Securing the Internet of things using Blockchain

Sadia Showkat
Department of Computer Science and Engineering
National Institute of Technology Srinagar
J&K , India
sadia_01phd18@nitsri.net

Shaima Qureshi
Department of Computer Science and Engineering
National Institute of Technology Srinagar
J&K, India
shaima@nitsri.net

***Abstract*-At present, the networks are vulnerable to various security problems like intrusion, phishing, hacking, to mention a few, and various encryption techniques are employed to curb the same. IoT environments are susceptible to various attacks that compromise the basic Confidentiality-Integrity-Availability triad of network security. IoT applications range from baby monitors to high-end military systems. With a plethora of devices transmitting sensitive information, the security of IoT environments becomes pivotal. However, it is not viable to extend the traditional dense encryption methodology to resource-inhibited IoT devices. Thus, lightweight algorithms are devised to meet the needs of their constrained architecture. Blockchain is a technology that helps in achieving a peer-peer secure and tamper-proof transfer of data between two objects. Blockchains can thus empower integrity in networks. Extending the concept of Blockchains to constrained IoT ecosystems, however, meets with its challenges. This paper focuses on the applications and challenges of Blockchain technology in securing IoT environments.**

Keywords: IoT, Security, Blockchain.

I. INTRODUCTION

Internet of things (IoT) is a network that intends at fusing every possible "thing" to the internet. "Things" refer to anything that has the potential to perceive and transmit data over a network. Gartner Research makes a forecast of a total of 20 billion IoT devices and 65% of organizations taking up IoT by 2020 [1]. IoT encompasses various sensitive sectors like business, finance, banking, military, etc., making the security aspect of IoT fundamental. IoT devices are constrained in nature and exhibit typical characteristics like heterogeneity, dynamicity, plurality, making the adoption of security mechanisms strenuous. Forefending the attack prone constrained devices is thus exigent. Blockchain is an open, transparent, distributed ledger that timestamps digital documents that cannot be meddled. Blockchain provides a transparent yet secure decentralized approach for maintaining the information and information flow in a system. With Blockchain, it is possible to maintain the entire trail of data flow in a system, and information can be traced to from where it originated. Blockchain provides a secure approach that validates the entities involved in communication in a distributed and decentralized way [2]. Blockchain can address various threats in an IoT environment. Adoption of Blockchain technology in IoT can help control the end-devices, create unique identities for nodes, and keep trail the data from and to its point of origin, making the system reliable and immune to malicious attacks. Many applications in IoT need a decentralized architecture to further their capabilities. The benefit of Blockchain comes from the interconnection of devices owned by various users who share their computational power and storage in a trusted, secure manner. Blockchain-based networks can thus replace the cloud by providing a decentralized and trusted storage facility than can help process the data transmitted over the network. Blockchain technology, however, has pressing challenges that upsurge in a resource-constrained environment. It may be feasible to employ Blockchain-based security in specific environments while being counter-productive in others, thus whether or not to use Blockchain technology in an IoT environment is an application-centric decision. Many Blockchain-based secure IoT systems have been conceived already. This paper is divided into 6 sections. In Section II, we describe the security issues in IoT ecosystems, in Section III we present an overview of Blockchain technology and Section IV discusses the Blockchain-based solutions for IoT security. In Section V, we discuss existing models of Blockchain-based secure Vehicular IoT applications. Challenges of fusing Blockchain in IoT are discussed in the subsequent section.

.

II. SECURITY ISSUES IN IOT

IoT comprises a wide range of devices like temperature sensors, fitness trackers, cameras, GPS monitors, etc. These devices perceive, store and transmit critical and personal information. Compromise in the end-device and transmission channel security can lead to the disclosure of private, financial and sensitive information e.g., the breach in a GPS enabled device can lead to the revelation of private

978-1-7281-2791-0/20/$31.00 ©2020 IEEE

information like address and the current location of the user. In most IoT based applications IoT devices transmit private and critical information. The sensitivity of the information transmitted may be more in some than others. IoT devices are vulnerable to various security threats, especially in critical sectors. A typical IoT network demands data sensing, transmitting data, and communication between entities. IoT based system usually comprises 3 layers- the perception layer, network layer, and application layer. IoT infrastructures face various security threats at all of these layers [3]. Fig. 1 illustrates the main security issues pertaining to IoT security in these layers [3], [4].

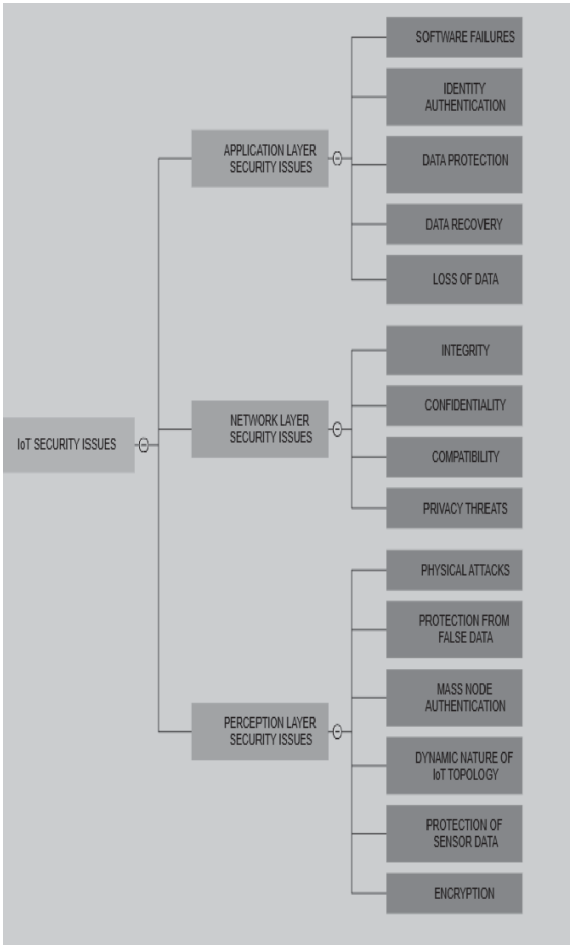

Fig. 2. IoT security issues

Frequent security attacks across these layers include:

Unauthorized Node capture: IoT nodes are usually disposed of in profusion, thus vulnerable to attacks.

Sinkhole attack: Sinkhole is a node that has been seized by an attacker, thus compromising the integrity of the network. Sinkhole provides an alternate route to the neighbors derailing the intended transfer of information in the network.

Man in the middle attack: This refers to an attempt to intercepting the communication between two nodes. The communicating devices are incapable of gauging the legitimacy of the end nodes.

Denial of Service: The attackers overload the network with surplus traffic hampering the original communication and resource allocation in the network.

Hostile malware attacks: Malware / Malicious codes briskly diffuse through the whole communication network and, in so doing, compromise the veracity of the entire network.

Identity theft: Identity theft refers to the masquerading of devices. The authors of [5] present various identity thefts in IoT infrastructure.

Loss of data: The unreliability of the communication channel in the IoT infrastructure may lead to loss of important data.

Sybill attacks: In Sybill attack, attackers compromise the reputation of a system by manipulation and creation of fabricated identities.

Middleware security attacks: A middleware is employed usually in heterogeneous IoT environments for smooth integration, and the middleware is susceptible to attacks.

Software failures: At the application layer, the software is susceptible to failure. Various security threats comprise remote configuration, misconfiguration, the unwanted outflow of information, etc.

Privacy threats: Disclosure of personal information in the network is one of the pre-eminent matters in IoT environments.

Routing attacks: Networks are not immune to routing attacks. Secure but low power consuming routing protocols is essential in IoT environments.

Sleep deprivation attack: For the sake of energy conservation, IoT devices shut off for a pre-defined interval regularly. In this type of threat, the nodes are barred from sleeping, decreasing the network lifetime of the system.

Replay attack: In replay attacks, the data is reduplicated, leading to resource wastage.

III. BLOCKCHAIN TECHNOLOGY

The concept of Blockchain technology was conceived by Satoshi Nakamoto, who aimed at resolving the “double-spending problem” and eliminating the requirement of intermediation for a direct peer-peer transaction. Blockchain is often confused with Bitcoin in our vernacular. However, Bitcoin is a cryptocurrency that works on the Blockchain technology, and Blockchain itself is a distributed ledger system that provides secure peer-peer transactions. Since its inception, the researchers have worked on exploring the features of Blockchain, and today Blockchain find application in various sectors like business, healthcare, education, equity, crowdfunding, voting, smart contracts,

insurance, financial services, etc. [6],[7],[8], [9]. Blockchain eliminates the middleman between individuals who do not find each other reliable by acting as a database for keeping a mutually trusted, joint, tamper-proof, timestamped count of records. The workload in a Blockchain network is distributed over several computational devices rather than a central node.
The critical characteristics of Blockchain include

Decentralization: A Blockchain network is decentralized, having no central authority.

Transparency: The data in a Blockchain network is visible to all.

Security: The transactions are digitally signed.

Integrity: The new blocks are added based on a consensus mechanism.

Other features include verifiability, availability, programmability, efficiency etc. [6].

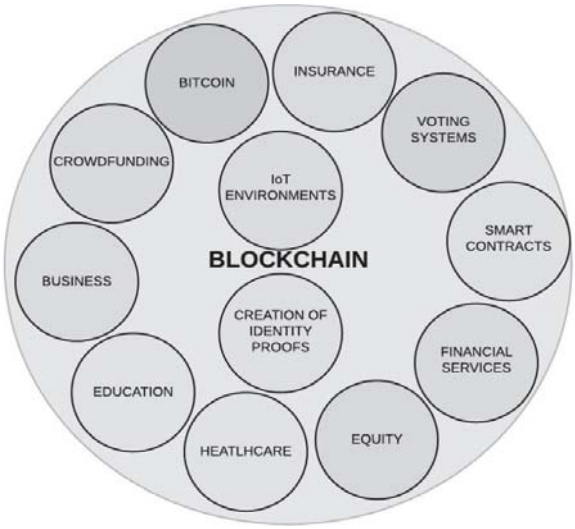

Fig. 1. Some applications of Blockchain Technology

A) Key terms related to Blockchain technology

Block: Blocks are the units that store every bit of relevant information about the transactions. Blocks are inalterable and transparent to other blocks in the network. A block consists of Block header and block body.

Block head: It contains the previous address (hash value of the previous node), timestamp (for chronological organization), Merkle root (holds the hash value of the present node), and a nonce (to verify hash).

Block body: It comprises a Hash transaction account (transaction history) and transaction count (the number of awaited transactions).

Genesis block: The first block in a Blockchain network.

Transaction: refers to the tasks one can avail in a Blockchain network like exchanging money, framing contracts, etc. Every transaction in the Blockchain network is digitally signed. Digital signatures are created using public key –private key mechanism.

Mining and Proof of Work: In a Blockchain network, there are special stakeholders called miners who validate transactions. The participants of the network already have the recorded history of all transaction thus duplication cannot occur. Newer blocks are added by miners to the network using a consensus algorithm agreed upon by all existing users. Miners are paid for their services.

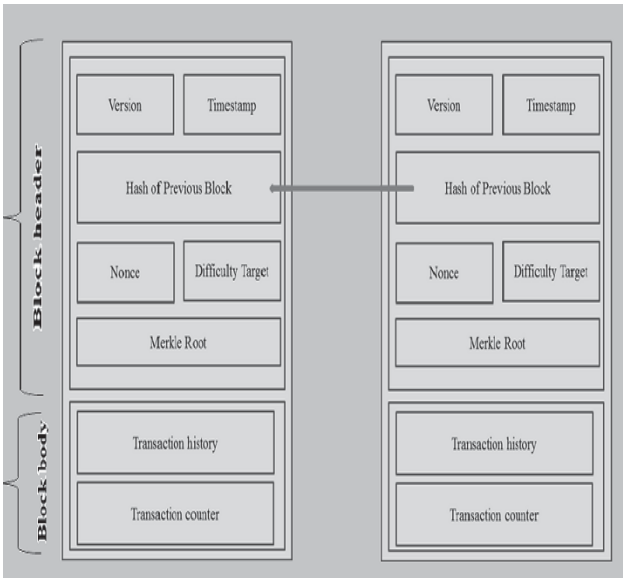

Fig. 3 : Basic Block structure

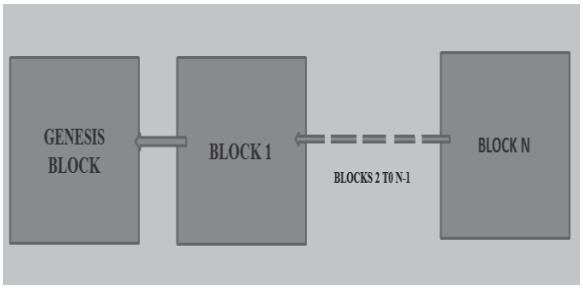

Fig. 3. Basic Blockchain structure

B) Basic working of Blockchain

Blockchains are typically either public or permissioned [10]. In the permissioned scenario, only a selected set of people are part of the Blockchain network, while in the case of a public Blockchain, anybody can join. The underlying mechanism on which Blockchain works is based on ECC or elliptic curve cryptography, and SHA-256 hashing and transactions between entities are signed using public-key

cryptography [11]. ECC is an encryption mechanism that provides security using smaller size keys, thus making it apt for constrained environments. Hashing primarily refers to a mapping of values/strings of random sizes to values of static size. SHA-256 is one of the resistant hashing functions that are impervious to brute-force attacks. Every block in the Blockchain network has the hash of the previous block, thus tampering with a block would require the hacker to alter the hashes of all previous blocks in the blockchain. A new block is added to the chain by means of a consensus protocol to safeguard the integrity of the ledger. For a new block to be added to the system, miners solve a computational puzzle that lays some time off before the block addition. This is called Proof of Work (PoW) and is done to carry out a consensus. The complexity of the task depends on the complexity of the network itself. After PoW, the block is published and must be verified by other nodes in the network. When a new block is to be added to the network, hashes of other blocks automatically change. Thus if a hacker intends to add a malicious block in the network, it would require him to compute PoW faster than other trusted nodes in the network and hijack more than half of the resources in the chain which is in majority. PoW ensures the integrity of the network by protecting it against malicious attackers.

IV. BLOCKCHAIN-BASED SECURITY SOLUTIONS FOR IOT

Various security attacks pertaining to IoT environments have already been discussed in Section 2. The transactions in a Blockchain network are digitally signed using a public key cryptography mechanism. Blockchain can help in ensuring the integrity of the information. The following are some Blockchain-based security solutions for IoT.

Tracking of messages: The messages in the IoT environment can be traced to their point of origin. A hacker can't conduct a man in the middle attack [11]. The flow of data occurs in a transparent manner. Using the Blockchain technology, only valid messages can be transmitted through the system. The validity of the information can thus be ensured in IoT infrastructures by employing Blockchain technology.

The integrity of data: To alter the data in one block, the hacker has to change the hashes of all blocks involved in the network and unless a hacker somehow gets control of the majority of the chain, the data cannot be altered and is consistent throughout. PoW ensures that the malicious nodes need to spend a lot of computing power to overload the network thus providing protection against the overloading of the network by hackers.

The legitimacy of nodes and Identity theft protection: Checking the legitimacy of the sender is no longer a problem as in a Blockchain, only verified blocks are added to the chain. Nodes are verified using a consensus mechanism and only trusted nodes can be part of the network chain. In a Blockchain network, unique identities can be created and stored for a network, thereby eliminating the threat of identity theft and spoofing. Blockchains also prevent the creation of pseudo-identities. The fake nodes cannot derail the flow of data to alternate routes. This ensures authenticity and prevents attacks like Sybill attacks.

Privacy: Privacy has been a major issue in IoT infrastructures. In fact, the privacy issues on the internet are older than IoT itself. The data that the user owns is usually stored on a cloud-managed by private organizations leaving the user with a bare minimum control of his data. In a Blockchain, a user is in full control of his data instead of a central authority. Further, the data across the network is shared in a transparent yet protected manner.

Reliability: IoT systems typically rely on a cloud server for storage and processing, making it the principal point of failure in the system. In Blockchain-based systems, the data is stored across a number of computational devices making the network fault-tolerant [11]. The data stored on a cloud is stored in a centralized manner while using Blockchain technology, the data is stored across a number of devices in a decentralized manner. The decentralization in data storage makes the system more reliable and robust.

V. BLOCKCHAIN-BASED SECURE INTERNET OF VEHICLES (EXISTING PROPOSED MODELS)

The concept of IoT has been extended to various domains. Internet of Vehicles (IoV) refers to a network of communicating vehicles connected to the internet using the underlying sensor technologies of IoT. Like most IoT ecosystems, IoV systems are heterogeneous, dynamic, complex, and prone to security threats. IoV involves humans directly, and a security attack on the network may lead to loss of lives. Further, privacy threats surround IoV environment as information like location, and the usual route of the vehicle is susceptible to leakage. Apart from privacy threats like leakage of GPS data, various attacks on IoV networks include Sybill attacks, route modification attack, wormhole attacks, masquerading attack, eavesdropping, DoS, replay attacks, etc.[12] [13]. Even a small fault in IoV networks can lead to fatal results. Thus security in IoV is critical. As mentioned earlier, the advantages of Blockchain technology can be extended for securing IoT environments. Many use cases of Blockchain-based secure and decentralized models that encompass various IoT domains exist. The following are a few proposed models in literature on Blockchain-based secure IoV.

The authors of [14] propose an intelligent transportation system based secure and trustworthy Blockchain model. The model comprises 7 layers. The physical layer consists of vehicles and related entities. The data layer is based on the Blockchain technology and enables the blocks to be stored in chronological order. This layer enables the security and integrity of data and helps to trace the data. The network layer enables peer-peer communication eliminating a central authority, helps in verification of data. The consensus layer is used for data validity. The incentive layer is used to award coins to the nodes that provide services of data verification. The contract layer constitutes of rules that the involved nodes have to abide by. Finally, at the top is the application layer.

The authors of [15] propose a vehicular decentralized Ad-hoc network based on Blockchain Technology, which can work on its own without the involvement of an external authority. The concept employs Euthereum's smart contract system. End-user can subscribe to any application of interest and make payment using Blockchain methodology, which helps in maintaining the infrastructure.

The authors of [16] propose a Blockchain mechanism in vehicular systems to enhance trust management. The proposed design constitutes of checking the credibility of the messages generated using specific rules, calculation of normalized offsets based on an equation to verify the credibility of a message, miner selection in a conventional manner, and finally consensus but in a distributed manner.

The authors of [17] propose a Blockchain-based IoV system. The communication is based on vehicular cloud computing and the Blockchain mechanism. In the model proposed, a unique ID called Bit trust ID is assigned to each vehicle using Blockchain technology. Bit Trust is received by solving a computational puzzle. Bit trust enables to store the entire transaction history of the vehicle. Thus, Blockchain acts as a database for storing all the communication history between vehicles. After a vehicle broadcasts a message and using the consensus mechanism, the data is verified. The data is stored on trust bit Id enabled cloud.

VI. CHALLENGES

IoT-Blockchain integration has not been yet conceived to its full potential. The incorporation of Blockchain technology in IoT environments has its fair share of challenges. Some challenges arise due to the nature of IoT devices while certain others due to the limitations of the Blockchain technology itself. The following are some of the challenges that can be encountered in IoT-Blockchain integration.

Complexity: Blockchain technology employs complex consensus protocols for achieving validation, verification, integrity, authentication, etc. IoT devices are constrained in computational and power capabilities that can prove as a bottleneck for employing the complex Blockchain mechanisms in an IoT environment.

Computational overhead: A decentralized ledger is maintained in a Blockchain network. It increases overheads in the network which may not be suitable in a resource-constrained environment.

Latency: Blockchain technology provides security by employing computational tasks like Proof of work which take time. In Bitcoin, the PoW time is 600 seconds. In certain IoT applications, data may need to be processed on the go in real-time and is rendered useless otherwise and in some cases, the delay can prove catastrophic.

Lack of a common set of rules: Blockchain network lacks a basic set of legal rules and the absence of a central authority which makes Blockchain susceptible to fraudulent transactions. Compliance issues between different participants can also occur.

Growth of chain: The scalability of blockchain is a crucial issue. Scalability also affects the consensus process. The nodes(full nodes) keep a copy of the entire chain and as the network grows, storage limitations at some point can easily become a bottleneck.

Majority attack: The hacker can manage to control more than half of the Blockchain network launching a 51% attack. The hacker can gain control of the chain and can mine as many malicious blocks disrupting the entire network.

VII. CONCLUSION

Extending Blockchain technology to IoT environments, although enables a secure peer-peer transaction between nodes thus improving the integrity of the system, but it increases the complexity of the system. Blockchain technology involves the use of computational resources for performing tasks like PoW, which also brings added latency to the system making it infeasible for an IoT environment [18]. The scalability of Blockchains is another standing issue. The appositeness of engaging Blockchain technology in resource-inhibited environments appears questionable, but if the right balance is struck between the limitations of IoT environments and the benefits of the Blockchain technology, the desired secure peer-peer functionality can be realized.

REFERENCES

[1] M. Hung. "Leading the IoT: Gartner Insights on How to lead in a Connected World," *Gartner Inc*, p. 5, 2017. [Online]. Available: Gartner, www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf. [Accessed Nov. 20, 2019].

[2] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," *Journal of Internet of Things Class Files*, vol. 14, no. 8, March 2018.

[3] K. Zhao and L.Ge, "A Survey on the Internet of Things Security," in *Ninth International Conference on Computational Intelligence and Security*, Leshan, China, December 14-15, 2013: IEEE 2013. pp. 663-667.

[4] N. Ye, Y. Zhu, R. Wang, R. Malekian and L. Qiao-min, "An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things," *Applied Mathematics & Information Sciences* vol. 8, no. 4, pp.1-8 , 2014.

[5] S. Vidalis and O. Angelopoulou, "Assessing Identity Theft in the Internet of Things," *Journal of IT Governance Practice*, vol. 2 (1), pp 15-21, 2014.

[6] D. Josephine, "Secure Voting System Using Block Chain Technology," *in International Conference on Recent Trends in Computing, Communication and Networking Technologies*, Chennai , 2019.

[7] G. Chen, B. Xu, M. Lu and N. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learning Environments* , 2018.

[8] M. Miraz and M. Ali, "Applications of Blockchain Technology beyond Cryptocurrency," *Annals of Emerging Technologies in Computing (AETiC)* , vol. 2, no. 1, 2018.

[9] M. Nofer, P. Gomber,O. Hinz and D. Schiereck, " Blockchain," *Business & Information Systems Engineering* vol. 59, issue 3, pp. 183–187, June 2017.

[10] M. Khan and K. Salah, "IoT security: Review, Blockchain solutions, and open challenges," *Future Generation Computer Systems* 82 pp. 395–411 ,2018.

[11] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," *IEEE IT Professional*, vol. 19, issue 4, pp. 68-72, Jan. 2017.

[12] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu and Y. Xiong, "Security and Privacy in the Internet of Vehicles," in *2015 International Conference on Identification, Information, and Knowledge in the Internet of Things*, Beijing: IEEE, 2015, pp. 116-121.

[13] S. Zahra, "MNP: Malicious Node Prevention in Vehicular Ad hoc Networks" in *International Journal of Computer Networks and Applications,* IJCNA 2018, vol. 5, no. 2, pp. 9-21.

[14] Y. Yuan and F. Wang, "Towards Blockchain-based Intelligent Transportation Systems," in *19th International Conference on Intelligent Transportation Systems*, Brazil : IEEE, 2016.

[15] B. Leiding, P. Memarmoshrefi, and D. Hogrefe, "Self-managed and Blockchain-based Vehicular Ad-hoc Networks," *2016 ACM International Joint Conference- UbiComp*, Heidelberg, Germany, September 12-16.NY, USA: ACM 2016. pp. 137-140.

[16] Z. Yang, K. Yang, L. Lei, K. Zheng, C. Victor and M. Leung," Blockchain-based Decentralized Trust Management in Vehicular Networks," *IEEE Internet of Things Journal,* vol. 6, no. 2, pp. 1495-1505 , 2019.

[17] M. Singh and S. Kim, "Trust Bit: Reward-based Intelligent Vehicle Commination Using Blockchain Paper," 2018 IEEE *4th World Forum on Internet of Things (WF-IoT)*, Singapore, February 5-8. IEEE, May 2018. pp. 62-67.

[18] A. Dorri, S. Kanhere, R. Jurdak and P. Garavaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," *2017 IEEE PerCom Workshop On Security Privacy And Trust In The Internet of Things*, Kona HI, USA, March 13-17. IEEE, May 2017.