Defining Trust in IoT Environments via Distributed Remote Attestation using Blockchain

Uzair Javaid
National University of Singapore
uzair.javaid@u.nus.edu

Muhammad Naveed Aman
National University of Singapore
naveed@comp.nus.edu.sg

Biplab Sikdar
National University of Singapore
bsikdar@nus.edu.sg

ABSTRACT

The constantly growing number of Internet of Things (IoT) devices and their resource-constrained nature makes them particularly vulnerable and increasingly attractive for exploitation by cyber criminals. Current estimates commonly reach the tens of billions for the number of connected "things". The heterogeneous capabilities of these devices serves as a motivation for resource sharing among these devices. However, for effective resource sharing, it is essential that trust be retained in the multitude of pervasive and diverse IoT devices. Remote attestation is a well-known technique used to build such trust between devices. This paper proposes a blockchain based remote attestation protocol to establish trust between IoT devices. The blockchain offers a secure framework for device registration by keeping a list of trusted devices while the attestation is based on Physical Unclonable Functions (PUF). This combination results in a tamper resistant scheme with protection against physical and proxy attacks.

CCS CONCEPTS

• **Computer systems organization** → **Peer-to-peer architectures**; **Embedded and cyber-physical systems**; • **Security and privacy** → *Security protocols*; Security in hardware;

KEYWORDS

Blockchain; remote attestation; Internet of Things (IoT)

1 INTRODUCTION

The sheer number of devices in IoT environments manifest many of the same resource constraints as last generation of "disconnected" embedded systems such as extensive hardware support, prolonged device life cycles, high security fidelity, and low power consumption [1, 14]. However, the limited computational capabilities of these devices, economic forces, and lack of security expertise often contribute to a rush towards commercialization with minimal consideration for security implications. IoT has thus, unfortunately inherited security vulnerabilities from the firmware, software, and hardware of the previous generation. This starkly highlights that given the security failings of IoT combined together with its inconspicuous, always-on, and non-interactive nature, IoT-targeted attacks are now a real threat and a legitimate concern [28].

IoT systems are composed of largely heterogeneous devices with diverse capabilities. This leads to resource sharing among IoT devices. However, establishing trust in an IoT device needs to be a pre-requisite for any kind of resource sharing in IoT systems. Software attestation is a process via which verifiable evidence about the state or properties of a system can be shared between devices in an IoT environment [3]. It traditionally involves a Prover and a Verifier in its operation, where the trustworthiness and reliability of this evidence is based on a root of rust; often a hardware device such as a trusted platform module (TPM). However, as IoT devices often lack advanced hardware such as TPMs, software based attestation is preferred. Such software based attestation techniques rely on two major assumptions out of many: (i) adversary is passive during the attestation period, and (ii) prover hardware is safe against any kind of modification. This presents a security concern, i.e., if an adversary gains access to a prover, such techniques immediately become vulnerable. To address this, this paper integrates the software component of the attestation technique with a hardware primitive, Physical Unclonable Function (PUF). A PUF is used here to establish the root of trust for each device via challenge-response pairs (CRP). PUFs are an attractive choice for IoT devices as they have very low cost of production with minuscule amount of energy footprint and silicon area. This makes PUFs an attractive choice for remote attestation in IoT systems [23].

Traditional software attestation techniques assume the devices to be physically protected. However, this assumption is not valid given their simple and low cost nature and deployment in remote locations [21, 22]. Moreover, attestation techniques fundamentally require a-priori knowledge about the "good" properties of a system in an IoT environment, which is usually stored in a database. Arguably, a data storage solution with secure device registration mechanism for a heterogeneous, distributed, and multiorganization IoT attestation network ought to be decentralized. Blockchain provides such a decentralized and cryptographically secure distributed ledger [15–17]. This paper explores blockchain for establishing trust via distributed attestation in IoT environments. This is achieved by integrating the PKI fundamentals of blockchain with PUFs. Thus, this paper makes the following main contributions:

i. A distributed remote attestation protocol for IoT.
ii. A registration mechanism to register or remove devices.
iii. A device registry to authorize only registered devices.
iv. A hardware primitive based attestation technique that also offers a defense mechanism against physical attacks.

The remainder of the paper is structured as follows: Section 2 discusses the related works. Section 3 defines the preliminaries while Section 4 describes the network model. Section 5 explains the proposed protocol. Sections 6 and 7 present the security and performance analyses. Finally, the paper is concluded in Section 8.

2 LITERATURE REVIEW

Recent literature in different IoT avenues include [25–27] as the most common software attestation techniques. During an attestation procedure, the device that needs to be attested is the Prover, whereas the device that verifies the prover (i.e., its software state) is called the Verifier. Thus, in existing attestation techniques design

thinking, a prover has to check its current firmware version or software configuration and send a status acknowledgement to the verifier, which then uses this acknowledgement to confirm if the prover is in a trustworthy state. However, malicious software (malware) or hardware may be able to forge the system status reports at the prover side. Therefore, to safeguard against physical attacks, [19, 24] stress on the importance of PUFs and their use in software attestation techniques. However, both of these techniques operate on a similar design pattern, i.e., they require the output of each iteration of the attestation algorithm be taken as an input to the PUF, thereby producing a hardware footprint, which is input again to the checksum procedure. This presents a feasibility problem: these techniques need a very large challenge-response PUF space to operate when the challenge-response space of existing PUFs is very limited, which makes such techniques infeasible and impractical. Thus, to solve this, the attestation technique proposed in this paper is independent of large challenge-response PUF space and can function with limited challenge-response pairs (CRPs) of PUFs.

We can now infer that the aforementioned works suffer from centralized storage, high computational overhead due to complex schemes, and high trusted hardware or memory modules costs, which mainly function to preserve secrets from physical attacks. Therefore, to solve these issues, this paper proposes a blockchain and PUF based attestation technique, which does not require any expensive hardware module, offers immutable and distributed storage, and uses PUFs which have very low cost [2]. The technique also uses symmetric key encryption and timing information that results in lower overhead for IoT devices.

3 PRELIMINARIES

Many software attestation techniques operate under the assumption that only a set of specific algorithms can be executed by exploiting the computing capability of a prover within a certain time period. Thus, the attestation operation requires the following two steps: (i) the verifier needs to use a reference software state and computes a reference checksum while the prover calculates a checksum over its memory contents; (ii) attestation is only guaranteed upon the successful reception of the checksum by the verifier from the prover within a specific time threshold and that the checksum generated by the prover is identical to the reference checksum. We can now define this set of interactions in terms of blockchain as verifier and IoT devices as provers.

3.1 Blockchain

A blockchain is a globally distributed online/digital ledger that can be public, private, or semi-private, where the ledger primarily records transactions by verifying the authenticity of their data. It uses public key infrastructure (PKI) and economic modeling, which is applied to a peer-to-peer (P2P) network and a shared consensus algorithm to achieve synchronization. It typically operates on millions of devices/nodes where information and anything of value such as digital assets, identities, deeds, and even votes can be securely stored, managed, and moved. Its properties of decentralization, transparency, immutability, and fault-tolerance render it suitable for decentralized IoT environments. In this paper, the blockchain is responsible for successfully registering the devices and storing their associated CRPs as well as maintaining a list of trusted devices, thereby acting as a verifier.

3.2 Physical Unclonable Function

A PUF is a noisy or fuzzy function that is inherently embedded in electronic circuits due to the random variations introduced by the semiconductor chip manufacturing process [4, 7]. Moreover, when a PUF is queried with a challenge i, it produces a response: $j \leftarrow PUF(i)$. This response primarily depends on the internal structure of a device as well as on i. Due to variations naturally associated with environmental factors such as pressure, temperature, and voltages, the output of a PUF may slightly vary when excited or input with the same challenge a polynomial number of times. A remedy to rectify this involves fuzzy extractors, which eliminate such design constraints and translate PUFs to behave like deterministic functions [12].

A PUF can be used as a tool for generating secure keys and enabling hardware authentication among others [5]. The ability of PUFs to retain keys without actually storing them and their robustness against invasive and physical attacks, makes them potential candidates for addressing security issues in IoT. Moreover, a PUF has many different types in which some are memory based that exploit the random process variations in memory cells, and delay based that leverage the variation in circuit delays [11]. In this paper, PUFs is used to assign each device a unique hardware fingerprint which is then used in the attestation routine to calculate the software state of a device.

3.3 SWATT

One of the first and popular software attestation techniques is SWATT [27]. SWATT can verify the memory contents and detect any malicious tampering of an embedded device's memory. SWATT is based on a pseudorandom traversal of memory. A verifier sends a challenge in the form of a random seed to the prover, who then uses that seed to randomoly iterate over its memory and calculate a hash digest of the memory. The usage of pseudorandom numbers as memory addresses protects SWATT from various type of adversarsaries. However, due to the absence of a root of trust in SWATT, it is vulnerable to physical attacks. This paper addresses this issue by introducing PUFs into the attestation routine.

4 NETWORK MODEL

The network model for the proposed attestation protocol is shown in Figure 1, where the yellow spaces represent different IoT applications generating different types of data. Note that the server instances are shown twice to highlight the decentralization property of blockchain. The magenta lock icons represent the encrypted communication between the blockchain and the IoT devices, while the exclamation mark on top of them signify the point where the proposed protocol operates. Thus, the network model has the following major entities:

4.0.1 Server. This represents a set of devices that can provide different kinds of services to users and devices of the network, i.e., registering IoT devices and verifying their CRP during attestation. The servers are the trusted hosts of blockchain, i.e., they initiate a blockchain with the first (genesis) block, but instead of being

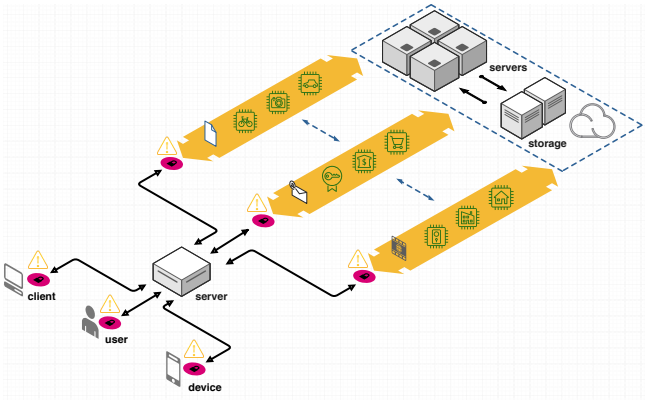

Figure 1: A holistic view of a blockchain-IoT network model.

centralized, their distribution is decentralized here. Moreover, they may employ permissioned or permissionless blockchain protocols to achieve consensus in the network. They also act as miners to generate new blocks, i.e., they are responsible for providing the computing power required by the blockchain to operate.

4.0.2 Storage. This represents the process of reading and/or writing data to storage devices. The storage may be temporary like RAM (random access memory) or permanent like ROM (read only memory). Different forms of data (json, xml, csv etc.) can be stored on them that can be used by other devices.

4.0.3 User device. This represents desktops, smartphones, and laptops, which are used by a user to conveniently check and enjoy the services provided by the servers (e.g., register a device) as well as read data from or write to a storage device.

4.0.4 IoT device. This represents "things", i.e., the key players of the proposed protocol responsible for sensing data, and processing and communicating it to the servers via gateways. A gateway here is responsible for handling and providing connectivity to multiple devices together, thereby forming a cluster of devices. Note that these devices may also read data from or write to the storage devices of the network.

4.0.5 Infrastructure based links. This represents infrastructure based communication technologies such as GSM/GPRS/UMTS/LTE via WiFi through wireless local area network (WLAN) access points (AP) and cellular base stations. As WLAN APs and cellular base stations may act as the gateways to provide Internet connectivity to IoT devices, they are termed as server nodes.

4.0.6 Device-to-device links. This represents proximity based wireless interfaces such as Bluetooth Low Energy (BLE), WiFi Direct, and near field communication (NFC) that allows IoT devices to communicate with each other.

4.1 System assumptions

We make the following set of assumptions and system configuration regarding the proposed protocol:

a. Proof-of-work (PoW) consensus is used where honest miners are not resource constrained and always control more than 50% of the total computing power, thereby restricting an adversary/a group of adversary from compromising the blockchain.
b. Elliptic Curve Cryptography (ECC) with Elliptic Curve Digital Signature Algorithm (ECDSA) is used to register and assign IDs to each IoT device.
c. Each IoT device is equipped with a PUF and is an embedded system-on-chip (SoC). Any sort of tampering with the PUF will render it useless [13, 18].
d. The physical communication link between the PUF and microcontroller can be assumed secure as they coexist on the same SoC [13, 18].
e. ID_A, $\{M\}_k$, C^i, and R^i denote the ID of an IoT device, message M encrypted with key k, challenge for i^{th} iteration, and the PUF response for C^i, respectively.

4.2 Security objectives

The primary security requirements of the proposed protocol are:

i. To provide a platform for registering and storing device IDs.
ii. To attest the software running on an IoT device.
iii. To not store secrets on a device.
iv. To restrict an adversary from breaking the protocol even if a device is compromised.

4.3 Threat model

To formulate a threat model for the proposed protocol, we use [9] where an adversary is able to eavesdrop and intercept any message in the blockchain-IoT network, inject spam packets to overload the network, replay older messages, and impersonate devices. We also assume that the adversary is able to compromise IoT devices which may be subjected to physical attacks.

The adversary intends to bypass the verifier without detection and subsequently, plans to corrupt the compromised IoT device by modifying its memory contents and install malware. The adversary aims to launch attacks on the compromised device to cause economic and physical damage. For instance, to install malware by gaining unauthorized access into the database of a factory, an adversary can effect an incident that may potentially involve human-in-the-loop. Therefore, we develop a distributed remote attestation protocol that offers immutable and distributed storage, and is also secure against different types of attacks that include single point-of-failure, physical, man-in-the middle, cloning, and tampering, among others.

5 HARDWARE PRIMITIVE BASED ATTESTATION TECHNIQUE

The principles of the proposed PUF based attestation technique for the blockchain-IoT network are explained in this section. Thus, we herewith discuss the details of the protocol and the roles of the two modules, i.e., blockchain and IoT devices. The protocol operates in two phases.

5.1 Device registration

Before a device can be attested, it has to be registered first in the blockchain-IoT network. To do so, it needs to interact with any of

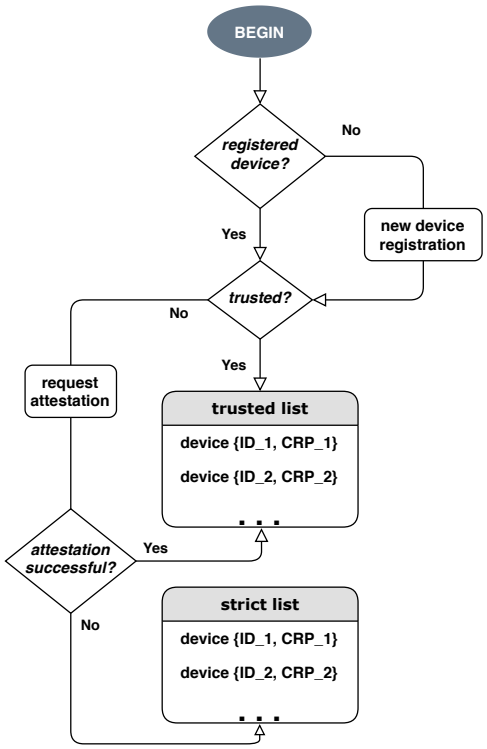

Figure 2: Proposed Protocol.

the distributed servers in the network, which assigns it a pseudo-random ID based on ECDSA algorithm and then, stores its ID along with its associated CRP in the blockchain. Thus, whenever a device needs to be attested, it is first checked if it is registered.

5.2 Device attestation

After the successful registration of a new IoT device, it now needs to be attested to verify the integrity of its software. The proposed attestation technique introduces PUFs to SWATT as a hardware root of trust. Figure 3 shows the operation of the proposed attestation technique. Let us denote the verifier by V which is attesting the software running on an IoT device (prover) P. Then, the steps for the proposed attestations protocol are as follows:

1. V records the current time t and sends a random seed S_d to P.
2. P initializes the checksum using a hash of S_d, i.e., $\sigma_0 = H(S_d)$ and iterates over multiple words in its memory and combines its PUF output in each iteration with SWATT as follows:
   - Use an exclusive or of the PUF output (via the stored challenge C) and a random number x_{i-1} to calculate an input variable y_{i-1} for SWATT. Note that the seed sent by V is used as the initial random number, i.e., $x_0 = S_d$.
   - To bind every iteration of the attestation routine to the IoT node's hardware characteristics, y_{i-1} is input to the SWATT routine. This can be achieved by using y_{i-1} as an additional input to SWATT's pseudo-random number generator.
   - The random number for the next iteration x_i is obtained using the output of the SWATT function.

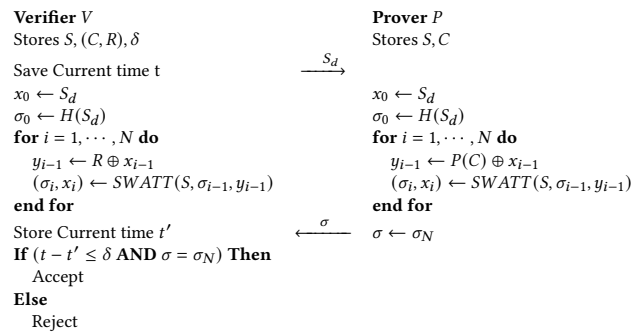

Figure 3: PUF based attestation routine.

3. After iterating over the memory N times, P sends the final checksum value back to V.
4. V calculates the checksum value in a similar fashion as P using the stored state S of P. Moreover, while P uses its PUF in each iteration, V employs CRP value that is stored in its memory.
5. The attestation is considered successful if the following two checks are satisfied:
   - The final checksum value measured by V is the same as that received from P.
   - The time difference $t - t'$, where t' denotes the time when V received the checksum value from P, is less than a threshold δ. Note that δ is the time required by an honest device to calculate the checksum.
6. If either one of the two conditions is violated, the IoT nodes is tagged as compromised.

5.3 Proposed Protocol

The proposed protocol is shown in Figure 2. It uses the following three levels for network isolation of IoT devices:

a. **Trusted:** Every new IoT device that is registered and which does not have any pre-installed or pre-embedded malware in it, and is not compromised is added to the list of trusted devices after successful attestation. IoT devices in this list are free to communicate with each other using all of the available communication interfaces. Note that the devices may have multiple communication interfaces such as LTE, WiFi, and Bluetooth etc. This list is maintained on the blockchain.
b. **Strict:** If an IoT device is new to the network or if it may be potentially compromised, it is added to the strict list. This is to filter the traffic generated by these devices to block any malicious packets, or connection requests to the external network or other IoT devices. This list is also maintained on the blockchain.
c. **Isolated:** If an IoT device is compromised by malware or an adversary, it is simply dropped from the network, i.e., it is delisted from both lists. Thus, all future interactions, connection requests, and packets from such delisted devices are immediately dropped/blocked. There is no list associated with this level, therefore, to join the network again, delisted devices must register themselves again.

6 SECURITY ANALYSIS

We herewith discuss the security features of the proposed protocol.

6.1 Protection against Tampering

A PoW based blockchain starts with a genesis block and adds every subsequent block with its proof to itself chronologically in such a way that the latest block is able to point to the genesis block. Therefore, to create an alternative and dishonest chain, an adversary needs to successfully redo the PoW for the latest block as well as all of its preceding ones. However, the adversary needs to have more than 50% of the total computing power of the blockchain network to achieve this [8, 20]. Thus, a dishonest chain can potentially be mined by using $> 50\%$ mining power [20]. Given a decent sized blockchain network, such attacks have extremely low probability. Thus, the PoW consensus used in the proposed protocol offers high security fidelity against tampering if the number of honest miners is always greater than the malicious ones. To guarantee the security of the blockchain-IoT model with consensus algorithm Δ, the number of malicious miners m should be restricted by the following constraint: $m \leq v_\Delta, \forall\ \Delta = PoW$, where $v_\Delta = \lfloor \frac{n-1}{2} \rfloor$ represent the maximum tolerable number of malicious miners (i.e., $< 50\%$).

6.2 Protection against Physical Attacks

IoT devices are generally located at remote locations and an attacker may gain physical access to these devices. This exposes the secrets that are stored in the memory of an IoT device and puts them at risk, i.e., using physical attacks an attack may be able to reveal the stored secrets of the device such as secret keys [6]. This may lead to compromising the security of attestation techniques using proxy nodes. However, the proposed attestation technique embeds PUFs into the attestation routine and does not require any stored secrets. Therefore, the proposed attestation routine can be considered safe against physical attacks.

6.3 Protection against Proxy attacks

A proxy may be used to attack an attestation technique. In this type of attack, the attestation request from the verifier is forwarded by a compromised device to a proxy one. The proxy device (with the legitimate software) runs the attestation routine and sends the checksum value to the prover. The prover in turn forwards the checksum value back to the verifier. However, the proposed technique is safe against this type of attack in the following way:

(1) To correctly calculate the checksum, the proxy needs the PUF of the compromised IoT node as shown in Figure 3. However, without the actual PUF, the proxy cannot calculate the correct checksum value. Note that even if the compromised node sends the PUF response to the proxy, the attestation routine uses $P(C)$ instead of the response. Therefore, to bypass the PUF, the code on the proxy needs to be modified, which will also yield an invalid checksum.
(2) The attestation will fail because of the additional time incurred by forwarding and receiving the attestation request from the proxy.

This shows that the proposed attestation technique is safe against proxy attacks.

7 PERFORMANCE ANALYSIS

7.1 Attestation

Due to the high throughput and low power requirements of PUFs, they do not introduce any extra overhead to security protocols. As the proposed attestation routine is an extension of SWATT by adding a PUF to it, therefore, we can consider the complexity of the proposed attestation routine the same as SWATT. If we denote the number of iterations for the proposed attestation technique by N, then the worst case running time for the proposed attestation technique is $O(N)$ as compared to $O(Nm \ln m)$ for the existing attestation techniques [6]. This shows that the proposed attestation routine does not add any extra overhead to SWATT.

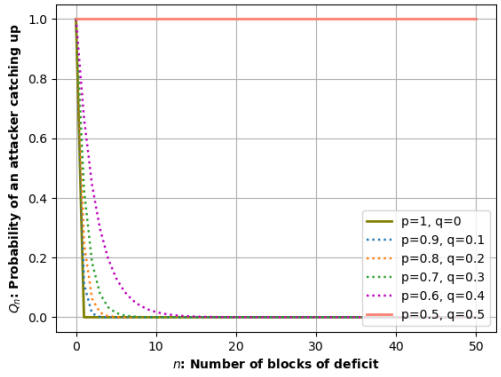

Figure 4: Probability of an adversary reaching break even.

7.2 Blockchain robustness

Since the blockchain is responsible for storing and maintaining the trusted list of devices, it is indispensable that it be secure and tamper resistant. To quantify this, we measure the robustness of blockchain in the proposed protocol. Let us consider a case where an adversary tries to compete with the honest miners of blockchain by creating an alternate/dishonest chain at a faster rate. Recall our assumption that honest miners control more than 50% of the total network resources. Thus, this competition between the honest miners and adversary can be modelled as a function of binomial random walk. Thus, the event of "success" here signifies that the honest chain is extended by one block, thereby increasing its lead over the alternate chain by +1, while the event of "failure" signifies that the alternate chain is extended by one block, thereby reducing the gap by −1.

Moreover, the probability that the adversary catches up from i blocks behind the honest chain can be formulated in terms of a Gambler's Ruin problem. Let us consider a player who starts off at a given deficit with unlimited credit and then potentially plays infinite trials to try to reach a break even point. The probability that the gambler ever reaches break even or that an adversary is ever

successful in catching up with the honest chain in a blockchain can be formulated as [10]:

$$Q_i = \begin{cases} 1 & if\ p \leq q \\ (\frac{q}{p})^i & if\ p > q \end{cases}, \quad (1)$$

where p represents the probability that an honest miner finds the next block, q represents the probability that the adversary finds the next block, and Q_i represents the probability that the adversary will catch up from i blocks behind the honest chain. Figure 4 demonstrates the ineffectiveness of this attack as long as the honest miners have > 50% of the total computing capacity, which startkly highlights the robustness offered by the blockchain. It can be seen that when $p = 1, 0.9, 0.8, 0.7$, and 0.6, Q_i exponentially decreases with the increasing number of blocks of deficit, i.e., after just 10 blocks, Q_i reduces to 0. When $p = 0.5$, Q_i increases to 1, which confirms that whoever controls > 50% of the total network resources, controls the blockchain. However, given our assumption $p > q$, Q_i is only able to retain extremely low probability of success.

8 CONCLUSION

This paper investigated the issue of retaining trust in the multitude of pervasive and diverse computing devices in IoT environments, and presented a distributed remote attestation protocol using blockchain. The registration of devices is securely handled by the blockchain, which is also able to provide distinction between trusted and rogue devices via a list of trusted devices. The proposed attestation technique is based on PUFs that also enable device resistance to physical attacks. To study the security and feasibility of the proposed protocol, security and performance analyses were presented which demonstrate that the protocol able to achieve distributed IoT remote attestation with protection against tampering, physical, and proxy attacks.

REFERENCES

[1] Z. Ali, S. A. Chaudhry, M. S. Ramzan, and F. Al-Turjman. 2020. Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles. *IEEE Access* 8 (2020), 43711–43724.

[2] Massimo Alioto. 2017. *Enabling the Internet of Things: From Integrated Circuits to Integrated Systems* (1st ed.). Springer Publishing Company, Incorporated.

[3] M. N. Aman, M. H. Basheer, S. Dash, J. W. Wong, J. Xu, H. W. Lim, and B. Sikdar. 2020. HAtt: Hybrid Remote Attestation for the Internet of Things with High Availability. *IEEE Internet of Things Journal* (2020), 1–1.

[4] M. N. Aman, M. H. Basheer, and B. Sikdar. 2019. Two-Factor Authentication for IoT With Location Information. *IEEE Internet of Things Journal* 6, 2 (2019), 3335–3351.

[5] M. N. Aman, K. C. Chua, and B. Sikdar. 2017. Physically secure mutual authentication for IoT. In *2017 IEEE Conference on Dependable and Secure Computing*. 310–317.

[6] M. N. Aman, K. C. Chua, and B. Sikdar. 2019. *Cryptographic Security Solutions for the Internet of Things*. IGI Global USA, Chapter Hardware Primitives-Based Security Protocols for the Internet of Things, 201–213.

[7] M. N. Aman, B. Sikdar, K. C. Chua, and A. Ali. 2018. Low Power Data Integrity in IoT Systems. *IEEE Internet of Things Journal* 5, 4 (2018), 3102–3113.

[8] Vitalik Buterin. 2014. Ethereum: A next-generation smart contract and decentralized application platform. https://github.com/ethereum/wiki/wiki/White-Paper.

[9] D. Dolev and A. Yao. 1983. On the security of public key protocols. *IEEE Transactions on Information Theory* 29, 2 (1983), 198–208.

[10] William Feller. 1991. *An Introduction to Probability Theory and Its Applications*. Wiley.

[11] Blaise Gassend, Dwaine Clarke, Marten van Dijk, and Srinivas Devadas. 2002. Silicon Physical Random Functions. In *Proceedings of the 9th ACM Conference on Computer and Communications Security* (Washington, DC, USA) *(CCS '02)*. Association for Computing Machinery, New York, NY, USA, 148–160. https://doi.org/10.1145/586110.586132

[12] P. Gope, A. K. Das, N. Kumar, and Y. Cheng. 2019. Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks. *IEEE Transactions on Industrial Informatics* 15, 9 (2019), 4957–4968.

[13] Sylvain Guilley and Renaud Pacalet. 2004. SoCs security: a war against side-channels. *Annales Des Télécommunications* 59 (2004), 998–1009.

[14] A. Irshad, S. A. Chaudhry, M. Sher, B. A. Alzahrani, S. Kumari, X. Li, and F. Wu. 2019. An Anonymous and Efficient Multiserver Authenticated Key Agreement With Offline Registration Centre. *IEEE Systems Journal* 13, 1 (2019), 436–446.

[15] Uzair Javaid, Muhammad Naveed Aman, and Biplab Sikdar. 2018. BlockPro: Blockchain Based Data Provenance and Integrity for Secure IoT Environments. In *Proceedings of the 1st Workshop on Blockchain-Enabled Networked Sensor Systems* (Shenzhen, China) *(BlockSys'18)*. Association for Computing Machinery, New York, NY, USA, 13–18. https://doi.org/10.1145/3282278.3282281

[16] U. Javaid, M. N. Aman, and B. Sikdar. 2019. DrivMan: Driving Trust Management and Data Sharing in VANETs with Blockchain and Smart Contracts. In *2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*. 1–5.

[17] Uzair Javaid, Ang Kiang Siang, Muhammad Naveed Aman, and Biplab Sikdar. 2018. Mitigating LoT Device Based DDoS Attacks Using Blockchain. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems* (Munich, Germany) *(CryBlock'18)*. Association for Computing Machinery, New York, NY, USA, 71–76. https://doi.org/10.1145/3211933.3211946

[18] M. Kirkpatrick, S. Kerr, and E. Bertino. 2012. System on Chip and Method for Cryptography using a Physically Unclonable Function.

[19] Joonho Kong, Farinaz Koushanfar, Praveen K. Pendyala, Ahmad-Reza Sadeghi, and Christian Wachsmann. 2014. PUFatt: Embedded Platform Attestation Based on Novel Processor-Based PUFs. In *Proceedings of the 51st Annual Design Automation Conference* (San Francisco, CA, USA) *(DAC '14)*. Association for Computing Machinery, New York, NY, USA, 1–6. https://doi.org/10.1145/2593069.2593192

[20] Satoshi Nakamoto. 2009. Bitcoin: A peer-to-peer electronic cash system. (03 2009).

[21] M. Naveed Aman, M. H. Basheer, and B. Sikdar. 2019. Data Provenance for IoT using Wireless Channel Characteristics and Physically Unclonable Functions. In *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. 1–6.

[22] M. Naveed Aman, M. H. Basheer, and B. Sikdar. 2019. Data Provenance for IoT With Light Weight Authentication and Privacy Preservation. *IEEE Internet of Things Journal* 6, 6 (2019), 10441–10457.

[23] M. Naveed Aman, S. Taneja, B. Sikdar, K. C. Chua, and M. Alioto. 2019. Token-Based Security for the Internet of Things With Dynamic Energy-Quality Tradeoff. *IEEE Internet of Things Journal* 6, 2 (2019), 2843–2859.

[24] Steffen Schulz, Ahmad-Reza Sadeghi, and Christian Wachsmann. 2011. Short Paper: Lightweight Remote Attestation Using Physical Functions. In *Proceedings of the Fourth ACM Conference on Wireless Network Security* (Hamburg, Germany) *(WiSec '11)*. Association for Computing Machinery, New York, NY, USA, 109–114. https://doi.org/10.1145/1998412.1998432

[25] Arvind Seshadri, Mark Luk, and Adrian Perrig. 2011. SAKE: Software Attestation for Key Establishment in Sensor Networks. *Ad Hoc Netw.* 9, 6 (Aug. 2011), 1059–1067. https://doi.org/10.1016/j.adhoc.2010.08.011

[26] Arvind Seshadri, Mark Luk, Adrian Perrig, Leendert van Doorn, and Pradeep Khosla. 2006. SCUBA: Secure Code Update By Attestation in Sensor Networks. In *Proceedings of the 5th ACM Workshop on Wireless Security* (Los Angeles, California) *(WiSe '06)*. Association for Computing Machinery, New York, NY, USA, 85–94. https://doi.org/10.1145/1161289.1161306

[27] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla. 2004. SWATT: softWare-based attestation for embedded devices. In *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004.* 272–282.

[28] L. D. Xu, W. He, and S. Li. 2014. Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics* 10, 4 (2014), 2233–2243.