Quantum1Net, The Smart City and IoT

In this paper we will be looking in to the opportunities that Quantum1Net offers Smart City development, specifically we will be looking in to security and hacking, privacy, infrastructure, and ease of use.

INTRODUCTION

Smart Cities contain large amounts of Internet of Things (IoT) devices that generate, process, and exchange vast amounts of critical data as well as privacy-sensitive information, and hence are appealing targets of various cyber-attacks.
Many new networkable devices, which constitute the IoT, are low energy and lightweight. These devices must devote most of their available energy and computation to executing core application functionality, making the task of affordably supporting security and privacy quite challenging. Traditional security methods tend to be expensive for IoT in terms of energy consumption and processing overhead.

Moreover, many of the state-of-the-art security frameworks are highly centralized and are thus not necessarily well-suited for Smart cities due to the difficulty of scale, many-to-one nature of the traffic, and single point of failure. To protect user privacy, existing methods often either reveal noisy data or incomplete data, which may potentially hinder some Smart cities applications from offering personalized services. Consequently, Smart Cities demands a lightweight, scalable, and distributed security and privacy safeguard. The Open Source technology that underpins Quantum1Net (Q1N) the first decentralized service system, has the potential to overcome aforementioned challenges as a result of its distributed, secure, and private nature.

Users on Q1N that are known by a quantum computer enhanced hacking safe changeable Public Key (PK), discussed in detail in [1] and in [2], that is used as an identifier for to the network to transfer information. These transactions are pushed into a block by users. Once a block is full, the block is appended to the Q1N Blockchain by performing a minting process. To mint a block, some specific nodes known as minters agree on whom in the Network has contributed the most in the latest block, contribution is calculated from shared computing power and network data relaying, and the node that is chosen mints the new block to the Q1N Blockchain. This novel approach to Blockchain storage, is not wasteful in anyway and uses as Proof-of-Work, the actual work in processing and transfer that a Node is contributing to Q1N, to keep the Network fully autonomous, the incentive of the minting will need to be adapted in amount to fit the current number of nodes and services running in the Smart City.

The Q1N framework is service and application agnostic through use of Service Manifests, and can be applied in any Smart City contexts. The design consists of three core tiers that are: smart home, decentralized storage, and overlay. Smart devices are located inside the smart home tier and connected to the Q1N and managed over the Network. Nodes constitute an overlay network along with storages, and can run on users' smartphones or personal computers. The overlay network is akin to the peer- to-peer network in Bitcoin and brings the distributed feature to our architecture. To decrease network overhead and delay, nodes in the overlay are grouped into clusters that can sign for transactions of data inside their own cluster, but needs to reach out to other clusters for transactions between clusters.

Q1N maintain a public overview of the key lists of Q1N. These key lists are: requester key lists that is the list of Q1N users Private Keys that are allowed to access data for the smart homes connected to a cluster; requested key lists that is the list of Public Keys of smart homes connected to a cluster that are allowed to be accessed. Storage is used by the minting devices to store and share data.

This paper's contribution is to give a comprehensive discussion on the details of how Q1N can be used to overcome all challenges with Smart City deployments using a smart home as an example. We first outline how the IoT devices are initialized and then explain how transactions are processed. A local and private embedded Blockchain is employed for providing secure access control to the IoT devices and their data. The Blockchain generates an immutable time-ordered history of transactions that is linkable to other tiers for giving specific services.

The design security comes from diverse features including:
(1) indirectly accessible devices; and
(2) different transaction structures in the smart home and the overlay network, as the home chain is private and embedded in the main chain of the overlay network.

To achieve a lightweight quantum computer enhanced hacking security, we developed a security system in-house, described in detail in [1] and [2]. We provide qualitative arguments to demonstrate that the Q1N connected smart home achieves confidentiality, integrity, and availability and also discuss how key security attacks such as linking attack and Distributed Denial of Service (DDOS) are thwarted. Finally, we present quantitative results using simulations and show that the overheads induced by Q1N are relatively small.

The rest of the paper is organized as follow:
In Section II we present the main components of the Q1N.
The Q1N based smart home is discussed in depth in Section III.
Simulation results and security discussions are presented in Section IV.
Section V summarizes related works, and finally Section VI concludes the paper.

II. CORE COMPONENTS

This section discusses the main smart home components as shown in Figure XXX.

A. Transactions

Communications between local devices or overlay network nodes are known as transactions. There are multiple different transactions defined by the service manifest used in the Q1N based smart home, each designed for a specific function.
Store transaction is generated by devices to store data.
An access transaction is generated by a device or the home owner to access the cloud storage.

A monitor transaction is generated to periodically monitoring device information. Adding a new device to the smart home is done via a rooting transaction and a device is removed via a remove transaction.

All of the aforementioned transactions use a shared key to secure the communication. Lightweight hashing is employed to detect any change in transactions' content during transmission. All transactions to or from the smart home are stored in a local private embedded Blockchain.

B. Embedded Blockchain

The Q1N Blockchain in Blockchain solution, embeds a private chain in the main chain and therefore gain the benefit of all Network contribution on the main chain.

For each smart home, there is a private embedded Blockchain that keeps track of transactions and has a service manifest to enforce users' policy for incoming and outgoing transactions. Starting from the rooting transaction, each device's transactions are chained together as an immutable ledger in the embedded BC. Each block in the embedded BC contains two headers that are block header and service header. The block header has the hash of the previous block to keep the embedded BC immutable. The service header points to the service manifest that is used for authorizing devices and enforcing owner's control policy over his home.

The policy part of a smart home service manifest has four parameters.

The Requester parameter refers to the requester Public Key in the overlay transaction. For local devices, this field is equal to the Device_ID in the first column of the proposed policy descriptors.

The second column of the policy descriptors, indicates the requested action in the transaction, which can be: store to store data in the cloud storage, access to access stored data of a device, and monitor to access real-time data of a particular device. The third column in the policy descriptors is the ID of a device inside the smart home, and finally, the last column indicates the action that should be done for the transaction that matches with the previous properties.

C. Local Storage

Local storage is a storing device e.g. backup drive that is used by devices to store data locally. This storage can be setup through the service manifest as a separate device, and can be used to store information and files as video recordings and other data locally and be retrieved using the Private Blockchain.

III. THE Q1N-BASED SMART HOME

First, we discuss the initialization steps, transactions handling, and shared overlay.

A. Initialization

In this section, we describe the process of adding devices and policy's for the private BC. To add a device to the smart home, the user App generates a rooting transaction by sharing a key with the device. The shared key between the miner and the device is stored in the rooting transaction. As for defining policy descriptor, the home

owner generates its own policies according to our proposed policy structure and adds the policy descriptors to the service manifest. The platform uses the policy descriptors in the latest service manifest referenced in the private BC; therefore, to update the policy the owner should update the latest service manifest.

B. Transaction Handling

The smart devices may communicate directly with each other or with entities external to the smart home. Each device inside the home may request data from another internal device to offer certain services, e.g., the light bulb requests data from the motion sensor to turn on the lights automatically when someone enters the home. To achieve user control over smart home transactions, a shared key should be allocated to devices which need to directly communicate with each other. To allocate the key, checks the policy descriptor or asks for permission from the owner and then distributes a shared key between devices. After receiving the key, devices communicate directly as long as their key is valid. To deny the grant permission, the distributed key can be marked as invalid by sending a control message to devices. The benefits of this method is twofold: on one hand, the the owner has a list of devices that share data, and on the other, the communications between devices are secured with a shared key. Storing data on the local storage by devices is the other possible transaction flow inside the home. To store data locally, each device needs to be authenticated to the storage that is done using a shared key. To grant the key, the device needs to send a request and if it has storing permission, the owner generates a shared key and sends the key for the device and the storage. By receiving the key, the local storage generates a starting point that contains the shared key. Having the shared key, the device can store data directly in the local storage.

The devices may demand to store data on the cloud storage that is known as store transaction. Storing data in the cloud is an anonymous process. To store data the requester needs a starting point that contains a block-number and a hash used for anonymous authentication purpose. The cloud storage may be either owned and managed by the SP (e.g. Nest thermostat) or paid for and managed by the home owner (e.g. Dropbox). In the former instance, the owner requests for the starting point by generating a signed transaction with the device key. In the latter case, payment is done through Quantum1Net. In either storage type, after receiving a request the storage creates a starting point and sends it to the owner. When a device needs to store data on the cloud storage, it sends data and the request to the owner's service manifest. By receiving the request, the owners service manifest authorizes the device for storing data on the cloud storage. If the device has been authorized, the miner extracts the last block-number and hash from the local BC, and creates a store transaction and sends it along with the data to the storage. After storing data, the cloud storage returns the address to the service that is used for further storing transactions.

The other possible transactions are access and monitor transactions. These transactions are mainly generated by either the home owner to monitor the home when he is outside or buy Service Providers to process devices' data for personalized services. By receiving an access transaction from nodes in the overlay, the service manifest checks whether the requested data is on the local or the cloud storage. If data is stored in the local storage, the service manifest authorizes the requests data from the local storage and sends it to the requester. On the other hand, if the data is stored in the cloud, the service manifest either authorizes the requests data from the cloud storage and sends it to the requester, or sends the service address and hash to the requester. The latter scenario empowers the requester to read entire data stored by the device in cloud storage and is suitable when the stored data are for a unique device. Otherwise, the user's privacy might be endangered as part of a linking attack which is discussed later in Section IV.

By receiving a monitor transaction, the service manifest sends current data of the requested device to the requester. If a requester is allowed to receive data for a period of time then the service manifest sends data periodically until the requester sends a close request to the service manifest and abolish the transaction. The monitor transaction enables home owners to watch cameras or other devices in which send periodic data. In order to avoid overhead or possible attacks, the owner should define a threshold in minutes for the periodic data. If the time in which the service manifest is sending data for the requester reaches to the threshold, then the connection is terminated by the service manifest.

IV. EVALUATION AND ANALYSIS

This section provides a complete discussion on the security, privacy, and performance of the Q1N-based smart home.

A. Security Analysis

There are three main security requirements that need to be addressed by any security design, namely: Confidentiality, Integrity, and Availability.
Confidentiality makes sure that only the authorized user is able to read the message. Integrity makes sure that the sent message is received at the destination without any change, and availability means that each service or data is available to the user when it is needed.
Employed methods to achieve the first two requirements are discussed in Section III. To increase smart home availability devices are protected from malicious requests. This is achieved by limiting the accepted transactions to those entities with which each device has established a shared key. Transactions received from the overlay network are authorized by the service manifest before forwarding them on to the devices. Furthermore, it can be argued that the Q1N platform only introduces a marginal increase in the transaction processing delays as compared to existing products. There is also an additional one-time delay during initialization for generating and distributed shared keys. In summary, the additional delays are not significant and do not impact the availability of the smart home devices.

Next, we analyze the effectiveness of our solution to prevent two critical security attacks that are particularly relevant for smart homes. The first one is Distributed Denial of Service (DDOS) attack in which the attacker uses several infected IoT devices to overwhelm a particular target node. Several recent attacks have come to light which have exploited IoT devices to launch massive DDoS attacks. The second is a linking attack in which the attacker establishes a link between multiple transactions or data ledgers with the same Public Key to find the real-world ID of an anonymous user. This attack endangers users privacy.

DDOS attack: Our design has a hierarchical defense against this attack. The first level of defense can be attributed to the fact that it would be impossible for an attacker to directly install malware on smart home devices since these devices are not directly accessible. All transactions have to be checked by the service manifest. Let us for a moment assume that the attacker somehow still manages to infect the devices. The second level of defence comes from the fact that all outgoing traffic has to be authorized by the service manifest by examining the policy descriptors. Since the requests that constitute the DDoS attack traffic would not be authorized, they would be blocked from exiting the home. The next two defense layers are specially designed and managed by the target of DDOS attack that can be any user in the overlay network. These defense layers, that are granting permission by using Service Manifest key lists and changing the Public Key in the Service manifest key lists, stops all foreseeable DDoS attacks

Linking attack: To protect against this attack, each device's data is shared and stored by a unique key. The Service Manifest retains a record for each device using a different Public Key. From the overlay network point of view, the Service Manifest should use a unique key for each transaction.

B. Performance Evaluation

Q1N based architecture incurs computational and packet overhead on the smart home devices and the service manifest for providing improved security and privacy.

The discussion on the evaluation is as follows:
Packet overhead: Using encryption and hashing increases the packets payload size; however, considering the lower layer headers, the increase in the data payload has relatively small effect.
Time overhead: The Q1N-based design consumes more time to process packets compared to the base method which can be attributed to the additional encryption and hashing operations. In the worst case for the query-based store transaction the additional overhead introduced by our method is 20ms, which is still small.

In summary, the low overheads introduced by Q1N-based method significantly outweigh given the significant security and privacy benefits on offer.

VI. CONCLUSION

Smart City and IoT security is gaining a lot of attention these days from both academia and industry. Existing security solutions are not necessarily suited for Smart City's due to high energy consumption and processing overhead. Quantum1Net proposes a method that addresses these challenges by leveraging overlay networking and Blockchain technology, which is an immutable ledger of blocks. Quantum1Net's approach was discussed using a smart home as a representative case-study. This paper, outlined the various core components of the smart home tier and discussed the various transactions and procedures associated with it. We also presented an analysis regarding its security and privacy.

REFERENCES

[1] https://quantum1net.com/wp-content/uploads/2018/07/quantum1net-quantum-security-overview.pdf

[2] https://quantum1net.com/wp-content/uploads/2018/07/quantum1net-key-exchange-protocol.pdf