IoT Course Project Report

(2020-2021)

Course Project Title: Attacks on IOT Devices and IOT Security Threats

Team No.: 16

Team Members Details:

USN	Roll No.	Name	Div
01FE18BCS182	362	Sakshi Jha	C
01FE18BCS183	363	Saloni Shah	C
01FE18BCS190	370	Sanjana Kambar	C
01FE18BCS196	405	Savitri Khyadad	D

INDEX

PROBLEM STATEMENT

Internet of Things (IoT) is one of the most discussed topics in the research field today. The IoT applications designed, increase comfort, efficiency and automation for users, however the security and privacy threats caused by IoT draw our attention. Due to these issues, the emerging IoT applications may lose their potential. Hence, there is a need for effective architecture in the IoT applications that can guarantee security and prevent attacks on the IoT devices.

We have 4 techniques that already exist in order to prevent these threats.

- Blockchain
- Machine learning
- Fog computing
- Edge computing

Study on various techniques for IOT security- Blockchain, Machine Learning, Fog Computing and Edge Computing.

ABSTRACT

The Internet of Things (IoT) is the next step in the evolution of communication. Physical items can be enabled to produce, receive, and exchange data in a seamless manner via the Internet of Things. Certain IoT applications aim to automate various processes and enable inanimate physical things to operate without the need for human involvement. To implement such a world in an ever-increasing way, high levels of security, privacy, authentication, and attack recovery are required. In order to achieve end-to-end secure IoT environments, it is critical to make the necessary modifications in the architecture of IoT applications. In the research carried out, we first surveyed 'IoT Features' to better understand reasons for security and privacy threats in recent years. The study will also highlight various IoT attacks happening, classifying them and give a comparison on the various attacks. Following a discussion of security concerns, different upcoming and existing solutions aimed at attaining a high level of trust in IoT applications will be addressed. The use of four distinct technologies, including blockchain, fog computing, edge computing, and machine learning, to improve IoT security is explored.

I. INTRODUCTION

Since the previous two centuries, the rate of human progress has been significantly growing due to the use of various technologies. Computing power, which is growing at an exponential rate, is one of the most promising technologies. As the number of users grows, the graph of cost and size shrinks, but the performance and number of users grows. There will be a massive growth in the number of connections and networks, with nearly everyone linked via various devices such as desktops, laptops, cellphones, PDAs, and so on. The most important reasons are size, cost, and IPv6, which provides for billions of addresses, enough to offer an IP address to each item rather than each device.

Because the Internet is at the heart and core of IoT, nearly all security concerns that exist on the internet also affect IoT. In comparison to other traditional networks, the IoT's critical nodes are allocated to places without manual supervision, with limited capacity and resources, making the IoT's security concerns extremely challenging. Furthermore, the rapid development and widespread acceptance of IoT devices in our daily lives underscores the need of addressing these security risks prior to deployment. Traditional security countermeasures are not applied to IoT-based security risks due to inherent processing capabilities and speed limitations.

Cyber-attacks will increase in tandem with the fast expansion of IoT applications and devices, posing a greater danger to security and privacy than ever before. Remote attackers, for example, may compromise patients' implanted medical devices or smart automobiles, causing not just significant financial losses but also putting people's lives in jeopardy. Furthermore, when IoT devices become more widely utilised in business, the military, and other critical areas, attackers will be able to put public and national security at risk. The majority of businesses and users, on the other hand, are unaware of the importance of data privacy and security. According to a recent Pew Research Center study, many Americans are overconfident in the way their data is used. Only 26% of Americans say they don't want their medical records shared with their doctor. Nearly half of Americans agree to allow auto insurance companies to track the location and speed of their vehicles in order to receive discounts on their car insurance.

There are four key levels in every IoT ecosystem or environment. The first layer employs a variety of sensors and actuators to perceive data or information and execute various functions. The gathered data is then transmitted over a communication network in the second layer. The third layer, known as the middleware layer, is used by most emerging IoT systems to function as a bridge between the network and application layers. Finally, on the fourth layer, different IoT-based end-to-end applications such as smart grids, smart transportation,

smart industries, and so on are present. Each of these four levels has its own set of security issues.

In this study, we first discuss IoT attacks with their existing solutions and compare them with their parameters. Further, we analyze the security issues using IOT features. To the end we highlight the major existing and upcoming solutions for IOT security, namely, blockchain, fog computing, edge computing and machine learning.

II. Literature Survey

IoT is a technology that is currently in its early stages of development and requires several upgrades at various levels. [4] [5] [6] go through the IoT architecture in great depth. Different vulnerabilities and possible attacks against IoT are discussed in [6] [9] [10] [11] [12]. [6] divides assaults into four categories according to the vulnerability exploited by the attacker. [13] [14] outline probable OSI layer assaults. Although the references [15] [16] [17] focus on the security issues of an IoT system, the majority of these articles only address certain types of attacks based on specific security objectives. There are currently no suggested approaches that are sufficiently strong to address the majority of IoT security concerns. Currently, only a few articles address the numerous challenges in IoT with common solutions.

The following are the key contributions of our work:
1. A classification of various IoT applications, as well as the security and privacy problems that these applications raise.
2. A thorough description of various threat sources in various IoT levels.
3. Specific and practical proposals for improving the IoT infrastructure to enable secure connections.
4. Consider the recommended remedies to IoT security concerns.

A. Organization of the report

The study involves the discussion of various attacks on IoT devices and the security threats.Section III discusses the various security attacks in IoT that are categorized into physical attacks,network attacks,software attacks and encryption attacks followed by comparison of these attacks.Section IV gives an overview about the effects of IoT features on security and privacy.There are six features discussed in this section along with challenges and the solutions.Section V discusses the critical areas of IoT where areas like smart cities,smart environments and smart agriculture etc. are explained.Section VI describes the improvements and enhancements required for upcoming IoT applications.Further sections discuss about the techniques that can be used to reduce these attacks and security threats on IoT ,the benefits and the challenges faced while implementing these solutions. Section VII gives the detailed explanation of IoT security using blockchain technology.Section VIII discusses how security can be provided using fog computing.Section IX gives an overview of IoT security using machine learning followed by section X that explains the IoT security using edge computing.Section XI is the conclusion of the study taken up followed by the references section.

III. Security Attacks in IoT

Malicious node injection assault is the most hazardous type of physical attack. Because it not only stops services but also modifies data. Sinkhole attack is the most dangerous network assault. It not only directs all traffic to the base station, but it also allows the attacker to launch additional attacks like selective forwarding, packet alteration, and packet dropping. We consider worm attacks to be the most dangerous type of software assault. Worms are the most deadly and destructive type of malware on the internet. It is a self-replicating malware that causes computer damage by exploiting security flaws in networking software and

hardware. The side channel attack is the most hardest to deal with among encryption attacks. Because the attacker uses side channel information to carry out the attack, it is extremely difficult to detect.

A. Physical Attacks

1) Node Tampering: In this approach, the attacker physically tampers with the compromised node in order to access sensitive data such as the encryption key.
2) RF Interference on RFIDs: By transmitting noise signals over radio frequency signals, the attacker executes a denial of service attack. RFID communication is based on these signals.
3) Node Jamming in WSNs: An attacker can disrupt wireless communication by deploying a jammer. It results in a Denial of Service (DoS) assault.
4) Malicious Node Injection: The attacker physically inserts a new malicious node between two or more nodes in this attack. It then changes the data and sends incorrect data to the other nodes. The attacker performs a malicious node injection attack using several nodes. The attacker begins by inserting a duplicate of node B. Then it adds more malicious nodes (node M1). Both of these nodes collaborate to carry out the attack. As a result, a collision occurs at the victim node. As a result, the attacked node is unable to receive or transmit any packets.

B. Network Attacks

1) Traffic Analysis Attacks: To gain network information, the attacker intercepts and analyses communications.
2) RFID Spoofing: When an attacker spoofs RFID signals, it is known as RFID spoofing. The information broadcast from an RFID tag is then captured.

Spoofing attacks deliver false information that seems to be correct and is accepted by the system.

3) RFID Cloning: This technique involves the adversary copying data from one RFID tag to another. It does not duplicate the RFID tag's original ID. The attacker can manipulate the data going through the cloned node by inserting incorrect data or controlling it.

4) RFID Unauthorized Access: If proper authentication is not given in RFID systems, an adversary can view, change, or remove data from nodes.

5) Sinkhole Attack: In a sinkhole assault, an adversary comprises a network node and uses it to carry out the attack. The hacked node transmits bogus routing information to its neighbours, claiming to have the shortest path to the base station, and subsequently draws traffic. The data can then be altered, and packets can be dropped.

C. Software Attacks

1) Phishing Attacks: By faking emails and utilising phoney websites, the attacker gets sensitive information such as usernames and passwords.

2) Viruses, Worms, Trojan Horses, Spyware, and Aware: Malicious code can be used by an attacker to harm the system. These viruses are distributed via email attachments and file downloads from the Internet. The worm can multiply itself without the need for human intervention. To identify the infection, we can employ worm detectors, anti-virus, firewalls, and intrusion detection systems.

3) Malicious Scripts: An attacker can get access to a system by inserting malicious script.

4) Denial of Service: By refusing services, the attacker prevents users from accessing the application layer.

D. Encryption Attacks

1) Side-channel Attacks: The attacker exploits information emitted by encrypting devices through the side channel. It comprises information regarding power, the time necessary to execute the operation, the frequency of errors, and so on. It is neither plaintext or encrypted text. This information is used by the attacker to deduce the encryption key.
2) Cryptanalysis Attacks: In this assault, the adversary uses plaintext or ciphertext to get the encryption key. Cryptanalysis assaults come in a variety of forms.

a) Ciphertext-Only Attack: In this attack, the attacker can obtain the ciphertext and deduce the plaintext from it.

b) Known Plaintext Attack: The attacker knows the plaintext for some sections of the ciphertext in this approach. The goal is to use this information to decrypt the rest of the ciphertext.

c) Chosen Plaintext Attack: The attacker chooses what plaintext is encrypted and where the encryption key is located.

d) Chosen Ciphertext Attack: The attacker can obtain the encryption key by utilising the plaintext of the chosen ciphertext.
3) Man in the Middle Attacks: An attacker intercepts a key exchange between two users and gets the key.

Comparison of different types of security attacks

The damage level, existing proposal and detection possibilities, vulnerability, and other characteristics are used to compare these four attacks, which are described in Table I. Malicious node injection attacks target the physical layer since the node is physically injected into the network. While a sinkhole attack is carried out at the network layer, routing information is drawn to the node with the shortest distance to the base station. Because the attacker utilises the side channel information emitted by the encryption device, the worm attack is done at the application layer by introducing malicious code,

and the side channel attack is performed at both the application and physical layers. All of these assaults, with the exception of the side channel attack, are active attacks since they may alter data. Because the attacker gets the encryption key via side channel information in a side channel attack, it is difficult to detect.

Classification	**Classification Types**			
Parameters	**Malicious Node Injection Attack**	**Sinkhole Attack**	**Worm Attack**	**Side-Channel Attack**
OSI Layer	Physical	Network	Application	Application/Physical
Attack Type	Active -As the attacker compromise the node	Active -As it provides the wrong information those results in packet dropping	Active -As it modifies the files	Passive -As the attacker can find encryption key by using the side channel information
Attacker Location	External, Internal	External	External, Internal	Internal
Attack threat	Availability -Due to collision at the victim node, it cannot transmit the packet	Availability, Confidentiality -As all the data is attracted to the compromised node	Availability, Integrity, Authenticity -As it can delete, modify the data	Confidentiality, Integrity _by using side channel information, it can find the encryption key
Damage Level	High -As it can modify the data and pass the info to other nodes	High -As all data is flowing through compromised node the attacker can do anything with packet	High -As it can delete files, mail documents	High -As the attacker can obtain the secret key without detecting
Detection Chances	Low -As it is replica of legitimate node	Difficult -To detect when it is near to base station	Antivirus can identify it	Negligible because adversary uses side channel information
Possibility Of Prevention	Yes -If we could avoid replication attack	Yes _If node authentication is provided	Yes -By avoiding suspicious sites, files	Yes _by using preventive measures
Attacks based on	Inserting Malicious Node	Routing	Malicious Code	Side-channel Information
Vulnerability	Wireless nature and hidden node problem	Node Authentication is not provided	Not following security policies	Side-channel Information
Existing solutions and their limitations	Not possible to detect if more than two nodes are malicious, consumes power because of over hearing	When Malicious Node near to the base station, Algorithm cannot accurately detect sink hole node	New worms are created everyday	Affect the performance od other system

TABLE I: COMPARISON OF DIFFERENT IOT ATTACKS

IV. Effect of IoT features on security and privacy

A. Interdependence

Description: The implicit dependence relationship between devices is described as an IoT feature named “Interdependence”.
Threats: Features could be maliciously used by attackers to reduce the difficulty of direct attack the target devices and bypass original defense mechanism.
Challenges: Because the IoT device behaviors could be changed by other devices or environmental conditions, it is difficult to define a certain set of fine-grained permission rules for them. Thus, the overprivileged has become a common problem in the permission model of existing IoT platforms applications.
Solutions and Opportunities:
● ContexIoT, a new context-based permission system for IoT platforms to solve the overprivileged problem. It records and compares more context information such as procedure control flow, data source, and runtime data of every device’s behavior before it is executed, and then let the user allow or deny this behavior according to recorded information.
● However, this method relies too much on user decisions, once the user makes a wrong decision, the system will remember this wrong decision and will not prompt the user again.

B. Diversity

Description: The phenomenon that many different kinds of IoT devices and protocols appear in the current IoT market, we refer to as an IoT feature “diversity”.

Threats: Different protocols have different semantic definitions, the attackers could also take advantage of this point to find security vulnerabilities like BadTunnel when they incorrectly work together.

Challenges: How to discover and deal with so many security vulnerabilities among the various IoT devices needs to be addressed urgently.

Solutions and Opportunities:

- Framework is designed to support dynamic security analysis for a variety of embedded systems' firmware. However, it cannot simulate all action of the real devices and need to forward action from the emulator to the device by physical connection. Thus, it is unsuitable for large-scale automated firmware analysis.
- Framework exits for large-scale automated firmware dynamic analysis, but it is only applicable to the Linux-based system

C. Constrained

Description: The limitation of the computing/storage resource, power supply and latency of IoT devices as an IoT feature named "constrained" here.

Threats:

- Lightweight IoT devices do not have the memory management unit (MMU), so memory isolation, address space layout randomization (ASLR) and other memory safety measures cannot be applied to these devices.
- Most complicated encryption and authentication algorithms like public cryptography cannot also be implemented on such devices, because they occupy too much computing resource and cause a long delay, which seriously affects the normal operation and reduces performance for constrained IoT devices.

Solutions and Opportunities:

- Authentication and key generation algorithm based on physical unclonable functions, which use the unique physical structure of the device to identify itself. This method not only saves key storage space and simplifies the key generation algorithm, but can also effectively resist the side channel analysis.

D. Myriad

Description: The enormous number of IoT devices and the huge amount of IoT data is described as an IoT feature named “Myriad”.

Threats: As more industrial and public infrastructures are connected to the Internet, the target of IoT botnets would no longer just be the website, but also the important infrastructures, which would bring grave damages to social security.

Challenges:

● How to detect and resist IoT botnet virus in IoT devices is a great challenge for researchers.

● At the same time, how to stop the spread of IoT botnets is also a tough problem.

Solutions and Opportunities:

● A tool is designed that extracts several attack vectors from the Mirai botnet and uses them to detect potential vulnerabilities in IoT devices.

● Consider constraints of devices and environment when detecting malicious requests in a sensor network. However, their attack assumption is too simplistic. Attackers are unlikely to send requests with the same content, but usually forge normal users’ requests with different reasonable content.

E. Unattended

Description: The long-time unattended status of IoT devices is an IoT feature named “unattended”.

Threats:

● It is hard to physically connect an external interface to verify the state of these devices. Thus, the remote attacks targeted them are difficult to detect.

● Stuxnet worms could infect the programmable logic controllers (PLC) used in industrial control systems, which results in considerable physical damage.

Challenges: Building a trusted execution environment (TEE) to ensure

security-critical operations be correctly executed under remote exploits and verifying internal state of a remote unattended IoT device become important tasks in many scenarios.

Solutions and Opportunities:

● A lightweight trusted execution environment is built for small embedded devices, but it does not consider how to safely handle the hardware interrupt and memory exception

F. Mobile

Description: The frequent movement of IoT devices is described as an IoT feature named “mobile”.

Threats: The social IoT devices will carry more sensitive information and automatically follow the users joining many different social networks.

Challenges:

● To confront the potential threats, the main security challenge should be addressed is cross-domain identification and trust

● When data carried with mobile IoT devices pass from one network to another, the key negotiation, data confidentiality, integrity protection and other important security issues need to be carefully concerned.

Solutions and Opportunities:

● Decrease the probability of mobile IoT devices being attacked in different networks through dynamically changing the security configuration of devices according to different trust conditions.

Feature	Threat	Challenge	Opportunity
Interdependence	Bypassing static defenses, Over Privilege	Access control and privilege management	Context-based permission

Diversity	Insecure protocols	Fragmented	Dynamic analysis simulation platform, IDS
Constrained	Insecure systems	Lightweight defenses and protocols	Combining biological and physical characteristics
Myriad	IoT botnet, DDoS	Intrusion detection and prevention	IDS
Unattended	Remote attack	Remote verification	Remote attestation, Anonymous protocols
Mobile	Malware propagation	Cross-domain identification and trust	Dynamic configuration

TABLE 2 - THREATS, CHALLENGES, AND OPPORTUNITIES OF EACH IOT FEATURES

V. Security critical areas of IoT

1. **Smart Cities:** To improve people's overall quality of life, smart cities make significant use of new computing and communication capabilities. Cities are being pushed to become smarter, and governments throughout the world are promoting their growth through various incentives. Although the usage of smart apps is meant to improve people' general quality of life, it also poses a danger to individuals' privacy. Smart card services have a tendency to put individuals' credit card information and purchasing habits at danger. Users' location traces may be leaked by smart mobility applications. There are apps that parents may use to keep track of their

children. However, if such applications are hacked, then the safety of the child can come to risk.

2. **Smart Metering and Smart Grids:** Smart metering covers a wide range of measurements, monitoring, and management applications. Smart grids, where power usage is recorded and monitored, are the most prevalent application of smart metering. Smart metering might potentially be used to combat power theft. Smart metering may also be used to monitor water, oil, and gas levels in storage tanks and cisterns. However, smart metering systems are vulnerable to both physical and cyber-attacks as compared to analog meters that can be tampered only by physical attacks.

3. **Smart Environment:** A smart environment comprises a variety of IoT applications such as forest fire warning, high-altitude snow monitoring, landslide prevention, earthquake early detection, pollution monitoring, and so on. All of these Internet of Things applications are intertwined with the lives of people and animals in those locations. The information from these IoT apps will also be used by government bodies working in these fields. Security flaws and vulnerabilities in any sector involving IoT applications might have disastrous effects. Both false negatives and false positives might have devastating consequences for IoT applications in this scenario.

4. **Security and Emergencies:** Another significant area where many IoT applications are being implemented is security and emergencies. It may be used for things like letting only authorised individuals into restricted locations. Breach of security in such applications might have a variety of catastrophic repercussions. Criminals may, for example, try to get access to restricted locations by exploiting vulnerabilities in such apps. False radiation level alarms can also have serious immediate and long term repercussions. If babies are exposed to excessive quantities of radiation,

for example, it may result in significant life-threatening illnesses in the long run.

5. **Smart Retail:** Internet of Things (IoT) applications are widely employed in the retail industry. Several apps have been created to track the storage conditions of products as they go through the supply chain. Adversaries may attempt to breach IoT apps related to goods storage conditions, as well as provide incorrect information about products to consumers in order to enhance sales. Customers' debit and credit card information, phone numbers, email addresses, and other personal information may be stolen if security elements are not incorporated in smart retail, resulting in monetary losses for both customers and merchants.

6. **Smart Agriculture and Animal Farming:** Monitoring soil moisture, managing microclimate conditions, selecting watering in dry zones, and controlling humidity and temperature are all examples of smart agriculture. If such apps are hacked, it may result in the theft of farm animals, as well as agricultural damage by opponents.

7. **Home Automation:** One of the most commonly utilised and implemented IoT applications is home automation. This includes applications like those for remotely managing electrical appliances to save energy, intruder detection systems installed on windows and doors, and so on. Attackers may, however, obtain illegal access to IoT devices in the house and attempt to damage people.

VI. IMPROVEMENTS AND ENHANCEMENTS REQUIRED FOR UPCOMING IoT APPLICATIONS

The enormous number of Internet of Things (IoT) devices being placed throughout the globe to make it smart creates a tremendous amount of data on the environment and users. This data may be used to infer a lot of personal information, which can pose a threat to both individuals and society as a whole. As a result, significant additions and modifications to the present IoT application structure and framework are necessary in order to make it dependable, secure, and resilient.
In this case:

1. To assess the amount of risk associated in installing IoT devices in various applications, thorough penetration testing is required. A priority list may be created based on the risk involved, and the devices can be deployed properly in various applications.
2. Encryption methods are utilised at many levels and protocols in IoT systems. The whole system, however, has many levels of encrypt, decrypt, and re-encrypt cycles. The system becomes vulnerable to assaults as a result of these cycles. End-to-end encryption appears to be a viable option for preventing many types of assaults.
3. Authentication-as-a-service protocols must be implemented. An authentication procedure should be implemented whenever a device wishes to interface with another device. Digital certificates might be a viable approach for providing seamless authentication with cryptographic protocols-bound identities.
4. Any IoT security architecture that is deployed should have scalability tested and confirmed. The security protocols should not be restricted to a small number of users. Only when the application is made public and widely utilised in the public domain does it become vulnerable to actual dangers. As a result, adequate strategy and preparation are essential.
5. To prevent the acquisition of user and environment data, a method based on encryption techniques such as RSA, SHA256, or hash chains is necessary. IoT

devices must be constructed in such a way that the sensed data may be transmitted in a safe and encrypted manner. Individuals, government agencies, and industries will be more trusting of IoT applications as a result of this.

6. Because IoT devices and applications are quickly expanding, a strategy must be devised to address the cost and capacity restrictions that are likely to emerge soon. A paradigm change from a centralised to a decentralised model, where devices can automatically and securely connect with one another, may be required. This can assist to lower the cost of administering applications and alleviate capacity problems.

VII. IoT Security using Blockchain

The blockchain is a distributed ledger (sometimes known as duplicated log files) with a simple concept. The blockchain entries are both chronological and time-stamped. Using cryptographic hash keys, each entry in the ledger is firmly connected with the preceding item. Individual transactions are recorded in a Merkle tree, and the tree's root hash is saved on the blockchain. Individual transactions are represented by T1, T2, T3, and Tn. The transactions are cryptographically hashed and saved as Ha,Hb,Hc, and so on on the tree's leaf nodes. The hashes of the child nodes are combined to create a new root hash. On the blockchain, the final root hash is kept. Only the root hash may be verified to ensure that all transactions connected with it are safe and untampered with. Even if a single transaction is modified, it will affect all hash values on that side of the tree. The miner or ledger keeper verifies the logs or transactions and creates a key that allows the most recent transaction to be included in the full ledger. This procedure makes the most recent items visible to all network nodes. It is excessively time-consuming and difficult for adversaries to tamper with the blocks due to the existence of cryptographic hash keys in each block.

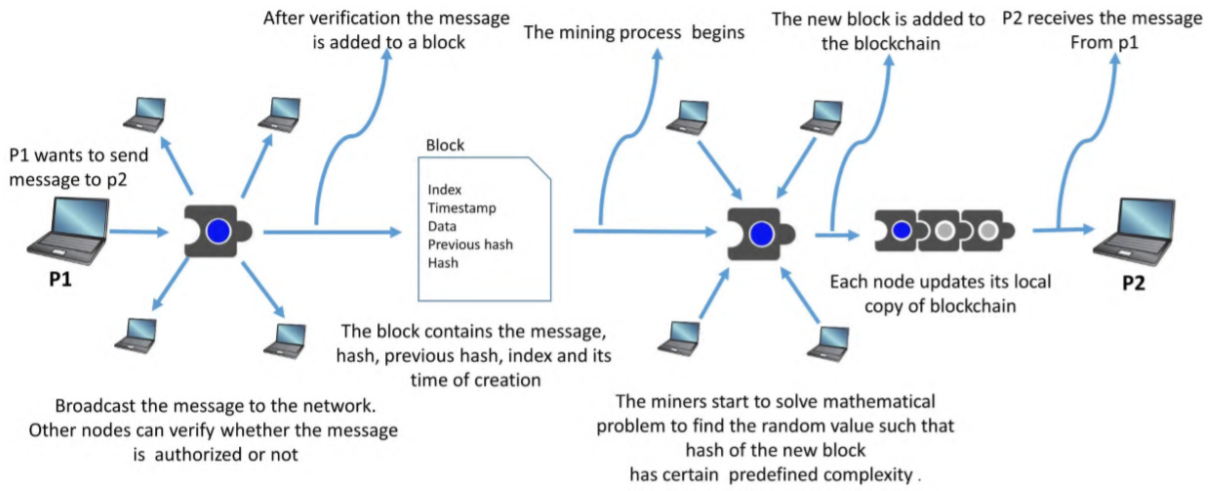

FIGURE 1. Working process of blockchain.

Benefits of Blockchain in IoT

1. **IoT data may be saved in Blockchain:** IoT applications involve a wide range of devices that are all connected to each other. Other devices can connect to these gadgets and control them. This system is also cloud-connected, allowing IoT apps to be used from anywhere. Blockchain is a potential option for storing data and preventing it from being exploited because of this huge space for data flow. Blockchain can function as a viable option for storing and transmitting data regardless of the layer in an IoT application.
2. **Blockchain's distributed nature allows for safe data storage:** Because the blockchain design is dispersed in nature, it can avoid the possibility of becoming a single point of failure, which is a problem with many cloud-based IoT systems. Regardless of the distance between the devices, the data created by them may be simply and securely saved on the blockchain.
3. **The hash key is used to encrypt data, which is then verified by miners:** In blockchain, only the 256-bit hash key for the data can be stored, rather than storing the actual data. The original data can be saved on the cloud, and the hash key can be linked to it. If the data changes, the hash of the data will change as

well. This keeps the information safe and confidential. Because only hash values are recorded on the chain, the size of the blockchain is unaffected by the amount of the data. Using the hash of the data, only the intended parties who are allowed to use the data may access the data from the cloud.

4. **Blockchain to prevent unauthorized access:** To avoid unwanted access, many IoT systems need regular communication between different nodes. Because blockchain communication is based on public and private keys, data can only be accessed by the intended person or node. Even if the data is accessed by an unwanted person, the contents of the data will be unintelligible since it is encrypted using keys. As a result, the blockchain data format attempts to address a variety of security concerns that IoT applications confront.
5. **Elimination of centralised cloud servers:** Because blockchain eliminates centralised cloud servers and makes the network peer-to-peer, it can improve the security of IoT devices. Data thieves are mostly interested in centralised cloud servers. The data will be disseminated across all nodes of the network and encrypted using a cryptographic hash function utilising blockchain.

Challenge Towards IoT	**Specification**	**Possible Blockchain Solution**
Privacy in IoT devices	IoT devices are vulnerable to exposing private user data	To address such a challenge, the proposed solution is to use a Permissioned Blockchain that can secure the IoT devices.
Cost and Traffic	To handle exponential growth in IoT devices	Moving towards decentralization using blockchain. The devices can directly connect and communicate with the

		peers rather than communicating via central servers.
Heavy load on cloud service and services insufficiency	Cloud services are unavailable due to attacks, bugs in software, power or other problems	Records are updated on different nodes on the network that hold the same data so there is no single point of failure.
Defective architecture	All the parts of IoT devices have point of failure that affects network and the whole device	Validity of devices is verified due to blockchain. The data is also verified cryptographically to ensure that only the main originator can send it.
Data manipulation	Data is extracted from IoT devices and after manipulating the data it is used in some appropriate way.	Due to blockchain, devices are interlocked. If any device updates data the system rejects it.

TABLE 3. Challenges in IoT and possible blockchain solutions.

VIII. IoT Security using Fog Computing

A. SOLUTIONS PROVIDED BY FOG COMPUTING TO OVERCOME IoT SECURITY THREATS

1. **Man-in-the-middle attack:** Fog works as a security layer between the end-user and the cloud or IoT system, preventing a man-in-the-middle attack. All threats or assaults on IoT systems

must travel through the fog layer in the middle, which can detect and neutralise anomalous activity before it reaches the system.

2. **Data transit attacks:** When compared to IoT devices, data storage and management on secure fog nodes is significantly superior. When data is kept on fog nodes rather than end-user devices, it is more secure. Fog nodes also aid in the accessibility of user data.
3. **Eavesdropping:** Instead of routing information via the whole network, fog nodes allow communication just between the end-user and the fog node. Because the network traffic is minimised, the odds of an enemy attempting to eavesdrop are greatly reduced.
4. **Issues with resource constraints:** Most IoT devices have limited resources, which attackers take advantage of. They aim to break the edge devices and utilise them as weak points to get access to the system. Edge devices can be supported by fog nodes, which can protect them from such assaults. The more advanced security functions required for protection can be performed by a nearby fog node.
5. **Services for incident response:** Fog nodes may be configured to deliver incident response services in real time. When fog nodes meet questionable data or requests, they might send a signal to the IoT system or end users. In-transit malware detection and issue resolution are possible thanks to fog computing. In many important applications, stopping the entire system to handle malware incidents may not be viable. While the system is up and operating, fog nodes can assist in such resolutions.

B. SECURITY CHALLENGES AND SOLUTIONS IN FOG LAYER

1. **Real-Time Services:** Fog computing in IoT systems tends to deliver near real-time services by doing computation near data creation sites.

- Intrusion detection: Without a suitable intrusion detection strategy in place, policy breaches and harmful activity on fog nodes and IoT devices would go undetected. Although the assaults may not affect the entire fog computing architecture, the attacker can influence the local services. Fog nodes can identify attacks against local services by cooperating with their neighbouring nodes. The assault on the cloud can be identified by analysing programme behaviour and host file systems.

2. **Transient Storage:** With the aid of transient storage, users may temporarily store and preserve their data on fog nodes. On the one hand, it facilitates data management on local storage, but it also introduces additional problems and security concerns, particularly in terms of data privacy.
    - Identifying and safeguarding sensitive data: Social events, traffic conditions, personal activities, temperature, and other data can be saved in IoT devices. Some of the information may be private or sensitive, while others may be made public. Furthermore, the same data has various security standards for different users.
    - Sharing data safely: Data uploaded to fog nodes is first encrypted to ensure security. Once the data has been encrypted, it can only be viewed by the owner. This causes a difficulty when it comes to data sharing. Some cryptographic approaches, such as key-aggregate encryption, proxy re-encryption, and attribute-sharing, have been used to address this problem.
3. **Data Dissemination:** Due to security concerns, data cannot be transmitted to the fog node without encryption.Many useful capabilities, including sharing, searching, and aggregation, are sacrificed as a result of moving encrypted data to the fog node.
    - Securing data searches: As mentioned in the section on temporary storage, data is encrypted before being uploaded. However, once information is encrypted, owners and other entities will have a difficult time searching for or retrieving the ciphertext. Searchable

encryption and its privacy settings are defined in order to extract information from encrypted text.

- **Data aggregation:** In some instances, fog nodes may need to aggregate data to prevent data leakage and save connection costs. To avoid data theft, it's critical to build safe aggregation methods. To accomplish safe data aggregation, many homomorphic encryption methods have been suggested, such as BGN encryption and Paillier encryption.

4. **Decentralised computation:** Data saved on fog nodes may be processed and analysed for better outcomes via decentralised computation. However, there are a number of dangers and risks connected with such calculations. For example, attackers can reveal processed data as well as manipulate the analysed findings.
    - Computation with the help of fog nodes: Tasks that cannot be completed by IoT devices are calculated with the help of fog nodes. However, if the fog nodes that receive data from IoT are already hacked, this may expose data to attackers. One such approach is server-assisted computing, which aims to enable secure computation.
    - Verifiable computation: Users rely on fog nodes to calculate their data, which is verifiable. There must be a safe method in place to validate the fog node's compute results.

Characteristics	**Solutions Provided By Fog**
Decentralization	Verifiable computation Server-aided exchange Big data analytics
Data dissemination	Designing protocol Sharing data securely

	Searching data securely
Real-time series	Identity recognition Access management Intrusion detection
Transient Storage	Recovery from attacks Data distribution Identifying and protecting sensitive data

TABLE 4. Characteristics and solutions provided by fog computing

IX. IoT Security using Machine Learning

A. Solutions provided by ML to overcome security threats

1. **DoS Attacks:** DoS attacks from IoT devices are a major source of worry. A Multi-Layer Perceptron (MLP)-based protocol that protects networks against DoS assaults is one way to prevent such attacks. To train an MLP that helps to improve the security of wireless networks, researchers developed a particle swarm optimization and back propagation technique. Machine learning approaches aid in improving deduction accuracy and protecting IoT devices that are susceptible to DoS assaults.
2. **Eavesdropping:** During data transfer, attackers may listen in on communications. ML methods such as Q-learning based offloading schemes or non-parametric Bayesian techniques can be utilised to guard against such assaults. Q-learning and Dyna-Q are examples of machine learning algorithms that may be used to defend devices against eavesdropping.
3. **Spoofing:** Using Q-learning, Dyna-Q, Support Vector Machines, Deep Neural Network model, incremental aggregated gradient, and distributed FrankWolfe methods, spoofing attacks may be prevented. These methods not only improve

detection and classification accuracy, but they also assist to lower the average error rate and false alarm rate.

4. **Privacy Leakage:** Personal information such as health data, location, or photographs is collected, putting the user's privacy at risk. To prevent privacy leakage, privacy-preserving scientific computations (PPSC) should be used. Another approach for developing IoT application trust is the commodity integrity detection algorithm (CIDA), which is based on the Chinese remainder theorem (CRT).
5. **Privacy Leakage:** Personal information such as health data, location, or photographs is collected, putting the user's privacy at risk. To prevent privacy leakage, privacy-preserving scientific computations (PPSC) [180] should be used. Another approach for developing IoT application trust is the commodity integrity detection algorithm (CIDA), which is based on the Chinese remainder theorem (CRT).
6. **Digital Fingerprinting:** One of the new and promising methods for securing IoT systems and assisting end users in gaining sufficient confidence in the apps is digital fingerprinting. Fingerprints are often used to unlock cell phones, approve payments, and open vehicle and house doors, among other things. Digital fingerprinting is becoming a prominent biometric identification technology due to its low cost, reliability, acceptance, and high security level. Apart from the advantages of digital fingerprinting, there are a number of obstacles to overcome in order to effectively apply this approach in IoT, including fingerprint classification, picture improvement, feature matching, and so on.Several machine learning-based methods have been created to give non-traditional solutions to these problems , some of which are mentioned here.
    - **Support Vector Machine:** SVM is a nonlinear and linear classification, principal component analysis, text categorization, speaker identification, and regression training method. The distance between the decision boundary and the training patterns is maximised. The SVM is trained using a feature vector created from the fingerprint's pixel values. Various

patterns hidden behind the fingerprint are examined, and then a fingerprint is matched based on the patterns found.

- **Artificial Neural Networks (ANN)** are one of the most widely utilised machine learning methods. It has a lot of benefits, including fault tolerance, adaptive learning, and generalisation. The back propagation technique of ANN is used to feed the digital values of different features in the fingerprint, such as minutiae, ridge ending, and bifurcation, into the neural network for training purposes. The fingerprint is verified based on previously entered experience values in the database.

X. IoT security using Edge Computing

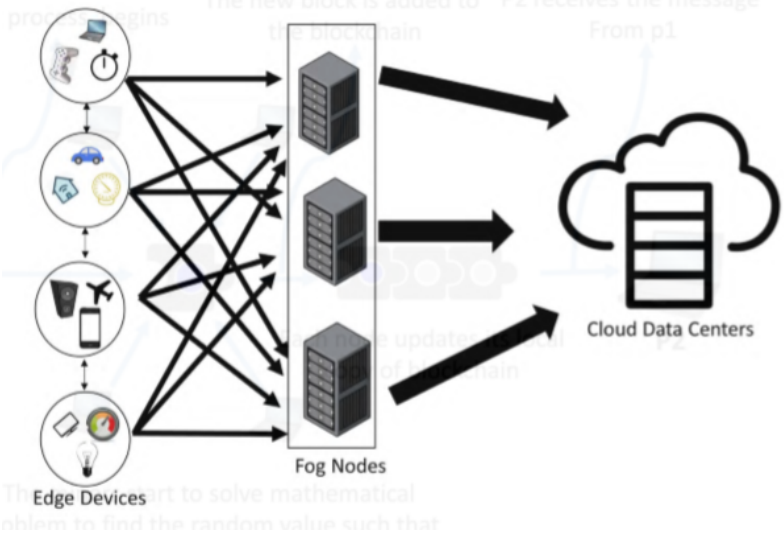

FIGURE 2. Edge computing architecture

A. Solutions provided by edge computing to overcome security threats

1. **Data Breach:** All data is saved and processed within the device or local network with edge computing. There is no data flow from the data source to the processor. This keeps the data safe while it's in transit, reducing the danger of data theft and breaches. There is some data flow from a device to the fog layer in fog computing, and attackers can take advantage of this movement.
2. **Issues with Data Compliance:** Many nations have strong legislative measures in place to prohibit data from being transferred outside of their borders, such as the European Union's GDPR (General Data Protection Regulation). Organizations may use edge computing to keep data within their borders and guarantee compliance with data sovereignty regulations.
3. **Issues of Security and Safety:** As the deployment of cyber-physical systems grows, security and safety are becoming more important concerns. If there is even a slight delay in replies, physical safety problems may arise. For example, if a car's sensors indicate that a collision is imminent, the air bags must be deployed quickly. If the sensors rely only on transmitting data to the cloud and waiting for a response from the cloud before taking action, it may be too late to avert injury or death.Edge computing may also be used to enhance surveillance cameras, allowing them to evaluate abnormalities and relay the aggregated and suspected data to data centres for faster reaction times.
4. **Bandwidth Issues:** IoT applications produce a large amount of data at a rapid rate. The majority of this information is unprocessed and of poor value. Sending all of the data to the cloud comes with a high expense in terms of bandwidth, as well as data security concerns. If edge computing is employed, a lot of data cleaning and aggregation may be done at the edge nodes, with just the summary data being transferred to the cloud if it is needed.

XI. Conclusion

As IoT uses network architecture which is similar to traditional network architecture for communication among different devices, flaws of traditional network architecture are also inherited in it. With the development of IoT, many kinds of attacks have also been invented to breach the security of IoT devices. We have first surveyed about the various security attacks. We then examine and discuss IoT security and privacy problems via the lens of a new feature - IoT. The security concerns, existing solutions, and research difficulties connected with these IoT characteristics are all highlighted. We have also discussed the existing and upcoming solutions to IoT security threats including blockchain, fog computing, edge computing, and machine learning.

XII. References

[1]. **AlJemy, Khalid, Mohammed AlAnazi, Mohammed AlSofiry, and Adeel Baig. "Improving IoT Security Using Blockchain." In *2019 IEEE 10th GCC Conference & Exhibition (GCC)*, pp. 1-6. IEEE, 2019.**

[2]. Hussain, Fatima, Rasheed Hussain, Syed Ali Hassan, and Ekram Hossain. "Machine learning in IoT security: Current solutions and future challenges." *IEEE Communications Surveys & Tutorials* 22, no. 3 (2020): 1686-1721.

[3]. Khan, Saad, Simon Parkinson, and Yongrui Qin. "Fog computing security: a review of current applications and security solutions." *Journal of Cloud Computing* 6, no. 1 (2017): 1-22.

[4]. Endler, Markus, Anderson Silva, and Rafael AMS Cruz. "An approach for secure edge computing in the Internet of Things." In *2017 1st Cyber Security in Networking Conference (CSNet)*, pp. 1-8. IEEE, 2017.

[5]. Zhou, Wei, Yan Jia, Anni Peng, Yuqing Zhang, and Peng Liu. "The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved." *IEEE Internet of Things Journal* 6, no. 2 (2018): 1606-1616.

[6]. Lin, Jie, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. "A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications." *IEEE Internet of Things Journal* 4, no. 5 (2017): 1125-1142.

[7]. Fu, Kevin, Tadayoshi Kohno, Daniel Lopresti, Elizabeth Mynatt, Klara Nahrstedt, Shwetak Patel, Debra Richardson, and Ben Zorn. "Safety, security, and privacy threats posed by accelerating trends in the internet of things." *arXiv preprint arXiv:2008.00017* (2020).

[8]. Trappe, Wade, Richard Howard, and Robert S. Moore. "Low-energy security: Limits and opportunities in the internet of things." *IEEE Security & Privacy* 13, no. 1 (2015): 14-21.

[9]. Liu, Hui, Changyu Li, Xuancheng Jin, Juanru Li, Yuanyuan Zhang, and Dawu Gu. "Smart solution, poor protection: An empirical study of security and privacy issues in developing and deploying smart home devices." In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*, pp. 13-18. 2017.

[10]. Langner, Ralph. "Stuxnet: Dissecting a cyberwarfare weapon." *IEEE Security & Privacy* 9, no. 3 (2011): 49-51.