Using Blockchains to Strengthen the Security of Internet of Things

Charalampos S. Kouzinopoulos[1], Georgios Spathoulas[2], Konstantinos M. Giannoutakis[1(✉)], Konstantinos Votis[1], Pankaj Pandey[2], Dimitrios Tzovaras[1], Sokratis K. Katsikas[2], Anastasija Collen[3], and Niels A. Nijdam[3]

[1] Information Technologies Institute, Centre for Research and Technology Hellas, Thessaloniki, Greece
{kouzinopoulos,kgiannou,kvotis,Dimitrios.Tzovaras}@iti.gr
[2] Center for Cyber and Information Security, Norwegian University of Science and Technology, Gjøvik, Norway
gspathoulas@dib.uth.gr, {pankaj.pandey,sokratis.katsikas}@ntnu.no
[3] University of Geneva, Geneva, Switzerland
{Anastasija.Collen,Niels.Nijdam}@unige.ch

Abstract. Blockchain is a distributed ledger technology that became popular as the foundational block of the Bitcoin cryptocurrency. Over the past few years it has seen a rapid growth, both in terms of research and commercial usage. Due to its decentralized nature and its inherent use of cryptography, Blockchain provides an elegant solution to the Byzantine Generals Problem and is thus a good candidate for use in areas that require a decentralized consensus among untrusted peers, eliminating the need for a central authority. Internet of Things is a technology paradigm where a multitude of small devices, including sensors, actuators and RFID tags, are interconnected via a common communications medium to enable a whole new range of tasks and applications. However, existing IoT installations are often vulnerable and prone to security and privacy concerns. This paper studies the use of Blockchain to strengthen the security of IoT networks through a resilient, decentralized mechanism for the connected home that enhances the network self-defense by safeguarding critical security-related data. This mechanism is developed as part of the Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control (GHOST) project.

Keywords: Internet of Things · Blockchain · Security · Cyber-security

1 Introduction

A Blockchain is a cryptographically-linked list of records that maintains a publicly verifiable ledger without the need for a central authority; as such, it is a new paradigm of trust between entities in various application domains. The technology behind Blockchains originated in cryptocurrency applications, while

E. Gelenbe et al. (Eds.): Euro-CYBERSEC 2018, CCIS 821, pp. 90–100, 2018.
https://doi.org/10.1007/978-3-319-95189-8_9

its advancements over existing architectures motivated researchers to apply it to domains that prioritize security. The main benefits of this new architecture are the decentralized nature, the inherent anonymity, resilience, trust, security, autonomy, integrity and the scalability. Some implementations support Smart Contracts for interactions between the Blockchain and third-party stakeholders.

A suitable application of the Blockchain technology is to the Internet of Things (IoT) which had a tremendous growth during the past few years, while their security mechanisms are often light-weight due to resource constraints, thus threatening user trust. As discussed in [1], IoT networks are vulnerable to external threats for a variety of reasons. It is easy to gain physical access to individual devices since they are often isolated and there is no administrator to manage them; They usually communicate with each other and with a gateway using different wireless communication protocols, making eavesdropping very easy; and finally, most devices have low processing capabilities and thus it is difficult to implement complex security schemes on a per device basis.

This paper discusses the main security-related benefits of integrating a Blockchain infrastructure in IoT ecosystems, and more specifically in smart homes installations. The inherent benefits of using a Blockchain in such systems are considered, while supplementary use cases are proposed to strengthen the security aspects of IoT installations. The proposed use cases are mainly focused on the interaction of data generated by IoT devices with external entities, while the relation with the Safe-Guarding Home IoT Environments with Personalised Real-time Risk Control (GHOST) project main architectural elements is defined.

The rest of the paper is organized as follows. Related work regarding the use of Blockchain in IoT environments is summarized in Sect. 2. Section 3 reviews security and privacy requirements in IoT environments, and it discusses the GHOST architecture and the use of Blockchain technology in GHOST. Security enhancements that the use of blockchain technology induces are discussed in Sect. 4. Concluding remarks and future work are discussed in Sect. 5.

2 Related Work

With the evolution of IoT networks and their strictly centralized architectures for manipulating device data, the new Blockchain distributed ledger technology inherently solves many fundamental security issues. The use of Blockchain technology in the IoT domain to facilitate the sharing of services and resources, and automate in a secure manner several time-consuming workflows, is studied in [2]. The authors concluded that the Blockchain-IoT combination is powerful and can pave the way for novel business models and distributed applications. Moreover, relative literature and work designed for Blockchain use in IoT was studied in [3]. The paper identified different research efforts, [4–6], that utilize the Blockchain infrastructure as a data storage management solution. In all cases, data exchanged between IoT devices are stored as unique transactions within the Blockchain and are subsequently distributed among the nodes, ensuring the integrity and security of the communication between them.

A decentralized peer-to-peer platform based on Blockchain networks for Industrial IoT was proposed in [7]. Their use cases focus on industrial and manufacturing applications, where Smart Contracts act as intermediaries between the Blockchain ecosystem and outside stakeholders. Dorri et al. proposed a private Blockchain infrastructure for Smart homes, [8]. They focus on security issues with respect to confidentiality, integrity and availability, while simulation results indicate that the overheads imposed by the use of such technology remain at low levels. Additionally, [9] discusses the security enhancements with the use of Blockchain in IoT. The role of Blockchain is examined through four challenges, namely: Costs and capacity constraints, Architecture, Unavailability of services and Susceptibility to manipulation. They conclude that with the decentralized and consensus-driven structures of Blockchain, more secure IoT ecosystems can be provided as the network size increases. Recently, FairAccess, a token-based access control model with the use of Blockchain, has been proposed in [10], that provides an access control mechanism for the transactions realized within a Blockchain infrastructure.

IT companies have also shown a great interest in applying Blockchain architectures in IoT ecosystems. The IBM Watson IoT platform supports private Blockchain ledgers for sharing IoT data via transactions. ADEPT (Autonomous Decentralized Peer-To-Peer Telemetry), a research project for Blockchain in IoT that uses the technology of Ethereum, Telehash and BitTorrent, was also announced [11]. Targeting an economy of Things, ADEPT focuses on Distributed Transaction Processing and Applications, Robust Security and Privacy By Design and Default. There are also other companies and start-ups that focus on transaction integrity, trust and security in the IoT domain.

Almost all relevant research work utilize the Blockchain technology as a data storage management solution, taking advantage of the underlying infrastructure that provides decentralization, resilience, trust, security, scalability, autonomy and integrity. This work proposes additional use cases for further enhancement of the security of IoT smart homes, especially regarding their interaction with external entities, such as caregivers.

3 Security in IoT Environments

An IoT installation consists of interconnected heterogeneous devices that collect sensitive user information and share it with other devices of the network, the gateway or third-party nodes connected via the Internet. Furthermore, modern IoT installations come in different configurations and modes of deployment. The decentralized deployment, high connectivity, diversity and heterogeneity results in a number of security and privacy challenges, that in turn induce requirements. These can be categorized in five groups, namely network security, identity management, privacy, trust and resilience. Network security requirements are split into confidentiality, integrity, authenticity and availability. Identity management requirements are separated into authentication, authorisation, accountability and revocation. Privacy requirements are split into data privacy, anonymity,

pseudonymity and unlinkability. Trust requirements are divided into device, entity, and data trust. Finally, resilience requirements are split into robustness against attacks and resilience against failures [12].

3.1 The GHOST Approach

The H2020 European research project GHOST aims to develop a cyber-security layer on IoT smart homes installations. The proposed system analyses packet level data flows for building patterns of communications between IoT devices and external entities. The architecture of GHOST is detailed in [13]. GHOST includes the Data Interception and Inspection layer that is responsible to gather, aggregate and analyze data; the Contextual Profiling layer that builds behaviour trees for devices and data-flows and provides current state of data identification and related behaviour; the Risk Assessment layer that gathers information about the current risks and analyzes in real-time current network traffic flows; and the Control and Monitoring layer that presents a graphical interface to the end user.

Moreover different components are utilized, including the GHOST Blockchain Defence Infrastructure component that uses Blockchain and Smart Contracts to ensure data integrity in the process of distributed decision making, as well as additional security countermeasures; the Cross Layer Anomaly Detection Framework where traditional cyber security features are exploited, extended and adapted for the needs of the smart home environment; the Cyber Security Knowledge Base that consists of a cloud-based knowledge repository to collect anonymized security intelligence and insights to enhance the automatic decision making and improve end-user visual experience within the Control and Monitoring layer; and the Shared Data Storage, a single-storage framework.

3.2 IoT Blockchain Component

A Blockchain component can be incorporated, together with a Risk Assessment mechanism, at the core of IoT installations to offer an additional layer of security. It can ensure the integrity of such a mechanism through the decentralisation and replication of trusted decisions on the Blockchain network. Additionally, the Blockchain component can be used to capture data flows exchanged between IoT devices and the IoT gateway. The data flows captured, that represent part or all the messages exchanged, based on predetermined filtering settings, can be stored in the form of transactions that in turn can be subsequently published to the Blockchain distributed ledger.

A possible interaction between Blockchain nodes in smart homes is depicted in Fig. 1. As can be seen by the Figure, the IoT devices of each smart home communicate and exchange data flows with an IoT gateway, in this case the GHOST gateway. The gateway can function at the same time as Blockchain nodes if they possess adequate processing power or else perform the role of light Blockchain nodes. In this second scenario, additional, full Blockchain nodes must be used that can be installed either on a per smart home basis or centrally on an external location. These nodes can be used to serve as miners in order

to achieve consensus in cases of validation of transactions and to publishing these transactions to the distributed Blockchain ecosystem of smart homes. Any external entities can interact with the Blockchain network through the use of the appropriate Smart Contracts.

4 Enhancing Security and Privacy in Smart Homes Using Blockchain

Section 3 identified security and privacy requirements of current smart home IoT installations. This Section details different ways an IoT device network can utilize the Blockchain technology to fulfil security and privacy requirements in a smart home context. Some of these cases will be modified and used appropriately as part of the operation of the GHOST network.

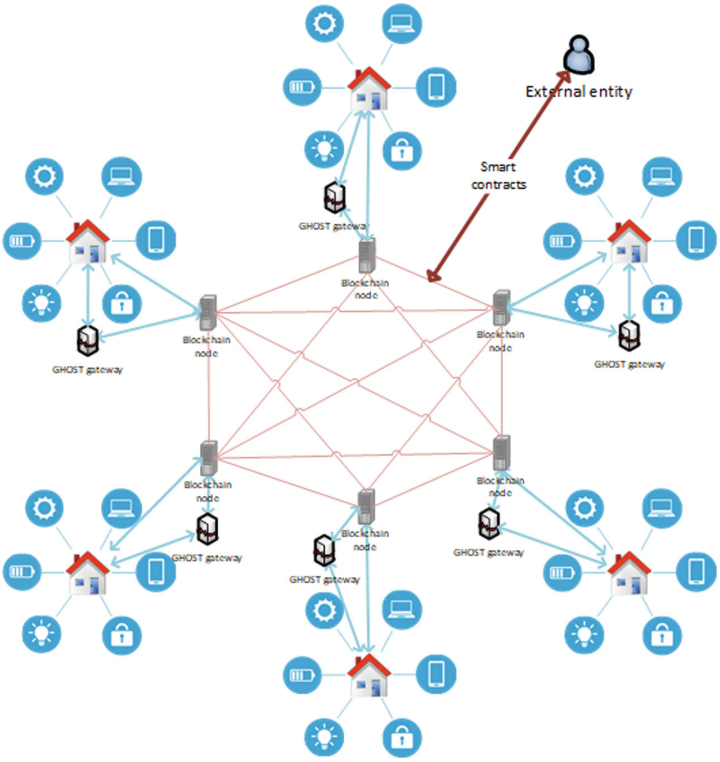

Fig. 1. GHOST Blockchain nodes interaction

4.1 Resilience

A widely used mechanism that can address part of the resilience requirement of IoT environments is intrusion detection, the monitoring and investigation of system events so that the attempts to access system resources in an unauthorized manner can be identified [14] and mitigated. There are two primary approaches to intrusion detection algorithms: signature based, where a collection of signatures that characterize known security threats is maintained as well as anomaly detection based, where network traffic is monitored continuously and compared against an established baseline of normal traffic profile [15]. However, both approaches are resource-intensive, making their execution by most low-powered and limited-processing IoT devices prohibitive.

The IoT network can use high-processing Blockchain nodes as the basis for its infrastructure. These nodes are using their computing power to verify and record transactions to a public ledger as per the standard Blockchain specification but also to execute intrusion detection algorithms. Since the public ledger contains a list of all transactions in the network in chronological order, and is synced across all the gateway nodes, the intrusion detection algorithms can be executed in parallel, speeding up their operation.

The use of high-processing Blockchain nodes to increase the resilience of IoT installations directly impacts the total energy consumption of the system. However, the energy increase can be kept at moderate levels if only a limited amount of Blockchain nodes is used and if a lower difficulty for the mining algorithm is selected. Both of these measures are valid for a private Blockchain network where access to unauthorized users is prohibited.

4.2 Identity Management

Device authentication is a mechanism to be used towards fulfilling the identity management requirement of IoT environments. It involves the connection of trusted devices to the IoT network excluding insecure devices or devices that an unauthorized user would try to add. Its enforcement is challenging though, due to the decentralized nature of IoT installations, in conjunction with the lack of secure authentication protocols in IoT gateways. The GHOST network maintains two lists of IP addresses, a whitelist and a blacklist. The initial whitelist is created by the Knowledge Base and contains a range of IP addresses marked as safe. This list consecutively is extended by the verified behaviour of the devices on the network by Risk Engine and direct end-user configurations through Control and Monitor layer.

The blacklist in turn consists of IP addresses that were flagged as unsafe by the Risk Engine, while correlating device activity on the network with profiles available from a Contextual Profiling layer. These lists are stored locally on the GHOST gateway with a limited corresponding information stored in a component called Shared Data storage. The Knowledge Base can also communicate with the Risk Engine to update the blacklist based on additional intelligence.

Both the whitelist and the blacklist are retrieved from the Risk Engine for any Smart Contract that requires them via the appropriate calls. If the lists cannot be sourced, a static list of IP addresses is hard-coded in a Smart Contract with its life limited to a fixed-time period. Once such a Contract expires, a new one is deployed with an updated list, for protection against any additional nodes that were flagged as unsafe. A similar mechanism based on Blockchain and Smart Contracts for collaborative DDoS mitigation strategy that is used to block suspicious IP addresses was detailed in [16].

4.3 Network Security

The firmware of IoT devices is a crucial part of their operation. Once a device is deployed, its firmware can be updated to address known bugs, increase its stability or add new functionality. At the same time though, its upgrade process can be easily hijacked by a malicious user [17] resulting to the compromise of the security of the network. Due to the always-on nature of many of these devices, their low processing capabilities and the reluctance of device manufacturers to improve their security for cost reasons, a successful attacker can intercept the updating firmware and replace it with a harmful version that makes the device operate in an unpredictable way.

The subject of firmware attacks in IoT devices has been extensively studied. In [18] it is shown that the firmware verification done by the Nest thermostat can be bypassed, due to the lack of protection by the device's hardware infrastructure. In [19], a security analysis of both consumer and industrial IoT devices is performed and is concluded that both types of devices are vulnerable to attacks. Moreover, in [20] was shown that it is trivial to intercept the firmware update process of Philips Hue lamps by plugging infected bulbs in the network and then exploiting bugs in the implementation of the Touchlink part of the ZigBee Light Link protocol and performing a side-channel attack to extract the global AES-CCM key that Philips uses to encrypt and authenticate new firmware.

IoT networks can utilize a new firmware update scheme, based on the Blockchain network. That way, the version of the firmware can be checked securely, its correctness can be validated and the installation of the most up-to-date firmware on all the devices of the network can be ensured.

4.4 Trust

Each IoT device can have a unique identification ID number assigned to it. The ID is created through a Smart Contract, by providing the "Entity ID" of the device and the "User ID" of the smart home user. The "Entity ID" depends on the underlying protocol of each device; it is the MAC address in case of a WiFi or Zigbee capable device, the Bluetooth Device Address in case of a Bluetooth capable device or the Network ID/Node ID pair in the case of a Z-Wave device. This procedure is performed centrally by an authorized user, such as the network administrator and is published as a Smart Contract in the Blockchain network.

Registering an IoT device creates an additional complexity layer to the IoT architecture but has the benefit of knowing the exact state of the IoT device infrastructure. Moreover, and since devices are uniquely identified, they can be managed both individually and in groups. Finally, by restricting connection to authorised devices, the network can be managed easier and with additional security.

Blockchain networks are built from the ground up based on a trustless proof mechanism of all recorded transactions [21], including all data circulated by the individual devices. In this type of network, all message exchanges between devices can be performed with the use of Smart Contracts and stored as records in a public ledger. The network cryptographically signs these records and verifies the signatures to ensure that they originate from each corresponding device, eliminating various potential threats including proxy or man-in-the-middle attacks and replay attacks [9].

On an already established IoT system, there is often a lack of motivation for individual users to enhance its security past its deployment, by updating the device firmware or substituting insecure and vulnerable devices with safer alternatives. For this reason, a virtual currency can be used. The concept behind the use of a virtual currency is to increase the safety of the network by assigning different costs to different devices based on risk assessment of previous tasks or on known vulnerabilities. Then, a higher virtual cost has to be paid by the users to access less secure devices. Furthermore, a virtual currency can be used not only at the device level but at the network level as well.

As part of the operation of an IoT device network, it is important to inform the participating users about its operating principles of the network as well as to request their acceptance by the users. This procedure can be performed by digital signing a Form of Consent. The signing is performed upon the users' first connection to the network as well as every time the principles are modified. The IoT devices of the users are only allowed to operate on the network after the user has signed the latest issued Form of Consent.

The digital signing of the Form of Consent is performed in the following steps:

- The Blockchain service receives the external connection request and asks the user to digitally sign/accept a Form of Consent using a Smart Contract
- The user signs the form and the transaction is added to the ledger
- The block containing the transaction will eventually be mined and received by the rest of the decentralized nodes.

4.5 Privacy

Often, IoT devices in a smart home capture sensitive private data for their users. It is imperative therefore that a permission handling mechanism is established. For this reason, the user must authorize access to exchange data between each of the IoT devices in their smart home and third-party entities. This access can be granted or revoked using a Smart Contract with the following inputs:

- Device ID number. This is a unique identification number for the devices in a users' smart home network, as discussed in Sect. 4.4
- Third party ID number. This is a unique identification number for a third party entity
- Status. Determines the status of the data access and can be set to either "grant" or "revoke"
- Time limit. This is an optional input and can be set to a specific time period that the access status change will take place. If the input is omitted, the status change is indefinite and can be only changed with a new call to the Smart Contract.

5 Conclusions

This paper presented a decentralized mechanism based on the Blockchain technology and Smart Contracts to improve the security of IoT in smart home installations. The mechanism is being developed as part of the GHOST project.

IoT installations in a smart home come with a number of security and privacy requirements, whose fulfilment is non-trivial, due to the unique structural and operational characteristics that such installations have. Blockchain technology can be used in such contexts to enhance security and privacy, by contributing to satisfying several of these requirements. Possible ways of doing so have been presented and discussed.

Further work will focus on the implementation details of the proposed Blockchain mechanism, as well as on its validation and performance evaluation within the GHOST environment.

Acknowledgments. This work is partially funded by the European Union's Horizon 2020 Research and Innovation Programme through the GHOST project (https://www.ghost-iot.eu/) under Grant Agreement No. 740923.

References

1. Atzori, L., Iera, A., Morabito, G.: The Internet of Things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
2. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the Internet of Things. IEEE Access **4**, 2292–2303 (2016)
3. Conoscenti, M., Vetró, A., Martin, J.C.D.: Blockchain for the Internet of Things: a systematic literature review. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6, November 2016
4. Wörner, D., von Bomhard, T.: When your sensor earns money: exchanging data for cash with Bitcoin. In: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication, UbiComp 2014 Adjunct, pp. 295–298. ACM, New York (2014)
5. Zhang, Y., Wen, J.: The IoT electric business model: using blockchain technology for the Internet of Things. Peer-to-Peer Netw. Appl. **10**(4), 983–994 (2017)

6. Zyskind, G., Nathan, O., Pentland, A.: Enigma: decentralized computation platform with guaranteed privacy. arXiv preprint arXiv:1506.03471 (2015)
7. Bahga, A., Madisetti, V.K.: Blockchain platform for industrial Internet of Things. J. Softw. Eng. Appl. **9**(10), 533 (2016)
8. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for IoT security and privacy: the case study of a smart home. In: 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 618–623, March 2017
9. Kshetri, N.: Can blockchain strengthen the Internet of Things? IT Prof. **19**(4), 68–72 (2017)
10. Ouaddah, A., Elkalam, A.A., Ouahman, A.A.: Towards a novel privacy-preserving access control model based on blockchain technology in IoT. In: Rocha, Á., Serrhini, M., Felgueiras, C. (eds.) Europe and MENA Cooperation Advances in Information and Communication Technologies, pp. 523–533. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-46568-5_53
11. Veena, P., Panikkar, S., Nair, S., Brody, P.: Empowering the edge-practical insights on a decentralized Internet of Things. IBM Institute for Business Value 17 (2015)
12. Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., Kikiras, P.: On the security and privacy of Internet of Things architectures and systems. In: 2015 International Workshop on Secure Internet of Things, pp. 49–57 (2015)
13. Collen, A., et al.: Ghost - safe-guarding home IoT environments with personalised real-time risk control. In: Gelenbe, E., et al. (eds.) Euro-CYBERSEC 2018. CCIS, vol. 821, pp. 68–78. Springer, Cham (2018)
14. William, S.: Computer Security: Principles and Practice. Pearson Education India, Delhi (2008)
15. Kumar, S.: Survey of current network intrusion detection techniques. Washington University in St. Louis (2007)
16. Rodrigues, B., et al.: A blockchain-based architecture for collaborative DDoS mitigation with smart contracts. In: Tuncer, D., Koch, R., Badonnel, R., Stiller, B. (eds.) AIMS 2017. LNCS, vol. 10356, pp. 16–29. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60774-0_2
17. Lee, B., Lee, J.H.: Blockchain-based secure firmware update for embedded devices in an Internet of Things environment. J. Supercomput. **73**(3), 1152–1167 (2017)
18. Hernandez, G., Arias, O., Buentello, D., Jin, Y.: Smart nest thermostat: a smart spy in your home. Black Hat USA (2014)
19. Wurm, J., Hoang, K., Arias, O., Sadeghi, A.R., Jin, Y.: Security analysis on consumer and industrial IoT devices. In: Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific, pp. 519–524. IEEE (2016)
20. Ronen, E., Shamir, A., Weingarten, A.O., O'Flynn, C.: IoT goes nuclear: creating a ZigBee chain reaction. In: 2017 IEEE Symposium on Security and Privacy (SP), pp. 195–212. IEEE (2017)
21. Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc., Sebastopol (2015)