Malicious Activity Detection using Smart Contracts in IoT

Mwangi Eric[1], Hany F. Atlam[2] and Nawfal Fadhel[3]
[1]*Faculty of Engineering and Physical Sciences, University of Southamton, Southampton, U.K.*
[2]*Department of Engineering and Technology, University of Derby, Derby, U.K.*
[3]*Cyber Security Group, University of Southamtpon, Southampton, U.K.*

Keywords: IoT, Blockchain, Hyperledger Fabric, Smart Contracts, Security, Risk, Attacks, Cybercrime.

Abstract: Internet of Things (IoT) is a unique element in the realm of Cybersecurity. It constitutes countless applications, including defense, health, agriculture, finance, amongst other industries.
The majority of existing studies focus on various developments of IoT products and services essential to our day-to-day activities, with little emphasis on the security of developed systems. This has led to the proliferation of IoT solutions acquired through rapid development and overlooking the need for a structured security framework during the systems' development stages.
IoT security capability can be improved by using complementary technologies. This paper explores applying Risk-Based Access Control Model using Blockchain to control access to IoT devices. Although current access control models provide efficient security measures to control who can access the system resources, there is no way to detect and prevent malicious attacks after granting access.
The proposed solution utilizes smart contracts under the Hyperledger Fabric (HLF) Blockchain Framework to create access permissions and measure the security risks associated with any event in the IoT system and create access permissions to determine what processes may be performed. This will allow the detection of any malicious activity at the early stages of the attack and grant or deny access based on the risk associated with any activity.

1 INTRODUCTION

Blockchain is currently receiving much traction from both corporate and enterprise space as well as governments and financial institutions. COVID 19 pandemic has also accelerated digital transformation where the world has witnessed an exponential growth of ICT innovations and solutions across all industries during the pandemic. Similarly, there has been an equal measure of increase in cyber attacks with hackers continuing to develop sophisticated hacking techniques to penetrated their targets.

IoT has emerged as a critical target to cybercriminals leading to privacy and security issues where the attackers use the vulnerabilities in the interconnected devices to penetrate and compromise the IoT systems. Apart from DDoS attacks as reported by Natalija and Daiwei, on their paper titled *IoT as a Land of Opportunity for DDoS Hackers* (Vlajic and Zhou, 2018), other IoT attack vectors include but are not limited to Botnets, Man-in-the-Middle, Phishing, Social Engineering and Remote Recording.

Because of the limited security capability of the majority of IoT devices, this research seeks to identify a viable solution for securely deploying the IoT systems and ensuring the many devices/things connected to the internet over the IoT infrastructure operate with minimal risks and repercussions in the event of exploitation by intruders and hackers.

IoT devices in general should be capable of remote control, access, monitoring, and management of things via the internet (Suryadevara and Mukhopadhyay, 2015). Most IoT frameworks are built on three pillars derived from the ability of the smart objects to:-

(a) Have a unique identifier;

(b) Be able to communicate by receiving and emitting communication signals and;

(c) Be able to interact through an inherent computing capability (Miorandi et al., 2012).

Besides, "Things" have the ability to understand and adapt to their environment, learn from each other, and

Eric, M., Atlam, H. and Fadhel, N.
Malicious Activity Detection using Smart Contracts in IoT.
DOI: 10.5220/0010474802860295
In *Proceedings of the 6th International Conference on Internet of Things, Big Data and Security (IoTBDS 2021)*, pages 286-295
ISBN: 978-989-758-504-3

make appropriate decisions through their reasoning capabilities.

In May 2014, the Pew Research Centre released a paper analysed from feedback obtained for predictions on the future of the Internet from expert researchers with long-standing credibility, titled *The Internet of Things will thrive by 2025* (Anderson and Rainie,). The interviewed observed that this technology would come with insurmountable challenges whose risks have to be minimised to reap the indispensable benefits.

1.1 Problem Statement

Lack of computation power on IoT devices cripples the security capability which shifts the security measures from the edge IoT devices to IoT data collection servers.

1.2 Research Objectives

The research will be based on the following key objectives:

1. Provide an understanding of the emerging IoT technology and the threats associated with it.
2. Provide an assessment of the suitability of utilisation of the Risk-based Access Control Model with Smart Contracts over a decentralized network, to mitigate the security risks associated with IoT systems.
3. Design and implement an IoT prototype system as a proof of concept for the proposed IoT security solution.

1.3 Research Question

How can Risk-Based Access Control Model be used to strengthen the security of the Internet of Things while mitigating the risks associated with cyber-attacks?

1.4 Hypothesis

A dynamic Risk-Based Access Control model is applicable in a distributed network to enhance IoT security by determining access decisions for each access request in the IoT system in Realtime.

The study will be achieved by investigating the effectiveness of the Risk-Based Access Control model over Blockchain technology and, more specifically, the Hyperledger Fabric (HLF) framework with Byzantine fault-tolerant (BFT) ordering service.

1.5 Test Case: Gated Community Security Solution

Security Guards at a gated community may not be sufficient to guarantee adequate security for the residents. The gatekeepers generally rely on the information provided by the visitors and allow them into the gated community without any means of verification of the details provided.

A prototype for an IoT solution for securing access to a gated community will be designed and used to demonstrate the application of a risk-based access control model to achieve a secure IoT system using smart contracts over hyperledger fabric blockchain framework.

2 LITERATURE REVIEW

This section is intended to provide the reader with a clear understanding of emerging IoT and Blockchain technology.

2.1 Internet of Things (IoT

The Internet of Things is a rapidly evolving smart technologies that will soon become indispensable, with all objects in the world having the ability to interconnect and communicate over the Internet. The main challenge that will impede IoT's rapid deployment is the security capability since hackers are increasingly developing hacking tools and techniques to penetrate assets available on the Internet.

Intelligence collected over time by the US Directorate of National Intelligence (DNI) during James R. Clapper's tenor, who was the longest-serving Director as at 2016, warned that in addition to the traditional threats that the US was facing, the Internet of Things would be a major national security threat in the foreseeable future. He further divulged that IoT would be one of the most destructive technologies interconnecting tens of Billions of new exploitable physical devices (ODNI Public Affairs, 2016)

All these were early warnings that the future of IoT is bright but will come with insurmountable challenges whose risks have to be minimized to reap the indispensable benefits.

2.1.1 Problems Associated with IoT

The most common attack vectors in IoT systems are Malicious code injection at the endpoint devices to steal login credentials, Impersonation, Data Modification, Denial of Service (DDoS) attack, Side-channel

attacks (SCAs), Replay attacks, Man-in-the-middle (MitM) attacks amongst others (Ali and Awad, 2018), (Jurcut et al., 2020). The aforementioned brings about the need to have the following challenges associated with IoT addressed:-

Privacy and Security: The overall control over Personally Identifiable Information (PII), and protection from unlawful surveillance are fundamental rights for individuals as stipulated in most countries' constitutions (Solove, 2008). Protection against privacy invasion is a prevalent challenge that will require to be addressed for the successful implementation of IoT.

In the IoT domain, privacy, as observed by Abeer Mohammed Assiri and Haya Almagwashi in their research on *Iot Security and Privacy Issues*, can be compromised at the Device level, Storage level, Processing level, or Communication level (Assiri and Almagwashi, 2018).

Single Point of Failure: IoT systems are mainly set up using centralised cloud technology, which creates a major security weakness in IoT applications since an attack or downtime occasioned by power outage or malfunctioning of the cloud server would bring down the entire IoT application (Kshetri, 2017).

Insecurity by Design: The attribute of interconnecting several physical devices poses a significant threat to the IoT system since a successful attack on one embedded device, e.g. a light bulb, might lead to the whole system being compromised as disclosed by Maire O'Niell et al (O'Neill et al., 2016). Attackers could use an 'unsecured' refrigerator to gain entry to the same network running the target's computer, laptop, or data servers (Arndt, 2018). In the same way, a DDoS attack on one of the devices on the network could lead to the whole system being disabled (Lyu et al., 2017). *A chain is as strong as its weakest link*, so any vulnerability in any of the interconnected devices opens the entire system to attack, leaving individuals and organizations potentially exposed (Shackelford et al., 2017)

2.2 Blockchain

Most of the inherent problems associated with IoT deployed over a centralized network can be overcome by use of Blockchain, a distributed ledger framework that ensures a copy of each information in the IoT system is stored and synchronized in several nodes over the distributed network.

Blockchain technology started as a cryptocurrency solution with Bitcoin as the first public use case. Blockchain has lately experienced rapid diffusion into various other economic and social fields, as witnessed in its reliable use by governments, financial institutions, and corporates to achieve the much-needed decentralized applications. As of 2016, Blockchain had emerged as the most significant type of distributed ledger technology as reported in the journal for the UK Government Office for Science. (Walport et al., 2016) Immutability is one of the key cornerstones for blockchain that guarantees non-repudiation and integrity of the data stored in the distributed ledger.

2.3 Hyperledger Fabric

Hyperledger Fabric (HLF) is a permissioned blockchain network where all members participating in the distributed network require prior permission with authorised crypto keys to enable them gain access and transact in the blockchain network (Androulaki et al., 2018). It is a modular, scalable and secure framework for implementation of a blockchain solution that has an inbuilt plug-'n-play ability to integrate components such as consensus algorithm and membership services. It has been established that implementation of HLF with BFT ordering service increases the transaction processing speeds and *"can achieve up to ten thousand transactions per second and write a transaction irrevocably in the blockchain in half a second, even with peers spread in different continents"* (Sousa et al., 2018). This is a crucial requirement and a significant boost for enabling HLF to achieve multiple ordering service at real time speeds, given the millions of transactions that are envisaged in a typical IoT network with multiple devices.

The proposed solution recommends the use of Hyperledger Fabric (HLF) with Byzantine fault-tolerant (BFT) ordering service. This offers an appropriate network where only approved residents in the gated community can join and participate in the blockchain network.

2.4 Access Control Models

The primary objective of any Access Control Model is to provide access rights in regard to authorized users and to avert system abuse from unauthorized persons.

Confidentiality, Integrity, and Availability are the core elements that guarantee the usability and effectiveness of any given access control model.

2.4.1 Traditional Access Control Models

Traditional access control models are anchored on protocols that have been established to be static and

equally rigid. The policies within are predefined, and they generate the same results no matter the environment; in essence, they fail to capture the various elements essential in making critical access decisions. The widely used traditional models include Discretionary Access Control (DAC), Role-Based Access Control (RBAC), and Mandatory Access Control (MAC) (Atlam et al., 2018)

The rigidity of traditional and dynamic access control methods and their context insensitivity renders them not suitable for IoT ecosystems.

2.4.2 Dynamic Access Control Models

Unlike the traditional access model, the dynamic access model is another concept characterized by access policies and unique contextual attributes that are more approximated in real-time. The captured elements consist of trust, history, context, as well as operational requirements.

2.4.3 Adaptive Risk based Access Control Model

Comparing different access control models, it is evident that they all have their unique inadequacies. However, the adaptive risk-based access control model is more dynamic, usable, and scalable. This approach has diverse advantages, including:

- Using estimation and prediction by exploiting game theory along with context awareness.
- Exploiting various security protocols based on real-time estimates, including predictions, whereby different sources are accessed to build reliable adaptive decisions.
- And as Habtamu and Langko puts it, *Learns, adapts, prevents, identifies and responds to new or unknown threats in critical time, much like biological organisms adapt and respond to threats in their struggle for survival* (Abie and Balasingham, 2012)

Figure 1 is a flowchart of Adaptive Risk Based Access Control Model that illustrates the amalgamation of above mention benefits. The flow starts when the user requested to access system resources. After the user is authenticated successfully, the risk value associated with the user is estimated using the risk estimation module. This risk is estimated based on various risk factors associated with the access. Then, if the estimated risk value is higher than a predefined threshold value defined in the risk policy, the access will be denied. While if the estimated risk value is lower than the predefined threshold value, the access will be granted. Then, the user activities during the access session will be monitored to detect and prevent

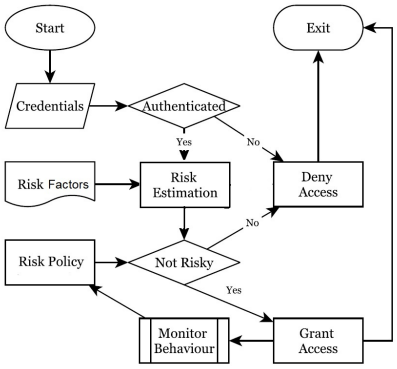

Figure 1: Flowchart of Adaptive Risk Based Access Control Model.

malicious activities. This approach is essential in as far as IoT communication is concerned as it aims at ensuring the system operates with minimal deviations from the conventional routine.

3 RESEARCH METHODOLOGY

This research will used both qualitative and quantitative data gathering procedures to guarantee the reliability and efficiency of the data. Data was collected using case studies and surveys to ensure the realisation of sufficient data for the research's success. This also ensured accurate scope of analysis and maintained research reliability and validity.

3.1 Case Studies and Analysis

Great care was employed in the selection process of case studies and surveys in this paper. In brief, it was elicited by necessity for a prime study with high efficiency. Considering the diverse nature of the research subject, and the multiple industries involved, the research focused on the following three cases:

3.1.1 Case Study No. 1: Healthcare Institutions

The majority of Iran's leading hospitals are based in Tehran and are the epitome of healthcare, research, consultancy, and referral solutions. Most of the health centers have deployed Computerised Health Information Systems (CHISs) (Zarei and Sadoughi, 2016) to handle sensitive information regarding patient history and clients' financial obligations, including blood group, among others; Healthcare systems are susceptible to attacks and any breach of security to this information would adversely affect the image, trust, and the operations of the institution.

The breach would lead to exposure of patients' personal health history, financial losses, loss of reputation, and intellectual properties as recently witnessed in the Hospital Chain Universal Services facilities in the U.S., where all the 250 facilities were attacked by ransomware. The affected facilities were forced to resort to manual systems amidst the COVID 19 pandemic's overwhelming workload. The attackers' motive could be financial gain through the payment of the ransom, data theft, or disruption of services. (Associated Press, 2020)

3.1.2 Case Study No. 2: Smart Homes - IoT

IoT in smart homes is a growing phenomenon that is being witnessed globally. In the Western world, smart homes have become the new buzz where light bulbs, security cameras, thermostats, fridges, cookers and doorbells are all being controlled remotely from a phone. Across the USA and UK, IoT is becoming the standard for diverse home applications that are being interlinked. The development of interconnected devices and people increases efficiency and, at the same time, risks, and threats. Technologies such as Bluetooth, WiFi, and cloud storage have become the most used technologies at home. The IoT makes smart homes highly sophisticated and intelligent, interlinked, and remotely accessed or controlled (Li et al., 2015), (Sicari et al., 2018). The Smart homes interconnected devices that are controlled remotely are all prone to hacking as witnessed in the baby monitoring IoT system that was hacked and remotely controlled by an attacker at midnight.(nbc, 2015)

A survey of 950 IT and business decision-makers by Gemalto in 2019 revealed that with the increase of attacks on IoT systems, security remained a major challenge. The survey observed that almost half of the businesses could not even detect that they had been breached and were seeking government intervention in securing connected IoT devices. However, the survey observed that the adoption of blockchain technology to secure the IoT was slowly being considered by some companies as they await government regulations on best security practices and policies to use for IoT security. (Living, 2019) Additionally, analysis of the US National Vulnerability Database (NVD) revealed an increase of high severity Common Vulnerabilities and Exposures (CVEs) on Internet devices such as routers, switches and other IoT devices that were being used by attackers to execute commands and gain remote access to the systems.

3.1.3 Case Study No. 3: Jurcut et al., 2020 Survey

The survey done by Jurcut et al., 2020 on security consideration for Internet of Things, where a number of key IoT security research papers were analysed, adequately covered the vulnerabilities and threats associated with IoT and went further to recommend viable solutions to ensure secure deployment of IoT systems. The authors recommended a myriad of security risk prevention methods for IoT and noted that mitigation of identified IoT threats required concerted effort amongst the developers, device manufacturers consumers and lawmakers. However, with the comprehensive IoT best practices and security solutions provided from the survey, the author admitted that more research was required as the solutions proposed would not provide a 100% security (Jurcut et al., 2020).

3.2 Results Analysis

3.2.1 Analysis of Case Study No. 1: Healthcare Institutions

The findings presented by the first case study illustrate that access control measures are handled differently by organizations and on as per need basis. The various security frameworks used do not provide a concise scope for information security or how data management is handled, specifically by healthcare service providers. Poor access control at Iran's public healthcare and the recent attack on the 250 health facilities in the U.S. indicate weak access control policies and procedures.

The deployment of a risk-based access control model to monitor the databases' behavior in the hospital chain would have helped prevent escalation of the attack to all the 250 networked facilities.

It is worth noting that several researchers have identified the potential of the emerging blockchain technology combined with smart contracts to solve the security and privacy issues on healthcare and other IoT systems. In most of these researches, Smart contracts has emerged as a technology that would ensure proper access control where predefined conditions must be met before the execution of the subsequent processes. It is however generally noted by the researchers that there are still several challenges to be addressed as pernicious users may still exploit the perceived security and compromise the IoT system (Pan et al., 2019), (Griggs et al., 2018), (Zheng et al., 2020). For example, the proposal by Griggs, Kristen N., et al. 2018 to integrate the Wireless Body Area

Networks (WBANs) with smart contracts on a consortium blockchain network addressed the problem of integrity of the data through immutability of the records that is offered by Blockchain (Griggs et al., 2018).

The Authors, however, cited securing each node for the interconnected devices as a significant security challenge. They proposed the introduction of human-based verification before a new transaction was accepted in the blockchain as a possible solution to ensure security and eliminate potential intruders from the system.

Our proposal is to introduce the deployment of a risk-based access control model to monitor the risks associated with every transaction at each of the connected nodes and automatically grant or deny permission based on the status of the associated risk, thereby eliminating the need for human-based verification.

3.2.2 Analysis of Case Study No. 2: Smart Homes - IoT

The second case study proves the increased attacks targeted at smart homes and the increased sophistication of the attack vectors. The proposed solution in the case of the compromised baby monitor would have a smart contract that would detect the abnormal behavior of attempts to remotely control and move the baby monitor at midnight. The movement of the baby monitor at midnight being a suspicious activity would automatically be denied access and transaction flagged appropriately. Notice that this would require a smart contract with predefined conditions on the time range within which the baby monitor is remotely controlled.

3.2.3 Analysis of Case Study No. 3: Jurcut et al., 2020 Survey

The survey from the third case shows that a lot of research has gone into securing IoT systems. However, with the increased sophistication of hackers, there is still concern about IoT systems' security as institutions are still being attacked.

With these findings, it is evident that there is a dire need for a security solution that would adequately address emerging IoT cyber threats.

Our proposed solution first aims at adopting the policies and security controls recommended by other researchers to mitigate potential cyber attacks and move a notch higher to provide measures to ensure an attack is not escalated to the entire system once access to a specific interconnected device is compromised.

4 DESIGN AND IMPLEMENTATION

This section presents the IoT system prototype design that will be used to build a proof of concept (POC) for the proposed proof of concept. The section will also depict the implementation of the risk-based access control model and smart contracts over a distributed ledger network.

4.1 Design

The design focuses on using smart contracts to define the process logic on Hyperledger Fabric network. The smart contracts will be designed to measure the security risks associated with any event in the IoT system and create access permissions to determine what processes may be performed. This will allow detection of any malicious behavior at the early stages of the cyber attack kill chain and grant or deny access based on the risk associated with any of the transactions of the networked devices.

The proof of concept is designed to be implemented on a private and permissioned blockchain network (ie Hyperledger Fabric network) as opposed to an open permissionless framework that allows unknown entities to participate in the network. Members authorised to participate in the Hyperledger Fabric network will be enrolled through a trusted membership Service Provider (MSP) to ensure only authorised users (ie residents of the gated community) are allowed to interact with the network. Any device or entity in use on the network will be preassigned a digital certificate by the certification authority and cryptographically linked to the network. This will help eliminate an attacker's possibilities of participating in the network with stolen login credentials.

The Permissioned blockchain network operates under a distributed ledger framework with a copy of each information stored and synchronized in all the nodes over the distributed network. This ensures transparency, immutability and integrity of the stored data. Additionally, the use of the channels for communication within the the hyperledger fabric network enhances the system's security and privacy.

The proposed IoT prototype for the gated community security solution, hereby dubbed HyperGate, will have an image sensor to capture visitors' images. The residents will be required to update the ledger with the visitor's information whenever they expect a new visitor, and update the visit date for returning visitors. The smart contract will ensure the following conditions are met before any new entry (transaction) takes place in the ledger:-

(i) The device from which the request is made is a known device

(ii) The time the request is made is within the agreed time range

(iii) The number of approved visitors at any given time range is within the agreed rules.

If any of these predefined rules are not achieved, the smart contract will flag the transaction as suspicious and immediately raise an alarm to the appropriate stakeholders.

A transaction can be a change in any of the visitors details in the ledger, update of visit time for returning visitors or an entry of new visitors record(s). For every successful transaction a new block will be created that is cryptographically linked to the chain thereby generating a blockchain containing accurate, time-stamped and verifiable record for every transaction ever made.

Upon arrival at the gated community entrance, the face image of the visitor will be captured by the image sensor and presented to the resident through a mobile app for them to validate the image as illustrated in figure 2. The synchronized information will be immutably stored in a blockchain ledger and used for subsequent visits. For any subsequent visit by a visitor whose records have already been updated and image synchronised, the resident will only require to update the expected date of visit in the ledger.

The guard at the main entrance will query the information in the ledger to either allow or deny access of a visitor to the gated community.

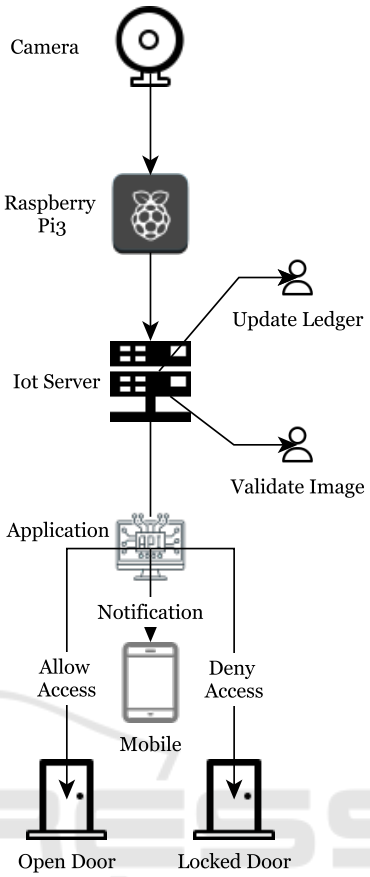

Figure 2: Image sensor connect to IoT Raspberry Pi IoT device.

4.2 Functional Requirements

This section identify the actions (features) of the system and provides a clear system overview by identifying all the functions that are required to be performed by each entity.

4.2.1 Resident/User

Average household resident should be able to

(i) Login to system

(ii) Register Visitor

(iii) Query/View Registered Visitors

(iv) Verify Photo

(v) Quarantine Registered Visitor

4.2.2 Guard

Which his duties should allow him to

(i) Login to system

(ii) Query/View Visitor details

(iii) Generate Reports

4.2.3 Admin

Which his duties should allow him to

(i) Login to system

(ii) Query/View Registered Visitors

(iii) Query/View Quarantined Visitors

(iv) Quarantine visitor

(v) Reverse quarantine visitor

4.3 Non Functional Requirements

The non functional requirements will offer direction on how the system will operate and equally set up constraints on all of its functionalities. The following are the identified non-functional requirements:-

(i) Authorisation and access levels

(ii) Audit tracking

(iii) Reporting requirements - who the Guards and the residents report to in respect to various arising issues

(iv) External interfaces eg with law enforcement in case of a robbery or crime incident in the gated community

4.4 Implementation

For a proof of concept (POC), the agile approach was used for the overall project management. The proposed HyperGate prototype was segmented into the following three modules needed to obtain the complete proof of concept:-

(i) User-based data input module : This is the module that provides the user with a graphical interface to accomplish most of the aforementioned functional requirements.

(ii) Sensor-based data input module : This is the module that will require an image sensor mounted and configured to provide automated input of the captured images onto the database

(iii) Mobile application - This is the application to be used by residents for records update and by the guards for querying visitor's information.

The first module was implemented using the following key software and coding tools-:

Hyperledger: For the generation and implementation of a permissioned blockchain network.

Couchdb: The underlying database for storing transactions - Provides GUI through Fauxton for viewing current state database.

Nodejs: For development of the backend REST API - Allow configuration of the server side.

Golang: For Design and Development of Smart Contracts (Chain Code) on the hyperledger fabric.

Docker: For containerisation of the micro-services of the Hyperledger blockchain. All the participating peers, orderers and ledgers/couchdb, will run on separate docker containers.

Postman: For interacting with the API- Provides a user-friendly interface to make requests (GET, POST) to the CoachDB.

React: For front end development of the user GUI.

VSCODE: For coding. Any code editor would work but VSCODE installed with YAML support and Go extensions is recommend.

The second and third modules have not been implemented in the POC. The second module will require an IP camera with an image sensor that will take the image of the visitor for approval by the respective resident before the transaction is committed in the ledger.

4.5 Hyperledger Fabric Network Setup

Hyperledger fabric version 2.2 was used to create the Hyperledger fabric network with the various courts in the gated community representing the Organisations and the various residents representing the Peers. Each court (organisation) was designed to have four peers, each peer representing one residential unit within the court. Additionally, each court was designed to have its own Certification Authority (CA) and each peer to have their ledger as shown in figure 3.

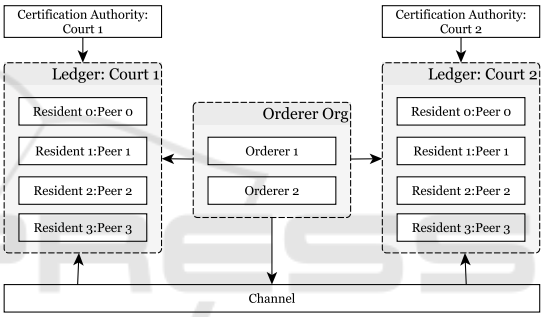

Figure 3: HLF Network setup.

The ledgers were created on the couchdb database under the docker containers. The docker containers communicate with each other and ensures prompt replication of any updates on the data for each peer under the docker containers.

4.6 Testing

Test data with random names and mobile numbers was used to create visitors records for the gated community using the developed user interface (UI) forms for data input. For each successful transaction, a new block was generated. The generated blocks in the developed Hypergate blockchain network are viewable from the Hyperledger Explorer as depicted in figure 4.

Notice that each court has their own local Membership Provider (MSP) for validating the clients and checking whether they have the required privileges for committing transactions. This distribution of the MSPs to all the courts ensures the system remains truly distributed and there are no bottlenecks for identity management.

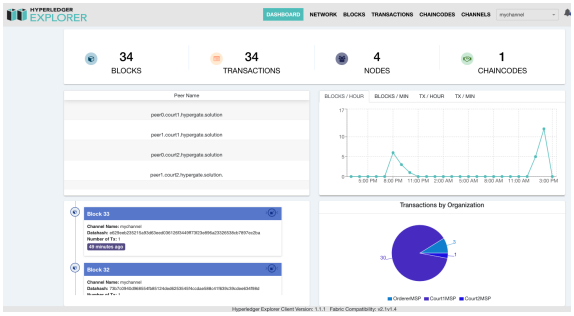

Figure 4: Hyperledger Explorer Blockchain view - with blocks generated from test transactions.

Any transaction performed by an authorised entity is flagged as suspicious and access denied.

4.7 Real Life Implementation

The Hypergate proof of concept is developed in a vagrant box using docker containers and cyptogen command tool to generate crypto material. The cryptogen tool is basically used for test environment setups.

Production environment will require real identities issued by the authorised certification authority (CA) from the Public Key Infrastructure (PKI) of the respective jurisdiction.

Hosting of IoT proof of concept implemented on a blockchain would best be done using Blockchain-as-a-Service (BaaS) provider. BaaS offers managed services for blockchain to simplify the setup complexity and reduce hardware costs. The following are some of the major companies offering BaaS:-

(i) International Business Machines Corporation (IBM)

(ii) Chainstack

(iii) Microsoft Azure

(iv) Amazon AWS Managed Blockchain and QLDB

(v) Oracle Blockchain Cloud

5 DISCUSSION

The number of interconnected IoT devices is growing daily in almost all industries. These interconnected devices communicate in an insecure channel and are, therefore, exposed to risks of cyber-attacks by design.

In contrast to traditional secured databases, private Blockchains are scalable by design. They offer pre-determined governance capabilities (the consensus algorithm) that clearly define how the system will be operated while ensuring that no network participant can manipulate the stored data to their benefit as well as are designed to reconcile data efficiently and in real-time across hundreds of participants. It is also worth noting that data reconciliation between multiple centralized systems requires each participant to connect their database via APIs with all other participant databases. Maintaining these (potentially) hundreds of API connections can create overhead costs than simply using one common Blockchain to manage this data.

The HyperGate solution implemented with Hyperledger Fabric provides an excellent use case that may be adopted in real life to enhance security for smart homes. The smart contract coupled with the immutability of the records and the use of certificates to validate members participating in the blockchain network is a sure way of ensuring the security and privacy of personal data amidst the proliferation of network attacks by hackers.

6 CONCLUSION

The Permissioned Blockchain framework using smart contracts on Hyperledger Fabric with Risk-based Access control model will eliminate possible hacks and data tempering thereby making it undoubtedly technology that organizations can rely on to implement secure solutions and promote confidence and trust in the use of the indispensable IoT solutions.

6.1 Future Work

Article 42 and 25 of the General Data Protection regulation (GDPR) enforces the requirement of ’right to forget” and ”right to erase” personal information. The rapidly deployed use case immutably stores Personal Identifiable Data in the Blockchain. To ensure compliance with GDPR, there is need to develop a decentralised personal data management system that utilizes zero knowledge proofs in combination with decentralised identifiers to enable hide specific pieces of Personal Identifiable Information (PII) during transactions in the gated community blockchain solution. The visitors will update the decentralized database by themselves and have full control of their identity. The only info that a gatekeeper needs to know is: does this person have permission to enter the gated community? This proof requires to be coded into a decentralized identifier that gives a ”yes” or ”no” results without divulging any personal information.

ACKNOWLEDGMENT

Our profound gratitude goes to members of the Faculty of Engineering and Physical Science, Southampton University, Department of Engineering and Technology, University of Derby, and the Cyber Security Group, University of Southampton, for their unreserved support and guidance that contributed to the conceptualization of this project.

REFERENCES

(2015). Man hacks monitor, screams at baby girl.

Abie, H. and Balasingham, I. (2012). Risk-based adaptive security for smart iot in ehealth. In *Proceedings of the 7th International Conference on Body Area Networks*, pages 269–275.

Ali, B. and Awad, A. I. (2018). Cyber and physical security vulnerability assessment for iot-based smart homes. *Sensors*, 18:817.

Anderson, J. and Rainie, L. The internet of things will thrive by 2025, pewresearch internet project, may 2014.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Ferris, C., Laventman, G., Manevich, Y., et al. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference*, pages 1–15.

Arndt, R. Z. (2018). Every device you own can get hacked.

Assiri, A. and Almagwashi, H. (2018). Iot security and privacy issues. *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, pages 1–5.

Associated Press, F. B. (2020). Hacked hospital chain says all 250 us facilities affected.

Atlam, H., Alenezi, A., Hussein, R., Hussein, K., Wills, G., et al. (2018). Validation of an adaptive risk-based access control model for the internet of things. *International Journal of Computer Network and Information Security*, 10(1):26–35.

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., and Hayajneh, T. (2018). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. *Journal of medical systems*, 42(7):130.

Jurcut, A., Niculcea, T., Ranaweera, P., and Le-Khac, N.-A. (2020). Security considerations for internet of things: A survey. *SN Computer Science*, 1(4).

Kshetri, N. (2017). Can blockchain strengthen the internet of things? *IT Professional*, 19(4):68–72.

Li, X., Nie, L., Chen, S., Zhan, D., and Xu, X. (2015). An iot service framework for smart home: Case study on hem. In *2015 IEEE International Conference on Mobile Services*, pages 438–445. IEEE.

Living, G. C. (2019). Almost half of companies still can't detect iot device breaches, reveals gemalto study.

Lyu, M., Sherratt, D., Sivanathan, A., Gharakheili, H. H., Radford, A., and Sivaraman, V. (2017). Quantifying the reflective ddos attack capability of household iot devices. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 46–51.

Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad hoc networks*, 10(7):1497–1516.

ODNI Public Affairs, B. M. (2016). Dni clapper provides series of threat assessments on capitol hill.

O'Neill, M. et al. (2016). Insecurity by design: Today's iot device security problem. *Engineering*, 2(1):48–49.

Pan, J., Wang, J., Hester, A., Alqerm, I., Liu, Y., and Zhao, Y. (2019). Edgechain: An edge-iot framework and prototype based on blockchain and smart contracts. *IEEE Internet of Things Journal*, 6(3):4719–4732.

Shackelford, S. J., Raymond, A., Charoen, D., Balakrishnan, R., Dixit, P., Gjonaj, J., and Kavi, R. (2017). When toasters attack: A polycentric approach to enhancing the security of things. *U. Ill. L. Rev.*, page 415.

Sicari, S., Rizzardi, A., Miorandi, D., and Coen-Porisini, A. (2018). Securing the smart home: A real case study. *Internet Technology Letters*, 1(3):e22.

Solove, D. J. (2008). Understanding privacy. *Legal Studies*.

Sousa, J., Bessani, A., and Vukolic, M. (2018). A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In *2018 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN)*, pages 51–58. IEEE.

Suryadevara, N. K. and Mukhopadhyay, S. C. (2015). *Smart Homes*. Springer.

Vlajic, N. and Zhou, D. (2018). Iot as a land of opportunity for ddos hackers. *Computer*, 51(7):26–34.

Walport, M. et al. (2016). Distributed ledger technology: Beyond blockchain. *UK Government Office for Science*, 1:1–88.

Zarei, J. and Sadoughi, F. (2016). Information security risk management for computerized health information systems in hospitals: a case study of iran. *Risk management and healthcare policy*, 9:75.

Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., and Imran, M. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, 105:475–491.