Research Article
Volume 10:8, 2021

International Journal of
Sensor Networks and Data Communications

ISSN: 2090-4886 Open Access

Security Issues with IoT for Smart Homes: Blockchain as a Solution

Mohammed I Al-Ghamdi*

Department of Engineering and Computer Sciences, Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia

Abstract

With the increasing use of smart technologies like the Internet of Things, home automation has become the hottest trend these days. It provides all the modern features and convenience that a homeowner can expect. Home appliances can be automated via wireless connectivity and they can be accessible on the go. However, there are so many security concerns with the significant rise of smart home appliances like light bulbs, power switches, door locks, home security, etc., especially because of limited processing power and storage. They are highly vulnerable to security threats. Hence, security has become the primary concern and matter of discussion among researchers in this area. This way, a decentralized database blockchain is gaining a lot of popularity to assure security in this field. This article is aimed to explore the security of smart homes and investigate the adoption of blockchain. This research paper is aimed to explore security measures that manufacturers should consider for IoT systems and the way Blockchain can help solve this problem.

Keywords

Blockchain ● Internet of things ● Smart homes ● Digital intelligence

Introduction

The IoT or Internet of Things consists of billions of physical devices interconnected over the web, sharing and collecting user data. Owing to the ubiquity of networks and affordable computer chips, it has become easier to turn almost everything, be it a small object like a pill to something huge like an aeroplane as part of IoT. The devices which would be just machines could gain some digital intelligence when they are connected and sensors are added to them, so that they can connect and work together with real-time data. The Internet of Things is filling the gap between physical and digital worlds. For example, one can turn on a light bulb with a smartphone app. Some other examples are connected streetlights, a smart thermostat, or a motion sensor.

An IoT device could be a driverless vehicle or a child's smart toy. IoT is mainly a broad term which consists of devices which were not supposed to be connected to the internet and that can be connected to other devices over the internet without human intervention. Considering this point, a smartphone and a PC are not IoT devices, even though the former has so many sensors. On the other side, a fitness band or smartwatch can be considered as IoT devices because they can work on their own and they were wearable gadgets which were not supposed to be connected to the internet.

The IoT is also designed to make homes, vehicles, offices, etc. smarter, more considerate, and more talkative. For example, Alexa and Google Home can be used to get daily scoops, set alarms, play music, etc. Home security solutions can keep track on outside and inside of a house or even to interact with visitors. At the same time, smart thermostats can keep a home environment warm before its owners come back and smart bulbs can make a home look like someone is inside even though it is vacant. Even better, sensors can tell the users how hot or cold the climate is going to be and how busy the traffic is around their house. Smart cities and self-driving vehicles are the most common examples of how IoT can change and make lives easier (Figure 1).

Figure 1. Smart cities.

Smart home is simply a home where consumers are likely to interact with IoT devices. Several tech giants like Google, Amazon, Apple, Microsoft, etc. are working hard in this field to provide the best possible experience to the consumers. Smart speakers like Amazon's Echo with Alexa are the most obvious examples, but smart light bulbs, plugs, smart fridge, and thermostats are no exception. Having smart home appliances are no longer luxury and the ways to show off the passion for having smart new gadgets. They can also serve various purposes and can even help elderly by connecting them to their care providers and families and even monitor their health and overall wellbeing. Ability to change some settings and knowledge of how things work can also save some energy and heating costs.

With all the above positive things about the Internet of Things, there is a dark side too. One of the major concerns is security and privacy. These sensors collect very sensitive information about the users in most cases for various reasons, such as what users do or what they say in their home.

***Address for Correspondence:** Mohammed I Al-Ghamdi, Department of Engineering and Computer Sciences, Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia; E-mail: mialmushilah@bu.edu.sa*

Received: July 27, 2021; **Accepted:** August 10, 2021; **Published:** August 17, 2021

Keeping it safe is very important to ensure customer trust. But the track record of IoT about security has not been so positive. IoT manufacturers don't give much thought about encrypting user data and this technology is also relatively new.

Even the most used and old codes in software are also discovered and there are so many software flaws that are not fixed for a long time. Most IoT devices are also not able to be patched. Hence, they are mostly at risk. Hackers know the inherent security flaws of emerging IoT devices and they are always in their radar, such as webcams and routers. They are easy target for attackers to turn them into botnets and compromise their security. Several smart home devices have been left open for attackers due to security flaws, such as ovens, refrigerators, and dishwashers. More than 100,000 webcams have been found to be hacked easily in a study while some kids' smartwatches have been found to have security flaws due to which hackers can track their whereabouts, communicate with them, and even eavesdrop on their chats.

The IoT serves as an important link between the real world and digital world, and it has a lot of potential to make users' lives easier. But the increasing risk of privacy attacks can be dangerous, and its consequences can even be life-threatening. For example, hacking into a driverless truck can cause an accident and finding out who was the main culprit (the owner, the manufacturer, or the traveller) will be even more complex due to lengthy legal procedures. An IoT is a revolutionary technology but still in its initial stages. It still has its weakest links and security flaws. Fortunately, Blockchain, with its modern technologies, can add a strong and unbreakable layer of security. Blockchain can create an almost unhackable framework. It has solutions for various issues like privacy, single point of failure, trust, time stamping, and scalability. There are so many benefits of integrating Blockchain with IoT

- High security and trust less network
- Distributed ledger to maintain a huge database for smart devices
- Smart Contract and Transparent Framework for IoT ecosystem
- Prompt and easy access to smart devices
- Eliminating third-party access
- No human contact

Sensors and inputs can be automated with IoT and Blockchain can automate responses in a decentralized way. Service providers, vendors, and homeowners can work together in a trust less way with no or minimal intervention. In this article, we are aimed to investigate the increasing use of IoT and smart home architectures and highlight important features of Blockchain that can help ensure security of smart homes.

Literature review

Smart home automation provides so many facilities and convenience and it is drastically gaining popularity with existing use cases of IoT. Sensors are employed via wireless connectivity in home appliances and they can be accessed remotely to operate such devices. Investigate the use of blockchain for smart home security [1]. They present a secure framework on the basis of Consortium blockchain and its opportunities and challenges. Propose a uniform IoT infrastructure on the basis of smart contracts and blockchain while considering all the primary challenges of the smart home environment [2]. They focus on three important concepts – private blockchain, smart contract, and public blockchain in their approach. They propose that it is the right time to make the best use of AI, smart contract, and blockchain and deepen this research on blockchain.

Present the case study of smart home systems (SHS) implementation in home appliances to ensure automatic operations of home security, air conditioning, lighting, heating, and healthcare systems [3]. It enables homeowners to perform and monitor various functions any time remotely over the web. They present Ethereum Blockchain implementation for SHS to deal with security and privacy issues. Present a deeper study on various functions and core components of smart home [4]. They propose a Blockchain-based smart home framework for IoT privacy and security. They also present their simulation outputs to prove that the overheads like processing time, traffic, and power consumption are insignificant for its privacy and security benefits.

Research questions

- What are the key features of IoT?
- What types of attacks are very common for IoT for Smart Homes?
- What security measures should be considered by manufacturers and end users?
- How can Blockchain help overcome security issues?
- How smart home payments will work in future and how blockchain can secure them?

Methodology

In order to investigate the key features of IoT and security attacks that might affect smart homes, we have presented some of our research in this paper. We also highlight the security measures that users and manufacturers should consider to secure their IoT systems and how block chain can help fulfil the needs of privacy and security for IoT systems. This research paper is entirely based on secondary data to answer all our research questions and make scope for further research in this topic. For collecting secondary data, our research relies on trusted sources like news portals, media, research papers from IEEE Access, Research Gate, etc. on blockchain and IoT, and official websites.

Results

Considering the above research questions and their answers, it is observed that Blockchain has a lot of potential to secure IoT devices. But they observed that implementing blockchain with IoT systems is still a far-fetched reality as it is very complex and smart contract solutions can also add up the production cost [1]. So, manufacturers need to look for the ways to make it easy to implement blockchain in smart homes. Further studies are needed to look for the ways to make blockchain easily accessible to IoT devices, considering their great potential in various industries.

In addition, public blockchain also has scalability problems and it is not ideal for smart homes as it can significantly increase the overhead. Meanwhile, manufacturers and users have to take certain measures to secure IoT devices that are discussed in this paper. There are different features of IoT devices for smart homes that can make our lives easier. It is still a relatively new technology and there are many loopholes to fix, so that we can make the most of these emerging devices as part of our daily lives.

Discussion

Q1: What are the key features of IoT?

Here are some of the most important features of IoT that make it work:-

Connectivity: It includes establishing a solid connection between all the IoT devices to the IoT platform which may be cloud or server. High speed communication is important after connecting IoT devices between them and the cloud to ensure bi-directional, secure, and trusted connection.

Integration: IoT integrates several models to provide the best user experience.

Analysis: After connection of all the objects, it is time to conduct real-time analysis of gathered data and build the appropriate business intelligence with it. A system can be smart only when there is an accurate insight to the collected data from all such things.

AI: IoT is designed to make lives easier and things smart with the use of data. For example, if a coffee machine is running out of coffee beans, it should order the desired coffee beans on its own.

Engagement: It engages the connected things, services, and/or technology and makes them work together.

Sensors: The IoT devices use sensors to measure and detect any change around them and notify the users. IoT turns passive networks into active ones. There would be no existence of a real IoT environment without sensors.

Endpoint management: It is the last but not the least feature of IoT systems. Endpoint management is important for IoT devices. Let's take an example of a coffee machine once again. When a coffee machine runs out of coffee beans, it orders coffee beans on its own. But what if the owner is going out of home for a few days? There would be no use of the IoT system. Hence, Endpoint management is essential for an IoT system.

Q2: What types of attacks are very common for IoT for smart homes?

All the hackers need is just one vulnerable device to infiltrate sensitive or personal information and leave the whole home network on the mercy of attackers. Smart home IoT systems may fall prey to dozens of attacks. Listed here are some of the most common types of attacks for Smart home IoT devices:-

Hijacking: In this type of attack, hackers have control over IoT devices. The device works really well and it is not easy to detect when it has been attacked. Once a hacker attacks a device, there are chances that other devices will be compromised.

Data breach: IoT devices collect a lot of user data. Smart home devices handle all the personal information like phone numbers, addresses, health records (by smart watches or other wearables), and even bank details. Hackers steal identities of the users by targeting these devices.

Man-In-The-Middle (MITM): In this type of attack, a hacker spoofs or interrupts the connection between two devices.

DDoS: Distributed Denial of Service can force devices, websites, or the whole IoT system to turn off or become inactive due to connection problems. It can flood the target device or system with plenty of traffic and keep it out of service. Hackers can use thousands of such compromised devices and their power to initiate DDoS attacks, even without letting the users knows.

Eavesdropping: An attacker needs a weakened connection between the server and IoT device to steal the sensitive data and intercept network traffic.

Brute force: It is another most common type of attack to access IoT devices by identifying their weakness of passwords.

Malicious nodes: Attackers inject malicious nodes physically between valid nodes in the IoT network. Then, they can use these nodes to spy on the flow of data between connected nodes and also control operations.

Firmware hijacking: If firmware updates are not checked in an IoT device to ensure legitimacy of the original source, an attacker can download malicious files by hijacking the device.

Physical threats: If IoT devices are installed in the environments where enterprises cannot control the people from accessing the device, physical tampering incidents are very common.

Q3: What security measures should be considered by manufacturers and end users?

Now that the types of security attacks on IoT devices have been discussed, it is the right time to discuss security measures users can consider:-

Changing router's default name: Even a default name of the router can give much insight to the hackers before planning attacks. They use every little bit of detail to hack into the network and the device's name is one of them.

Limiting Wi-Fi access: Limiting the use of Wi-Fi networks can significantly reduce the risk of IoT devices being compromised. This way, guest networks provide a separate account to other users without exposing IoT devices to any compromised device.

Unnecessary features should be disabled: Most IoT devices have remote access which is factory-enabled. It should be disabled when not in use. It is also recommended to disable other unnecessary features and settings that are not required.

WPA2 encryption: It is one of the strongest encryption methods to secure traffic and routers. It means one needs a password to access your network.

Keep devices up-to-date: It is important to check for updates for IoT devices and routers regularly. Otherwise, the user might miss out on some important features and security patches.

Unique passwords and 2-factor authentication: It is recommended to use different passwords for each device or account. In case one device is hacked, others will still be away from attacks. The 2-Factor Authentication also adds another layer of security. It sends a code to a tablet or smartphone for verification when someone tries to enter into the users' system.

Along with customers, manufacturers are also responsible for ensuring safety of these devices. Security should be on top priority from scratch. Here are some of the consideration's manufacturers should look for:-

Design: Security should be considered from the design stage itself. Manufacturers should ensure considering secure testing, code, and evaluation. Security should cover all the layers to be applied just from the beginning to the end.

Access control and encryption: When all the data and communications are encrypted, data can stay secure even when the device is compromised. It is important to comply with strict regulations, especially when it comes to processing personal data.

Authorization and authentication: Manufacturers can consider biometrics and two-factor authentication for access control. This way, only authorized people can use the system.

Educating customers: Manufacturers should also educate consumers about do's and don'ts of using their IoT devices. They should know how it works and how it is connected to other devices. They should teach how to protect these devices in an easy to understand manner.

Q4: How blockchain can help overcome security issues?

IoT requires administrator to control the network as it works on a server/client model. It is also the weakest link of cyber security. IoT devices depend on the centralized authority to determine their behaviour. If the central authority has a security breach, the hackers can send any information from the smart devices. This way, blockchain technology is known for its decentralized nature that can avoid any central attack. It means, hackers would have to attack every single node present on the network to get the information. Smart devices can validate transactions in a blockchain network. It means the network will validate the predefined 'authorized' behaviour and prevent any hack.

Users need to enter a key code for gaining the network access in blockchain ledgers. Hence, there is accountability integrated in all the transactions. Any changes should be signed and traced back to anyone who made them. The network will trace back all the changes that have been made. None of the nodes will accept any unauthorized change. Blockchain also secures IoT devices from incidents when smart devices are stolen. Once the device is reported to be stolen or identified with a suspicious behaviour as if it is stolen, it could be quarantined and all of its important data will be forwarded to the owners and law enforcement authorities, whatsoever.

Q5: How smart home payments will work in future and how blockchain can secure them?

To streamline the shopping experience for customers, it becomes very important for the merchants to promote smooth payments. They have to cut down the steps to make payments and remove obstacles to turn a browser into a shopper. With technological advances, customers have much smarter ways to make payments. They don't have to get their cards off their wallets and pay directly with their smartwatch or smartphone. But this smooth approach could easily be the thing of the past in the near future. IoT is known to have great interconnectivity to make transactions through all devices and objects, such as smart speakers, cars, and even coffee makers or fridge, while eliminating human intervention. For example, in the US, customers can order pizza with voice commands. Both Domino's and Pizza Hut support Google Assistant and Amazon Alexa. All the user needs to say is "Ok Google, call Domino's" and they are good to go. Next up, Google Pay handles the transactions and makes the whole process seamless [5].

There are also refrigerators, for example, by Samsung, which can order fresh groceries on users' behalf to keep themselves packed [6]. Even more amazing is the fact that connected cars will interact with parking meters and petrol pumps to pay parking fees and fuel cost [7].

Considering the above stats, there are around 3.6 billion smartphone users worldwide while the global population is around 7.5 billion (Figure 2). It means people will have several connected devices and they will no longer be limited to smartphones. For making the IoT successful, a smooth and secure payment experience will also matter. According to McKinsey 2015 report, the IoT is going to generate the revenue of $13 trillion by 2025 and it will be made possible when users are satisfied with the security and convenience of payments.

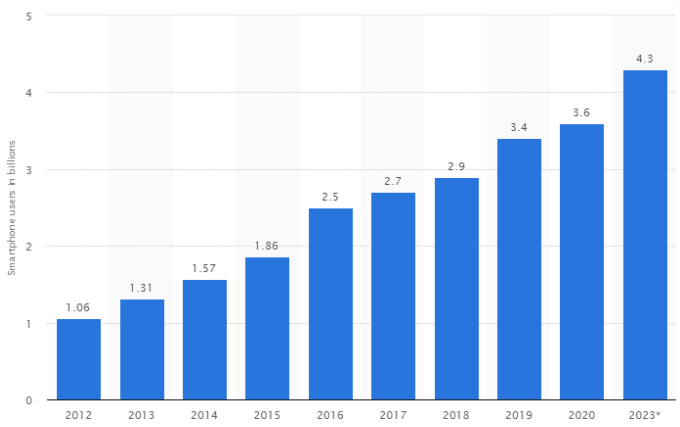

Figure 2. Number of smartphone users in the world (2016-2023).

This way, Blockchain trims down operations and improves security in smart homes. It builds a secure environment for connected devices and enhances the sharing economy for the transactions. It makes daily lives easier by preventing data breaches and hacks through its decentralized nature and other features. We have discussed some examples like refrigerators, cars, smart speakers, etc. but blockchain can be helpful when it is implemented with other home appliances like TV sets, smart locks, connected blinds, lamps, etc. It can even provide controlled, timely, and quality water supplies outside your house [8,9].

Conclusion

IoT security has been the matter of debate for both industry leaders and academia for all wrong reasons. Current security measures are still not sufficient because of processing overhead and high power requirements. Many studies have been done on privacy and security issues of smart homes and IoT infrastructure. Observed that modern IoT devices don't have proper security features like smart light bulbs, smoke alarms, light switches, etc. that hackers can easily access. Argue that users' smartphones are the weakest links to attack smart homes even with having proper control over the exchange of packets from home gateways. This paper has outlined all the important aspects of IoT devices and security threats we need to be aware of. We presented detailed analysis about Blockchain and its potential to secure smart homes. As far as we know, this research is the initial step towards further studies on the ways to optimize Blockchain to secure smart homes.

Conflict of Interest

Author has nothing to disclose.

References

1. Arif, Samrah, M. Arif Khan, Sabih Ur Rehman and Muhammad Ashad Kabir, et al. "Investigating Smart Home Security: Is Blockchain the Answer?" *IEEE Access* 1 (2020): 117802-117816.
2. Zhou, Yiyun, Meng Han, Liyuan Liu and Yan Wang, et al. "Improving IoT Services in Smart-Home Using Blockchain Smart Contract." 2018 *IEEE Int Conf Internet Things* 1 (2018): 81-87.
3. Aung, Nandar Yu and Thitinan Tantidham. "Review of Ethereum: Smart Home Case Study." 2017 *Int Conf Inf Technol* 1 (2017): 1-10.
4. Dorri, Ali, Salil S. Kanhere, Raja Jurdak and Praveen Gauravaram. "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home." 2017 *IEEE Int Conf Pervasive Comput Commun Workshops* 1 (2017): 1-7.
5. Bradford, Alina. "Gets Pizza Hut Or Domino's Delivered Using Just Your Voice."
6. Bohn, Dieter. "Samsung's new fridge can order Fresh Direct groceries from its humongous touchscreen." (2016).
7. Negru, Simona. "Connected Cars and In-Car Payments: The Road So Far and the Road Ahead." (2021).
8. Lashuk, Anton. "Blockchain Applications in Smart Homes." (2020).
9. Notra, Sukhvir, Muhammad Siddiqi, Hassan Habibi Gharakheili and Vijay Sivaraman, et al. "An Experimental Study of Security and Privacy Risks with Emerging Household Appliances." 2014 *IEEE Conf Commun Net Secur* 1 (2014): 79-84.

How to cite this article: Al-Ghamdi, Mohammed I."Security Issues with IOT for Smart Homes: Blockchain as a Solution." *J Sens Netw Data Commun* 10 (2021): 137.