Blockchain Ensured Physical Visitor Access Control and Authentication

Frederick Stock
Kennedy College of Sciences
UMass Lowell
Lowell, USA
frederick_stock@student.uml.edu

Jarel Hearst
TSYS School of Computer Science
Columbus State University
Columbus, USA
hearst_jarel@columbusstate.edu

Yesem Kurt Peker
TSYS School of Computer Science
Columbus State University
Columbus, USA
peker_yesem@columbusstate.edu

***Abstract*— In this study we explore the use of blockchain with IoT devices to provide visitor authentication and access control in a physical environment. We propose a "bracelet" using a NodeMCU that transmits visitor location information and cannot be removed without alerting a management system. Our results show that the proposed system has noticeable improvements over a similar system proposed last year, increasing the practicality of implementing such a system**

Keywords—blockchain, authentication, access control

I. Introduction

Blockchain is a decentralized, digital ledger first introduced in 2008 as a transaction ledger for the cryptocurrency Bitcoin. A blockchain consists of a series of "blocks" which can be thought of as pages in a traditional physical ledger. Each block is cryptographically linked such that a change to one block requires changing every following block. This makes blockchain systems tamper-resistant no matter what credentials the modifying user possesses; thereby protecting stored data from outsiders as well as insider threats. A blockchain is distributed across a peer-to-peer network consisting of devices called nodes. Many nodes on the network store the ledger. If several of these devices cease functioning, the network can run without a noticeable impact on performance or security.

In this study we use a private blockchain, instead of a typical central database, to store the data of visitors at a physical site. The stored data is for authentication as well as controlling access to different regions of the site. There are three main advantages of blockchain over a centralized database: 1. Tamper resistance; 2. Immediate shared access to records, and 3. Fault tolerance. Although our current work models one physical site with several nodes, the advantages of using a blockchain for visitor authentication and access control would be realized when a consortium of sites desire to track users' locations and behavior.

II. Methodology

The system we propose has four main components: Visitor devices, Access points, Blockchain, and a Management system. In this section, we provide a diagram of the system in Figure 1 and describe the functionality of each component.

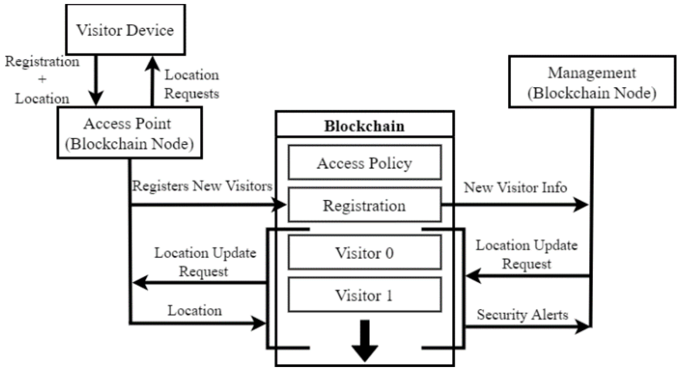

Fig. 1. System arhitecture

1) Visitor Devices

A visitor device is primarily responsible for reporting an assigned visitor's location. We implemented a bracelet-like system that consists of a nodeMCU and a wire, creating a circuit. This circuit breaks when the device is removed from the visitor's wrist, alerting the management system via a smart contract on the blockchain. The device determines and transmits its locations using nodeMCU's Wi-Fi capabilities and the Google Geolocation API. We propose that visitors are given these devices when entering the monitored area. The device computes the location periodically and sends it to the blockchain when requested by the management system. Possession of the device by its visitor can be assumed until an alert is received that the device has been removed. If possession of the device is still ensured, transmitted locations can be assumed to be the true location of the visitor. All transactions from the device are authenticated with a hash chain created and stored on the visitor device. In a hash chain, a random value is hashed repeatedly and the final hash is published. The device is authenticated using these hash values in reverse order. For example, the first message is signed with the second to last hash. The second to last hash is then published. Then the third to last is used to sign the next, et cetera.

2) Access Points

Access points are what the visitor device uses to send information to the blockchain. Access points serve as nodes on the blockchain. The visitor devices are assumed to be simple,

This research was supported by the U.S. National Science Foundation under grant award # 195041.

cheap devices and hence are assumed to not have the capability to directly interact with the blockchain.

3) Blockchain

In our system blockchain serves both as a database and an access control system. We use a private Ethereum blockchain with the Clique consensus algorithm. Clique is a proof of authority algorithm. The access control functionality in our system is implemented via smart contracts on the blockchain. Smart contracts are pieces of code deployed to the blockchain and can be executed to perform operations on the blockchain. There are three smart contracts in our system: Registration Contract (RC), Visitor Contract (VC), and Access Policies Contract (APC). RC is executed when a new visitor enters the monitored area. It authenticates registration requests and creates a new instance of the VC. An instance of a VC stores all the data for one specific visitor. It stores the access level for the visitor which determines the locations of the monitored area the visitor is allowed to enter. It also records each location the visitor's device has submitted to the chain. The final contract, APC, maintains access levels for locations. The levels are mapped to physical locations identified by latitudes and longitudes. When a visitor submits a new location, this contract verifies the submitted location is an allowed location for the visitor based on the visitor's access level.

4) Management System

The management system reads events from the blockchain, recording new visitors entering the monitored area, requesting visitors update their location regularly, and alerting security of any visitors who do not update their location within a certain time or are in unauthorized locations.

III. Results

We collected data on three aspects of our system: 1. The time to register a new visitor, 2. The time to update a visitor's location, and 3. The storage required of the system. These metrics allowed us to compare our system to the system presented in [1]. Instead of using our physical prototype, we simulated the actions of visitors with JavaScript code, a similar method to that used in [1]. Unless specified otherwise, data was collected with a trial of 10 simulated visitors running for 10 minutes, updating their location once every minute.

These experiments were conducted with two full nodes on our blockchain. One ran on a laptop with an Intel i7-11375H with a clock speed of 3.30 GHz, and the other on a Raspberry Pi 400 which has a Broadcom BCM2711 quad-core Cortex-A72 running at 1.8 GHz. The Raspberry Pi also served as an access point, running a Python flask server in addition to its blockchain node. The laptop served as the management system, running a JavaScript file in addition to the blockchain node. The laptop also ran the scripts for the simulated visitors.

A. Registration Time

Registration time is measured as the time it takes from the start of a visitor device creating its hash chain to the detection of a new visitor contract by the management system. The average registration time in our simulation was 155 milliseconds, a little more than 1/90th of the previous system [1] where the registration time was 13.5 seconds.

B. Location Update Time

Location update time was measured as the time elapsed from when a request by the management system to a visitor to update their location is sent, to when the management system receives the confirmation from the blockchain of a successful update. Our results indicate that the number of visitors, as well as the frequency of requests, has a direct relationship with the time of an update request.

C. Data Storage

To measure the data used by our system we recorded how much the "chaindata" folder in our blockchain's data directory grew for 10 visitors in 10 minutes, with updates every minute. We compared this data to that recorded in an identical manner in [1]. We then took this data and multiplied by 6 to get an estimate for one hour of use, and then by 24 to get an estimate for an entire day. Our system used 475,027 bytes for an estimated usage of 65.23 MB for 24 hours. The earlier study [1] measured 243,040 bytes for an estimate of 33.37 MB per 24 hours, which is almost half of the system our system uses. We are currently investigating how we can improve the storage usage in our system.

IV. Future Work and Conclusion

In this study, we propose a system that deploys blockchain technology for physical visitor access control. The proposed system improves over earlier work in registration time, location update time, and implementation. In particular, we constructed a physical visitor device that should be cheaper and easier to build than that proposed in [1], which used a fingerprint scanner to prove a visitor's possession of the device. Future work in this study involves investigating the storage needed by the system and exploring ways to reduce it. We also plan to test and improve the prototype bracelet to get "real-world" data and build a system that can be used in practice.

Acknowledgment

We would like to thank Dr. Alfredo Perez, the PI of the REU Site at Columbus State University for the opportunity he provided us to work on this project.

References

[1] K. Y. Chan, M. Lovett, and Y. K. Peker, "Private blockchain for visitor authentication and access control," 2021 IEEE International Conference on Big Data (Big Data), 2021.