https://onestore.nokia.com/asset/205835?did=d0000000016z&utm_-campaign=threatintelligence18&utm_source=marketo&utm_-medium=LandingPage&utm_content=report&utm_term=awareness.

[10] J. Robertson and M. Riley, "The big hack: How china used a tiny chip to infiltrate u.s. companies," 2018.

[12] U. Guin, A. Singh, M. Alam, J. Canedo, and A. Skjellum, "A Secure Low-Cost Edge Device Authentication Scheme for the Internet of Things," in *International Conference on VLSI Design*, 2018.

[11] U. Guin, P. Cui, and A. Skjellum, "Ensuring proof-of-authenticity of iot edge devices using blockchain technology," *IEEE International Conference on Blockchain*, 2018.

[13] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2009.

[14] W. Wang, A. Singh, U. Guin, and A. Chatterjee, "Exploiting power supply ramp rate for calibrating cell strength in SRAM PUFs," in *IEEE Latin-American Test Symposium*, 2018.

[15] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system, http://bitcoin.org/bitcoin.pdf," 2008.

[16] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," in *Peer-to-Peer Computing, 2001. Proceedings. First International Conference on*. IEEE, 2001.

[17] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Work Pap.–2016*, 2016.

[18] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake," *self-published paper, August*, vol. 19, 2012.

[19] M. O. T. de Castro, "Practical byzantine fault tolerance," in *OSDI*, 1999.

[20] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[21] F. X. Olleros, M. Zhegu, F. X. Olleros, and M. Zhegu, *11 Blockchain technology: principles and applications*, 2016.

[22] M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman *et al.*, "Blockchain technology: Beyond bitcoin," *Applied Innovation*, 2016.

[23] M. Pilkington, "11 blockchain technology: principles and applications," *Research handbook on digital transformations*, 2016.

[24] K. Toyoda, P. T. Mathiopoulos, I. Sasase, and T. Ohtsuki, "A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain," *IEEE Access*, 2017.

[25] F. Tian, "A supply chain traceability system for food safety based on haccp, blockchain & internet of things," in *2017 International Conference on Service Systems and Service Management*. IEEE, 2017.

[26] H. M. Kim and M. Laskowski, "Toward an ontology-driven blockchain design for supply-chain provenance," *Intelligent Systems in Accounting, Finance and Management*, 2018.

[27] Q. Lu and X. Xu, "Adaptable blockchain-based systems: A case study for product traceability," *IEEE Software*, 2017.

[28] K. A. Clauson, E. A. Breeden, C. Davidson, and T. K. Mackey, "Leveraging blockchain technology to enhance supply chain management in healthcare," *Blockchain in Healthcare Today*, 2018.

[29] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*. ACM, 2018, p. 30.

[30] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee, "Hypertext transfer protocol–http/1.1," 1999.

[31] Huawei HG532 with some customized versions has a remote code execution vulnerability, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE201717215.

[32] HyperLedger Fabric, https://github.com/hyperledger/fabric#releases.

[33] HyperLedger Composer, https://github.com/hyperledger/composer.

[34] Hyperledger Caliper,https://github.com/hyperledger/caliper.

[35] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data*, 2017.

[36] M. Amine Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges," *ArXiv e-prints*, Jun. 2018.

[37] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "Blockchain - the gateway to trust-free cryptographic transactions," in *ECIS*, 2016.

[38] J. M. Wilson and R. Kinghorn, "The global risk of product counterfeiting: facilitators of the criminal opportunity," *Center for Anti-Counterfeiting and Product Protection Backgrounder Series*, 2015.

[39] J. Robertson and M. Riley, "The big hack: How china used a tiny chip to infiltrate u.s. companies," 2018.

[40] Backdoors exist in 0.9 - 2.1% of 8,758 unique IoT products, https://conference.hitb.org/hitbsecconf2018dxb/materials/D1T1%20-%20Hunting%20for%20Backdoors%20in%20IoT%20Firmware%20at%20Unprecedented%20Scale%20-%20John%20Toterhi.pdf.

[41] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, 2017.

[42] A. Boudguiga, N. Bouzerna, L. Granboulan, A. Olivereau, F. Quesnel, A. Roger, and R. Sirdey, "Towards better availability and accountability for iot updates by means of a blockchain," in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*, April 2017, pp. 50–58.