INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 36 ISSUE 1 – MAY 2019 - ISSN: 2349 – 9303

Blockchain Enabled Smart Home Community System

Jayanth P[1]
Department of Computer Science Engineering,
EASA College of Engineering and Technology

S. Sudhakar[2]
Department of Computer Science Engineering,
EASA College of Engineering and Technology

Abstract— Block chain based decentralized security and privacy system provides huge lift for Internet of Things(IoT) infrastructure. In a smart home tier, blockchain acts as a perfect gatekeeper for all incoming and outgoing communication packets. It leverages capability of the system to prevent fundamental security triads such as confidentiality, integrity, and availability. The novel instantiation of blockchain by eliminating the concept of POW relies on hierarchical structure and distributed trust to maintain the security and privacy requirements of IoT. These user-centric models are not effectively utilizing the power of the peer-community interactions. It brings higher level of association among the known groups and helps to share the responsibilities as in a gated community. The new model enriches the traditional novel instantiation with more role or trust-based group identities. This approach enables other trusted communities or local protection authorities to monitor closely and help the affected home in a situation of complete outage of power or collapsed state. Finally, the discussion analyzing the overheads introduced by the variants.

Index Terms— Smart Home, Block Chain, Internet of Things, Drone, Gated Community

I. INTRODUCTION

The Internet of Things(IoT) is an intelligent network of embedded electronic devices, automobiles, home appliances and thousands of sensors and actuators. IoT exchanges vast amounts of critical data and privacy-sensitive information, and usually subjected to cyber-attacks. IoT devices have light-weight cost-effective components which cannot bear with any expensive additional security implications in terms of energy consumption and processing overhead. Blockchain provides efficient decentralized security and privacy approaches for the implementation of Internet of Things (IoT).

Blockchain is ultimately a distributed, immutable log of events. Blockchain enables IoT devices to perform transactions, and to be tracked relative to time and location. Salil S. Kanhere et. al [2] exploring a lightweight instantiation of a BC by eliminating the concepts of Proof of Work (POW) and the distribution of coins. The hierarchical three-tier framework co-ordinate data transactions with blockchain to provide privacy and security for IoT applications. Each smart home has a special equipment called as miner for handling all communications within and external to the home. It preserves a private and secure blockchain, used for controlling and auditing communications. A blockchain based smart home framework lenient to all fundamental aspects of security such as confidentiality, integrity, and availability.

The potential IoT applications with highly personalized services are often constrained with tremendous noises and inconsistency in data. It demands a lightweight, scalable, and distributed security and privacy safeguard. IoT devices have light-weight cost-effective components which cannot bear with any expensive traditional security implications in terms of energy consumption and processing overhead.

The smart home miners usually aligned with single owner instructions. If there is a critical power or network outage happen with home security system, the remote owner cannot be able to monitor the system closely. In such situations, the intruders can cause huge and untraceable loss for the user with in a short time. Also, here can be high chances for burglary attempts in empty homes and nearby homes. These statistics reveals the necessity of interactive community-based home tier system for demoting antisocial activities in the society. This study proposing a comprehensive model for supporting gated community of home tiers which focuses on owner as well as community instructions. The proposed model helps to predict the nearby intrusion attempts effectively.

The remainder of this paper is organized as follows. Section II walks through literature review. Section III presents the proposed system model. Section IV discuss about the evaluation results.

Section V concludes the paper and gives some future works.

II. LITERATURE REVIEW

Ali Dorri et. al. [1] explain the potential benefits of using blockchainin IoT distributed networks. The case study addresses the security and privacy aspects of participating components effectively. The study proposes an upgraded novel instantiation of block chain, with deeper excavation in the smart home tier. Each smart home is equipped with a special miner device for handling all communication within and external to the home. It preserves a private and secure blockchain for controlling and auditing communications and helps to achieve fundamental CIA goals of security. Blockchain significantly reduces the overheads of handling the security and privacy requirements of IoT devices and provide a transparent transactions and procedures for the infrastructure.

Salil S. Kanhere et. al [2] pursue the challenges while implementing block chain as a decentralized security solution for the world of resource constrained IoT devices. The major potholes on the road map mainly due to computationally expensive components and high bandwidth requirements of blockchain. The paper suggests light-weight architecture which eliminates overheads of blockchain. The hierarchical three-tier framework coordinate data transactions with blockchain to provide privacy and security for IoT applications. A qualitative analysis of the architecture highlights the effectiveness of the model in aspects of security and privacy.

Satoshi Nakamoto [3]enlighten the globe with the blockchain technology that underpins the first cryptocurrency system, bitcoin. Bitcoin is a pure electronic peer-to-peer cash system based on digital signatures which allows to make financial transactions without involvement of any financial institution. This paper proposes a hash-based longest chain of proof-of-work(POW) as a solution for the double-spending problem. If majority of CPU power is controlled by honest set of nodes, then computationally impractical to change history of transactions stored as proof-of-work by any attacker.

Antonio F. Skarmeta et. al. [4] provide a concise description of major challenges in the broad scale IoT deployments and propose a distributed capability-based access control mechanism for addressing the critical security and privacy challenges in the IoT applications. The proposed model built on public key cryptography and uses a lightweight token to access to CoAP resources. The smart objects are implemented with Elliptic Curve Digital Signature Algorithm (ECDSA) for handling complex scenarios and challenges.

Chan Hyeok Lee et.al. [5] recommend better approach to protect the personal and device authentication information which may be leaked through proof-of-work process. The proposed smart contract system with Zero-Knowledge Proof (ZKP) technology enhances the anonymity of blockchain and protects privacy of IoT data. The block retrieval mechanism denies the third parties to access user's original data. The smart contracts make transactions convenient and safe.

Jin Hyeong Jeon et. al. [6] introduce Mobius IoT server platform with blockchain to store sensor data, rather than vulnerable Mysql servers. This paper calibrating the various authentication standards arrives at highly productive real-time Ethereum encryption and authentication approach. Moreover the study recommends a smart contract based public fees system service with enhanced security features.

Marco Conoscenti et.al. [7] share the interesting facts about the decentralized IoT applications geared by blockchain and peer-to-peer approaches. The systematic literature review and research investigates the actual use cases of blockchain and its degree of integrity, anonymity and adaptability. The study leverages the blockchain approaches for a private-by-design IoT even with pseudonymity where data produced by devices are not entrusted to centralized companies.

Zhiqing Huang, et. al. [8] provide decentralized solution based on the blockchain for IoT data trusted exchange. The study encourages the blockchain technologies to maintain the reliability trust requirements of IoT data exchange. Trusted trading requirement ensures whole transaction process to get recorded and unchanged by either party once it confirmed. Trusted data access requirement allows the data owner to hold ownership, even after exchange of IoT data. Trusted privacy requirement enables the owner to protect their personal information while performing the data exchange. The final prototype with detailed trust component support smart contract features such as exchange, data and user management contracts.

Nabil Rifi et. al. [9] illustrate blockchain based cloud computing architecture and data access protocol, using smart contracts and publisher-subscriber message queue system. The paper mainly focuses on the feasibility study of implementing a blockchain data access mechanism in the area of IoT in secure way. The solution model basically acts as a contract model between a provider and consumer data controls.

Nikolay Teslya et. al. [10] describe integration of block chain with IoT to solve the interface issues between the smart factory components internally and externally. This way of smart interaction assurance provides enough trust between the participants of IoT, control over the distribution of resources and finished products. The study proposes an architecture as a combination of Smart-M3 information sharing platform and blockchain platform. The architecture uses smart contracts for processing and storing information related to the interaction between smart space components.

Xueping Liang et. al. [11]present the idea of securing drone data collection and communication in combination with a public blockchain for provisioning data integrity and cloud auditing. Instead of registering the drone itself to the blockchain, the proposed system collects hashed data records from drones and generates a blockchain receipt for each data record stored in the cloud, which reduces the burden of moving drones with limited processing capability and enhance security guarantee of the data.This system is capable of providing reliability and accountability, as well as data assurance for real-time data collection and drone control.

C. Tselios et. al. [12]provide an overview of common security issues of SDN when linked to IoT clouds, describes the design principals of the recently introduced Blockchain paradigm and advocates the reasons that render Blockchain as a significant security factor for solutions where SDN and IoT are involved. Software Defined Networking provides efficient entity interconnection for cloud computing infrastructure with dynamic network reconfiguration properties. The research investigates the possibility of utilizing blockchain, a distributed data structure that is used to create a digital transaction ledger and potentially a historical transaction record of massive proportions. This solution will allow encrypted data transfer between interconnected nodes regardless of the network size or its geographical distribution.

Kazım Rıfat Ozyılmaz et. al. [13] discuss about decentralized, trustless architecture for secure and scalable infrastructures to store and process data generated in IoT devices. The research creates a proof-of-concept to enable low-power, resource-constrained IoT end-devices accessing a blockchain-based infrastructure and enforce the use of the smart contracts demonstrated with proof of concept for the application development and data processing.

Pradip Kumar Sharma et. al [14] propose a novel blockchain-based distributed cloud architecture with a Software Defined Networking (SDN) enable controller fog nodes at the edge of the network to achieve fundamental design requirements such as high availability, real-time data delivery, scalability, security, resilience, and low latency. The proposed model is a distributed cloud architecture based on blockchain technology, which provides low-cost, secure, and on-demand access to the most competitive computing infrastructures in an IoT network. The fog nodes are distributed fog computing entities that allow the deployment of fog services and are formed by multiple computing resources at the edge of the IoT network. performance is improved by reducing the induced delay, reducing the response time, increasing throughput, and the ability to detect real-time attacks in the IoT network with low performance overheads. The proposed architecture can significantly reduce the end-to-end delay between IoT devices, computing resources and traffic load in the core network compared to the traditional IoT architecture and is an efficient solution for offloading data to the cloud with minimal overhead.

Bin Liu et. al. [15] discuss about a blockchain-based framework for Data Integrity Service with reliable data integrity verification provided for Data Owners and Data Consumers, without relying on any Third Party Auditor (TPA). The proposed model is more reliable and no single party cloud terminate it. Data Integrity Verification efficiency can be enhanced with increasing number of clients. It supports trading data with data consumers, and implement pay per transaction Data Integrity Service.

David W. Kravitz et. al. [16] discuss about Permissioned Blockchain technology which secures and manages embedded devices effectively and helps to meet the fundamental requirements for longevity, agility, and incremental adoption. ADistributed Identity Management (DIM) system based onpermissioned blockchain technologyprovides dynamic trust models that improves the robustness of user identity against the frauds. The final part of research explains a privacy-preserving rating system for early detection of anomalous device behavior.

Aymen Boudguiga et. al. [17] give insights on the process of updating the infrastructure of IoT environment periodically. The entire objects of the ecosystem are not connected to the internet and therefore the patching and botnet prevention is a tedious task for the administrator. The study helps to deploy updates in IoT devices using blockchain infrastructure which ensures high availability of the system. Also, the proposed model insists the identification of potentially malicious objects or manufactures for better accountability.

Yu Nandar Aung et. al. [18] demonstrate how to apply Ethereum private blockchain implementation cope with the privacy and security issues of a smart home system(SHS). The system integrates home appliances and sensors together and allows owner to monitor and perform appliances functions remotely. Owner can verify every transaction history and set up policies for handling transactions.

Donhee Han et. al. [19] demonstrate how a smart door lock system based on block chain is handling security issues. This mechanism provides authentication, data integrity and non-repudiation. It prevents an unauthenticated user from participating in the blockchain network. The research proposes a judging algorithm to operates under various sensor inputs.

George C. Polyzos et. al. [20]explore the potential of a blockchain-assisted information distribution system for the IoT. The study tries to identify key challenges related to security and trust and proposes a commonly agreed format of interactions using blockchain and smart contracts.

Runchao Hanet. al. [21]evaluate the performance of prominent blockchain that solve the classic Byzantine consensus problem. The main research focuses on the fundamental operational attributes such as throughput, performance and dynamic scaling of the devices. The first evaluation of Byzantine-tolerant blockchain is a adaptable option for IoT.

III. PROPOSED SYSTEM

A gated community perspective shares the responsibilities among the associated home tiers and help each other to track and report the malicious activity on the overlay or prediction of completely failed state of a community member. Normal smart home miner focuses on owner interactions. This study proposes a model interact with trusted external miners to identify unexpected and improper events. The proposed model helps to predict the nearby intrusion attempts and inform local protection authorities in a fraction of seconds.

A. Concepts and Components

Home Miner: A device that authenticates, authorizes, and audits all incoming and outgoing transactions to and from the smart home. The miner collects all transactions into local block chain and community block chain. It predicts the situation surrounds and informs local protection authorities or other nearer communities. The anonymous process for storing data at cloud storage starts with sending the storing request to miner. The miner authorizes the devices and extracts the last block from local block chain and attach with the sending data. After storing data, the cloud storage returns a new block-number to the miner that is used for further storing transactions. If the owner wants to monitor her home from outside, the miner validates her access request and share the last block number of the storage. If the request is just a monitor transaction, the miner sends current data of the requested device periodically until the requester close the channel. Otherwise the miner terminates the connection after reaching maximum threshold of data transfer. Confidentiality makes sure that only the authorized user is able to read the message locally or community level. 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. To protect devices from malicious requests and ensure the availability, the miner authorizes the incoming transactions using shared keys. The only delay incurs here is due to generation and distribution of shared keys. The system always immune to Distributed denial of service (DDOS) attacks and Linking attacks. A hierarchical defensive design does not allow any DDOS attacker to install malwares on smart home devices. An additional security layer cope with miner for examining policy header in all outgoing traffic. As the miner maintains unique ledger for each device in the cloud storage, it enforces unique key for each transaction rather than sustained linking channels.

Transactions: The communication between the devices or nodes are called as transactions. The proposed model supports seven types of transactions such as store transactions, access transactions, monitor transactions, genesis transactions, remove transactions, gossip transactions, community alert transactions.

Typical smart home tier system [1] supports the first five transactions. The gossip transactions makes smart contracts [8][13] between the home miners and build community overlay. Usually very limited number of trusted home miners will be part of a single community. Every community entity holds a community ID stamp. The communication initiated from a home miner append its own community ID signature for associating with the community transaction base. Whoever knows/part of the community can decrypt the payload and act based on the indented request. Each community keep track of their interaction transaction using light weight blockchain [2] decentralized storage system. It follows odd incidents rather than regular transaction history. So, the system never ends up with the

overheads of multiple blockchain in same miner nodes.

The community alert transactions are raised in two kinds of situations: Firstly, if a home tier recognizes the collapse of its working units in continuous and sequential manner by any intruder. Secondly if any home miner becomes completely inactive due to complete outage of power or network accidently or intentionally. The recipients trigger corresponding sensors and actuators. Neighborhood smart home tier system trigger lights surrounds to the impacted home and trigger sensor cameras for effective monitoring.

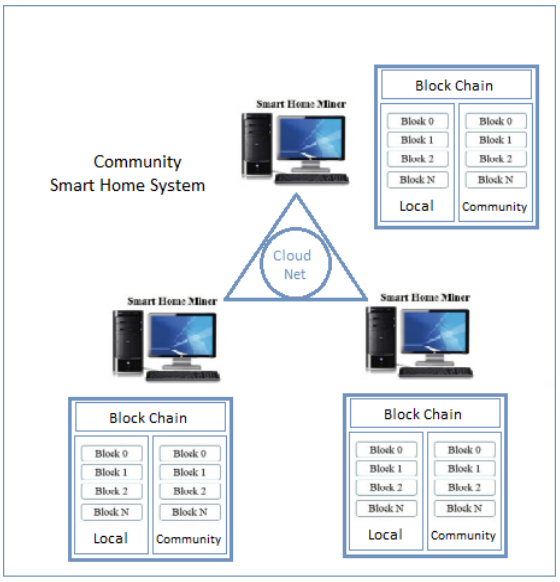

Fig. 1 Community smart home tier system

A single community alert transaction contains five parameters as Previous Transaction, Transaction Number, Target Device ID, Transaction Type and Transaction, Community ID as illustrated in Table 1.

TABLE 1
STRUCTURE OF TRANSACTIONS

Previous Transaction	Transaction Number	Device ID	Transaction Type	Corresponding multisig Transaction	Community ID
N = Genesis T.			Genesis : 0 Access: 1 Store : 2 Monitor : 3	If any (for keeping signature of requester).	

B. Data structures and Algorithms

Local Block Chain: A local private blockchain keeps track of transactions. The life cycle of transaction is starting from genesis transaction. Each block of local blockchain contains two headers as block header and policy header. When the block headers are assuring the immutable property of hash, the policy headers are lean towards the authorization and access control part of the system. A policy header constitutes 4 parameters as Requester ID, Action Type, Device ID and Action.

Community Block Chain: A private blockchain keep track of community alert transactions. The header constitutes three parameters as Request ID, Requester Community ID, Alert Details. The simplified form of block chain algorithm for community alert system.

Community Block Chain Algorithm: Fig. 2 depicts the simplified form of block chain algorithm for community alert system. It uses SHA256 for encrypting the signature of the requester. The append blocks receives transaction details and encrypt and append with the block chain. The verifier block method performs the proof-of-work but trusted community members if necessary.

```
require 'digest/sha1'
class CommunityBlockChain
  DEGREE=6
  def initialize(details)
    @@blocks = []
    append_blocks(details)
  end
  def chain(details)
    preceder = @@blocks.last
    append_blocks(details, preceder[:signature])
  end
  def verify_blocks
    blocks = @@blocks.last[DEGREE]
    for i in 1 to (blocks.size-1)
      signature = encrypt(create_record(blocks[i][:time], |
            blocks[i][:content], blocks[i-1][:signature])
      return false if signature!= blocks[i][:signature]
    end
  end
  private
  def append_blocks(details,signature='')
    block = create_block(details, signature)
    block[:signature] = encrypt(block)
    @@blocks << block
  end
  def create_block(content, signature='', time=Time.now())
    {
       :content => details,
       :signature => signature,
       :time =>time
    }
  end
  def encriypt(block)
     Digest::SHA256.hexdigest(block.to_json )
  end
end
```

Fig. 2Community block chain algorithm

IV. RESULTS AND DISCUSSION

This section evaluates packet overheads of the employed system and additional security requirements. To increase the 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 every community are authorized by the miner before forwarding them on to the devices. Symmetric encryption is using for establishing the peer-miner sessions. The community members handshake with digital signatures to validate the trusted neighbors. Table 2 show the additional requirements for the community smart home tier system.

TABLE 2
COMMUNITY SYSTEM REQUIREMENTS

Requirement	Employed Community Safeguard
Gossip	Achieved by additional handshake headers between miners.
Community Alerts	Independent hash bocks are emitted.

The study then analyzes responses of existing and proposed model towards various dynamic events. The basic analysis done with small community and interpolated results for detailed analysis. Overall responses for the proposed system provides the evidence of significant security benefits over the legacy model.

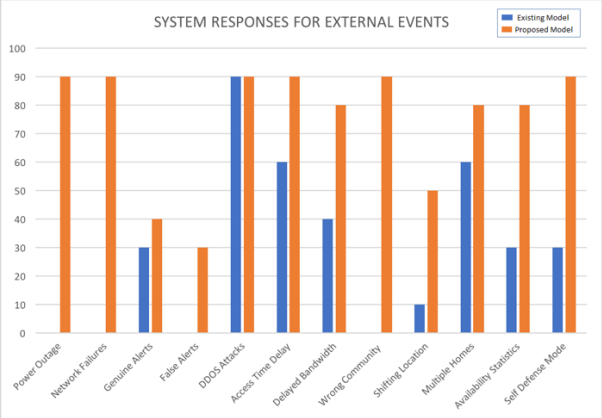

Fig. 3Comparison study on system responses against various events

V. CONCLUSION AND FUTUREWORK

As the user-centric models are not effectively utilizing the power of peer-community interactions, existing IoT security solutions is showing less immunity towards various external events. This study demonstrates different aspects of a self-governed self-sufficient security model for the smart home community. It brings higher level of association among the known groups and helps to share the responsibilities as in a gated community. The local protection authorities is able to monitor the affected home in a situation in any kind of collapsed state. In the future research, the community smart home model need to extend with the support of drones for chasing of intrusion attempts.

REFERENCES

[1] Ali Dorri, Salil S. Kanhere, Raja Jurdak and Praveen Gauravaram , "*Blockchain for IoT Security and Privacy: The Case Study of a Smart Home* ", IEEE May 4th, 2017.
[2] Salil S. Kanhere, Ali Dorri, Raja Jurdak and Praveen Gauravaram , "*Blockchain in Internet of Things: Challenges and Solutions* ", IEEE August 18th, 2016.
[3] Satoshi Nakamoto , "*Bitcoin: A Peer-to-Peer Electronic Cash System*", IEEE October 31st, 2008.
[4] Antonio F. Skarmeta, Jose L. Hernandez-Ramos, M. Victoria Moreno , "*A decentralized approach for Security and Privacy challenges in the Internet of Things* ", IEEE April 24th, 2014.
[5] Chan Hyeok Lee, Ki-Hyung Kim and Ajou Univ, "*Implementation of IoT System using BlockChain with Authentication and Data Protection*", IEEE April 23rd, 2018.
[6] Jin Hyeong Jeon, Ki-Hyung Kim and Jai-Hoon Kim, "*Block chain based data security enhanced IoT Server Platform*", IEEE April 23rd, 2018.
[7] Marco Conoscenti, Antonio Vetro and Juan Carlos De Martin, "*Blockchain for the Internet of Things: a Systematic Literature Review*", IEEE June 12th, 2017.
[8] Zhiqing Huang*, Xiongye Su, Yanxin Zhang, Changxue Shi, Hanchen Zhang and Luyang Xie, "*A Decentralized Solution for IoT Data Trusted Exchange Based-on Blockchain*", IEEE March 26th, 2018.
[9] Nabil Rifi, Elie Rachkidi, Nazim Agoulmine and Nada Chendeb Taher, "*Towards Using Blockchain Technology for IoT data access protection*", IEEE January 11th, 2018.
[10] Nikolay Teslya and Igor Ryabchikov, "*Blockchain-based platform architecture for industrial IoT*", IEEE January 11th, 2018.
[11] Xueping Liang, Juan Zhao, Sachin Shetty and Danyi Li, "*Towards Data Assurance and Resilience in IoT Using Blockchain*", IEEE December 11th, 2017.
[12] C. Tselios, I. Politis and S. Kotsopoulos, "*Enhancing SDN Security for IoT-related deployments through Blockchain*", IEEE December 11th, 2017.
[13] Kazım Rıfat Ozyılmaz and Arda Yurdakul, "*Work-in-Progress: Integrating Low-Power IoT devices to a Blockchain-Based Infrastructure*", IEEE December 1st, 2017.
[14] Pradip Kumar Sharma1, Mu-Yen Chen2, Jong Hyuk Park, "*A Software Defined Fog Node based Distributed Blockchain Cloud Architecture for IoT*", IEEE September 29th, 2017.
[15] Bin Liu, Xiao Liang Yu, Shiping Chen, Xiwei Xu and Liming Zhu, "*Blockchain based Data Integrity Service Framework for IoT data*", IEEE September 11th, 2017.

[16] David W. Kravitz and Jason Cooper, "*Securing User Identity and Transactions Symbiotically: IoT Meets Blockchain*", IEEE August 24th, 2017.
[17] Aymen Boudguiga, Nabil Bouzerna, Louis Granboulan, Alexis Olivereau, Flavien Quesnel, Anthony Roger and Renaud Sirdey, "*Towards Better Availability and Accountability for IoT Updates by means of a Blockchain*", IEEE July 3rd, 2017.
[18] Yu Nandar Aung and Thitinan Tantidham, "*Review of Ethereum: Smart Home Case Study*", IEEE January 15th, 2018.
[19] Donhee Han, Hongjin Kim and Juwook Jang, "*Blockchain based Smart Door Lock system*", IEEE December 14th, 2017.
[20] George C. Polyzos and Nikos Fotiou , "*Blockchain-assisted Information Distribution for the Internet of Things*", IEEE November 13th, 2017.
[21] Runchao Han, Vincent Gramoli and Xiwei Xu, "*Evaluating Blockchains for IoT*", IEEE April 2nd, 2018.