EasyChair Preprint

№ 7097

Emerging Technologies Approach to Secure IOT Data

Sandeep Singh Bindra, Aaisha Makkar and Piyush Samant

November 28, 2021

Emerging Technologies Approach to Secure IOT Data

ABSTRACT: Internet of Things (IoT) devices are working in different areas like smart city, medical services environment, agriculture, home automation. These devices send data or information through different actuators, sensors, handsets, or different wearable gadgets. The IoT produces a lot of data and this data might be utilized to identify security threats thus increasing the productivity of Artificial Intelligence (AI) techniques. As of now, security is a major issue in IoT, for this reason, researchers have presented numerous data security models in recent years. A critical need for empowering such methodologies is the improvement of adaptable foundations for gathering and handling security-related datasets from IoT frameworks and gadgets. Information in IoT devices is vulnerable to numerous threats or attacks and may be at risk. Therefore, there is a need for a security mechanism that is vital to coping up with privacy as well as security challenges concerned with IoT. Despite the research, researchers have not achieved much in security level. Through this chapter, analysis of security for IoT devices has been made considering emerging technologies like Mobile computing, Blockchain, Cybersecurity, Cloud Computing, and Big Data.

1. INTRODUCTION

IoT is quickly developing and growing advancements for the real world that communicate with each other. The result of IoT gadgets is consolidating the operational technology (OT) and information technology (IT) [1].

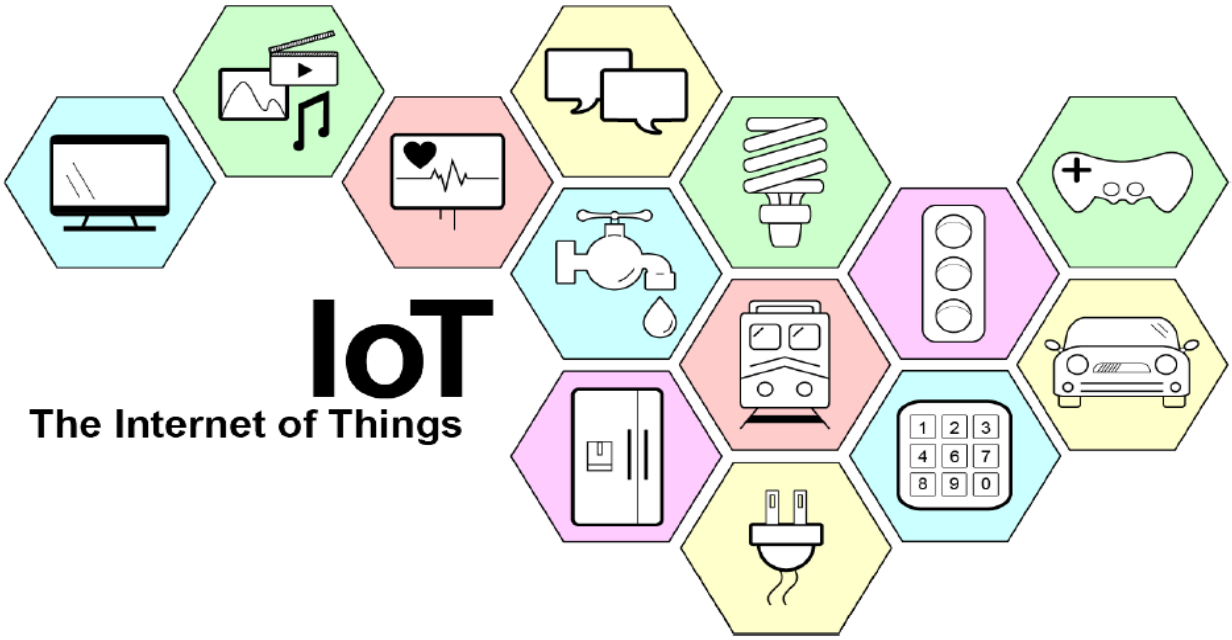

Fig 1: IoT devices [2]

IoT gadgets can be useful for organization networks and hardware that recently needed them, empowering new efficiencies and innovative abilities for the equipment, for example, remote monitoring setup, and investigating. IoT can likewise add the capability to examine the information and for decision making, utilizes the outcomes. While the extent of IoT isn't characterized, it is very vast. Each area has its kinds of IoT devices, for example, particular clinic hardware in the medical care area and smart lane advancements in smart transportation, and a lot of IoT gadgets that each area can utilize. Virtual variants of devices that are used on daily basis like light, bulbs, home automation, kitchen appliances, security systems, smart air conditioning systems, and LED TVs[3]. Many associations are not even aware of using IoT devices, so they need to know the importance of it. Organizations need to know how these IoT devices affect privacy and security. Once these organizations know the security issues of these devices

they will understand the risk and avoid the casual approach towards handling these devices. The actual idea of IoT gadgets is to gather information and transfer it through an interchanges channel and often control a lot bigger unit. The information being referred to can go from body temperature, heartbeat, room temperature, and an area used by the user[4]. IoT devices are given network connectivity all the time thus being targeted easily by malware so increasing the threat. For few devices, we can use different levels of software protection like firmware but these methods are considered to be easily bypassed able and hardware is left for attacks. Some IoT devices that are used for commercial purposes are directly connected with the end-users and are designed with the importance of secured features in an ad-hoc fashion where only the remote attack is considered as a threat, so commercial devices regularly experience the ill effect of equipment level weaknesses which might be exploited remotely[5].

1.1 IoT data advantages

When the gadgets and sensors are organized together? How could the IoT influence our day-to-day life? GPS frameworks, thermostats, and other systems, all send and get consistent data to screen and computerize exercises in our recheck our daily routine and activities. Every part of our life is connected to devices that may send or get information over the Internet. Openings, where flow of information will make business sectors move in this direction or to improve an existing system, are analyzed by organizations. A few instances of areas that are recorded beneath

1.2 Security Issues in IoT Data

1.2.1 End-to-end (E2E) data protection to ensure information security in IoT climate, E2E information protection over whole IoT administration ought to be given. Different type of information is produced from different sources suddenly imparted to cloud under open network. Thus, it requires the information security system to control and oversee security data and confidential information in its life cycle.

1.2.2 Secure Orchestration is the automated setup for coordination and configuration of computer systems. In such a circumstance, the associated devices ought to have the option to keep the required security level. For example, neighborhood gadgets and sensors utilized in the home ought for safe communication with one another.

1.2.3 Apparent Security and Privacy Many security issues are generally due to user misconfiguration. It is truly challenging and unreasonable for users to understand the complexity of rules. So there is a need for automatic security and privacy of the systems.

Fig 2: Security Vulnerabilities

1.3 Many points of Vulnerability

Every gadget and sensor is at risk in the IoT structure. These gadgets can't, consistently, be trusted to safeguard the privacy of the information gathered and the trustworthiness of the information sent. These gadgets are regularly left unattended and can be targeted easily. A malicious program that can catch these gadgets, can separate insider facts, modify programming and hold them under its influence, for example, web cameras, TVs, home automation, smart locks can be easily targeted. Passwords are critical concerning validation and numerous IoT gadgets. Most of the devices have weak authentication systems which can be easily cracked.

1.3.1 Encryption

IoT gadgets have explicit functional limitations which should be considered before to executing any safety efforts. A superior handling system expected to help encryption is hard to acknowledge as cost factor matters for the user.

1.3.2 Updates and Patches

IoT gadgets must be consistently updated to be safe from cyber threats. If the device is not updated there may be a chance of a cyber-attack. There are some cases in which security vulnerability is observed to be exceptionally late after production. There may be many reasons like cost factor to build low-cost devices, resource unavailability, so a user is left with unsupported IoT device which may be attacked. The majority of the IoT gadgets are worked from modest chips, which in itself doesn't permit producers to give security patches to them. Because of improper communication, a user might not be able to update the device.

1.3.3 Market Competition

Due to huge competition in the market, companies are releasing their devices in the market without security checks as the deployment of products is the main priority for developers. This may result in creating a poor system and may arise serious security issues.

1.3.4 Security Impact

As illustrated, unsecured IoT devices are easily attacked by attackers. The impacts of attackers could go from total loss of the device data[6]. Like unsecured Haier device can activate the hackers to hijack the device functionality. Moreover, considering the device particulars of the Haier base unit, an attacker can use malicious code and enter the device data to get the details or to connect with another device. As it gives a rich working framework environment, devices like Haier can be utilized to give services to the local networks. The device could likewise take an interest in handling attacks for Address Resolution Protocol (ARP), taking on the appearance of the router. Industrial devices represent a much greater danger whenever compromised, as a basic framework might be harmed. In a smart meter system, an attacker might steal the meter reading while transferring from the meter to a nearby meter reading office. So attacker may be capable to change the meter reading for false energy consumption reports. Moreover, reading can be modified to get the less consumption bill which may be a big issue [7]. This can affect the economy by generating less revenue for more energy consumption without making the proper records.

1.3.5 Safety Issues

The arrangement of compromised IoT gadgets will provoke security inconveniences. In view of the administrations these gadgets give, an attacker can utilize these gadgets to make harm to the system. Compromised IoT devices like smart meter Centron CL200, might be utilized to harm the frameworks, for example, giving the wrong reading will lead to unnecessary load on the power grid but generating less revenue.

1.3.6 Privacy Issues

Haier device being a home automation system offers a motion sensor, an attractive sensor that can be utilized to know if the door is being opened, and remote equipment to turn other devices on or off. An

attacker can create a similar profile like the user to operate a Compromised Haier device thus leaking the information of the user.

a) **Numerous IoT gadgets communicate with the actual world in manners regular IT gadgets generally don't** [2] The expected effect of some IoT devices making changes to actual frameworks and subsequently influencing the actual world should be explicitly recognized and tended to cybersecurity and protective points of view. Additionally, operational necessities for execution, dependability, strength, and security might be at chances with regular practices of cybersecurity and privacy for traditional IT devices.
b) **Numerous IoT gadgets can't be managed, accessed, or observed in similar ways conventional IT gadgets can** [4] This can require tackling assignments physically for huge quantities of IoT devices, extending staff information and devices to incorporate a lot more extensive variety of IoT device programming, and analyzing risk with creators and third parties that control the IoT devices remotely.
c) **The accessibility and efficiency of network cybersecurity and privacy abilities are regularly unique for IoT gadgets than conventional IT gadgets** [8] This implies associations may need to choose, actualize, and deal with extra controls, just as decide how to react to risks when adequate controls for relieving risks are not accessible.

1.4 Commercial and Home IoT Devices

1.4.1Smartcare Device, Powered by Haier

A SmartCare device designed by Haier company can be used to manage and study data from user homes with the help of a sensor that can manage smoke alarm, water spillage, door locking information, and an on/off button.

Fig 2: Smart Care System, powered by Haier [9]

The main purpose of this device is to allow a user to monitor their home remotely with sensor-based system. Users need to download an app from IOS/Playstore. Then, they should connect the SmartCare device to their internet, after that connecting smartphone to a nearby network similar to SmartCare connectivity. Whenever required, users can check the records on mobile applications from cloud services offered by the manufacturer, which permits users to check outside sensor information of neighborhood organizations. Whenever required, the user can check the data from the SmartCare application of mobile.

1.4.2 ITRON CENTRON CL200 SMART DEVICE

Fig 3: Itron CentronCL200 Smart Meter [9]

This IoT device is additionally utilized in applications of Industry. The essential usefulness of this device is to identify the energy usage of customers and report the gathered data through an RF channel to the meter reading office which is nearby. This data can be used to generate the power bill depending upon the energy utilization of the user.

2 CLOUD COMPUTING APPROACH FOR IoT DATA

The most recent thing in the Internet world is to interface all the devices to the Internet to redesign the idea of our everyday life, thus inciting the advancement of the Internet of things (IoT). In this way, there has been a colossal improvement in the number of smart gadgets that are web empowered, for instance, cell phones, Machine to Machine (M2M), home automation, and wearable gadgets, and this example is as yet expanding in future [10]. The possibility of IoT is just possible due to the new advances in, figuring, networking advances and Internet protocol. The most tedious task is still to deal with the enormous information that is produced through these IoT gadgets called as big data which is created through various remote IoT gadgets [11]. Other than these sources, information is quickly expanding consistently as distant gadgets are continually extending the volume which incorporates cell phones and IoT networks. Billions of these gadgets are associated with the web is making another skyline of the digital actual climate in the territory of cell phones, home automation, medical care, smartphones, transportation, etc. In these frameworks, most of the gadgets create huge information that requires capacity and investigating abilities in a secured way. So the thought of cloud resources can settle the issue of examining and security capacities with the advantage of accessing remotely[12]. Along these lines, cloud resources can assist with defeating the information burden of IoT gadgets. For IoT gadgets, there's consistently an issue of latency, real-time access that can be resolved. Due to a couple of drawbacks, the cloud can't fulfill the recently referenced necessities. Mobile Cloud computing is the result of interdisciplinary methodologies joining cloud computing and mobile computing.

Two viewpoints for which the term Mobile Cloud is taken: Infrastructure based, and Mobile Adhoc cloud. In the Infrastructure based and mobile ad-hoc cloud hardware infrastructure remains static which provides the services to the user.

2.1 Cloud Computing Features
Features of cloud computing can be analyzed as follows.

2.1.1 Storage over the internet
It can be characterized as an innovative system that utilizes TCP/IP network. This Storage is also called Storage over Internet Protocol (SoIP). In this combination, IP provides increased performance and scalable IP solutions.

2.1.2 Service over the internet
The primary target of the Service over the Internet is to be resolved to help clients all around the world better services of the Internet.

2.1.3 Applications over the internet
Programs that can be run on the Internet virtually and perform the desired task on a cloud server rather than the traditional approach of software installed on the systems and run on local machines. In this user only needs internet connectivity and a basic system with a browser that can do any task.

2.1.4 Privacy
Privacy of data is most important for users and this is the only constraint for users to adopt mobile cloud computing. So, the application models must support the privacy of the users. The service provider should guarantee that their framework is secure and that their customers' information and applications are ensured while the client should take measures to invigorate their application and use strong authentication methods and passwords.
Regardless, edge figuring adds various points of interest to cloud-helped IoT and supports recently referenced essentials by keeping information taking care of, capacity, and interchanges to the close by gadgets at edge servers to the significant distances[13]. It can be a smartphone or any other gadget which can collaborate successfully with the cloud servers. Expanding accessibility of smart gadgets provide data sharing inside cloud-enabled IoT applications. The information is of little use if the devices don't impart information to other associated devices. Information sharing at the edge permits smart gadgets with lower latency and quick information access with higher transfer speed. In the fifth generation (5G), all the types of wireless communication caching will be distributed on the network which will lead to a challenging task to coordinate the proper utilization of distributed data [14]. So, it will a tedious task to design future wireless IoT networks that lead to cloud computing which gives pervasive and on-request access to an essentially shared pool of configurable storage resources[15]. Cloud computing is a phenomenal platform to deal with the tremendous data produced from the IoT devices because of less expensive and virtual registering/processing power accessible at the cloud center. Consequently, the latest thing is towards IoT-cloud union with the vast majority of the IoT stages upheld with cloud computing. However, it isn't reasonable for the applications demanding low-latency and high quality of Service (QoS). Edge Computing is accepting significant consideration to overcome some cloud computing drawbacks. The fundamental objective of edge computing is to stretch out the cloud computing functions to the network edges. Because of nearness to the end clients and geologically appropriated arrangement, it can uphold the service requesting the necessities of low latency, high QoS, and greater mobility.

3 CYBERSECURITY APPROACH FOR IoT DATA
IoT is a quickly developing as well as growing assembly of different technologies. Numerous associations as of now utilizing and what IoT gadgets may mean for cybersecurity and protection risks uniquely in contrast to information technology (IT) gadgets do [16] [3].

3.1 Cybersecurity for IoT gadgets in terms of risk reduction goals:

3.1.1 Device security protection. All in all, keep a gadget from being utilized to direct attacks, including DDoS attacks by trading off different gadgets on a similar organization fragment [17].
3.1.2 Data security protection Security, easy accessibility, and integrity of the information gathered by or handled by the IoT gadget. The main objective is to protect the information of IoT gadgets that need security [18].
3.1.3 Privacy of individuals' protection. Ensure people's security, handling risk-managed by device security. This objective applies to all IoT gadgets that interact straightforwardly or by implication to anyone [19]. Every objective expands on the past objective and doesn't restore the requirement for it. Meeting every one of the risk objectives includes tending to migration regions. Each area characterizes a part of network safety or cybersecurity alleviation thought to be most essentially or surprisingly influenced for IoT by the risk considerations. At last, there is at least one difficulty that IoT gadgets may posture to every assumption. Figure 4 portrays the final product of these linkages, which is the distinguishing proof of an organized arrangement of possible challenges with relieving cybersecurity for IoT gadgets that can be followed back to the risk[2].

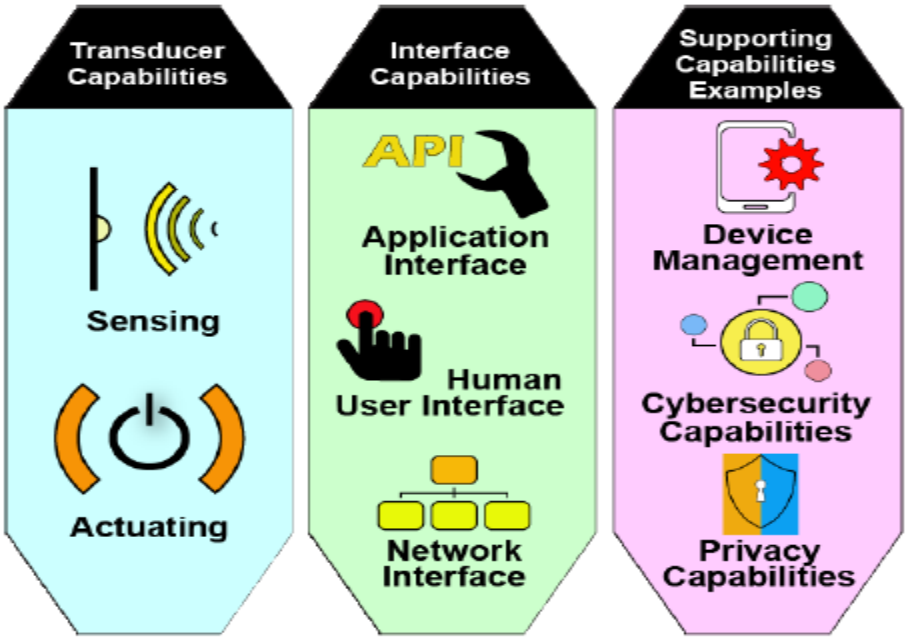

Fig 4: IoT Device Capabilities Potentially Affecting Cybersecurity and Privacy Risk [2]

3.2 IoT Device Capabilities Potentially Affecting Cybersecurity and Privacy Risk

3.2.1 Transducer capabilities: It connects with the actual world and fills in as the edge among computerized and actual conditions [20]. Transducer capacities give the capacity to figuring gadgets to connect straightforwardly with actual elements of interest. The two sorts of transducer capacities are:

a) Sensing: the capability to give a perception of a part of the actual world as estimation information which includes measurement of temperature check, audio sense, optical sense, etc.
b) Actuating: It is the capability to change something like activating capacities incorporate coil heating, electric shock, electronic lock, robotic arm, etc.

3.2.2 Interface capabilities: It empowers gadget associations (e.g., gadget to-gadget correspondences, human-to-gadget interchanges). The kinds of interface capacities are:
a) API-Application programming interface: Capacity of gadgets to speak with another gadget through an application.

b) Human User Interface: Capacity of gadget, individuals that discuss straightforwardly with one another. Instances of UI capacities incorporate microphones, speakers, touch screens, cameras, etc.
c) Network interface: the capacity to interface with a correspondence network to convey information to or from an IoT gadget—at the end of the day, to utilize a correspondence organization. An organization's interface ability incorporates both equipment and programming. Instances of organization interface abilities incorporate Bluetooth, Ethernet, Wireless fidelity, LTE, ZigBee, etc. Each IoT gadget has in any event one empowered organization interface capacity and may have multiple.

3.2.3 Supporting capabilities: It provides the functionality which can be used to support other IoT gadgets.

3.3 Cybersecurity at different levels of IoT data

3.3.1. Network Layer Cybersecurity

In the IoT framework, this layer assumes a basic part for the generally speaking IoT security execution, since secure information transmission over the organization is fundamental for the capacity of gadgets, handling stations, and the whole IoT framework. Attacks can be recognized by using an Intrusion Detection System(IDS), take restorative measures, and packet monitoring[21]. The IDS sends different interruption recognition procedures: measurable investigation for irregularity discovery[22]; developmental calculation for grouping interruptions dependent on error conditions and conduct[23]; convention check for ordering dubious practices; information mining strategies, for example, forest technique[24]; and DL for arranging network penetrate designs. Promising results are shown by DL models for detecting DDoS attacks[25]. Hybrid methods for identifying malicious exercises on the IoT networks additionally show promising outcomes[26]. The market of network security is the highest component of cybersecurity and the rising appropriation of IoT applications is a key contributing element to the development.

3.3.2. Processing Layer Cybersecurity

In this layer, there are two main stages

a) **Data Accumulation**: Each gadget is sending a lot of information across the IoT network. Here information comes in different structures, flows, and sizes. Isolating the fundamental information from these enormous sources is a concern that experts should focus on in this layer. Unstructured information, for example, photographs and video transfers can be very tremendous and should be done effectively to assemble knowledge factors for the business.
b) **Data Abstraction**: When the information collection stage is done, chosen information is taken out from the huge data for applications to upgrade their business systems. Here the information deliberation follows the way as:
    - Collecting data from all IoT and non-IoT frameworks
    - Using information virtualization to make information available from a solitary area
    - Managing raw information in numerous structures

When the information is gathered, it is simple for data analysts to utilize it for business logic

3.3.4. Application Layer Cybersecurity

Sharing of information is done by almost all enterprises like home automation systems require an exchange of personal information to a third party which initiates security issues Since numerous IoT applications might be claimed by an outsider or third party organizations, cyberattacks on these applications may influence the security of applications. Security issues incorporate the security, for example, XMPP and CoAP, insufficient audit, etc. These mentioned security issues have been tended to with different arrangements, for example, key administration, access control, and information security assurance [27].

3.3.5. Service Management Layer Cybersecurity

In contrast to the risk of different layers, cybersecurity at this layer centers around human and authoritative parts. Privacy issues are pertinent to IoT administration executives since these issues affect the utilization of IoT administrations and applications.

4 MOBILE COMPUTING APPROACH FOR IoT DATA

Counting the mobile environment, traditional safety systems are adjusted for the fulfillment of the requirements of clients. Given the IoT, various types of smart devices are completely associated naturally through controllers like smartphones. Hence, the controller like a smartphone should be secure contrasted with traditional mechanisms of security. As indicated by the current security threats, these are different than past ones. Hence, the countermeasures applied ought to be changed. From a usability perspective, the environment depends on mobility and is created in such a way as to increase the security of the device. Mobile-based[28] advancements are increasing on daily basis and taking us into the digital age. Slowly all our nearby devices are becoming mobile. So, it's a fact that our generation is becoming dependent on these devices. A smartphone with a lot of applications that are connected to our daily life needs to works efficiently. Also, IoT gadgets are completely associated with controllers, called smartphones. The future of IoT networks will be founded on high-speed devices like smartphones that will be accessible all over, even in remote areas. Along with this, the total number of connected people wirelessly will surpass the connected one with a wired connection. So the security issue will be an issue to be discussed and managed. Accordingly, the data of IoT gadgets are all the more firmly identified with individual protection. Thus, security and protection issues are more significant contrasted with non-IoT framework-based society. Also, the present gadget controllers incorporate different sensors like biometric data, since these sensors gather and oversee unique marks, voice recognition, iris recognition, signature verification, and even personal behavior[28]. These sorts of data are exceptional data that can be utilized to check the authenticity of a user. In this way, traditional approaches will not work for the security of the individual as well as of society which needs special attention.

4.1. Traditional threat

4.1.1 Simple Guessing Some simple guesses like random data or small information may crack the passwords. In this attack, users' information may be compromised as:

a) **Demon Force** In this, an attacker may try to enter every possible combination possible to crack the code. It works where the size of the password is short which can be cracked in less time.

b) **Spell check** Likewise demon force attack type, this type of attack try the most common keywords as passcode as easily exposable and simple keywords used in this. An attacker may try to crack the code with the help of words from the dictionary.

4.1.2 Replay Attack Replay Attack effectively moved packets are delayed to get attackers inside the system, claim to be the real client. However, it's a new type of attack in the mobile authentication environment [29].

4.1.3 Spyware It is transcendently utilized for virus purposes to hide the information from the user like the tracking behavior and monitoring system without the proper consent of the user [30].

4.2. Countermeasures for Attacks

4.2.1. Passwords based on Text Passwords dependent on content are most common, even though the weaknesses are known to all. The major impact factor of a text-based password is its length. A lot of effort is required by an attacker to crack long passwords. However, there is a tendency of users to prefer short passwords as they are easy to remember. To guarantee sufficient security, accompanying standards need to be followed when utilizing text-based passwords. Some general rules that need to follow are:

i. Always use long passwords, preferably eight characters long (long password is better)
ii. Always use words that don't have any meaning (meaningless words are better, that are not in the dictionary)
iii. Always remember your password (don't write it anywhere)
iv. Always use a different password for different devices (don't repeat the same password)

v. Always change the password regularly (don't keep the same password for long duration)

4.2.2 PIN It is a numerical code that is used for transactions of banking services, debit card authentication, unlocking a mobile device.

4.2.3 One-Time Password It is also known as a one-time PIN or dynamic password which is valid for only one login after that it expires and we need to generate it again. It can be used in SMS to generate a password at run time after getting the code on a mobile device.

4.3. Models of Attacks More number of mobile devices is increasing that is connected to the internet, so they are not supposed to be a safe device to use in public. Emerging attacks can even occur in a safe environment also because of the structural efficiency of mobile devices. So, the threat can be divided into two parts, one is for the owner and another is for the device. Owner threat is basically for the mistakes done by the user by not checking the environment where he or she is working which can lead to serious issues. Another one is for devices which can be the screen size or the touch screen issue, where the nearby person can easily see the information because of the big screen size. So the owner needs to protect the screen to be displayed to a nearby person [31].

4.3.1 Shoulder Surfing Shoulder Surfing It is the practice of spying on the phone user with a naked eye to get personal details[32].

4.3.2 Recording It is the advanced version of shoulder surfing where someone can use all the possible techniques of recording to get the personal information of the user.

4.3.3 Hybrid It is a combination of naked eye spying and recording techniques to get the sensitive information of the user.

4.3.4 Smudge Whenever we use a smartphone, because of our oily skin, unknowingly we make an impression on the mobile screen which is called a smudge. An attacker might follow that particular pattern, direction, and shape to crack the pattern lock and easily take the sensitive information.

4.4 Counter Techniques for Existing Attacks
To overcome the attacks, some techniques based upon the cost and security level are introduced.

4.4.1 Passwords based on Graphics Numerous graphical secret key systems have been proposed by scientists. A pattern-based system is also an example of the same which includes pattern lock developed by google in their android based phones.

4.4.2 Fingerprint Recognition It refers to the mechanism which automatically identifies or confirms the identity of the person; it is a good option for mobile devices to secure it.

4.4.3 Voice-based Authentication A machine can receive a sound, understanding it, and authenticate the user. For example, Apple Siri, Amazon Alexa, and Microsoft-based Cortina.

4.4.4 Iris Recognition It is a technique for effective authentication in which infrared flashes in the eye to recognize the authentic person. The smartphone can check one or both the eye to unlock the device.

4.4.5 Facial Recognition This technology is capable enough to match the face of a human from a video frame or digital image to identify the authorized user. It is used in smartphones although accuracy is lower than iris or fingerprint authentication, it is an effective technique.

5 BIG DATA APPROACH FOR IoT DATA

The innovative progressions and quick combination of wireless communication, computerized gadgets advancements have brought about the development of IoT. As indicated by the Cisco report, the quantity of devices associated with the internet has surpassed the total count of humans on the planet. These gadgets can be PCs, cell phones, tablets, WiFi-empowered devices, wearable gadgets, and home automation systems. Most of the tools that are used for IoT data collection include sensor-based devices that need to follow some protocols like DDS. IoT gadgets produce tremendous data that is useful for research as well as decision making by processing this data with the help of different tools [7]. To produce benefits from IoT, organizations should make a platform where they can gather, oversee, and investigate huge data collected from sensors in a versatile and practical way. In this situation, utilizing a major information stage that can help in understanding the data with different information sources gets crucial. Information incorporation and examination permit associations to reform their business interaction [12]. In particular, these undertakings can utilize data analytics to change an immense volume of sensor-gathered information into significant experiences [17].

5.1 Platforms for Big Data & Analytics for IoT Devices

A large amount of IoT device data is generated, so there is a need for a platform that can work with data sources using edge computing [33].

5.1.1 Apache Hadoop: The Apache Hadoop library is a structure that takes into consideration the appropriate preparation of huge informational indexes across clusters of PCs utilizing straightforward programming models. It is intended to scale up from a single server to many machines, each offering neighborhood calculation, and storage. Instead of depending on hardware to convey high accessibility, the actual library is intended to distinguish and deal with failures at the application layer, so conveying an availability of services on a cluster of PCs, each of which might be inclined to failures [34].

5.1.2 1010data: It comprises a column-oriented information base that generally manages semi-organized information, for example, IoT information [35]. Besides its information perception, revealing, and reconciliation abilities, this device offers analytic services and factual investigation. It is additionally strong for large infrastructures that work in a streamlined way and manages the back-end frameworks. It fulfills client interest by high-level scientific potential. Nonetheless, it is viewed as incapable as far as information extraction, change, and loading.

5.1.3 IBM and Cloudera: Gather, oversee, secure, and investigate huge information with IBM and Cloudera [36]. Advantage from an enterprise-grade information platform and a biological system of IBM and Cloudera. IBM and Cloudera are focused on the open-source local area, applying open norms and interoperability to their products and answers for cultivating development. It also safely unify information across your on-premises, multi-cloud, and hybrid environment which is benefited from more exact, information-driven choices.

5.1.4 SAP-Hana: It is a segment-arranged, social information base administration framework created and advertised by SAP SE [37]. Its essential capability as a data set server is to store and recover information as mentioned by the applications. Furthermore, it performs progressed investigation (predictive examination, spatial information processing, text analysis, text search, streaming examination, graph-based information preparing) and incorporates extricate, change, load (ETL) abilities just as an application server.

5.1.5 HP-HAVEn: HP HAVEn is the first of its kind for the industry which is the comprehensive, adaptable, open, and secure platform for Big Data. Industries are suffocating in an ocean of information and need a confided accomplice to help them. HP HAVEn is at present teaming up with a few organizations to compliment inheritance from data warehouses. HP likewise presented "Flex-Zone" that

encourages huge data sets investigation before characterizing data set plan. The solitary disadvantage of this system is an increment of the occupant's quantity that produces an enormous data set inventory where the lock holding and interaction of delivery taking everything together.

5.1.6 Horton works: It centers around plotting a major information investigation of IoT also the executive's stage dependent on Hadoop. It has open-source programming that focused on Hive. Although, plug-in of its HDP, Hortonworks can't decrease the number of hosts in the produced collection.

5.1.7 Infobright: This is explicitly intended for tackling information the executives and scientific issues, Infobright can inspect up to 50 TB of information. With its information skipping ratio and high compression technique, Infobright is viewed as appropriate for data generated through machines, for example, IoT information. Infobright generally works with Hadoop. The information skipping technique and columnar plan of this device guarantee that only the concerned information will be utilized in each inquiry. This information is likewise recorded naturally without the need for any division and tuning. In any case, all inquiries can't be addressed ideally utilizing the Infobright analyzer.

5.1.8 MapR: MapR programming gives admittance to a variety of information sources from a cluster system, including big data systems, for example, Apache Hadoop and Spark, a conveyed record framework, a multi-model data set management framework, consolidating investigation progressively with operational applications. It runs on both hardware and public cloud computing systems. In August 2019, following monetary challenges, the rights of the organization were sold to HP Enterprise

5.2 Big data and Analytics Environment

5.2.1 Connectivity: IoT worldview is steadily promoting omnipresent networks for smart sensor-based devices. Vital prerequisites of IoT are dependable network to big data and investigation that encourage blend & reconciliation of immense sensor information. Subsequently, various articles around us have an incredible potential to be associated with high processing foundations to improve the services of IoT. In any case, consistent association through various articles in smart urban areas[12], for example, IoT, cloud computing, huge information, and investigation, should be set up before understanding our current scenario.

5.2.2 Storage: The fast development of enormous IoT-empowered devices has brought about the storage of huge data from different sources with minimal effort. The range incorporates information from smart devices and online media that are displayed distinctively. Most of the IoT services depend upon M2M protocols, which require dealing with countless streams and straightforwardly advantage from the general cloud computing distributed storage [38].

5.2.3 QoS: For the quality, the primary requirement is the sensor's management of resources used in IoT to analyze the data. It must be reliable and must transfer the big data generated from the sources as it is most important for big data analytics[33].

5.2.4 Analysis of Real-time: Quite possibly the most important highlight of IoT is its continuous or close time correspondence of data in regards to connected things. Given that a lot of this unstructured information is streamed from web-enabled things, big data executions ought to examine with progressing requests to help the relationship for getting information quickly, rapidly, and interface with people and various gadgets constantly [38].

5.3 IoT APPLICATIONS AND BIG DATA ANALYTICS

Enormous data produced by IoT devices from which data analytics can be helpful for business people to decide on the field of home automation systems, smart cities, smart medical services, and smart transportation, etc [39][40][41].

5.3.1 Smart Transportation: Finding critical information has turned into an essential concern in this state where vehicles are related to the Internet and produce lot of data. The transport sector with the help of Data analytics, discover the historical backdrop of mishappening on-road (to exemplify: let us know about the conditions under which the mishap took place and speed of driver), limit road mishaps, choose when the traffic load shows up at its zenith and set up an ideal way which can resolve traffic. Investigation of this system may improve road safety, and upgrade the user experience [41].

5.3.2 Smart Medical: In recent years, a huge amount of information has been made in the medical services area. However, such fast expansion in information creation has made difficulties in removing important data from huge medical services datasets that can help foresee pandemics and discover solutions for different diseases. Data analytics can help medical services experts investigate a lot of patient information and get familiar with the historical data of different diseases. Insurance agencies may likewise utilize information investigation when making strategies. Medical care experts may likewise recognize the genuine disease at their beginning phases and in this way forestall the death toll [42].

5.3.3 Grid-based System: It quickly produces information, finds valuable data that is useful. A lot of information is gathered from various sources, for example, power utilization of a user, phasor estimation information, and energy utilization information estimated by smart meters, and many more[43]. Appropriate investigation-based analytics measures the power supply that they should give to users. It can be beneficial for enterprises also for a better understanding of power demand for the future.

5.3.4 Smart Inventory System: Valuable data from the inventor system can help entrepreneurs produce monetary benefits. Investigation of the dataset produced by this system can assist in securing information about market patterns. Item suggestions can be produced in the wake of examining occasional varieties. The investigation of stock information can likewise help recognize false cases. The examination may help advertisers for setting the strategies. Companies can also decide after risk analysis and opportunities[19][35].

6 BLOCKCHAIN APPROACH FOR IoT DATA

Blockchain technology can improve the worldwide framework of the advancements associated through the web. To arrive at a particularly immense development, the most important aspect is to build an IoT stack, normalize conventions and make the legitimate layers that offer types of assistance to IoT gadgets[44]. Presently, most IoT arrangements depend on centralized servers the brought the internet with cloud servers together. Among such propositions, decentralized structures were recommended in the past to make huge P2P Networks of sensors[45], but a few pieces may be absent corresponding to protection and security until the appearance of blockchain innovation. Blockchain technology can follow, arrange, do exchanges and store data from a lot of gadgets, empowering the production of uses that require no unified cloud. A few organizations like IBM go further and discussion about blockchain as an innovation for the public use shortly of IoT[46], since it tends to the difficulties for its huge adoption:

a) The cost of servers and cloud deployment is too high as the infrastructure cost includes middleman expenses.
b) Maintenance is likewise a difficult issue when a normal update is required for smart devices. There is a trust issue for IoT adopters with device access to authorities. So there is a need of securing IoT device data.
c) Source code is the main reason for the absence of trust, so to build trust, security and transparency are necessary, so open-source approaches ought to be considered for building up IoT solutions. Open-source code, as well as closed source code, are yet helpless to find bugs, at the same time, since it tends to be checked continually by numerous users, it is less inclined to be modified by others. Blockchain has been developing at tremendous speed in recent years. Investors in blockchain ventures rose from 93 million to 550 million USD in past few years. Moreover, the market for

blockchain overall is expected to develop to 2.3 billion USD by 2021. As indicated by McKinsey and the company, even though it is as yet in an early stage, blockchain has arrived at its maximum capacity depends on its present speed of advancement [47].

6.1 Framework of Blockchain

6.1.1 Components of a Blockchain : Blockchain infrastructure has 4 components:

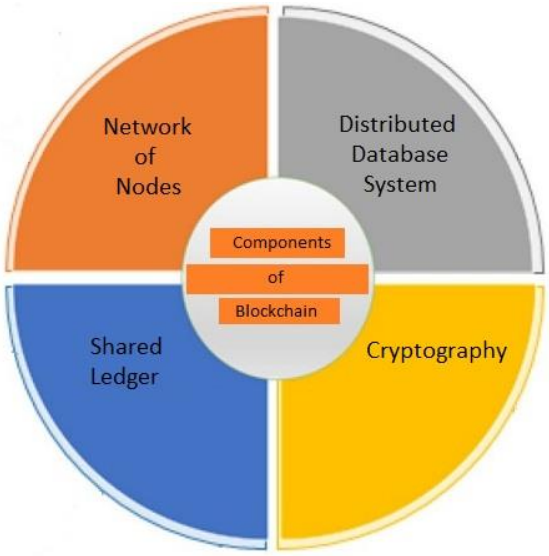

Fig 5: Components of Blockchain

1) Network of Nodes: Every node associated through the internet keep up track of transactions made on a blockchain network. The credibility of the transaction is checked which removes any involvement of a third party. Records are added to the ledger immediately after the completion of any transaction, this cycle is known as 'mining'. The confirmation of work should be checked by various nodes [48].
2) Distributed database: Each block contains the accompanying information in itself like transaction detail, timestamp, Information, which joins it to the block of the preceding chain[49].
3) Shared ledger: Whenever a transaction is made, the record is refreshed, thus creating a transparent system[50].
4) Cryptography: It ties the information with the exceptionally solid crypto mechanism, which isn't an easy task to track or alter the information by any user[51].

6.1.2 Constructing a blockchain: Another advanced transaction is made which is then changed over into a cryptographically ensured block. Miners rival each other to approve the transaction by tackling tremendous coded issues. The initial one to address gets an award with bitcoins[52] and blocks are added sequentially in a chain after being time-stamped [53].

6.1.3 Implementing a Blockchain
1) Public: In a limited area, each and every node can send or comprehend the exchange and can take an interest in the consensus cycle without requiring any consent. Cryptocurrency comes under this classification.
2) Consortium area: consortium blockchain technology where rather than just a single organization, various associations oversee the platform. It's just like a private blockchain.

6.1.4 Blockchain technology to strengthen IoT data Security
a) Secure communication: IoT gadgets need to exchange data with the help of transaction which is being stored in a ledger. These records can likewise be utilized to store encryption keys to make the trades more

private. IoT gadget sends an encrypted message utilizing the public key of the destination gadget, which is then stored in the network of blockchain. The sender then, at that point, requests its node to get a public key from the recipient from the record. Then, at that point, the sender encodes the message utilizing the public key of the recipient and decrypted the sent message utilizing their private key[54].

b) Authentication of users: The sender works out on the hash of a message that is then encrypted with its private key. The digital signature alongside the message is sent. The recipient then, at that point, decodes the digital signature utilizing the public key of the sender stored in a ledger to get the value of hash that is calculated by the sender. The message is legitimate provided that the determined hash and the protected hash of the message are the same. If the digital signature of both messages is stored in the ledger, a user is authenticated

c) Discovering genuine IoT: With possibly a huge number of IoT gadgets are to be associated with a similar organization, there is a dire need to get the capacity to find gadgets at scale and to observe genuine nodes. Exactly when another IoT gadget begins, it at first demands rootworkers to give a believed node list in the affiliation. Then, at that point, the gadget registers itself in a node, and in this manner, the trading of data begins. It gets data from different nodes and sends its data the other way around. DNSSec ought to be executed to get the name objective of rootworkers by trying to avoid spoofing attacks. For this, the rootworkers should validate the gadget before giving it the node list. To guarantee trustworthiness and classification, each correspondence made should be validated and encrypted proficiently.

d) Configuring IoT Blockchain The setup is needed to be encrypted in the record to forestall the revelation of IoT network topology or its properties by examining the data stored in the public record. The hash value of the most recent setup document for each gadget can be facilitated in the record. Utilizing a cloud administration the IoT gadget should download the most recent and believed arrangement document after a specific time interval. Then, at that point, the gadget can utilize the blockchain node API to recover and coordinate with the hash value, which is stored in the blockchain. This would permit the executives to eliminate any awful configurations routinely and reboot every single IoT gadget in the organization with the most recent trusted configurations.

7. CONCLUSION

IoT is one of the arising innovations in the worldwide IT industry, as more organizations are moving towards these cutting-edge arrangements. However components of IoT structure the center basics for a complete IT framework, the IoT Layers set out the way for the general organization's success. Each layer has a particular extension and job that takes into account addressing the IoT complexity across the organization. For small enterprises, it's very difficult to work with IoT layers of frameworks. However, the majority of the top worldwide associations offer e2e solutions for organizations to incorporate provisions of IoT in their premises. They offer comprehensive gadget control, information encryption measures, and consistent change to the future IoT frameworks. IoT devices like commercial and homes are vulnerable to IoT-specific attacks. We must consider security whenever talking about IoT device data protection as security is a major concern with the increase of internet-enabled IoT devices. Through this chapter, a top to bottom and broad security investigation of IoT devices has been made considering cybersecurity, cloud computing, mobile computing, big data, and blockchain technologies which is a novel approach.

REFERENCES

[1] A. Roukounaki, S. Efremidis, J. Soldatos, J. Neises, T. Walloschke, and N. Kefalakis, “Scalable and configurable end-to-end collection and analysis of iot security data: Towards end-to-end security in IoT systems,” *Glob. IoT Summit, GIoTS 2019 - Proc.*, pp. 1–6, 2019, doi: 10.1109/GIOTS.2019.8766407.

[2] K. Boeckl *et al.*, “NISTIR 8228 Considerations for Managing Internet of Things (IoT)

Cybersecurity and Privacy Risks," p. 44, 2019, [Online]. Available: https://doi.org/10.6028/NIST.IR.8228.

[3] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, 2019, doi: 10.1109/JIOT.2019.2935189.

[4] T. Poongodi, A. Rathee, R. Indrakumari, and P. Suresh, *Iot sensing capabilities: Sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition*, vol. 174. 2019.

[5] B. Prabhu kavin and S. Ganapathy, "A secured storage and privacy-preserving model using CRT for providing security on cloud and IoT-based applications," *Comput. Networks*, vol. 151, pp. 181–190, 2019, doi: 10.1016/j.comnet.2019.01.032.

[6] P. Adina, R. H. Venkatnarayan, and M. Shahzad, "Impacts & detection of network layer attacks on IoT networks," *Proc. 1st ACM MobiHoc Work. Mob. IoT Sensing, Secur. Privacy, Mob. IoT SSP 2018*, 2018, doi: 10.1145/3215466.3215469.

[7] E. Ahmed *et al.*, "The role of big data analytics in Internet of Things," *Comput. Networks*, vol. 129, pp. 459–471, 2017, doi: 10.1016/j.comnet.2017.06.013.

[8] A. Rao, N. Carreon Rascon, R. Lysecky, and J. W. Rozenblit, "Probabilistic Security Threat Detection for Risk Management in Cyber-Physical Medical Systems," *IEEE Softw.*, 2018, doi: 10.1109/MS.2018.110165557.

[9] J. Wurm, K. Hoang, O. Arias, A. R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial IoT devices," *Proc. Asia South Pacific Des. Autom. Conf. ASP-DAC*, vol. 25-28-Janu, pp. 519–524, 2016, doi: 10.1109/ASPDAC.2016.7428064.

[10] F. Loi, A. Sivanathan, H. H. Gharakheili, A. Radford, and V. Sivaraman, "Systematically evaluating security and privacy for consumer IoT devices," *IoT S P 2017 - Proc. 2017 Work. Internet Things Secur. Privacy, co-located with CCS 2017*, no. I, pp. 1–6, 2017, doi: 10.1145/3139937.3139938.

[11] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, "Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning," pp. 3491–3508, 2018.

[12] M. A. Amanullah *et al.*, "Deep learning and big data technologies for IoT security," *Comput. Commun.*, vol. 151, no. December 2019, pp. 495–517, 2020, doi: 10.1016/j.comcom.2020.01.016.

[13] J. S. Fu, Y. Liu, H. C. Chao, B. K. Bhargava, and Z. J. Zhang, "Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing," *IEEE Trans. Ind. Informatics*, vol. 14, no. 10, pp. 4519–4528, 2018, doi: 10.1109/TII.2018.2793350.

[14] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 854–864, 2016, doi: 10.1109/JIOT.2016.2584538.

[15] A. Makkar, U. Ghosh, and P. K. Sharma, "Artificial Intelligence and Edge Computing-enabled Web Spam Detection for Next Generation IoT Applications," *IEEE Sens. J.*, no. c, 2021, doi: 10.1109/JSEN.2021.3066492.

[16] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and iot cyber risk management," *Futur. Internet*, vol. 12, no. 9, 2020, doi: 10.3390/FI12090157.

[17] D. Puthal, R. Ranjan, S. Nepal, and J. Chen, "IoT and big data: An architecture with data flow and security issues," *Lect. Notes Inst. Comput. Sci. Soc. Telecommun. Eng. LNICST*, vol. 189, pp. 243–252, 2018, doi: 10.1007/978-3-319-67636-4_25.

[18] S. Tweneboah-Koduah, K. E. Skouby, and R. Tadayoni, "Cyber Security Threats to IoT Applications and Service Domains," *Wirel. Pers. Commun.*, vol. 95, no. 1, pp. 169–185, 2017, doi: 10.1007/s11277-017-4434-6.

[19] A. Dean and M. O. Agyeman, "A study of the advances in IoT security," *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3284557.3284560.

[20] A. Vaswani *et al.*, "Attention is all you need," *Adv. Neural Inf. Process. Syst.*, vol. 2017-Decem, no. Nips, pp. 5999–6009, 2017.

[21] E. Hodo *et al.*, "Threat analysis of IoT networks Using Artificial Neural Network Intrusion

Detection System," *arXiv*, pp. 4–8, 2017.
[22] J. Pacheco, V. Benitez, and L. Félix, "Anomaly behavior analysis for IoT network nodes," *ACM Int. Conf. Proceeding Ser.*, 2019, doi: 10.1145/3341325.3342008.
[23] J. Li, Z. Zhao, R. Li, and H. Zhang, "AI-based two-stage intrusion detection for software defined IoT networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2093–2102, 2019, doi: 10.1109/JIOT.2018.2883344.
[24] A. Subasi *et al.*, "Intrusion Detection in Smart Grid Using Data Mining Techniques," *21st Saudi Comput. Soc. Natl. Comput. Conf. NCC 2018*, pp. 1–6, 2018, doi: 10.1109/NCG.2018.8593124.
[25] M. Roopak, G. Yun Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," *2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019*, pp. 452–457, 2019, doi: 10.1109/CCWC.2019.8666588.
[26] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K. K. R. Choo, "A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks," *IEEE Trans. Emerg. Top. Comput.*, vol. 7, no. 2, pp. 314–323, 2019, doi: 10.1109/TETC.2016.2633228.
[27] D. Puthal, S. Nepal, R. Ranjan, and J. Chen, "Threats to Networking Cloud and Edge Datacenters in the Internet of Things," *IEEE Cloud Comput.*, vol. 3, no. 3, pp. 64–71, 2016, doi: 10.1109/MCC.2016.63.
[28] X. Su, Z. Wang, X. Liu, C. Choi, and D. Choi, "Study to Improve Security for IoT Smart Device Controller: Drawbacks and Countermeasures," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/4296934.
[29] H. Shin, D. Kim, and J. Hur, "Secure pattern-based authentication against shoulder surfing attack in smart devices," *Int. Conf. Ubiquitous Futur. Networks, ICUFN*, vol. 2015-Augus, pp. 13–18, 2015, doi: 10.1109/ICUFN.2015.7182486.
[30] E. Darbanian and F. Dastghaiby, "A graphical password against spyware and shoulder-surfing attacks," *CSSE 2015 - 20th Int. Symp. Comput. Sci. Softw. Eng.*, pp. 5–10, 2015, doi: 10.1109/CSICSSE.2015.7369239.
[31] H. M. Sun, S. T. Chen, J. H. Yeh, and C. Y. Cheng, "A Shoulder Surfing Resistant Graphical Authentication System," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 2, pp. 180–193, 2018, doi: 10.1109/TDSC.2016.2539942.
[32] T. S. Wu, M. L. Lee, H. Y. Lin, and C. Y. Wang, "Shoulder-surfing-proof graphical password authentication scheme," *Int. J. Inf. Secur.*, vol. 13, no. 3, pp. 245–254, 2014, doi: 10.1007/s10207-013-0216-7.
[33] S. K. Sharma and X. Wang, "Live Data Analytics with Collaborative Edge and Cloud Processing in Wireless IoT Networks," *IEEE Access*, vol. 5, pp. 4621–4635, 2017, doi: 10.1109/ACCESS.2017.2682640.
[34] R. Vinayakumar, K. P. Soman, and P. Poornachandran, "Detecting malicious domain names using deep learning approaches at scale," vol. 34, pp. 1355–1367, 2018, doi: 10.3233/JIFS-169431.
[35] V. Morabito, "Big data and analytics: Strategic and organizational impacts," *Big Data Anal. Strateg. Organ. Impacts*, no. Yan 2013, pp. 1–183, 2015, doi: 10.1007/978-3-319-10665-6.
[36] A. Bhardwaj *et al.*, "DataHub: Collaborative data science & dataset version management at scale," *CIDR 2015 - 7th Bienn. Conf. Innov. Data Syst. Res.*, 2015.
[37] F. Färber, S. Cha, J. Primsch, and C. Bornhövd, "SAP HANA database: data management for modern business applications," *ACM Sigmod …*, vol. 40, no. 4, pp. 45–51, 2012, [Online]. Available: http://dl.acm.org/citation.cfm?id=2094126.
[38] G. Suciu *et al.*, "Big Data, Internet of Things and Cloud Convergence – An Architecture for Secure E-Health Applications," *J. Med. Syst.*, vol. 39, no. 11, 2015, doi: 10.1007/s10916-015-0327-y.
[39] E. Al Nuaimi, H. Al Neyadi, N. Mohamed, and J. Al-Jaroodi, "Applications of big data to smart cities," *J. Internet Serv. Appl.*, vol. 6, no. 1, pp. 1–15, 2015, doi: 10.1186/s13174-015-0041-5.
[40] N. Bessis and C. Dobre, *Preface*, vol. 546. 2014.

[41] I. A. T. Hashem *et al.*, "The role of big data in smart city," *Int. J. Inf. Manage.*, vol. 36, no. 5, pp. 748–758, 2016, doi: 10.1016/j.ijinfomgt.2016.05.002.
[42] D. Ravi *et al.*, "Deep Learning for Health Informatics," *IEEE J. Biomed. Heal. Informatics*, vol. 21, no. 1, pp. 4–21, 2017, doi: 10.1109/JBHI.2016.2636665.
[43] C. S. Lai, L. L. Lai, and Q. H. Lai, *Smart Grids and Big Data Analytics for Smart Cities*. 2021.
[44] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surv. Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016, doi: 10.1109/COMST.2016.2535718.
[45] P. Fraga-Lamas, T. M. Fernández-Caramés, Ó. Blanco-Novoa, and M. A. Vilar-Montesinos, "A Review on Industrial Augmented Reality Systems for the Industry 4.0 Shipyard," *IEEE Access*, vol. 6, no. c, pp. 13358–13375, 2018, doi: 10.1109/ACCESS.2018.2808326.
[46] P. Brody and V. Pureswaran, "Device democracy: Saving the future of the Internet of Things - IBM Global Business Services Executive Report," *IBM Glob. Bus. Serv. Exec. Rep.*, pp. 3–25, 2015, [Online]. Available: http://m2mworldnews.com/download/white-papers/IBM-Saving-the-future-of-IoT.pdf.
[47] McKinsey & Company, "Blockchain Technology in the Insurance Sector - Quarterly meeting of the Federal Advisory Committee on Insurance (FACI)," pp. 1–16, 2017, [Online]. Available: https://www.treasury.gov/initiatives/fio/Documents/McKinsey_FACI_Blockchain_in_Insurance.pdf.
[48] M. Suárez-Albela, T. M. Fernández-Caramés, P. Fraga-Lamas, and L. Castedo, "A practical evaluation of a high-security energy-efficient gateway for IoT fog computing applications," *Sensors (Switzerland)*, vol. 17, no. 9, pp. 1–39, 2017, doi: 10.3390/s17091978.
[49] D. Datla *et al.*, "Wireless distributed computing: A survey of research challenges," *IEEE Commun. Mag.*, vol. 50, no. 1, pp. 144–152, 2012, doi: 10.1109/MCOM.2012.6122545.
[50] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 75–87, 2017, doi: 10.1109/JIOT.2016.2619369.
[51] S. Meiklejohn *et al.*, "A fistful of Bitcoins: Characterizing payments among men with no names," *Commun. ACM*, vol. 59, no. 4, pp. 86–93, 2016, doi: 10.1145/2896384.
[52] M. Marjani *et al.*, "Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges," *IEEE Access*, vol. 5, no. c, pp. 5247–5261, 2017, doi: 10.1109/ACCESS.2017.2689040.
[53] C. C. Liao, S. M. Cheng, and M. Domb, "On Designing Energy Efficient Wi-Fi P2P Connections for Internet of Things," *IEEE Veh. Technol. Conf.*, vol. 2017-June, 2017, doi: 10.1109/VTCSpring.2017.8108292.
[54] M. Vukolić, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9591, pp. 112–125, 2016, doi: 10.1007/978-3-319-39028-4_9.