2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems

Securing Smart Cities Using Blockchain Technology

Kamanashis Biswas
School of Information & Communication Technology
Griffith University, Gold Coast, Australia
Email: kamanashis.biswas@griffithuni.edu.au

Vallipuram Muthukkumarasamy
Institute for Integrated & Intelligent Systems
Griffith University, Gold Coast, Australia
Email: v.muthu@griffith.edu.au

***Abstract*—A smart city uses information technology to integrate and manage physical, social, and business infrastructures in order to provide better services to its dwellers while ensuring efficient and optimal utilization of available resources. With the proliferation of technologies such as Internet of Things (IoT), cloud computing, and interconnected networks, smart cities can deliver innovative solutions and more direct interaction and collaboration between citizens and the local government. Despite a number of potential benefits, digital disruption poses many challenges related to information security and privacy. This paper proposes a security framework that integrates the blockchain technology with smart devices to provide a secure communication platform in a smart city.**

***Keywords*-Smart city; Smart device; Blockchain; Security;**

I. Introduction

In recent decades, the world has experienced unprecedented urban growth due to population increase, climate change, and scarcity of resources. Recent research shows that more people dwell in cities (54%) than rural areas (46%) and this number will increase to 66% by 2050 [1]. To cope with these crises, cities are focusing on modern technologies as well as aiming to reduce costs, use resources optimally, and create more liveable urban environment. The significant advancements in IoTs and wireless communications have made it easy to interconnect a range of devices and enable them to transmit data ubiquitously even from remote locations. However, these systems are more instrumented with open data such as locations, personal and financial information, and therefore, must be capable to defend against security attacks. The Kaspersky Lab shows that smart terminals such as bicycle rental terminals, self-service machines, and information kiosks have a number of security flaws [2]. These devices can be exploited by the cybercriminals and they may get access to personal and financial information of the users. It is also worth noting that implementation of traditional security mechanisms into a city's critical infrastructure to make it *smarter* has failed. Thus, new solutions based on the nature of the data (private or public) and communication platforms have to be developed to provide privacy, integrity, and data confidentiality. This paper proposes a security framework based on blockchain technology which allows to communicate the entities in a smart city without compromising privacy and security.

II. Security Threats

Due to the heterogeneous nature of resource constrained devices, a smart city is vulnerable to a number of security attacks. It is important to identify those threats and their possible consequences in order to design an effective solution. A number of research has been conducted in this field such as Open Web Application Security Project (OWASP) enlisting common security attacks, Computer Emergency Response Teams (CERT) providing graphical representation of potential vulnerabilities, G-Cloud presenting a series of Cloud Computer Service Provider (CCSP) requirements [3], [4], [5]. The following threat categories are identified for the smart cities: i) *Threats on Availability*- are concerned with the (unauthorised) upholding of resources, ii) *Threats on Integrity*- include unauthorized change to data such as manipulation and corruption of information, iii) *Threats on Confidentiality*- include disclose of sensitive information by unauthorized entity, iv) *Threats on Authenticity*- are concerned with gaining unauthorized access to resource and sensitive information, and v) *Threats on Accountability*- include denial of transmission or reception of a message by the corresponding entity.

III. The Proposed Security Framework

A. Blockchain Technology

Blockchain is a peer-to-peer distributed ledger technology which records transactions, agreements, contracts, and sales [6]. Originally developed to support crypto-currency, blockchain can be utilized for any form of transactions without an intermediary. The benefit of blockchain is that an attacker has to compromise 51% of the systems to surpass the hashing power of the target network. Thus, it is computationally impractical to launch an attack against the blockchain network. The following example demonstrates working procedures of the blockchain technology.

Let *A* and *B* be two entities in a blockchain based parking system and *A* is paying parking fee to *B*, the parking authority. This transaction is represented online as a block including information such as block number, proof of work, previous block, and transaction records and this block is broadcast to every entity in the network. The other entities verify the block and if more than 50% of the entities approve

978-1-5090-4297-5/16 $31.00 © 2016 IEEE
DOI 10.1109/HPCC-SmartCity-DSS.2016.178

the block then the transaction is confirmed and added to the chain. After that, the fee is transferred from entity *A* to authority *B*'s account.

B. Security Framework

1) Physical Layer: As shown in Fig. 1, smart city devices are equipped with sensors and actuators which collect and forward data to the upper layer protocols. Some of these devices such as Nest thermostat and Acer Fitbit are vulnerable to security attacks due to lax encryption and access control mechanisms [7]. Further, there is no single standard for smart devices so that the data generated by them can be shared and integrated to provide cross-functionality. Vendors require an agreed-upon implementation and communication standards to overcome these problems in smart devices.

2) Communication Layer: In this layer, smart city networks use different communication mechanisms such as Bluetooth, 6LoWPAN, WiFi, Ethernet, 3G, and 4G to exchange information among different systems. The blockchain protocols need to be integrated with this layer to provide security and privacy of transmitted data. For example, the transaction records can be converted into blocks using telehash which can be broadcast in the network. Protocols like BitTorrent can be used for peer to peer communication whereas Ethereum can provide smart contract functionalities. However, integration of existing communication protocols with blockchain is a major challenge since the requirements vary from application to application. A potential solution can be implementing multiple blockchains with the help of a blockchain access layer to provide application specific functionalities.

3) Database Layer: In blockchain, distributed ledger is a type of decentralized database that stores records one after another. Each record in the ledger includes a time stamp and a unique cryptographic signature. The complete transaction history of the ledger is verifiable and auditable by any legitimate user. There are two different types of distributed ledger in practice: i) permissionless and ii) permissioned. The key benefits of permissionless ledger are that it is censorship-resistant and transparent. However, the public ledger has to maintain complex shared records and it consumes more time to reach the consensus compared to the private ledger. Further, public ledgers may also be subjected to anonymous attacks. Therefore, it is recommended to use private ledgers to ensure scalability, performance, and security for realtime applications like traffic systems in a smart city.

4) Interface Layer: This layer contains numerous smart applications which collaborate with each other to make effective decisions. For example, a smart phone application can provide location information to the smart home system so that it turns on the air conditioner 5 minutes prior to reach at home. However, the applications should be integrated carefully since vulnerabilities in one application may give intruders access to other dependent processes.

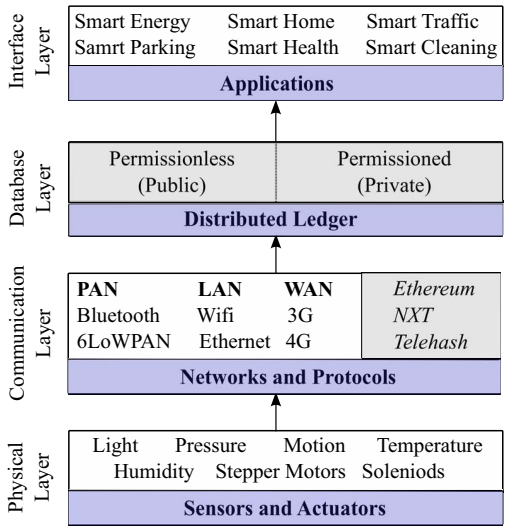

Figure 1: Smart city security framework

IV. Conclusion

This paper proposes a blockchain based security framework to enable secure data communication in a samrt city. The main advantage of using blockchain is that it is resilient against many threats. Further, it provides a number of unique features such as improved reliability, better fault tolerance capability, faster and efficient operation, and scalability. Thus, integration of blockchain technology with devices in a smart city will create a common platform where all devices would be able to communicate securely in a distributed environment. The future works will aim to design a system level model in order to investigate the interoperability and scalability of different platforms used in a smart city.

Acknowledgment

This research is partially funded by the Institute for Integrated and Intelligent Systems, Griffith University.

References

[1] United Nations, *World Urbanization Prospects: The 2014 Revision, Highlights (ST/ESA/SER.A/352)*, Dept. of Economic and Social Affairs, ISBN: 978-92-1-151517-6, pp. 1–32, 2014.

[2] D. Makrushin and V. Dashchenko, *Fooling the 'Smart City'*, Technical Report, Kaspersky Lab, pp. 1–22, Sep. 2016.

[3] OWASP Foundation, *OWASP Top 10-2013: The the Most Critical Web Application Security Risks*, 2013.

[4] W. R. Claycomb and A. Nicoll, *Insider Threats to Cloud Computing: Directions for New Research Challenges*, in 36th Annual Computer Soft. and Appl. Conf., pp. 387–394, 2012.

[5] HMGovernment, *Government cloud strategy*, pp. 1–24, 2011.

[6] K. Christidis and M. Devetsikiotis, *Blockchains and Smart Contracts for the IoTs*, IEEE Access, Special section on the plethora of Research in IoT, pp. 2292–2303, 2016.

[7] M. Selinger, *Test: Fitness wristbands reveal data*, Test AV-TEST GmbH, Klewitzstr, Germany, pp. 1–7, Jun. 2015.