ISSN 2395-1621

IOT Based Secure Smart City Architecture Using Block Chain

Prof.Rajkumar Bhosle, Sagar Tupe, Shubham Khemnar, Abhijit Musmade, Harshal Dhone

bhos_raj@rediffmail.com,
sagartupe7028@gmail.com,
shubhamkhemnar1@gmail.com,
abhimusmade@gmail.com,
harshaldhone99@gmail.com

Department of Information Technology, AVCOE Sangamner,
SavitribaiPhule Pune University,Maharashtra.

ABSTRACT

Standard security protocols like SSL, TLS, IPSec etc. have high memory and processor consumption which makes all these security protocols unsuitable for resource constrained platforms such as Internet of Things (IoT). Blockchain (BC) finds its efficient application in IoT platform to preserve the five basic cryptographic primitives, such as confidentiality, authenticity, integrity, availability and non-repudiation. Conventional adoption of BC in IoT platform causes high energy consumption, delay and computational overhead which are not appropriate for various resource constrained IoT devices. This work proposes a machine learning (ML) based smart access control framework in a public and a private BC for a smart city application which makes it more efficient as compared to the existing IoT applications. The proposed IoT based smart city architecture adopts BC technology for preserving all the cryptographic security and privacy issues. Moreover, BC has very minimal overhead on IoT platform as well. This work investigates the existing threat models and critical access control issues which handle multiple permissions of various nodes and detects relevant inconsistencies to notify the corresponding nodes. Comparison in terms of all security issues with existing literature shows that the proposed architecture is competitively efficient in terms of security access control.

ARTICLE INFO

Article History

Received: 6th June 2020

Received in revised form :

6th June 2020

Accepted: 9th June 2020

Published online :

10th June 2020

I. INTRODUCTION

Network technology and increasing number of smart devices makes IoT very relevant for research exploration. Conversely the existing literature survey notices that IoT platform still suffers from privacy and security vulnerabilities . The centralized architecture and less resource availability in most of the IoT devices have made the conventional security and privacy preservation approaches inappropriate for IoT platforms. The decentralized security and privacy on IoT applications can be facilitated by blockchain technology but conventional blockchain approaches have significant energy consumption, latency and execution overhead which are improper for most resource budgeted IoT platforms. This research exploration studies how the blockchain becomes lightweight and suitable for IoT based smart city applications with smart ML based access control. A decentralized capability based access control approach to control access of sensitive information. This proposed method has high latency and overhead and also compromised with user privacy. TLS and IPSec protocols for sensor data authentication and privacy but these approaches are very resource expensive for IoT platform.

II. PROBLEM STATEMENT

In this paper we are going to capture the images at the junction on roads. The captured image is transferred with the help of block chain. By using 'Machine Learning' and 'Image Processing' we count the number of vehicles. According to the basics of the traffic we set dynamically time for the signals by using linear regression algorithm.

III. OBJECTIVES

To preserve five basic cryptographic primitives,
1.Aunthenticity
2.Integrity
3.Confidentiality
4.Availability
5.Non-repudiation for IoT architecture using blockchain.
-Considering the issues of the low computational budget of IoT platform.

IV. MOTIVATION

Lightweight in terms of computation and Efficient resource usage. The decentralized security and privacy.

V. LITERATURE SURVEY

The author Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan. Smart contract-based access control for the internet of things. In this paper The authors of [1] proposed a smart contract-based access control framework, which has multiple access control contracts, one register contract and one judge contract. This framework was proposed to attain distributed and trustworthy access control for IoT applications. This proposal talks about access control algorithm which grants the permission of subject and object by checking its access control header and charges a blocking time as a penalty if any time related inconsistency is detected[1].

The author Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. The authors proposed an access control which is based on policies and it combines different types of attributes, like node attributes, objects like nodes that holds resources attributes etc. All these attributes set certain conditions for access rights grants to nodes. It validate access rights of nodes that are usually performed by a centralized entity which implies an issue of single point of failure[2].

The authors Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman. Fairaccess: a new blockchain-based access control framework for the internet of things. Security and communication.have implemented smart contract using blockchain technology to achieve distributed trust and privacy of IoT platform. Additionally blockchain utilizes resources of all participating nodes to address scalability and robustness which decrease many-to-one traffic flows. As a result it solves the issue of single point failure and delay issues. The inherent anonymity of blockchain is appropriate for IoT applications where the identity of the users is kept private. Blockchain technology serves a trustful network over dishonest nodes which is appropriate in IoT platforms where huge number of heterogeneous devices are interconnected[3].

VI. SYSTEM ARCHITECTURE

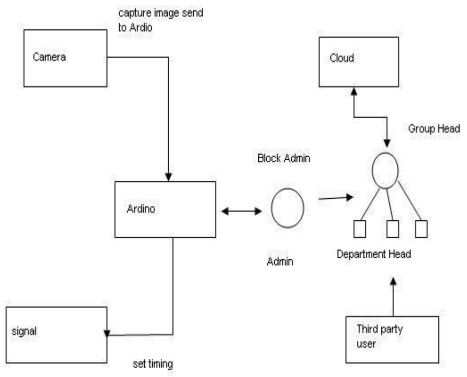

Fig 1. System Architecture

The whole architecture can be divided into 3 different parts, such as smart block, canopy network and cloud storage. The detail description of these three parts are stated below.

A. Smart Block

A city is divided into small blocks which are called *smart block*. Each *smart block* consists the variety of sensors like camera, the rmostat, LDR etc. All of these sensor mounted devices are owned by a *block admin*, who has permissible access to all of these smart devices. The *block admin* maintains a private blockchain to store various information generated from devices. Unlike the blockchain of bitcoin whose management is decentralized, here the local BC is centrally controlled by its *block admin*. All the transactions from the devices or by the devices are chained together by the *block admin*. The *block admin* is responsible for adding new devices or removing an existing device by deleting it's from the ledger. It is to be noted that the addition of device transaction will be similar to 'create coin' transaction in bitcoin. The local BC has an access header, which allows the *block admin* to control all transactions occurring in it's block. All the information transactions of smart devices are possible only if the *block admin* permits them to do so. The permissions of the transactions could be possible by sharing a shared key using the Diffie-Hellman algorithm key exchange algorithm. While all blocks in blockchain have an access header, the most updated one, placed in the header of the last block, is used for checking. The proposed private blockchain avoids PoW or other puzzles to reduce the associated overheads. The user adds a pointer to the previous block copies the policy in the previous block header to the next new block and chains the block to the blockchain. The difference with bitcoin technology is that when a transaction is added to a block, it is treated as an honest transaction, whether the block is mined or not. It is t be noted that a private blockchain is configured to perform not only user authentication but also mutual authentication between devices, generating and securely recording operation details and scenario-based IoTcontracts. In each smart block, there will be local storage for storing data and a list of public keys to give others permission to access smart block data.

B. ***Canopy Network***

The canopy network is peer to peer network which consists of smart blocks, and other users like local police stations or state public administrative bodies. To reduce network overheads, nodes in the canopy network are grouped in clusters and each group elects a Group Head (GH). Each GH maintains a public blockchain. The GHs holds the public key list of requesters who are allowed to access data for the smart blocks connected to this group. The GHs also maintains public keys of requestees of smart blocks connected to this group that is allowed to be accessed.

C. Cloud

The cloud is also a member of GH. In some cases, devices of the smart block may want to store it's data in the cloud. Those data should be accessed by the third party to provide some certain services to the smart devices. For an example say few other states organizations or few central organizations want to access the data of smart blocks, they can read or in certain cases can write those through cloud storage. All the communications in local devices and canopy nodes are tagged as transactions. Five types of transactions may occur in this proposed platform. If the devices inside the smart block want to store its data in the local storage of *block admin* or in the cloud, it will be termed as Write transaction. The read transaction will be coined if other states/central organization or *block admin* want to access cloud data. If other states/central organization or *block admin* want monitor device data directly a monitor transaction will be generated. Adding a new device to the smart block is done by a genesis transaction and a device is removed by a remove transaction. It is to be noted that all the transaction to or from the smart block will be stored in the local blockchain. All the above 5 transitions will use shared key to encrypt their communication. The data integrity issue will be managed by lightweight hashing technique. The whole smart city architecture including smart block, canopy network and cloud storage are stated in fig. 1.

VII. SOFTWARE/HARDWARE REQUIRENMENT

-Hardware Requirements
Input device : Standard Keyboard and Mouse,OV7670 Camera.
Controller Board : Arudino UNO
Other LEDs, HC05 Bluetooth module
Processor : i3 onwards

-Software Requirements
Operating System: Windows, Ubantu
Technology: Python 3, Arduino1.8.5
Database : MySql

VIII. APPLICATIONS

Smart city, smart Home, Smart Agriculture, Public Governance, Military purpose.

IX. CONCLUSION AND DISCUSSION

Standard security protocols are not suitable for IoT application due to its immense time-space requirements. This proposed article modified the architecture of conventional blockchain technology to adopt it in IoT application. The automated code generation for block admin and IoT nodes make the platform user convenient. This architecture preserve authenticity, confidentiality, availability, integrity and non-repudiation. Several standard attacks such as stated in TableIII can be prevented by this ML based smart access controlled blockchain platform used in IoT application. The comparison with existing literature establishes that the proposed architecture is satisfactorily better in terms of few important issue.

REFERENCES

[1] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan.Smart contract-based access control for the internet of things. IEEE Internet of Things Journal, 6(2):1594–1605,April 2019.

[2] Smriti Bhatt, Farhan Patwa, and Ravi Sandhu. Access control model for aws internet of things. In Zheng Yan, Refik Molva, Wojciech Mazurczyk, and Raimo Kantola, editors, Network and System Security, pages 721–736,Cham, 2017. Springer International Publishing.

[3] Aafaf Ouaddah, Anas Abou Elkalam, and Abdellah Ait Ouahman. Fairaccess: a new blockchain-based accesscontrol framework for the internet of things. Security and communication.

[4] A. F. Skarmeta, J. L. HernÃ ˛andez-Ramos, and M. V.Moreno. A decentralized approach for security and privacy challenges in the internet of things. In 2014 IEEE World forium on internet of things(WF-IoT)march2014.

[5] Hannes Gross, Marko Hölbl, Daniel Slamanig, and Raphael Spreitzer. Privacy-aware authentication in the internet of things. In Michael Reiter and David Naccache, editors, Cryptology and Network Security, pages 32–39, Cham, 2015. Springer International Publishing.

[6] A. Ukil, S. Bandyopadhyay, and A. Pal. Iot-privacy: To be private or not to be private. In 2014 IEEE Conference.

[7] Manik Lal Das. Privacy and security challenges in internet of things. In Raja Natarajan, Gautam Barua, and Manas Ranjan Patra, editors, Distributed Computing and internet technology pages33-48 cham 2015 springer international publishing.

[8] Johannes A. Buchmann. Introduction to Cryptography.Springer, 2002