IOT-BLOCKCHAIN- REVIEW, SECURITY REQUIREMENT AND CHALLANGES

Mirza Furqaanbeg, Gayatri Pandi
Student, Head of Department (CE)
ME(IT)LJIET
Ahmedabad,Gujarat

Abstract: With arrival of smart devices, smart homes and smart everything, the Internet of Things (IoT) has appeared as an area of unbelievable growth, having potential, great impact in current era predicting to have 50 billion or more connected devices by 2020. However, there is no global standard for IoT devices to be deployed by any company, different companies used their own policies for the deployment of the IoT devices. With the effect of this most of the IoT devices are easy to hack and data can be compromised. Also, the IoT devices are vulnerable to the attacks as the devices are limited in computing, storage and network capacity. In this paper, we survey about the IoT and some of its applications. We have also reviewed the security requirements and categorized the security issues of IoT. Further, we discuss about the blockchain and its benefits. We also discuss about the attacks can be done on the blockchain. We have proposed a solution with the objective to make sure that integrity of the data is increased.

Keywords: Internet of Things, Blockchain, Security.

I.INTRODUCTION

The internet of things is simply an interconnection of various devices which might be merged in everyday items, allows them to do communication through the internet[1].The Internet of Things (IoT) has strong connectivity from “anyplace” to “anyone” at “anytime” for “anything[1].The growth of Internet of things(IoT) is at fast pace, and some report predicts that the growth of IoT devices will reach to 30 billion by 2020, which are 30 time more devices deployed in 2009[4].As the growth of IoT devices increases the security issues for the data of these devices will also be boosted. The problem to maintain data integrity, confidentiality and availability of the data is an issue for all the owner of the IoT device. Securing data on Internet of Things (IoT) is a challenging affair faced by the industry. The global expenditure on IoT security is expected to rise at an annual rate of 25%, embracing up to 900 million USD in 2020[5]. IoT deployment raises many security issues related to the characteristics of IoT devices, such as the need for lightweight cryptographic algorithms in terms of processing and memory capabilities, and the use of standard protocols, such as the necessity to minimize the size of data exchanged between nodes[2] There can also be another issue can occur for the securing data when the third party breakdown or do any malicious activity which in turn effect make loss of the private data for the owner which is critical. To secure data of the IoT devices and to remove the third party from the communication, we can use the technology named Blockchain.

Blockchain is a consensus based secure decentralized which store information over a network. It is completely decentralized, and it depends on the peer-to-peer network. Blockchain technology has attracted the attention of many stakeholders in many industries such as agriculture, cryptocurrency, supply chain, Home automation etc. The Gartner report predicts that $ 3.1 trillion in business value will be added by 2030. By taking advantage of the blockchain technique in the IoT network, we can offer new ways to automate business processes without the need for costly and complex centralized IT infrastructure [3]. It will help the device users to trust the other users and the companies and it will reduce the risk of any loss of data of the users. The confidentiality, integrity and availability complications can be solved by using blockchain as it removes third party involvement between the devices to communicate. By using blockchain the data is stored securely as it uses the SHA-256 which provide the digest of the data which can't be generated again once it is generated by blockchain. Blocks of data are available to all the users which are connected in the network. As the blockchain is decentralized in nature, if any of the server fails in the network, we can access data from another server. The paper is organized as section-II gives brief idea of IoT, section-III explains different applications of IoT, section-IV shows requirement of security in IoT, section-V categorize the security issues of IoT, section-VI gives brief idea of blockchain, section-VII shows benefits of blockchain and section-VIII explains the attack can happen on blockchain, section-IX explain the proposed model by which data integrity is preserved. At last we conclude the paper.

II.INTRODUCTIO OF INTERNET OF THINGS (IoT)

The concept of the Internet of Things (IoT) seems to first appear in Kevin Ashton in a presentation delivered at Procter & Gamble in 1999 (Ashton 2009), which was then described as a large-scale network of smart RFIDs (Radio Frequency Identification) [6]. The IoT has become a common news item and marketing trend. Beyond the hype, IoT has emerged as an important technology with applications in many fields. Most IoT devices are connected to form purpose-specific systems; they are less frequently used as general-access devices on a worldwide network [7]. So far, the IoT has been defined in several

different ways, and its meaning has become so broad that it often includes any object on earth that is connected to the Internet, such as connected cars, drones, smartphones, smart appliances, industrial tools, and so on [6]. The IoT is drastically reshaping how individuals interact with other people, devices, organizations, their surroundings, and the world. In its contemporary form, IoT is meant to refer to an infrastructure consisting of constantly communicating objects, or "things" that may be smart and process or act on data [8]. It is also said that if a device has an on/ off switch, generates data, and can connect to the Internet, chances are that it can be part of the IoT [9]. However, even though the term Internet of Things was coined in 1999, the concept of collecting and transmitting data goes back earlier than that. ATMs (Automated Teller Machine) did it as far back as 1974. Still, with the recent movement and excitement around big data and IoT, IoT is still a new concept to a lot of people [9]. An IoT system may consist primarily of sensors; in some cases, it may include a significant number of actuators. In both cases, the goal is to process signals and time-series data [7]. Data sharing provides both huge benefits and presents substantial risks for society. We should be able to provide previously unimaginable insights and a level of control unequal to anything prior. The substantial benefits make it worth overcoming the issues of sharing and meeting the IoT's goal of providing an extremely high level of automaticity and device intercommunication [10].

In its simple form, IoT may be considered as a network of physical elements empowered by: Sensors: to collect information, Identifiers: to identify the source of data e.g., sensors and devices), Software: to analyze data, and Internet connectivity: to communicate and notify. Putting it all together, IoT is the network of things, with clear element identification, embedded with software intelligence, sensors, and ubiquitous connectivity to the Internet [11]. The main idea of IoT is to physically connect anything/everything (e.g., sensors, devices, machines, people, animals, and trees) and processes, over the Internet for monitoring and/or control functionality. Connections are not limited to information sites, and they are actual and physical connections allowing users to reach "things" and take control when needed. Connecting objects together is not an objective by itself but gathering intelligence from such objects to enrich products and services is [11]. IoT refers to anything and everything (including people). We can state a more comprehensive definition of IoT as follows: IoT is the network of things, with device identification, embedded intelligence, and sensing and acting capabilities, connecting people and things over the Internet [11]. There are some basic requirements for IoT to uniquely identify per "thing" (e.g., IP address) and the qualification to communicate between things (e.g., wireless communications) also the qualification to sense specific information about the things (sensors). With these three requirements, one should be able to monitor things from anywhere in the world. Another requirement can be a medium to communicate and such requirement is typically handled by a telecommunications network [11].

There are many reasons to monitor and control things remotely over the Internet: audit and controlling things by experts; learning about things by pointing a smartphone to a thing of interest for instance; searching for things that portals do not provide currently; allowing authorities to manage things in smart cities in an optimal manner; and, finally, providing more affordable entertainment and games for children and adults. Monitoring and control of IoT services may be done by any person or any machine, for example, a homeowner monitoring his own home on a mobile device based on a security system she or he has installed and configured [11].

III.APPLICATIONS OF IoT

a. **Smart homes**: Smart homes are a natural extension of current information, electronic, and communication technologies. Few years before, its concept mainly refers to comfort, leisure and healthcare. Through these smart home systems, remote meters reading can be achieved. The data associated with home water, power, gas, and telecommunications can be transmitted to the corresponding utility company automatically to improve the work efficiency. Furthermore, by smart home systems, the home ventilation, doors and windows, air conditioning, and lighting can be manipulated by remote control. And each electrical device like refrigerators, cooking devices and washing machines can be controlled by programs or remote platforms [12].

b. **Wearables:** Wearable devices, such as the Apple Watch, and a host of other smart devices by other companies, such as Samsung, Google, Jawbone, Fitbit, Adidas, Pebble, Motorola, Johnson & Johnson, etc., will drive the market for the IoT. From Google Glass and Apple iWatch to fitness bands and patient vital sign monitors, the body area networks (wearable, patchable, or implantable devices connected to your smartphone or tablet, or a more specialized device such as a hospital patient monitor, neuro-stimulator or sleep apnea system) these devices will inhabit present fewer development obstacles and lower infrastructure costs than larger networks [13].

c. **Connected cars:** Modern vehicles are equipped with several ECUs (Electronic Control Units) responsible for the main functions of the vehicle. These functions include the engine system, brake system, headlights, power windows, air bags, air conditioners etc. Moreover, vehicles are getting additional functions to interact with their surroundings. There are multiple sensors such as cameras, LIDAR's(Lighting Detection and Ranging) and radars that provide input to features such as adaptive cruise control, lane keep assist systems, collision avoidance systems as well as automatic parking. In addition, vehicles are increasingly being connected to the digital world by using telematics, Wi-Fi and Bluetooth technologies [14].

d. **Industrial internet:** Industrial automation is a most used application of IoT. With help of IoT infrastructure backed with advanced sensor networks, wireless connectivity, and machine-to-machine communication, conventional automation process of industries will transform completely. The driving philosophy behind IIoT(Industrial IoT) is that good machines square measure higher than humans at accurately and systematically capturing and communication period knowledge. This knowledge permits corporations to choose informed inefficiencies and issues sooner, saving time and money and supporting

business intelligence (BI) efforts. In producing specifically, IIoT holds nice potential for internal control, property and inexperienced practices, provide chain traceability and overall provide chain potency. In an industrial setting, IIoT is key to processes such as predictive maintenance (PdM), enhanced field service, energy management and asset tracking [15].

e. **Smart cities:** The good town is another powerful application of IoT generating curiosity among the world's population. Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security, and environmental observation all square measure samples of the internet of things applications for smart cities. IoT can solve major issues visage by the individuals living in cities like pollution, tie up and absence of energy supplies etc. Products like cellular communication enabled good Belly trash can send alerts to municipal services once a bin must be emptied [16].

f. **IoT in agriculture:** Over 570 billion farms around the globe are facing threat of climate change had on it and yet we demand more from agriculture than ever before. The more food for our growing population better incomes for those working across the food chain and the careful management about soil and water resource. This is no easy task. How can now agriculture step up to this challenge. The answer is smart agriculture. Smart agriculture aims to find new ways to adapt and thrive under climate change. It is based on three intelligent courses. While increasing agriculture productivity and incomes sustainably and equitably helping food system and farming livelihood be more resilient and minimize agriculture greenhouse gas emissions. Farms of every type and every size can become climate smarter. For example, by identifying and promoting sustainable farming practices and tools using inputs more efficiently and effectively to grow more from less and building markets where farmer can access what they need and sell any surplus of what they produce.

   Climate change is a challenge to our food system, but it is also an opportunity for us to innovate and adapt. It is easy to say but hard to do. With the combination of both advanced technologies in hardware and software, the internet of things can track and count everything which can greatly reduce effort and cost. The information of parameters of interest can be simply obtained at finger tips using electronic device which ease user to take further action. The internet of things transforms the agriculture industry and enable farmer to contend with their challenges. Innovated applications can address these issues and therefore increase quality, quantity, sustainability and cost effectiveness of crop production.

g. **Smart retail:** In today's highly competitive vendors of grocery, retailers make great effort to create a flawlessly shopping experience that drives sales and builds trust within their customers. IoT connected devices such as beacons, video cameras, and digital signage and smart shelves provide a new concept for the customer to access to a huge amount of new data on customer timeline and present more chances for sophisticated insights and immersive customer involvement. IoT data is used to track the effectiveness of store layouts exposure to promote the product interaction and use of digital kiosk and mobile applications. This data is analyzed in real time to create deep insights into customer preferences and path to purchase. Digital assistance allows customers to find the items on their list, interest them in new product and select promotion to save money and for marketers identifying customer desires delivering curate content to up-sell and cross-sell and measuring the success of promotions has never been simple and more accurate.

   IoT provides service level metrics and enable store manager to eliminate long queues, schedule staff efficiently through cognitive intelligence and make sure customer expectations are being met at every service point in the store. Today the business is evolving with the technological upgrading so does the retail industry. For example, beacon-based contextual retailing platforms are given tough fights to an e-commerce business. Smart retail solutions interpret the path to a new dynamic cost-effective inventory, accuracy, smarter marketing, and better customer happenings, in fact, there is new IoT centric system which is helping retailers to increase functioning performance. The use of RFID tags by retailers to increase the productivity of their stock chain is one of the most well-known patterns of early IoT adaption.

   IoT system can also help retail shop owners to decrease on the employee stealing and burglary by giving retailer power to increase liability at operational levels with the availability of smart shelves, source tags cubes and video surveillance equipment keeping a precise record of everything has never been so easy. We can do many different operations in retail industry using IoT like NFC payment, automated home replenishment, maintaining record efficiency, predictive preservation of store facilities, RFID on item-level inventory, Supply chain inventory tracking, and sensor-based proximity marketing, and sensor-based security solution.

h. **Energy management:** It is easy to take electricity for granted but in today's life, it is not possible without it to do our daily chores, we need more well-organized ways to manage electricity. The smart grid is developed for over 100 years of coal and fossil fuels and it is been used by different power plants to produce the electricity we use every day. The grid is a network of power lines and substations that carry electricity from power plant to homes and business places. Today grid has problems, it needs to modernize and is running at capacity when power line break or power plant can't produce enough power, blackouts can occur and that's a problem that can cause accidents at the same time today's grid often relies on a single power source and it doesn't provide detailed information on usage making electricity hardship to manage [50]. To address these problems in the past, we simply built a new power plant but now we can work towards sustainability and reduce our dependence on fossil fuel by using a smart grid. A smart grid is an intelligent digitized energy network delivering electricity in an optimal way from source to consumption. This is achieved by integrating information, telecommunication, and power technologies with existing electricity system [51].

   The smart grid suggests adding few needed sensors and software to the existing grid that will give you privileges and individual's new information that will help them to conjecture and react to changes quickly. Let's say a tree falls on a power line, 1000 quarters lose power with the current grid utility, operators often reroute power which demands time. With the

smarter grid sensors, the software would identify and promptly route the power around the problem restricting the issue to fewer quarters. The price of electricity changes during the day but we can't see it with the current meters on our quarters and cheap late at night. With new smart meters at the quarters, we could set our device to operate when the power is cheap. This affords you to move the handle of our energy bill and helps avert blackouts at peak hours. The smart grid also means new ways to use renewable energy [51]. Power generation can now be scattered across multiple origins, so the system is more stable and productive. It is the understanding to communicate and manage electricity that makes the grid smarter and helps us avoid consuming more fossil fuels in the future.

Most of the world relies on the electricity system built around 50 years ago. These are incapable and cannot offer an appropriate acknowledgment to today's urgent global challenge. Smart grids will be a necessary enabler of this transition. The benefit of smart grid includes renewed productivity and commitment of the electricity supply mixture of more renewable energy into the existing network. Encouraging the development of electric vehicle at a scale, a new solution for the customer to optimize their electricity expenditure compression of carbon emission [50].

i. **IoT in healthcare:** Technology is guiding in a new era of health care fundamentally changing how and where medical decisions are made, and treatment is rendered through a combination of wearable health monitor technology, telemedicine, home diagnosis and even pop up retail settings, healthcare providers have begun to recognize the importance of treating patients remotely. The rising trend of remote healthcare coined house calls plus has allowed for a convenient management of treatment for patients at their homes. Significantly diminishing the cost of invasion as well as enhancing the quality of care.

Pilot programming is showing excellent results with the one program in the U.S reducing the admission rate to the hospitals by 18% for its diabetic patient community who use remote monitoring and interaction and their readmission rates have also dropped by 31%. All this has reduced the cost to the test center by 7%. A dilemma to hospitals runs healthcare program is the approach towards patients using wearables and other personalized technologies to support a variety of examinations which they can directly associate to several benchmarks and decide whether to proceed to a health care professional. Other patients may instead choose to consult the health social network to share a report from their automated reading, consult a physician during Q&A session or even endeavor heartfelt support. Patients may further utilize applications to detect a correlation their condition and medication interaction or bad health practices to make the decision on how to improve their health for the in-depth testing patient could further determine to use home kits or personalized genomic assistance, blood and biomarkers testing. Environmental testing and even predicted by bio-simulation, such a style of healthcare is being termed local convenience store. For those who choose to discuss with health care expert, several options may arise that redirect the patient away from the hospital. Retail outlet in common city centers and clinic location can receive patients, review their information and decide whether to continue with further care by the physician.

IV.SECURITY REQUIRMENTS IN IoT

a. Confidentiality, Integrity, Data privacy

There must be a proper mechanism of encryption to guarantee the confidentiality of data as the IoT data travels through multiple nodes in a network. The integration of services, devices and network, the data stored on a device can be exposed to privacy violation by negotiating nodes exist in an IoT network. The IoT devices sensitive to attacks may cause an intruder to impact the data integrity by altering the stored data for ill-disposed purposes [49].

b. Accounting, Authorization, Authentication

To secure communication in IoT, the authentication is required between two parties communicating with each other. For privileged access to services, the devices must be authenticated. The diversity of authentication mechanisms for IoT exists mainly due to the diverse heterogeneous underlying architectures and environments which support IoT devices. These environments pose a challenge for defining standard global protocol for authentication in IoT. Similarly, the authorization mechanisms ensure that the access to systems or information is provided to the authorized ones. A proper implementation of authorization and authentication results in a trustworthy environment which ensures a secure environment for communication. Moreover, the accounting for resource usage, along with auditing and reporting provide a reliable mechanism for securing network management [49].

c. Availability of Service

The attacks on IoT devices may terminate the outline of services through the traditional denial-of-service attacks. Various tactics including the sinkhole attacks, jamming adversaries or the replay attacks exploit IoT components at different layers to depreciate the quality-of-service (QoS) being produced to IoT users [49].

d. Energy Efficient

The devices are typically resource-constrained and characterized by minimum power and less accommodation. The attacks on IoT architectures may appear in an increase in energy expenditure by flooding the network and consuming IoT resources through redundant or reproduced service requests [49].

V.CATEGORIZATION OF SECURITY ISSUES IN IoT

As IoT comprises of wide variety of devices and equipment from small embedded processing chip to large servers, there are some security issues to be addressed at different level. We have categorized security issues about IoT deployment architecture as below:

1. Low level
2. Intermediate level
3. High level

1. Low level

a. **Jamming adversaries:** The jamming attacks on wireless devices in IoT target degeneration of the networks by releasing frequency signals while not obeying a particular protocol [18,19]. The radio interference severely affects the network operations and can affect the sending and receiving of data by genuine nodes, resulting in malfunctioning or irregular behavior of the system.

b. **Low-level Sybil and spoofing attacks:** The Sybil attacks in a wireless network are prompted by ill-disposed Sybil nodes which use fake identifications to diminish the IoT functionality. On the physical layer, a Sybil node may use random faked MAC values for masquerading as a different device while aiming at the consumption of network resources [20,21]. Consequently, the legitimate nodes may be denied admittance to resources.

c. **Insecure physical interface:** Several physical factors intensify pressing threats to the customary functioning of devices in IoT. The poor physical security, software access through physical interfaces, and tools for testing/debugging may be overworked to negotiate nodes in the network [22].

d. **Sleep deprivation:** The energy compelled devices in IoT square measure prone to ‘‘sleep deprivation’’ attacks by inflicting the detector nodes to remain awake [23]. It results in exhaustion of the battery when a large number of jobs is set to be accomplished in the 6LoWPANenvironment.

2. Intermediate level

a. **Sinkhole and wormhole attack:** Among the sinkhole attacks, the attacker node counters to the routing requests, thereby composing the packets routed through the attacker node which can then be used to perform an ill-disposed activity on the network [25,26]. The attacks on the network might additionally deteriorate the operations of 6LoWPAN (Low Power Wireless Personal Area Network) because of hollow attacks during which a tunnel is formed between 2 nodes in order that packets incoming at a node reach another node instantly [27–29]. These attacks have severe associations including eavesdropping, privacy violation, and denial-of-service.

b. **Sybil on intermediate level:** Similar to the Sybil attacks on low-level layers, the Sybil nodes can be extended to diminish the network performance and even outrage information privacy. The communication by Sybil nodes victimization pretend identities during a network might end in spamming, disseminating malware or launching phishing attacks [30,31].

c. **Authentication and secure communication**: The devices and users in IoT need to be authenticated through key management systems. Any deception in security at the network layer or large overhead of securing communication may exhibit the network to a large number of vulnerabilities [32–34]. For instance, due to constrained resources, the overhead of Datagram Transport Level Security (DTLS) requires to be depreciated, and the cryptographic mechanisms assuring secure communication of data in IoT must be taken into account the performance as well as the scarcity of other resources [35,36].

d. **Transport level end-to-end security:** The transport level end-to-end security strives at rendering a secure mechanism so that the data from the sender node is received by the aspired destination node in a reliable manner [37,38]. It requires absolute authentication mechanisms which assure secure message communication in encrypted form without infringing privacy while working with the merest overhead [39,40].

e. **Session establishment and resumption:** The session hijacking on transport layer with transcribed messages can result in denial-of-service [41,42]. An attacking node can portray the victim node to continue the session between two nodes. The human activity nodes sway even need for re-transmission of messages by neutering the sequence numbers.

3. High level

a. **CoAP security with internet:** The high-level layer containing the application layer is also exposed to attacks [44–46]. The Constrained Application Protocol (CoAP) being a web transfer protocol for compelled device uses DTLS bindings with various security modes to provide end-to-end security. The CoAP messages follow an appropriate format outlined in RFC-7252 (Remote Function Call) [17], which need to be encrypted for secure communication. Similarly, the multicast support in CoAP needs adequate key management and authentication mechanisms.

b. **Insecure interface:** For accessing IoT services, the interfaces employed within web, mobile, and cloud are exposed to different attacks which may rigorously sway the data privacy [22].

c. **Insecure software/firmware:** Various vulnerabilities in IoT include those generated by insecure software/firmware [22]. The code with languages like JSON, XML, SQLi, and XSS needs to be examined carefully. Similarly, the software/firmware updates got to be disseminated during a secure manner.

d. **Middleware security:** The IoT middleware composed to furnish communication among heterogeneous entities of the IoT criterion must be secure enough for the prerequisite of services. Different interfaces and environments using middleware need to be consolidated to provide secure communication [47,48].

VI. INTRODUCTION TO BLOCKCHAIN

A blockchain may be a chain of blocks that contains information. It is a technique described in 1991 by a group of researchers and it is originally intended to timestamp the digital document. So that, it is not possible to change the date of document or to tamper with them almost like a notary. However, it has not in use until it was redefined by Satoshi Nakamoto in 2009 to create digital cryptocurrency called Bitcoin. A blockchain may be a distributed ledger that's fully receptive anyone. They have a noteworthy property: once some knowledge has been recorded within a blockchain, it is not an easy task for any human to change it. How it will work? By taking a closer look at the block, each block is having some knowledge, the hash of the block and the hash of the previous block. The data that's held on within a block depends on the sort of blockchain. The bitcoin blockchain for instance stores the small amount of the print data like a few dealings in here, such as sender, receiver and amount of coins. It also contains a hash value for the block. Comparison of a hash can be done with the fingerprint of a human. It indicates a block and all its content, and it is always as unique just like a fingerprint.

As soon as a block is formed its hash is being calculated. When we are changing one thing within the block can make the hash to vary. So, in other words, when you want to detect changes in any block the hash value is very useful. If the signature of a block is changed its not the same block as per the previous block. The third component within every block is that the hash of the previous block. This mainly creates a chain of a block and it's this technology that makes a blockchain so secure. Let's take an example, Here we have the chain of 3 blocks, As shown in fig, each block has a hash and the hash of the previous block, so block number:3 have the hash of the block number:2 and block number:2 have the hash of the block number:1. Now the first block is a bit special, it cannot direct to the previous block because it's the first block called as a genesis block.

Now let's say anyone tamper the any one of the three blocks. It can cause the hash value of that intended block change as well. In turn that will make block 3 and blocks after the block 3 invalids because they are no longer store a valid hash value of the previous block, so changing only a single block or changing the small amount of data will make all following blocks invalid. Using only hash value to secure data is not enough to prevent an adversary. The computers these days are very fast enough to calculate hundreds or thousands of the hash values per second. Any malicious person could effectively change the data within a block and recalculate all the hash value for the other blocks to make your blockchain valid again. To make less effect of this, blockchain has something called Proof-of-Work. It is a mechanism which slows down the formation of the new blocks. In the case of the bitcoin, the calculation time is about 10 minutes to calculate the appropriate proof of work and add a new block to the chain. This mechanism makes it very hard to tinker with the blocks because if anyone tampers with one block, you'll need to calculate the proof of work again for all the following blocks. The security of the blockchain comes from its effective use of the hashing and proof of work mechanism.

But there is also one more way that blockchain can secure themselves and that is by being distributed in nature. Instead of engaging a central entity to manage the chain. The Blockchain uses a peer-to-peer network and everyone can join the desired network. When someone enters into this network, he/she gets the full copy of blockchain. The node will use this to verify that all the things continue to be so. When someone forms a new block in the network, that block is sent to each and every one on the network. Each node then certifies the block to form a certain signature that it hasn't been tinkered with. If all the things or the data is verified out, then each node add this new block to their own blockchain. Each of the nodes in this network creates consensus. They all agree upon which blocks are verified and which are not. The Blocks that are tinkered with are going to be rejected by different nodes within the network. To successfully tinkered within a blockchain you will need to tinker with all blocks on the chain, also recalculate the proof of work for each block and then dominate more than 50% of the peer-to-peer network. Only then the tinkered block is accepted by everyone else. This is almost absurd to do. The blockchain technology can be used for another thing like storing medical record, creating a digital notary and collecting taxes.

VII. BENEFITS OF BLOCKCHAIN

- **No Third-Party Seizure**: No central authority can manipulate or seize the currency since every currency transfer happens peer-to-peer just like hard cash. Bitcoins are yours and only yours, and the central authority can't take your cryptocurrency, because it does not print it, own it, and control it correspondingly [52].
- **Namelessness and transparency**: Unless Bitcoin users publicize their case addresses in public, it is extremely hard to trace transactions back to them. However, even if the wallet addresses were publicized, a new wallet address can be easily generated. This greatly increases privacy. when compared to traditional currency systems, where third parties potentially have access to personal financial data. Moreover, this high anonymity is achieved without sacrificing the system transparency as all the bitcoin transactions are documented in a public ledger [52].

- **No taxes and lower dealings fees**: Because of its redistributed nature and user namelessness, there is no viable way to implement a Bitcoin taxation system. In the past, Bitcoin provided instant transactions at nearly no price. Even now, Bitcoin has lower dealings prices than a MasterCard, PayPal, and bank transfers. However, the lower transaction fee is only beneficial in situations where the user performs a large value international transaction. This is as a result of the common dealings fee becomes higher for terribly tiny price transfers or purchases like paying for normal social unit commodities [52].
- **Theft resistance**: Stealing of bitcoins is not possible until the adversary has the private keys (usually kept offline) that are associated with the user wallet. Bitcoin provides security by design, for instance, unlike with credit cards you don't expose your secret (private key) whenever you make a transaction. Moreover, bitcoins are free from Charge-backs, i.e., once bitcoins are sent, the transaction cannot be reversed. Since the ownership address of the sent bitcoins will be changed to the new owner, and it is impossible to revert. This ensures that there's no risk concerned once receiving bitcoins [52].

VIII. ATTACKS ON BLOCKCHAIN

1. **Double spending or Race attack**
   In this attack it appends the same bitcoins in multiple transactions and send two conflicting transactions in rapid successions. The primary targets of this attacks are sellers and merchants. The adverse effect of this attack are sellers lose their product, it drives away the honest users and creates blockchain forks. There can be possible counter measures for this attack like inserting observers in the network, communicating with the double spending alert among the clients and merchants can disable the direct incoming connections.
2. **Finney attack**
   In this Finney attack there are dishonest miners which broadcast the pre-mined block for the purpose of double spending as early as it receives product from a merchant. By this attack the primary targets are also sellers and merchants. The effect of this attack is it facilitate the double spending of the bitcoin.
3. **Brute force attack**
   The brute force attacks the attackers privately mining on the blockchain fork to perform the double spending attack. By this attack the primary targets are seller and merchants. There are adverse effects of this attack as it facilitates double spending and creates large size of blockchain forks.
4. **One configuration attack**
   The one configuration attack is the combination of the double spending and Finney attack. It targets the bitcoin exchange services. The adverse effect of this attack is that it facilitates double spending of larger number of bitcoins. There can be possible counter measure for this attack can be like inserting the observer in the network and notify the merchant about ongoing double spending.
5. **Block discarding or selfish mining**
   In this attack the attacker abuses the bitcoin forking feature to derive an unfair reward. The primary targets of this attacks are honest miners or mining pools. The adverse effect of this attacks is it introduce the race conditions of forking, wasting of the computational power of the honest miners, and with >50% it leads to the gold finger attack. The possible counter measures of this attacks are use of the zero-block technique.
6. **Greater than 50% hash power**
   In this attack the adversary controls more than 50% of the hash rate. The primary target of this attack is the bitcoin network miners, bitcoin exchange centers and the users. The adverse effect of this attack is to drive away the miners working alone or within small mining pools, and it weakens the consensus protocol, and denial of services. There can be some of the possible counter measures for this attack can be like by inserting observers in the network and communicating double spending alert among the communicating peers.
7. **Block withholding**
   In this attack, the miner in the pool submits only PPoWs (Partial Proof of Work) but not the FPoWs (Full Proof of Work). By this attacks the primary target of the attackers are the honest miners or mining pools. The adverse effect of this attack is it wastes the resources of fellow miners and decrease the pool revenue. There can be some possible counter measure as it can include only known and trusted miners in the pool, it dissolves and close the pool hen revenue drops from expected.
8. **Fork after withholding attack**
   In this attack, it improves on the adverse effect of the selfish mining and block withholding attack. The primary targets of the attackers in this attack are honest miners or mining pools. The adverse effect of this attack is it wastes resources of the fellow miners and decreases the pool revenue. There is no practical defense reported so far for this attack.
9. **Refund attack**
   In this attack, the attackers exploit the refund policies of the existing payment processes. The primary targets of this attack are sellers or merchants and users. The adverse effect of this attack is merchant losses the money while honest users might lose their reputation. To counter this attack possible counter measure can be as on can have publicly verifiable evidence.
10. **Time jacking**

In this attack the adversary speeds up the majority of the miner's clock. The target in this attack is the miners. The adverse effect of this attack is it isolate a miner and waste its resources, it influences the mining difficulty calculation process. The possible counter measures are constraint tolerance ranges or network time protocol.

11. **Distributed Denial of Service**
    In this attack, there is a collaborative attack to exhaust network resources. The primary targets of this attack is bitcoin network business miners and users. The adverse effect of this attack is it deny the services to honest user/miners, it isolates or drive away the miners. There are possible measures can be applied to counter the attack are Proof of Activity protocol and fast verification signature-based authentication.
12. **Sybil**
    In this attack, the adversary creates multiple virtual identities. The primary targets of this attack are bitcoin network, miners and users. The adverse effect of this attack is it facilitates the time jacking, DDoS, and double spending attacks, also it threatens the user privacy.
13. **Eclipse or net split**
    In this attack, the adversary monopolizes all incoming and outgoing connections of the victims. The primary targets of this attack are miners and users. The adverse effect of this attack is the inconsistent view of the network and block chain, it enables double spends with more than one confirmation. The counter measure for this attack can be use of the whitelist and disabling incoming connections.

IX. PROPOSED MODEL

The IoT requires third party authority for storage of data on the server which are semi trusted, it means they can do any misuse of data of the owner as they can sell the data to make more profit from it. There is also an issue when the user creates a weak password for his account. If any attacker can gain the password, then he/she can get the access to the data and can misuse the data. This is a vulnerability in the existing system. It can hinder the integrity of the data which can change the meaning of the data.

To overcome this vulnerability, we use blockchain technology with IoT to secure the data and preserve the integrity of the data. Blockchain provides several benefits over existing IoT technology as it provides decentralized storage of data, immutability of data, and transparency to the data which is not present in the existing third-party authority.

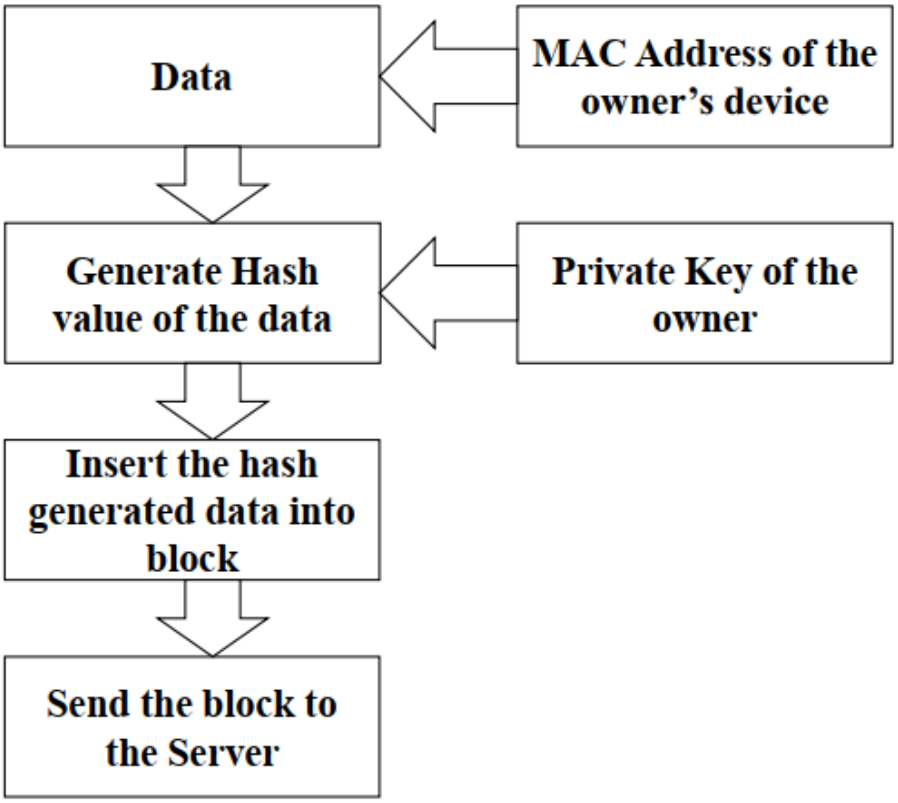

Figure-1 Generating Block of Data and Sending to the server

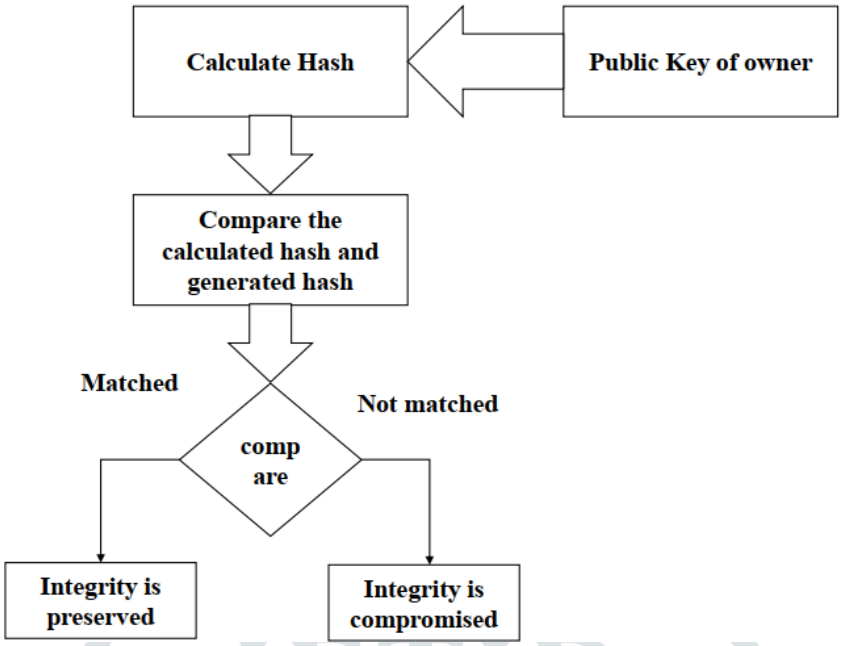

Figure-2 Checking Integrity of Data

X. CONCLUSION

The IoT devices are insecure and incapable to defend any attack happen on it. This is because resources in IoT devices are limited, no global standards, and there is no guarantee of secure hardware and software design, development, and deployment. In this paper, we survey and review main IoT security issues. We categorize them in different layers as high layer, intermediate layer, low level. Also discuss about different application of IoT. The paper also give review of the blockchain. Benefits of blockchain with respect to the security. At last we discuss the attacks that can affect the blockchain. Here we also proposed a solution to make sure that integrity of data is preserved using the Blockchain and in future we would implement the proposed model in real world.

REFERENCES

[1] Ashwini , k., & sonali , b. (2018). SURVEY ON INTERNET OF THINGS (IOT) SECURITY ISSUES & SOLUTIONS. *Proceedings of the Second International Conference on Inventive Systems and Control (ICISC 2018)*, 307-312.

[2] Göran Pulkkis, Jonny Karlsson, and Magnus Westerlu. (2018). Blockchain-Based Security Solutions for IoT Systems. *Internet of Things A to Z: Technologies and Applications*, 255-273.

[3] Pradip Kumar Sharma, Jong Hyuk Park. (2018). Blockchain based hybrid network architecture for the smart city. doi:https://doi.org/10.1016/j.future.2018.04.060

[4] TIAGO M. FERN`NDEZ-CARAMÉS, & PAULA FRAGA-LAMAS. (2018). A Review on the Use of Blockchain for the Internet of Things. *6*, 32979-33001.

[5] Yash Gupta, & Rajeev Shorey, Devadatta Kulkarni and Jeffrey Tew. (n.d.). The Applicability of Blockchain in the Internet of Things. 561-564.

[6] Alioto, M. (2017). *Enabling the Internet of Things From Integrated Circuits to Integrated Systems.* Springer International Publishing AG 2017.

[7] Dimitrios Serpanos, Marilyn Wolf. (2018). *Internet-of-Things (IoT) Systems Architectures, Algorithms, Methodologies.* Springer International Publishing AG 2018. doi:https://doi.org/10.1007/978-3-319-69715-4

[8] Shahrestani, S. (2017). *Internet of Things and Smart Enviroment Assistive Technologies for Disability, Dementia, and Aging.* Springer International Publishing AG 2017. doi: 10.1007/978-3-319-60164-9

[9] Klein, S. (2017). *IoT Solutions in Microsoft's Azure IoT Suite Data Acquisition and Analysis in the Real World.* Apress. doi:10.1007/978-1-4842-2143-3

[10] Sayed Hadi Hashemi, F. F. (2016). World of Empowered IoT Users. *2016 IEEE First International Conference on Internet-of-Things Design and Implementation*, 13-24. doi:10.1109/IoTDI.2015.39

[11] Ammar Rayes, S. S. (2017). *Internet of Things—From Hype to Reality.* Springer International Publishing AG 2017. doi:10.1007/978-3-319-44860-2

[12] Kang Bing, L. F. (2011). Design of an Internet of Things-based Smart Home System. 921-924.

[13] http://blog.externetworks.com/iot-wearable-technologies-the-future/

[14] Dennis Kengo Oka, T. F. (2014). Survey of Vehicle IoT Bluetooth Devices. *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, 260-264. doi:10.1109/SOCA.2014.20

[15] https://internetofthingsagenda.techtarget.com/definition/Industrial-Internet-of-Things-IIoT

[16] https://www.analyticsvidhya.com/blog/2016/08/10-youtube-videos-explaining-the-real-world-applications-of-internet-of-things-iot/
[17] Z. Shelby, K. Hartke, C. Bormann, The constrained application protocol (CoAP), 2014. URL https://tools.ietf.org/html/rfc7252.
[18] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, MobiHoc '05, ACM, New York, NY, USA, 2005, pp. 46–57. http://dx.doi.org/10.1145/1062689.1062697.
[19] G. Noubir, G. Lin, Low-power DoS attacks in data wireless LANs and countermeasures, SIGMOBILE Mob. Comput. Commun. Rev. 7 (3) (2003) 29–30
[20] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Channel-Based detection of sybil attacks in wireless networks, IEEE Transa. Inf. Forensics Secur. 4 (3) (2009) 492–503.
[21] Y. Chen, W. Trappe, R.P. Martin, Detecting and localizing wireless spoofing attacks, in: 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2017, pp. 193–202
[22] OWASP, Top IoT Vulnerabilities, 2016. URL https://www.owasp.org/index. php/Top_IoT_Vulnerabilities
[23] T. Bhattasali, R. Chaki, A survey of recent intrusion detection systems for wireless sensor network, in: D.C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, D. Nagamalai (Eds.), Advances in Network Security and Applications: 4th International Conference, CNSA 2011, Chennai, India, July 15–17, 2011, Springer Berlin Heidelberg, Berlin, Heidelberg, 2011, pp. 268–280.
[24] A. Dvir, T. Holczer, L. Buttyan, VeRA - version number and rank authentication in RPL, in: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 2011, pp. 709–714. http://dx.doi.org/10.1109/MASS.2011.76.
[25] K. Weekly, K. Pister, Evaluating sinkhole defense techniques in RPL networks, in: Proceedings of the 2012 20th IEEE International Conference on Network Protocols (ICNP), ICNP '12, IEEE Computer Society, Washington, DC, USA, 2012, pp. 1–6. http://dx.doi.org/10.1109/ICNP.2012.6459948.
[26] F. Ahmed, Y.-B. Ko, Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks, Secur. Commun. Netw. 9 (18) (2016) 5143– 5154 SCN-16-0443.R1.
[27] A.A. Pirzada, C. McDonald, Circumventing sinkholes and wormholes in wireless sensor networks, in: International Workshop on Wireless Ad-Hoc Networks, 2005.
[28] W. Wang, J. Kong, B. Bhargava, M. Gerla, Visualisation of wormholes in underwater sensor networks: A distributed approach, Int. J. Secur. Netw. 3 (1) (2008) 10–23.
[29] M. Wazid, A.K. Das, S. Kumari, M.K. Khan, Design of sinkhole node detection mechanism for hierarchical wireless sensor networks, Sec. Commun. Netw. 9 (17) (2016) 4596–4614. http://dx.doi.org/10.1002/sec.1652.
[30] K. Zhang, X. Liang, R. Lu, X. Shen, Sybil attacks and their defenses in the internet of things, IEEE Internet Things J. 1 (5) (2014) 372–383. http://dx.doi.org/10.1109/JIOT.2014.2344013.
[31] G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng, B.Y.Zhao, Social turing tests: Crowdsourcing sybil detection, in: Symposium on Network and Distributed System Security, NDSS, 2013.
[32] J. Granjal, E. Monteiro, J.S. Silva, Network-layer security for the Internet of Things using TinyOS and BLIP, Int. J. Commun. Syst. 27 (10) (2014) 1938–1963. http://dx.doi.org/10.1002/dac.2444.
[33] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, U. Roedig, Securing communication in 6LoWPAN with compressed IPsec, in: 2011 International Conference on Distributed Computing in Sensor Systems and Workshops(DCOSS), 2011, pp. 1–8. http://dx.doi.org/10.1109/DCOSS.2011.5982177.
[34] J. Granjal, E. Monteiro, J.S. Silva, Enabling network-layer security on IPv6 wireless sensor networks, in: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, 2010, pp. 1–6. http://dx.doi.org/10.1109/GLOCOM.2010.5684293.
[35] P.N. Mahalle, B. Anggorojati, N.R. Prasad, R. Prasad, Identity authentication and capability based access control (iacac) for the internet of things, J. Cyber Secur. Mobility 1 (4) (2013) 309–348.
[36] D.U. Sinthan, M.-S. Balamurugan, Identity authentication and capability based access control (IACAC) for the Internet of Things, J. Cyber Secur. Mob.1 (4) (2013) 309–348.
[37] M. Brachmann, O. Garcia-Morchon, M. Kirsche, Security for practical CoAP applications: Issues and solution approaches, in: 10th GI/ITG KuVS Fachgespraech Sensornetze (FGSN 2011), 2011.
[38] J. Granjal, E. Monteiro, J.S. Silva, End-to-end transport-layer security for internet-integrated sensing applications with mutual and delegated ecc public-key authentication, in: 2013 IFIP Networking Conference, 2013, pp.1–9.
[39] G. Peretti, V. Lakkundi, M. Zorzi, BlinkToSCoAP: An end-to-end security framework for the Internet of Things, in: 2015 7th International Conference on Communication Systems and Networks (COMSNETS), 2015, pp. 1–6. http://dx.doi.org/10.1109/COMSNETS.2015.7098708.
[40] S. Raza, T. Voigt, V. Jutvik, Lightweight IKEv2: a key management solution for both the compressed IPsec and the IEEE 802.15. 4 security, in: Proceedings of the IETF Workshop on Smart Object Security, vol. 23, 2012.
[41] N. Park, N. Kang, Mutual authentication scheme in secure internet of things technology for comfortable lifestyle, Sensors 6 (1) (2016) 20–20.
[42] M.H. Ibrahim, Octopus: An edge-fog mutual authentication scheme, Internat.J. Netw. Secur. 18 (6) (2016) 1089–1101.

[43] M. Henze, B. Wolters, R. Matzutt, T. Zimmermann, K. Wehrle, Distributed configuration, authorization and management in the cloud-based internet of things, in: 2017 IEEE Trustcom/BigDataSE/ICESS, 2017, pp. 185–192. http://dx.doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.236.

[44] M. Brachmann, S.L. Keoh, O.G. Morchon, S.S. Kumar, End-to-end transport security in the IP-based Internet of Things, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN, 2012, pp. 1–5.http://dx.doi.org/10.1109/ICCCN.2012.6289292.

[45] J. Granjal, E. Monteiro, J.S. Silva, Application-layer security for the WoT: extending CoAP to support end-to-end message security for internet-integrated sensing applications, in: International Conference on Wired/Wireless Internet Communication, Springer Berlin Heidelberg, 2013, pp. 140–153.

[46] M. Sethi, J. Arkko, A. Kernen, End-to-end security for sleepy smart object networks, in: 37th Annual IEEE Conference on Local Computer Networks - Workshops, 2012, pp. 964–972. http://dx.doi.org/10.1109/LCNW.2012.6424089.

[47] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, M.A. Spirito, The VIRTUS middleware: An XMPP based architecture for secure IoT communications, in: 2012 21st International Conference on Computer Communications and Networks, ICCCN, 2012, pp. 1–6. http://dx.doi.org/10.1109/ICCCN.2012.6289309.

[48] C.H. Liu, B. Yang, T. Liu, Efficient naming, addressing and profile services in Internet-of-Things sensory environments, Ad Hoc Netw. 18 (Suppl. C) (2014) 85–101. http://dx.doi.org/10.1016/j.adhoc.2013.02.008.

[49] Minhaj Ahmad Khan, K. S. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems 82 (2018)*, 395-411. doi:https://doi.org/10.1016/j.future.2017.11.022.

[50] Junaid Ahmed Khan , Hassaan Khaliq Qureshi, & Adnan Iqbal. (2014). Energy management in Wireless Sensor Networks: A survey. *Computers and Electrical Engineering*, 1-13.

[51] Waleed Ejaz, M. N. (2017). Effcient Energy Management for the Internet of Things in Smart Cities. 84-91.

[52] Mauro Conti, Sandeep Kumar, Chhagan Lal, & Sushmita Ruj. (n.d.). A Survey on Security and Privacy Issues of Bitcoin