An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology

Longfei Wu[§], Xiaojiang Du[†], Wei Wang[*], and Bin Lin[‡]
[§]Dept. of Mathematics and Computer Science, Fayetteville State University, Fayetteville, NC, USA, lwu@uncfsu.edu
[†]Dept. of Computer and Information Sciences, Temple University, Philadelphia, PA, USA, dux@temple.edu
[*]Beijing Key Laboratory of Security and Privacy in Intelligent Transportation,
Beijing Jiaotong University, 3 Shangyuancun, Beijing 100044, China, wangwei1@bjtu.edu.cn
[‡]Dept. of Information Science and Technology, Dalian Maritime University, Dalian, Liaoning, China, binlin@dlmu.edu.cn

***Abstract*—While the rapid development of IoT devices is changing our daily lives, some particular issues hinder the massive deployment of IoT devices. For example, current network ID management system cannot handle so many new terminals; there is no agreed security standards for IoT manufacturers to follow when designing their products. The whole IoT industry is expecting the breakthrough in network infrastructure and the development of novel security mechanisms that can enable the flexible, secure and reliable access and management of IoT devices. Bitcoin, first released in 2009, breeds the decentralized Blockchain technology. The decentralization, anonymity and proof of security characteristics of Blockchain can prevent collusion and single point failure of a centralized server. We believe that the application of Blockchain into the IoT system can clear the obstacles facing the development of IoT architecture and security. To this end, we propose an out-of-band two-factor authentication scheme for IoT devices based on Blockchain infrastructure. We implemented the IoT and Blockchain integrated system with Eris Blockchain and equivalent computing devices to emulate IoT devices. The overheads to run Blockchain and smart contract services on the emulator devices are measured. The BeagleBone Black and Raspberry Pi 3 nodes have an average memory usage of 29.5M, and the CPU usage of 29.55% and 13.35%, respectively.**

***Index Terms*—Internet-of-Things; Out-of-band; Authentication; Blockchain;**

I. Introduction

Internet-of-Things (IoT) is a network of interconnected objects embedded with electronics, software and sensors. IoT devices are gaining growing popularity on consumer electronics market in the last few years. Increasingly more IT companies have added their IoT products line. According to [1], consumer devices lead the increase of IoT devices and the total amount of the "connected things" will reach 20.8 billion by 2020. Needless to say, it's a huge market and a field of promising technology innovation.

However, IoT devices could suffer a variety of malicious attacks, either the traditional Internet attacks or the specifically designed attacks targeted at IoT devices. The traditional Internet threats they are facing include message replay, impersonation, and man-in-the-middle attacks that can violate the authenticity principle of security. They may also suffer the denial of service (DoS) attacks can prevent legitimate users from being successfully authenticated. IoT devices are more vulnerable to these attacks compared with computers, due to their limited computational and memory resources. Meanwhile, IoT devices are also susceptible to IoT-specific attacks such as in-home smart appliances [2]–[5] and general wireless attacks [6]–[22].

There is no common security standards for IoT devices. The commercial IoT devices on the market are protected by the security schemes designed by each individual manufacturers. This poses huge potential safety hazard since instead of boosting the sales of their products, developing and implementing more robust security mechanisms could only lead to the increase of cost and complexity. The numerous IoT security flaws reported [23], [24] all warn us that the existing protection provided by the manufacturer is far from sufficient. Traditional authentication by password requires human interaction. To enhance the security, two-factor authentication schemes taking advantage of SMS and phone calls require additional infrastructure and human involvement.

The Bitcoin system [25] is peer-to-peer without a central repository or administrator. All transactions take place between users directly. The transaction data are cryptographically secured and maintained by "miners" all over the world. Miners are computer nodes that contribute their computing resources to help maintain and verify bitcoin transactions. As incentives, miners who generate the next transaction block will be rewarded with some bitcoins which they can redeem for money through online bitcoin exchanges. The Blockchain is a distributed database that maintains a continuously growing list of ordered records called blocks. As the core component of the bitcoin system, Blockchain serves as the public ledger for all transactions. By design, Blockchain allows add-only transaction data and prevents the tampering of historical data. In this paper, we propose a novel two-factor authentication scheme based on on Blockchain technology. We summarize our contributions below:

- To the best of our knowledge, this is the first work to use Blockchain to assist the authentication of IoT devices.
- We design a secondary authentication over an out-of-band channel (light, acoustic, etc.), which can detect outside malicious devices even if they have stolen the passcode or the access token.

978-15386-3652-7/18/$31.00 ©2018 IEEE

- Our scheme uses only IoT devices within the home for the secondary authentication. No private information is leaked to external devices.
- We set up the experimental environment with commercial Blockchain and emulator devices. The performance of devices running our proposed scheme is evaluated.

We organize the rest of the paper as follows: Section II gives the adversary model. The proposed two-factor authentication scheme is described in Section III. In section IV, we present the implementation details and the evaluation of our scheme. We discuss the related works in section V, and conclude this paper in section VI.

II. Adversary Model

In this paper, we mainly consider the household scenarios, in which a group of different IoT devices collaborate (e.g., share their sensed data) to better serve the house owner. However, to preserve the privacy of sensitive data, the requester device must first authenticate itself to the provider device and gain the authorization to access the data. To better describe the problem studied in the paper and the threat model, we use the automatic light control based on Nest learning thermostat and Philips Hue Smart Bulb as an example. Specifically, we use Nest thermostat as the ambient light condition and temperature data acquisition device and the Philips Hue smart bulb as the light controller. The thermostat sends the measured data to the Nest server, and the smart bulb access the data from Nest server to adapt its color and brightness to the change of ambient light condition and temperature. For example, the Hue bulbs automatically increase brightness when the Nest device senses dim ambient light and change to warm color when the room is cold.

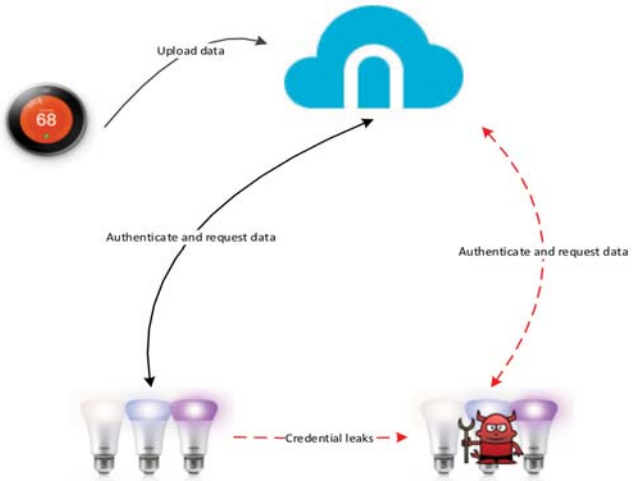

Fig. 1: Light Auto-adaptation Use Case

In order to achieve the auto-adaptation of brightness and color, the Philips Hue bulb first needs to authenticate itself to the Nest server and obtain the sensing results. Figure 1 describes the light auto-adaptation use case. The nest server can be reached and verified by checking the certificate issued by certificate authenticators such as Symantec and Trustwave through the SSL/TLS communication. The Nest API uses the

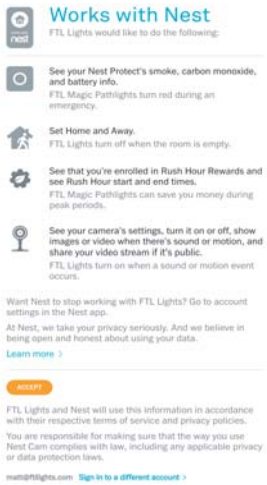

Fig. 2: Nest Authorization Page

OAuth 2.0 protocol for authentication and authorization. Before an IoT product of other brands can access the private data via the Nest API, it must obtain an access token granted for access to that API. For the smart bulb, in order to be authorized to access the Nest server, it has to register to the Nest server and get the authorization code from the authorization server. The user grants an authorization by logging into the account and accepting the privacy and permission agreements using a browser or the smart bulb mobile application, as shown in Figure 2. After the user pressed the ACCEPT button, an access PIN code will be issued for the smart bulb, as shown in Figure 3, which will be exchanged to the access token to access the Nest server.

The process that the user obtains and enters the access code to the smart bulb mobile application leads to a relatively vulnerable channel between the bulb and the Nest server, considering the following potential compromises:

1) The attacker launches phishing attack to steal PIN code.
2) The attacker physically approaches the user to oversee the PIN code during the initial setup process.
3) The user may store the PIN code in an insecure storage, which may be obtained by an attacker.

Given these potential attacks, serious data leakage could happen. In the use case shown in Figure 1, the attacker can impersonate to be the real smart bulb and gain access to the data using the stolen access code. In this paper, our proposed scheme focuses on the defense to an external adversary who has compromised the access token in home IoT scenarios.

III. Out-of-band Two-factor Authentication

In this section, we present the out-of-band two-factor authentication scheme to enhance the authentication and authorization process. Apart from the existing authentication on commercial IoT devices, our scheme takes advantage of the out-of-band channel to conduct a secondary authentication. The secondary authentication factor is able to distinguish a home IoT device from the malicious device (e.g. software-defined radio controlled by the attacker) outside the house, even if the malicious

Fig. 3: Pin Code for Smart Bulb

device impersonates the legitimate IoT device using the correct access token.

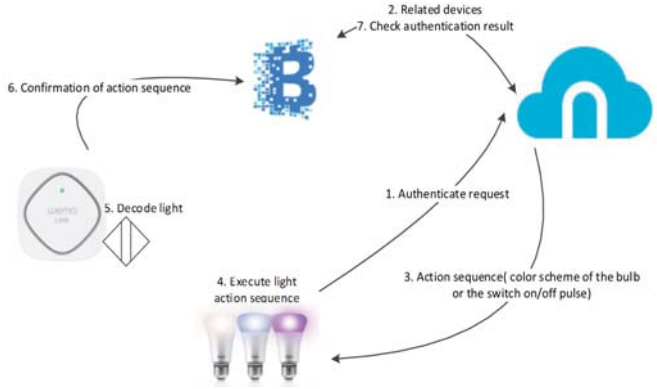

Fig. 4: Out-of-band Secondary Authentication

Following the aforementioned light auto-adaptation use case, we define the four entities considered in our scheme as follows (depicted in Figure 4):

1) **Authentication Subject (AS)** is the device that needs to be authenticated in order to access services or data, which is the Philips Hue Bulb in the aforementioned case.
2) **Related Device (RD)** is the verifier device for the secondary authentication. We assume that RD and AS has been mutually authenticated with each other. In the aforementioned use case, the RD can be any other smart home devices (e.g. WeMo, Belkin, etc.).
3) **Blockchain** stores the relationship information for each AS, namely the RDs that are able to serve as the authenticator in an out-of-band channel. It also provides storage for the verification results.
4) **Authentication Executor (AE)** is the entity that performs and coordinates the two-factor authentication. The Nest server is the AE in the light auto-adaptation use case.

The core idea of the out-of-band secondary authentication is to verify whether an access requestor AS locates within the home (i.e. physically near its RDs) or not. Specifically, AE sends a sequence of action code (bit stream) to AS, which will then flash according to the sequence of action code (e.g. 1 for ON and 0 for OFF), in a high frequency that human eyes cannot notice. Meanwhile, AE chooses one or multiple RD(s) of AS to confirm that the action has been correctly executed by AS. Each RD has an established relationship (e.g., in proximity) with AS, and can accurately measure the bit stream

TABLE I: Emulator Device Specification

IoT Device	Emulator Device	Specification
Philips Hue bulb	BeagleBone Black	• 1GHz ARM Cortex A8 processor • 512 MB DDR3 RAM and 4GB 8-bit embedded MultiMediaCard (eMMC) on-board flash storage • USB Wi-Fi Dongle
Nest data server	Raspberry Pi 3	• 1.2 GHz ARM Cortex-A53 • 1G RAM • On-board Wi-Fi and Bluetooth
WeMo Link	Raspberry Pi 3	Same as above.
WeMo Switch	Raspberry Pi 3	Same as above.

embedded in the changing of lighting conditions. In contrast, the outside adversary have no control over the indoor lighting conditions, hence the RD(s) will not get the right action code and the adversary will fail the secondary authentication. The verification result will be recorded on the specific address on Blockchain. Finally, AE will read RD's verification result to decide whether to grant the access request of AS. Similarly, the secondary authentication can also be performed on other out-of-band channels (e.g. using acoustic signals).

Figure 4 presents the out-of-band (light) secondary authentication. The detailed procedure is listed as below:

1) AS (Philips Hue bulb) requests for the room temperature from AE (Nest server) so that it can changes color based on the current temperature.
2) AE retrieves the relationship information of AS from Blockchain.
3) AE selects the RD (WeMo Link) that is in close proximity with AS, then it sends the action sequence to AS.
4) AS receives and executes the action sequence by encoding the sequence code to the on/off light switchings.
5) The proximity RD decodes the code embedded in the light switchings.
6) Proximity RD sends the verification result to Blockchain by invoking function of the Smart Contract on Blockchain.
7) AE checks Blockchain for the verification result through smart contract.

IV. Implementation and Evaluation

A. Evaluation Environment Setup

Since the aforementioned commercial IoT devices use closed-source hardware and software systems, we are not able to modify and add our authentication scheme onto those devices. Instead, we set up our experimental environment on other developer-friendly devices, which have the similar processing power to WeMo devices and the Philip Hue bulb. Table I shows the emulator devices we used (Column 2) together with their specifications (Column 3), in contrast to the real-world IoT devices (Column 1).

Figure 5 illustrates the experimental setup. The emulator devices we used are Beagle Bone Black and Raspberry Pi 3 boards, both are widely-used prototyping platforms in Internet-of-things and embedded systems. They have Wi-Fi communication interface built on board and can connect to the Internet and the Blockchain. The mutual authentications between AS and its related devices (RD_1, RD_2) have already

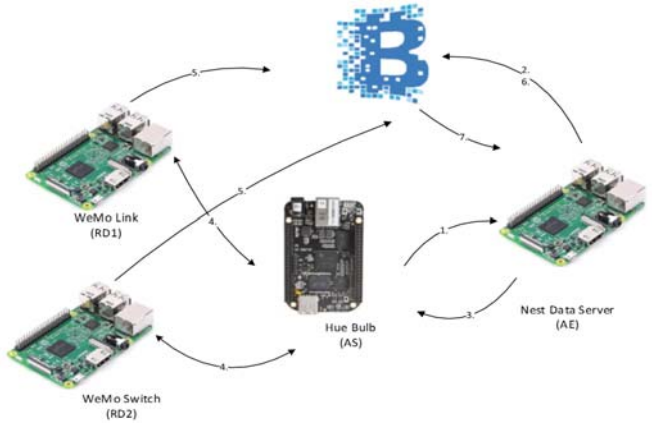

Fig. 5: Experimental Environment Setup

been completed, and their relationship information have been posted to the Blockchain.

B. Relationship Establishment on Blockchain

There are two parts for the relationship establishment on Blockchain: the device profile and the pairing of related devices. As in Eris Blockchain implementation, the two parts correspond to two separate smart contracts: one is the device contract and the other is the relationship contract. The device contract stores the device profiles and the relationship contract stores the related device pairing information. Figure 6 shows a sample of the smart contract execution logs.

```
Related devices (1):
E9E3DF04AFF1DDE81B470FE25474EE07E99F844D
Related devices (2):
410671FB1558D61727295998945C7082C14F6CBE

Device name: RD2-Wemo Switch
Device address: 410671FB1558D61727295998945C7082C14F6CBE
Wireless I/F: Wi-Fi, Bluetooth
Resources: light, microphone

Device name: RD1-Wemo Link
Device address: E9E3DF04AFF1DDE81B470FE25474EE07E99F844D
Wireless I/F: Wi-Fi, Bluetooth
Resources: light, microphone
```

Fig. 6: Relationship and Device Logs

As for the device contract, the device profiles are stored in a mapping data structure which uses address and profile information as the (key, value) pair of the mapping. The profile data includes the following information:

- Device name
- Device address
- Device registration date
- Wireless I/F (Wi-Fi, Bluetooth, etc.)
- Resources (Light sensor, microphone, speaker, etc.)

Likewise, the relationship contract contains the mapping of the AS address to the relationship data, including the following information:

- Related device address
- Proximity (optional)
- Relationship establishment date
- Relationship expiration date

Fig. 7: Memory Usage of Blockchain Process

C. Blockchain Performance

To evaluate the performance of the Blockchain based authentication scheme, we measured the memory and CPU usage of each node in the system. These results are obtained by using the "top" command of Linux to get a runtime screenshot of the Blockchain process every 10 seconds and calculating the average value of 100 consecutive screenshots. Figure 7 shows the results of the memory usage of the Blockchain process. The memory consumptions on the Beaglebone Black board and Raspberry Pi 3 are similar. The average memory usage for running the Blockchain is around 29.5 MB, which is trivial compared to their total memory resources (512M and 1G). Table II presents the CPU usage of the Blockchain process. The percentage of CPU overhead on BeagleBone Black and Raspberry Pi 3 nodes in average are 29.55% and 13.35% respectively, which are considered acceptable since it happens only in the authentication process.

TABLE II: Summary of CPU Usage

Node @ CPU Freq. (GHz)	**CPU (%)**		
	High	***Low***	***Avg.***
AS @ 1.0	29.6	29.5	29.55
AE @ 1.2	13.0	12.9	12.97
RD1 @ 1.2	13.8	13.7	13.76
RD2 @ 1.2	13.4	13.3	13.31

V. Related Work

There are related works on multi-channel authentication and Blockchain based authentication. However, none of them was designed for large scale IoT devices.

Aboshosha et al. [26] proposed an efficient one time password (OTP) based authentication protocol over a multi-channel architecture. The purpose of the protocol is to integrate a web based application with mobile-based technology to communicate with the remote user through a multi-channel authentication scheme. Another paper [27] on multi-channel authentication uses mobile phones as the second channel.

Garman et al. [28] proposed a novel anonymous credential scheme without the need of a trusted credential issuer. Specifically, a public append-only ledger (Blockchain) is employed to conduct the authentication. The authors provided a proof of security for an anonymous credential system that allows users to make flexible identity assertions with strong privacy guarantees without relying on trusted parties. They exploit namecoin, a system built on top of bitcoin Blockchain to provide name-value mappings, to store public key and the corresponding credential.

Only one recent work has studied the secondary authentication in IoT context. Griffin [29] discussed the idea of utilizing biometrics for authentication such as speaker recognition, hand gesture, and gait biometrics. A knowledge-based authentication using both password strings and data extracted from biometric sensors is proposed. For example, voice is chosen as the biometric, then the first authentication factor "something-you-know" comes from the words spoken by a user, and the second authentication factor "something-you-are" is the biometric matching data (i.e., speech recognition). While biometrics are characteristics for human identification, our scheme focuses on the authentication of IoT devices instead of the user/owner.

The combination of Internet-of-things and Blockchain has been studied in another recent work [30]. The authors found that Blockchain can facilitate the sharing of services and resources between IoT devices, and allows users to automate several existing time-consuming workflows in a cryptographically verifiable manner. However, this work only highlighted the Blockchain's benefits in automating the interactions between transacting parties (e.g. transactions), and in developing new business models. Instead, our work takes advantage of Blockchain to assist the authentication of IoT devices.

VI. Conclusion

Securely and reliably authenticating the large scale Internet-of-things devices is not trivial with current network framework and existing security mechanisms. We proposed a out-of-band two factor authentication scheme that exploits device relationship, supported by Blockchain technology. The secondary authentication of our scheme can prevent the access of external malicious devices, even if the first factor fails (e.g., the access token is stolen by the adversary). The out-of-band channel can be either light or audio channel. The device relationship information is stored on Blockchain, which is resistant to collusion and single point failure of the centralized server. We implemented the proposed authentication scheme with emulator devices that have similar computational resources as real IoT devices and commercial Blockchain platform. The performance of the emulator devices running Blockchain tasks is evaluated. The experimental results indicate that the CPU and memory overheads are well acceptable, considering they occur only during the authentication phase.

Acknowledgement

This publication was made possible in parts by NPRP grant #8-408-2-172 from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors.

References

[1] "Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015," http://www.gartner.com/newsroom/id/3165317.
[2] Wikipedia, "Mirai," https://en.wikipedia.org/wiki/Mirai_(malware), 2016.
[3] Swati Khandelwal, "New iot botnet malware discovered; infecting more devices worldwide," 2016.
[4] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, "Smart nest thermostat: A smart spy in your home," in *Black Hat USA*, 2014.
[5] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1250–1258, Oct 2017.
[6] X. Yao, X. Han, X. Du, and X. Zhou, "A lightweight multicast authentication mechanism for small scale iot applications," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3693–3701, Oct 2013.
[7] D. B. Rawat, M. Garuba, L. Chen, and Q. Yang, "On the security of information dissemination in the internet-of-vehicles," *Tsinghua Science and Technology*, vol. 22, no. 4, pp. 437–445, Aug 2017.
[8] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 24–34, 2007.
[9] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, Oct 2015.
[10] D. B. Rawat, G. Yan, B. Bista, and M. Weigle, "Trust on the security of wireless vehicular ad-hoc networking," *Ad Hoc & Sensor Wireless Networks Journal*, vol. 24, no. 3-4, pp. 283–305, Feb 2014.
[11] X. Du, M. Guizani, Y. Xiao, and H. H. Chen, "A routing-driven elliptic curve cryptography based key management scheme for heterogeneous sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1223–1229, March 2009.
[12] Y. Xiao, H. H. Chen, X. Du, and M. Guizani, "Stream-based cipher feedback mode in wireless error channel," *IEEE Transactions on Wireless Communications*, vol. 8, no. 2, pp. 622–626, Feb 2009.
[13] X. Du, M. Shayman, and M. Rozenblit, "Implementation and performance analysis of snmp on a tls/tcp base," in *IEEE/IFIP International Symposium on Integrated Network Management*, May 2001.
[14] X. Du, M. Zhang, K. E. Nygard, S. Guizani, and H.-H. Chen, "Self-healing sensor networks with distributed decision making," *International Journal of Sensor Networks*, vol. 2, no. 5-6, pp. 289–298, 2007.
[15] S. Liang and X. Du, "Permission-combination-based scheme for android mobile malware detection," in *2014 IEEE International Conference on Communications (ICC)*, June 2014, pp. 2301–2306.
[16] X. Du and D. Wu, "Adaptive cell relay routing protocol for mobile ad hoc networks," *IEEE Transactions on Vehicular Technology*, vol. 55, no. 1, pp. 278–285, Jan 2006.
[17] X. Du and H. h. Chen, "Security in wireless sensor networks," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 60–66, Aug 2008.
[18] W. Chang, J. Wu, C. C. Tan, and F. Li, "Sybil defenses in mobile social networks," in *2013 IEEE Global Communications Conference (GLOBECOM)*, Dec 2013, pp. 641–646.
[19] A. Burns, L. Wu, X. Du, and T. Ge, "A novel traceroute-based detection scheme for wi-fi evil twin attacks," in *IEEE Global Communications Conference (GLOBECOM)*, 2017.
[20] W. Chang, J. Wu, and C. C. Tan, "Wormhole defense for cooperative trajectory mapping," *IJPEDS*, vol. 27, pp. 459–480, 2012.
[21] C. Fu, T. Kezmane, X. Du, Y. Fu, and C. Morrisseau, "An location-aware authentication scheme for cross-domain internet of thing systems," in *International Conference on Computing, Networking and Communications (ICNC)*, 2018.
[22] W. Chang and J. Wu, "A survey of sybil attacks in networks," *Sensor Networks for Sustainable Development*, pp. 497–534, 2014.
[23] "Hackers found 47 new vulnerabilities in 23 iot devices at def con," http://www.csoonline.com/article/3119765/security/hackers-found-47-new-vulnerabilities-in-23-iot-devices-at-def-con.html.
[24] "Akamai finds longtime security flaw in 2 million devices," https://www.wired.com/2016/10/akamai-finds-longtime-security-flaw-2-million-devices/.
[25] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[26] A. Aboshosha, K. ElDahshan, E. Elsayed, and A. Elngar, "Multi-channel user authentication protocol based on encrypted hidden ot," *International Journal of Computer Science and Information Security (IJCSIS)*, 2015.
[27] S. Mizuno, K. Yamada, and K. Takahashi, "Authentication using multiple communication channels," in *Workshop on Digital Identity Management*, 2005.
[28] C. Garman, M. Green, and I. Miers, "Decentralized anonymous credentials," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2014.
[29] P. H. Griffin, "Security for ambient assisted living: Multi-factor authentication in the internet of things," in *IEEE Globecom Workshops*, 2015.
[30] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.