Home Automation Security using Blockchain

Suvith K S, SashikiranGavanivari, Ronith Gowda, VishwamohanNarendra, Shyamala G
Department of Computer Science & Engineering, B.M.S College of Engineering

Abstract - Smart homes are currently being implemented everywhere. It is an extremely efficient and convenient combination of tSmart homes are currently being implemented everywhere. It is an extremely efficient and convenient combination of technology and services, which is handled through a network for better quality of lifestyle. Internet of things is the main backbone behind a smart home system, which is becoming even more popular by the day. With a single mobile device, various facilities in the household can be controlled remotely. Security is also an important implementation, with the installation of CCTV cameras as an example. You can view what's going on inside or outside your house from anywhere in the world thanks to this technology. However, it is all based on a single server which can be hacked into easily. A hacker could gain control of devices in your house as well as the security systems, which can lead to dire consequences. In order to prevent this from happening, we can secure the server using blockchain. It allows you to operate the entire system using a private key, making it difficult for the hacker to do anything. This report examines the implementations in detail which have been used in the process of securing the server. Ethereum has been used as the blockchain platform. In addition to the implementations, functional, non-functional, hardware, and software requirements have also been discussed in detail. Technology and services, which is handled through a network for better quality of lifestyle. Internet of things is the main backbone behind a smart home system, which is becoming even more popular by the day. With a single mobile device, various facilities in the household can be controlled remotely. Security is also an important implementation, with the installation of CCTV cameras as an example. You can view what's going on inside or outside your house from anywhere in the world thanks to this technology.

I. INTRODUCTION

The rise of cryptocurrency in today's world is evident. The decentralisation and low transaction costs have touted it to be the next worldwide acceptable currency. The main software concept to have led to the development of cryptocurrency is blockchain. Blockchain in a simple sense could just be a chain of blocks. But here the blocks represent data and the chain represents any data storage unit like a public or private database. Blockchain has been implemented in many IOT based systems throughout the world like smart cities and security of personal data. One of the main concerns of IOT based home automation system is the security of it. As the convenience of using appliances from your phone over the wi-fi increases the risk and ease of hacking into one's house also increases. By viewing the benefits of blockchain in the cryptocurrency scenario, the security of servers in home automation can be improved. The server can be implemented as a decentralised server. A private key generated once will be the only access to the system for a given period and once that period expires the same private key cannot be reused. The system cannot be hacked as well due to the hashing power of the blockchain system. In this way the server security of an IOT based home automation system can be drastically increased by the implementation of a blockchain.

II. LITERATURE SURVEY

Home automation systems are now being used for controlling and monitoring devices in one's home with the help of a mobile device. For example, you can tap a button on your mobile to turn on the lights instead of having to walk up all the way to flick the switch, or you can stream a song from your phone to the home speakers. These are minor examples, which can range from something huge such as home security. Everyone these days owns a smartphone, which makes the product both marketable and convenient. It also helps environmentally,by maximising energy efficiency. An important aspect is video surveillance for security, which involves installing a camera with microphone and motion sensors to monitor the house while inside it or away from it. The various devices will be controlled on the mobile phone with different applications, and can work on both iOS and Android platforms. If the user clicks the monitor home status button, then they will be shown details like which lights are on, power usage, A/C temperature and security settings. If the user decides to not make any changes, they can return to the home screen. The user can also select to choose the audio features of the smart system. This window will show the user a library of songs that are stored either on the phone or the computer and the user can select a song to play on the sound system. The music can be stopped by just pressing a button. For the video system, the user will see a screen and streamed video data from the camera. The user can then watch the video from this screen for as long as he/she wants.[1]

The application has graphical user interfaces which consists of 5 different activities. In Start mode activity, all rooms in the house are displayed, and the user can select which appliance to control in which room. Option mode activity gives the user the choice to choose either switch mode or voice mode to control the appliances. In voice mode activity, user can give speech feedback to control. Switch mode activity provides the user with switches to turn appliances on or off. Lastly, the video mode activity displays the video that is being shown by the monitoring camera. One limitation is that during voice mode, other noises in the background may affect the result. The intended instruction that we give with our voice may be misinterpreted because of the external noises. The limitation to control only a few devices can be overcome by extending automation for all home appliances. The scope of home automation is huge. Security cameras can be controlled even from a different state, and motion sensors can be used to detect any kind of suspicious unauthorized movement, after which the user can be notified immediately. The project is based on Raspberry pi, Java, and Python. These are all free open source software which results in a low implementation cost and easy configuration as well.[2]

There are mainly 3 network types of home automation systems. Power line systems are the most affordable. They depend on existing power lines to transfer security camera feeds and details about the lights to a common control interface. Wired systems use cables for communication. They are easy to install. The last network type is wireless systems. These do not use any cables, and make use of Wi-Fi networks. This factor makes them very compatible with existing home networks. The system relies completely on power. In case of a power failure, the entire system will be halted. Without a strong network, the Ethernet shield will not be able to work to its full potential as a network provider to the circuit. Hence, the system will be halted. These things need to be taken care of. The working procedure involves updating data which will go to the server and process with time. All data will process according to a time that is given through the input before. Once the input data is processed, the system will get a signal from the internet. Based on the type of signal, the system will respond accordingly. In the experiment conducted, high signal was sent when motion detector detected any movement within 20 feet. When no motion was detected, low signal was sent. Accordingly, the appliance was turned on when high signals were received by the microcontroller, and turned off when low signal was received. [3]

Blockchain is like a public ledger where all transactions committed are stored in a list of blocks. New blocks are added resulting in the chain growing continuously. Cryptography and distributed consensus algorithms are incorporated to add security and consistency. Blockchain is part of the implementation layer of any distributed software system. One can say it is a peer to peer system composed of individual nodes. Blockchain was started for cryptocurrency where it was used for trestles and reliable translations where a centralised management is not required. Even though blockchain was initially started for cryptocurrency it’s no being used in fields like smart contracts, public services, Internet of Things (IoT), reputation systems and security services.

Architecture of a blockchain consists of a chain of blocks where each block contains a block header. This header includes a Block version, Merkle tree roots hash, Timestamp, nBits, Nonce and a Parent block hash. There are a variety of consensus algorithms being used in the current scenario that include Proof of Work, Practical byzantine fault tolerance, Proof of stake, delegated proof of stake, Ripple and Tendermint. Some of the challenges of blockchain include scalability where more transactions bulkier and slower the blockchain becomes. Blockchain cannot guarantee absolute user privacy. It is also susceptible to selfish mining. The future of blockchain implementation and development lies in Blockchain testing, decentralisation, big data analytics and its applications. [4]

Blockchain has various research challenges. It still struggles to deliver a complete level of anonymity. Another is issue is that its security and privacy features were never really formally stated and proven. Even with all these uncertainties blockchain is still rapidly developing and new blockchain technologies are emerging. Blockchain is now being developed by practitioners rather than cryptographers thereby giving it more practicality rather than just application on paper. A common vocabulary is first created associated with blockchain. One way to improve blockchain is by adding anonymisation by using techniques like confidential transfers. One can also use other technologies than Bitcoin which offer more features like zero-cash. This increase in anonymity will result in a whole new plethora of uses for blockchain. [5]

Some commercial applications of blockchain are discussed. Blockchain has a very important financial service where it has increased the popularity of cryptocurrency. Mining is a process of adding a new block into the chain. Each block contains a list of transactions with respect to that coin. It is a very intensive task to validate an invalid transaction. Blockchain is also used in smart contracts. Its simple non-turing complete scripting language enables in helping to improve the limitations of the system. Security features of blockchain enable it to be used in healthcare where it helps in keeping patient data private. In business and industries moving towards cloud computing and internet of things blockchain plays a massive role. It introduces distributed autonomous computing and also makes RFID process more efficient. It also supports edge and fog computing. Blockchain is also used in right management systems, reputation systems, digital content distribution system, wi-fi authentication and IoT security. [6]

Blockchain has many security features which can be used to optimize some existing software systems. It finds itself in various major industries offering cheap and reliable security alternatives. Blockchains are used in smart cities. A smart city can be defined as one that uses information technology to integrate and manage physical, social, and business infrastructures in order to provide better services to its dwellers while ensuring efficient and optimal utilisation of available resources. With the advent of IoT and cloud computing cities are continuously trying to grow and improve themselves by constantly analysing day to day data. This involves setting thousands and thousands of sensors and servers that span the entire city. Maintaining security of such wide network can prove to be a major problem. Sensors are usually very simple to hack and are mostly hosted off public networks. The main use of blockchain can be seen in the fact that any hacker needs to use 51% of his resources just to surpass the hashing power of blockchain. An example of its implementation can be seen in a parking system where A is paying parking fee to B. This transaction I represented as a clock. If more than. 50% of the entities approve of the block then transaction is confirmed. [7]

Healthcare systems contain a huge database of data regarding patient history, logs, inventories and other related information. This data is continuously created, disseminated, stored and accessed daily. Patient information and data is of critical privacy and maintaining this should be of utmost importance. In various instances Blockchain has been used to solve this problem. In general this data is stored in the form of EMRs or electronic medical records. In order to create, store and query EMRs health information systems or HIS were designed. In today’s society patient mobility has increased widely from one place to another and stand-alone EMRs have become very impractical and unpopular. Also, the rapid growth in cloud and smartphones means people require on hand real time data processing. This gives rise to personal health records or PHRs. These PHRs are hosted on a cloud-based system. The security and privacy is handled by Blockchain. For every new PHR a new block is instantiated and distributed to all peers in the patient network. After a majority of the peers have approved the new block, the system will insert it in the chain. This allows for a global view of the patient’s medical history in an efficient, verifiable way. If an agreement is not reached the block is not added to the main chain. Because of the patients have control over their data, avoids performance bottleneck and single point failures and all changes on the blockchain are visible. As a result, medical history is complete, consistent, timely, accurate and distributed. [8]

The amount of data being generated by the world on a daily basis is very huge. This includes huge technological companies, Social media outlets, Weather forecasters, Streaming services to name a few. In this data driven society the main concern is user privacy. Users are little to no control on what data is being stored about them. For this there are various techniques of anonymization like k-anonimity and differential privacy. Another way to incorporate privacy is by using blockchain. A blockchain is combined with an offshore blockchain storage thereby developing a personal data management platform. Through this system, users have complete control of their data and there is complete transparency over what is being collected about the respective user. The System has Users and Services. During access the blockchain verifies that the digital signature belongs to either the user or the service. Data saved by user is routed to an off blockchain key value store while retaining only a pointer to the data on the public ledger. [9]

BlockChain: A Distributed Solution to Automotive Security and Privacy

Smart vehicles are connected to so many entities, it is not an easy task to secure them. When a vehicle is compromised, the security of the vehicle as well as the safety of the passengers are both compromised as a result.

The common security and privacy methods used in smart vehicles are becoming obsolete due to the following challenges:

- Centralization: The current model involves connection of all vehicles via cloud servers and is unlikely to scale as large number of vehicles are connected. These cloud servers are essentially a bottleneck and a single point of failure that can disrupt the entire network.
- Lack of privacy: There is no consideration for user privacy, e.g. exchange of all the data of the vehicle without the owner’s permission, producing noisy or summarized data to the requester. In most smart vehicle applications, precise vehicle data needs to be shown to provide personalized services.
- Safety threats: Many smart vehicles are self driving. Compromised security can cause malfunctions which could in turn cause crashes. This could result in the passengers losing their lives.

BlockChain (BC) encompasses an evergrowing list of blocks that are interconnected. BlockChain possesses important features such as security, immutability and privacy. It can therefore be used to tackle the above mentioned problem by creating a private and secure smart vehicle ecosystem. The BC-based architecture for automotive

security and privacy is an amalgamation of numerous parts. The main part of the architecture is the overlay where a public BC is managed by the overlay nodes which are the smart vehicles. Each vehicle has its own wireless interface along with an SD card. The vehicles are connected to the overlay via the interface. The important data which needs to be stored securely and privately is stored in the in-vehicle storage. The vehicle creates unique transactions in previously decided intervals having the signed hash of the stored data. This transaction is given to the vehicle's associated OBM and stored in the BC. Eventually, the hash of the transaction can be compared by the vehicle to show that there is no change in the stored data. A back up storage is used in the residence of the owner because of minimal storage space. The vehicle occasionally moves data from the in-vehicle storage to the backup storage. In such a case, back up storage's hash is stored in the BC. To conclude, the advantages are: Strong communication security and authentication introduced by BC reduces risk. Distributed data exchange and security increases scalability.
The same BC based architecture has a number of other applications such as:

1. Remote Software Updates
2. Vehicle Insurance
3. Electric Vehicles and Smart Charging Services
4. Car Sharing Services [10]

Blockchain in Internet of Things: Challenges and Solutions
Blockchain is considered a desirable technology for tackling the security and privacy challenges in Internet of Things (IoT):

- Decentralization: There is no central point of control. This makes for a more scalable and robust model by making use of the resources of every single participating node and putting a stop to many-to-one traffic flows. This consequently reduces the delay and tackles the problem of a single point of failure.
- Anonymity: The anonymity that comes with BC afforded is useful for most IoT use cases where the identity of the users must not be revealed.
- Security: BC provides a network which is safe and secure which is desirable in IoT as it includes a large number of devices which may or may not be trusted devices. However, incorporating Blockchain in IoT has a few challenges that need to be overcome:
- Mining demands a lot of computation, however, a large number of IoT devices are resource restricted.
- Mining of blocks takes a significant amount of time while in most IoT applications minimum delay is desirable.
- An IoT network usually contains a large number of nodes. This is a problem because as the number of nodes in the network increases, the scalability of BC decreases.
- The protocols of BC create quite a lot of overhead traffic. This is a disadvantage while working with IoT devices which have limited bandwidth. [11]

III. PROPOSED SYSTEM

In the existing systems, each smart home is equipped with an always online, high resource device, known as ”miner” that is responsible for handling all communication within and external to the home. The miner also preserves a private and secure BC, used for controlling and auditing communications. Though it is only by a small amount, there is an increase in energy consumption, packet overhead and time overhead. This implementation supports only the personal cause of the owner.

The proposed system uses blockchain technology for automation and security of homes. We know the vast use of Airbnb across the world. We can implement blockchain technology integrated with IoT for ease of the tenant as well as the landlord or the owner of the house.

The tenant does not have to wait for the owner to arrive and provide him with the keys at the location. This is where blockchain comes into use. The tenant can request for accommodation. Upon acceptance of the request, he can pay for the accommodation with ether units which he can purchase. The owner generates and shares the QR code to the tenant. The tenant can scan the QR code generated for the access of the house. Smart homes allow the user to easily access the appliances of the house as well. Surveillance cameras also help in live security broadcasts. Usually tenants misuse the amenities like electricity consumption, water consumption. Through IoT and block chain we can help the owner to charge the tenant based on this usage. Also, other facilities like two-wheeler rentals etc. can be charged as well.

As we know, the tenant can purchase ether units using blockchain technology and payment is done through blockchain. The owner also can monitor his previous transactions, requests, consumption and usage of amenities on blockchain as well. The front end is used to generate and display the QR code. This is done using AngularJS. NodeJS is used for the back end. Ethereum TestRPC is used as the customizable blockchain emulator. It allows making calls to the blockchain without the overheads of running an actual Ethereum node. The raspberry pi is used to create and maintain the node server which communicates directly with the blockchain. Various IoT devices and components are connected to the raspberry pi as well which will in turn monitor their actions. Once the tenant decides to check out, he has to scan the QR code. This will send a notification to the owner with the help of wi-fi module integrated with raspberry pi. Upon checkout, based on other rental requests, the ethereum node changes hence keeping the blockchain network secure and only upon the owner's confirmation another tenant can be able to check in.

IV. CONCLUSION

The main task of the proposed system is to have a hassle-free concept of rentals. This makes it simpler and easier for accessing, accommodating places online. Blockchain also helps the owner to have a secure automated system, where monitoring of resources can also be done. Blockchain also helps in building an non-hackable system due to its use of nodes and private keys. This is the future of airbnb and hotel rentals as it is easy for both the tenant and the owner. This system also helps in saving resources like water and electricity as they will be charged based on their consumption. This is useful for both parties.

REFERENCES

[1] Vu Ha, Joel LeGros, ThienLuu, Daniel Moody. "SMART HOME SYSTEMS". 3rd August, 2012.
[2] Arafat Jahangir, Tamanna Jahan, S.M Shamsraj, Abu Raihan. "WEB BASED HOME AUTOMATION". 26th April, 2015.
[3] Sabin Adhikari, Sangam KC, Santosh Lamichanne, UrjalaBajracharya. "ANDROID CONTROLLED HOME AUTOMATION". September, 2014.
[4] An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends Zibin Zheng, ShaoanXie
[5] A Critical Review of Blockchain and Its Current Applications Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, Kyung-Hyune Rhee
[6] Introduction to Security and Privacy on the Blockchain Harry Halpin, Marta Piekarska
[7] Securing Smart Cities Using Blockchain Technology Kamanashis Biswas
[8] Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy? Christian Esposito
[9] Decentralizing Privacy: Using Blockchain to Protect Personal Data Guy Zyskind
[10] BlockChain: A Distributed Solution to Automotive Security and Privacy Ali Dorri, Marco Steger, Salil S. Kanhere, and Raja Jurdak
[11] Blockchain in Internet of Things: Challenges and Solutions Ali Dorri, Salil S. Kanhere, and Raja Jurdak
[12] Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity Lei Hang