PRIVACY & SECURITY OF IOT

Abstract

The Internet of Things (IoT) is a network of devices that share information and coordinate their actions without human intervention. It is used in various industries, including manufacturing, healthcare, logistics, energy, and agriculture. IoT systems consist of wireless networks, cloud databases, sensors, data processing software, and networked smart devices. The functionality and implementation of IoT depend on the industry, but businesses must invest significant resources in cybersecurity. IoT authentication helps establish trust in IoT machines and devices, protecting data and managing access. Cost, convenience, and practicality are also important factors for IoT businesses. Data protection and asset management are crucial, with user privacy protection being more important than ever. Identity and access management (IAM) can help businesses set procedures to protect themselves from cyberattacks and data leaks. The IoT has become a highly influential sector in the tech industry, providing vital services like automatic home appliance management, healthcare monitoring, and transportation control. However, it also has security and privacy concerns. IoT data can be used for academic and research purposes, but data analysis must first remove identifying or private information to protect confidentiality. Users' privacy can be protected throughout the data processing lifecycle, with anonymous data collecting methods becoming increasingly common. Cloud storage services often store IoT data, and encryption methods, such as homomorphic encryption, are used for secret analysis and retrieval.

Authors

Rohit Aggarwal
Department of CSE – Data Science
Meerut Institute of Engineering & Technology
Meerut, India.
rohit.aggarwal@miet.ac.in

Basudeo Singh Roohani
Department of Computer Science & Engineering
IMS Engineering College
Ghaziabad
India.
bsroohani2007@gmail.com

Nitin Goyal
Department of Computer Science & Engineering
IMS Engineering College, Ghaziabad
India.
nitingoyal0925@gmail.com

Rashmi Gupta
Department of Computer Science & Engineering
AMITY University
Manesar, Gurugram
India.
goyal.rashm18@gmail.com

I. INTRODUCTION

The term "Internet of Things" is used to describe a network of devices that may share information and coordinate their actions without any human intervention.

IoT systems typically have a framework of wireless networks, cloud databases for communication, sensors, data processing software, and networked smart devices.

The Following Elements Are Used By Iot Systems To Process And Exchange Data

- Environment and other gadget/part information gathering, storing, and sharing smart devices
- Smart devices use embedded systems with processors, sensors and communication devices to collect, send and respond to environmental data.
- Cloud or on-premises data centres with wirelessly connected remote servers;
- Gateways, hubs, and other edge devices in the Internet of Things that act as a communication link between IoT gadgets and the cloud.

IoT is used in manufacturing, healthcare, logistics, energy, agriculture, and other industries. Depending on the needs of the IoT system, the "smart devices" connected to it could include sensors or even DNA analysis machinery.

Most Iot Devices and Applications Are

- Home automation systems monitor and control functions like temperature, lighting, entertainment systems, appliances, and security systems. Common smart home automation devices include assistant speakers, thermostats, refrigerators, plugs, and light bulbs.

- Because to medical IoT, doctors and patients alike may keep tabs on one other's health status through a variety of different channels (MIoT). Smart devices for the Internet of Things include wirelessly connected health monitoring like Fitbits and glucometers (IoT).

- With the information collected by smart devices, smart cities may better provide for its citizens in terms of public services, utilities, and infrastructure. Such gadgets can be linked to a wide variety of sensors, lights, metres, trash cans, and air quality monitors.

- Wearables are mostly used in sports and healthcare. These gadgets include blood pressure monitors, smart watches, ECG

- Businesses can increase their output and efficiency with the help of "smart warehouses" that employ automated and networked technologies. Typical components of a smart warehouse include robots, drones, RFID scanners, artificial intelligence software, and advanced warehouse management systems.

II. ARCHITECTURE OF INTERNET OF THINGS (IOT)

Internet of Things (IoT) technology is rapidly growing in popularity due to its versatility. To the extent that it has been put to use in the different fields for which it was designed and developed, the Internet of Things performs as expected. Yet, there is not a commonly accepted, well-defined design for how it should function. The functionality and implementation of IoT depend on the industry in which it is used. Yet, the foundation of IoT is a basic industrial flow.

There are four distinct layers, which can be further subdivided into the sensing layer, the network layer, the data processing layer, and the application layer.

Here are The Justifications behind these.

- **Sensing Layer:**There are sensors, actuators, and other devices in this sensing layer. Devices like this take in data (such as physical or environmental features), process it, and then send it on to other devices via some sort of network.

- **Network Layer:**This layer contains Internet/Network gateways and data acquisition systems (DAS). DAS is in charge of all data collection and transformation processes (data collection, aggregation, conversion of analogue sensor data to digital data, etc.). Connecting Sensor networks to the Internet is the primary role of an advanced gateway, but it also does other basic gateway tasks like filtering incoming data, protecting the network from malicious software, and even making choices based on the information it receives.

- **Data Processing Layer:**This is the brains of the Internet of Things ecosystem. Data is processed and analysed here before being delivered to the data centre, where it will be accessible by software programmes often referred to as business applications. This is where "edge analytics" or "edge IT" comes into play.

- **Application Layer:** The fourth step of the IoT architecture is this layer. Data centres, often known as the cloud, are places where data is handled and used by end-user applications including those in the fields of agriculture, health care, aerospace, farming, and military, among others.

III. THE IMPORTANCE OF IOT SECURITY

Due to the widespread use of IoT systems, businesses must devote considerable resources to ensuring their integrity.

Perhaps hundreds or thousands of people could be impacted by a failed hacking effort or system failure caused by any vulnerability. It's possible for criminals to disable a home security system, or faulty traffic lights could cause accidents. In light of the fact that some IoT devices are employed in life-or-death contexts like security and healthcare, ensuring their safety is of paramount importance.

To keep their data safe, IoT systems must prioritise security. The huge amounts of sensitive data, including personally identifiable information, collected by smart devices requires strict adherence to a wide range of cybersecurity laws, standards, and regulations. Legal action and sanctions could result from a breach of such information. It can also lead to a drop in customer confidence and undermine your brand's reputation.

Defending the physical items, networks, processes, and technology that comprise an IoT ecosystem from a wide variety of IoT security incursions is the primary goal of Internet of Things security.

IoT Security's Two Main Objectives Are To:

- Guarantee the safe collection, processing, storage, and transmission of any and all information.
- Find and solve security flaws in IoT parts.

IV. IOT SECURITY CHALLENGES

There were 1.51 billion IoT device breaches from January to June of 2021, compared to 639 million disclosed by Kaspersky for the entirety of 2020. Inadequate attention to cybersecurity during the design of Internet of Things (IoT) systems is not acceptable.
Researching possible cybersecurity threats is a crucial first step in learning how to secure IoT equipment.

List of Typical Iot Security Issues:

1. **Software and Firmware Vulnerabilities:** It is difficult to guarantee the safety of IoT systems due to the limited resources and processing power of numerous smart gadgets. As a result, they are more vulnerable to security flaws than non-IoT devices because they can't operate robust, resource-intensive security operations.

This Is Because Many Iot Systems Suffer From The Following Security Flaws

- Inadequate processing capacity prevents the use of effective in-built security measures.
- Poor security measures for IoT devices
- Insufficient funding to adequately test and develop firmware security
- There is a lack of regular patches and upgrades because of limited resources and the inherent technical constraints of IoT devices.
- Because of this, security updates may not be widely distributed if users are unable to update their devices.
- It's possible that support for newer versions of software will be discontinued for older devices.
- The device has poor security against physical attacks; an attacker can easily add their own chip or hack it via radio waves if they get close enough.

By taking advantage of security holes, hackers hope to get access to a victimised IoT system, disrupt its communications, introduce malicious software, and steal private data. Example: hackers were able to compromise Ring smart cameras because users used passwords that were easy to crack, such as those that reused previous passwords or were the system default. Using the camera's built-in microphone and speakers, they were even able to have a remote conversation with the victims.

2. **Insecure Communications:** Implementing existing security programs on resource-constrained IoT devices is difficult because they were originally developed for desktop computers. This means that conventional security methods aren't as effective in keeping the data exchanged between IoT devices safe.

   One of the biggest threats posed by insecure communications is the possibility of man-in-the-middle attacks (MitM attacks). If your smartphone doesn't have strong authentication and encryption in place, it could be subject to Man-in-the-Middle attacks, which hackers can use to easily hijack your device during an update process and take full control of it. If your device transmits data in plain text, hackers can still access the information it shares with other devices and systems, even if it is not affected by a man-in-the- middle". This is the case even if the attack does not succeed in compromising your device.

3. **Data Leaks from IOT Systems:** The data handled by your IoT system is vulnerable to hackers who are able to intercept its unencrypted communications, as we have shown. Your home address, bank account details, and even medical history could be compromised. Attackers can get sensitive information in a number of ways, one of which is via exploiting unsecured channels of communication.

   The cloud is used for data transit and storage, and it is also possible for malicious actors to compromise cloud-hosted services. As a result, data from the devices themselves and the cloud services they connect to can be compromised.

   Data leaks might also originate from third-party services used by your IoT systems. One example is the revelation that Ring smart doorbells were secretly disclosing customers' private information to third parties like Facebook and Google. This issue has arisen because of the availability of third-party tracking services within the Ring mobile app.

4. **Malware Risks:** According to a new survey by Zscaler, smart TVs, smartwatches, and set top boxes are the most vulnerable to malware attacks.

   If hackers can compromise an IoT system, they could use it to spy on users, steal sensitive information, or perform other malicious acts. Some gadgets may even come pre-infected with viruses if manufacturers don't take software security seriously.

   The most well-known pieces of IoT-focused malware have been met head-on by certain companies, but others are still working on mitigation strategies. An FBI agent revealed the agency's tactics for countering the Mirai botnet, and Microsoft published advice for protecting against the MoziIoT botnet in advance of any potential attacks.

However, cybercriminals continually develop new methods of attacking the Internet of Things. BotenaGo, a piece of malware built in Golang, was found to attack over 30 different flaws in smart devices in 2021.

5. **Cyber Attacks:** Other types of assaults, such as malware and MITM attacks, can target IoT equipment as well. The most typical forms of attacks against the Internet of Things are as follows:

Common Attacks on IOT Systems

- **Denial of Service (DoS) Attacks:** IoT devices are highly vulnerable to denial-of-service attacks due to their low computing power. A device's capacity to react to valid requests is jeopardised during a DoS assault as a result of a massive phoney traffic flow.

- **Denial of Sleep (DoSL) Attacks:** Sensors hooked up to wireless networks typically utilise long-lasting batteries to allow for constant environmental monitoring. Smartphone battery life can be significantly elongated if the device is left in sleep mode for the vast majority of the time. Different protocols, such as media access control, have different communication needs, which in turn affects how much sleep and how much awake a person gets (MAC). To perform a DoSL attack, hackers can exploit a vulnerability in the MAC protocol. This type of attack drains the battery's MAC protocol in order to carry out a DoSL attack. A depleted battery renders the sensor useless, which is the intended effect of this type of assault.

- **Device Spoofing:** When a device is mishandled, this attack is conceivable. This technique can compromise devices that do not properly integrate digital signatures and encryption. Inadequate public keys, such as an inadequate public key infrastructure (PKI), can be used by hackers to "spoof" network devices and interfere with IoT adoption.

- **Physical Intrusion:** Even though the majority of attacks are carried out remotely, it is still feasible for a device to be physically compromised if it is taken. Hackers are able to manipulate the components of a gadget and make it behave in a manner that was not intended.

- **Application – based Attacks:** When there are vulnerabilities in cloud servers or backend applications, or when there is a security hole in the firmware or software used on embedded systems, these kinds of assaults become possible.

With these obstacles in mind, let's go on to discussing some best practises for the security of the Internet of Things, which can assist you in protecting your IoT system.

V. BEST PRACTICES FOR ENSURING THE SECURITY OF IoT SYSTEMS

Implementing security best practises for the Internet of Things (IoT) will assist you in better protecting the devices, networks, and data that make up the three primary aspects of IoT systems. Let's begin by talking about the different approaches to keep smart gadgets safe.

1. How to Secure Smart Devices?

- **Secure Hardware:** Attackers may steal IoT devices to tamper with them or access private data. It is important to make your product tamper-proof in order to keep sensitive data on devices safe. Port locks, camera covers, and strong boot level passwords are all examples of physical security measures that can be taken to make a product useless in the event of tampering.

- **Patch and Update:** The ongoing upkeep of devices results in further expenditures. The only way to guarantee adequate product security, however, is via regular updates and patches. It's preferable to implement mandated automatic security upgrades that consumers aren't able to opt out of. Give your customers an idea of how long you'll be offering product support, and inform them what they should do once that time is up. Once you've deployed your system, it's important to keep a watch out for security flaws so you can patch them as soon as possible.

- **Test thoroughly:** Penetration testing is your major tool for detecting IoT firmware and software vulnerabilities and minimising the attack surface. Static code analysis finds obvious problems, whereas dynamic testing finds hidden vulnerabilities.

- **Protect Device Data:** IoT gadgets should protect information before, during, and after its use. Always use non-volatile memory for storing cryptographic keys. In addition, you can provide a means of safely discarding used materials or offer to do so yourself.

2. How to Secure IoT Networks?

- **Secure Authentication:** Using special default credentials, this is possible. Use current conventions when giving your products names or addresses to prolong their useful life. Include multi-factor authentication in your product if at all possible.

- **Encrypted and Secure Communication:** The data exchanged during inter-device communication must also be safeguarded. There needs to be a change in encryption algorithms to accommodate the low processing power of IoT gadgets. Transport Layer Security and Lightweight Cryptography are two methods that can be used for these aims. RFID, Bluetooth, Cellular, ZigBee, Z Wave, Thread, and Ethernet are just some of the wireless and wired technologies that can be used with an IoT architecture. Network security is also possible with the help of improved protocols like IPsec and SSL.

- **Reduce Bandwidth:** To ensure that the IoT device continues to function, only the minimum amount of network traffic is allowed. If at all possible, you should configure the device to show suspicious activity and restrict its bandwidth at the hardware and kernel levels. This will prevent denial-of-service attacks against your product. When malware is found, the product should be set to reboot and delete its code to prevent it from being utilised in a botnet to launch distributed denial-of-service attacks.

- **Network Segments:** Divide large networks into multiple smaller ones and use next-generation firewall protection. Use IP address ranges or virtual local area networks (VLANs) for this. Use a virtual private network (VPN) to connect your IoT devices securely to the internet.

3. How to Secure Data in IoT Systems?

- **Secure Sensitive Data:** Install one-of-a-kind passwords as the default for each product, or demand that users immediately change their passwords after using a device for the first time. Implement strong authentication methods to make certain that only authorised users can access the data. If the user decides to return or resell the product, you can design a reset mechanism that will allow the erasure of sensitive data and the wiping of configuration settings. This will go the extra mile to ensure that the user's privacy is protected as thoroughly as possible.

- **Collect only Essential Information:** Ensure that your Internet of Things product only collects the data required for its operation. This will limit the danger of data leakage, safeguard the privacy of consumers, and eliminate the possibility of noncompliance with numerous data protection regulations, standards, and laws.

- **Secure Networking:** Protect your product from cybercriminals by limiting its interaction with the internet of things. Make your product invisible to inbound connections by default to maintain secure communication and avoid over-reliance on network firewalls. The Advanced Encryption Standard, Triple DES, RSA, and the Digital Signature Algorithm are all excellent examples of encryption algorithms that can be adapted to the specific requirements of IoT systems.

VI. AUTHENTICATING IOT DEVICES

In order to have faith that devices on the Internet of Things (IoT) are who or what they claim to be, strong authentication of these devices is necessary. Therefore, each IoT device requires a distinct identifier that can be verified upon authentication with a gateway or centralised server. IT administrators will be able to keep tabs on all of their devices, have private conversations with them, and stop them from performing malicious tasks if they have a way to identify them individually. Administrators can easily withdraw access from a device if it starts acting strangely.

1. **The Leading Iot Authentication Techniques And Options:** When information travels over an unprotected network, like the Internet, IoT authentication is a methodology for developing trust in the identification of IoT machines and devices to protect data and manage access.

In addition, authentication helps stop hackers from pretending to be IoT devices in order to get access to servers storing sensitive information like audio and video recordings.

Several approaches exist for implementing robust authentication to safeguard connections between IoT devices:

- **Single Sided Authentication:** When two parties want to connect with each other, only one party will verify itself to the other, while the other party will not.
- **Dual-factor Authentication:** Is also known as mutual authentication, which describes a situation in which both entities act as authenticators for one another.
- **Three-factor Authentication:** Is a process in which a third-party act as an authenticating authority between two parties and also assists the parties in authenticating each other.
- **Distributed:** Utilising a method of direct distributed authentication between the several parties involved in the communication.
- **Centralized:** Employing a centralised server or a reliable third party to handle the distribution and management of authentication certificates is a recommended practise.

VII. IOT IDENTITY MANAGEMENT

Our world will continue to become more complicated even as it becomes more interconnected. In particular with regard to the management of identities and access (IAM). This is a problem that affects all of us, from the people who use services to the businesses and operators whose job it is to verify and approve the people and devices that access the internet on a daily basis.

1. **How Important Is Identification And Access Control (Iam) In IOT:** Cost, convenience, and practicality are just a few of the many things that IoT businesses must take into account. Data protection and asset management, however, stand out. User privacy protection is now more important than ever. Identity and access management (IAM) may help businesses set certain procedures in place that will eventually keep them safe from cyberattacks and data leaks, which is where they come in handy. Let's examine the idea in greater detail:

   The Internet of Things (IoT) industry is growing quickly. Connected devices continue to simplify consumer lives and business operations, generating exciting new revenue streams for IoT-related businesses.

   This is understandable considering how it is now possible to produce improved consumer experiences across industries by building a solid and reliable interface between devices, sensors, servers, and of course, data.

Time, cost, and convenience present a huge issue for businesses operating in the IoT world. Assuring consumer data security and privacy, however, is of more significance.

- **Data breaches in the IoT Space:** As the Internet of Things (IoT) becomes more pervasive in our daily lives, it becomes harder to protect users' privacy. As a result, there is less opportunity to exercise oversight over growing quantities of collected data and network traffic.

  Actually, control can be lost if an unauthorised party gains access to the computer or smartphone and uses it as a universal remote. If the victim isn't shaken up by a series of important events, this type of cybercrime may go unnoticed for a long time.

  Additionally, smartphones in particular store a massive amount of user information. There are apps that may be connected to your email, bank account, and even your home and car. The consequences of data theft are often insurmountable.

- **Consumers Demand Data Control:** No user wants to feel like they have given up control of their information because of an IoT app. They want control over who can see what about their personal data, for how long, and under what conditions.

  As our planet shrinks and gets more interconnected, this difficulty will only grow. Both the end-users who access the IoT services and the service providers who authenticate and authorise them are considered part of this category.

  The problem with the Internet of Things era is not that things cannot be accessible. Instead, data must be safeguarded because access to devices raises the likelihood of leaking.

VIII. IAM AND IOT

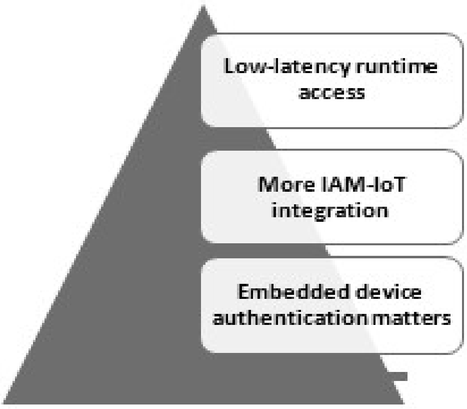
1. **Optimizing Access:** Identify Access Management (IAM) is a set of tools and guidelines for controlling who has entry to sensitive data and systems. In addition to controlling who can access what data, IAM can be used to track down misplaced or stolen gadgets.

   An IAM solution needs to be in step with the needs of today's mobile and digital workforce while also being effective, productive, and secure. As was previously said, it is crucial for businesses to establish and maintain control over device identities inside the IoT ecosystem.

   With the proliferation of connected devices and growing security threats, it is clear that current IAM solutions are unable to meet the needs of the Internet of Things.

IX. MARKET TRENDS IN IAM FOR IOT

When it became clear a few years ago that IoT technology was here to stay, the need for IAM exploded. It's fascinating to see how three market factors have converged to drive identity, access, and connection in the IoT landscape:


Low-latency runtime access
More IAM-IoT integration
Embedded device authentication matters

Key benefits of IAM

1. **Low-Latency Runtime Access:** As more and more IoT devices flood the market, providers in this space need to offer reliable, scalable runtime access for protecting authentication and authorization in the face of a surge in transactions without compromising on response times.As time goes on, providers will need to better enable deployment on-premise and in the cloud by decreasing the data storage footprint and managing both structured and unstructured data sets.

   When the groundwork has been completed, data can be transmitted between devices with fewer delays. Why else would we have Internet of Things platforms?

   - **More IAM-IoT integration:** In most cases, companies that sell Internet of Things platforms have no idea how to handle user identity management. Nevertheless, this is starting to change as more and more people use IoT platforms to integrate device identification and access technologies for straightforward security layouts in IoT apps. Because of this, the incorporation of IAM into numerous IoT markets is accelerating even further. That's exactly what needs to happen to guarantee the security of user information forever.

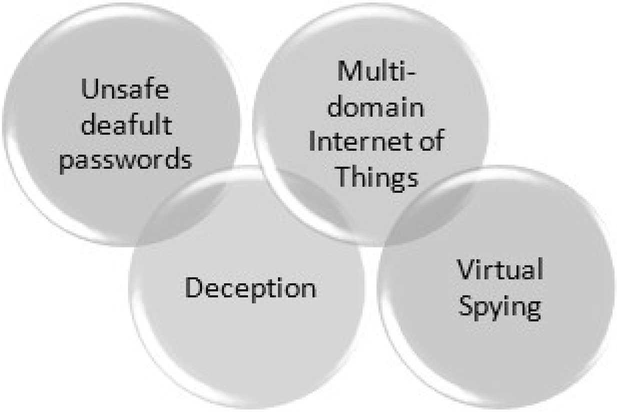
   - **Embedded device authentication matters:** Most companies making IoT hardware aren't prepared to meet authentication needs, and that includes providing adequate design and security controls as well as firmware for their products.

     As more specialised Internet of Things (IoT) goods enter the market, it's no surprise that their manufacturers are teaming up with similarly specialised authentication service providers and product experts to develop a flexible and secure authentication system.

It is obvious that there is still a significant amount of work to be done before the industry-specific authentication standards can become stable and gain acceptance in the market. Notwithstanding this, there is a stronger emphasis than ever before placed on the promotion of industry-specific standards.

X. IOT IAM ROLES

With no further ado, let's examine the four ways in which identity and access management play a crucial part in the provision of IoT app development services:



1. **Unsafe Default Passwords**: There are default passwords on a lot of IoT devices. Customers are then told to update them later, in other words. But not everyone bothers or remembers to behave responsibly. Also, individuals that alter the password employ standard username/password combinations.

   That defeats the objective of connecting the IoT gadget to a secure line. Since the California Consumer Privacy Act (CCPA) was passed by California lawmakers, all manufactured and sold unique passwords for connected IoT apps must be encrypted. But there is also an opposite.

   Even individuals with restricted access to the company will have access to the gadget if everyone has the passport. However, this can be resolved by including plugins and processes.

2. **Multi-Domain Internet of Things:** Having a firmer grasp on how modern digital identities function is essential in light of the IoT ecosystem's rapid growth. Because the Internet of Things spans so many disciplines, it's important to coordinate the various identities that emerge from it.

   For optimal identity management across all company-issued devices and domains, consider implementing a cross-domain IAM solution. This will improve their ability to function in that setting.

3. **Deception:** In common parlance, credential stuffing is the intentional use of compromised login information (such as a username and password) to access private data.

It is a serious crime that occurs frequently. One common way this occurs in the workplace is when workers give out their passwords to other workers, either knowingly or unknowingly.

In common parlance, credential stuffing is the intentional use of compromised login information (such as a username and password) to access private data. It is a serious crime that occurs frequently. One common way this occurs in the workplace is when workers give out their passwords to other workers, either knowingly or unknowingly.

Without a solid IAM solution in place, it's simple for hackers to get unauthorised access to sensitive systems or information. Nonetheless, this is largely solvable and under your control. You may secure your network's data at the enterprise level by using an IAM platform to manage all your connected devices.

4. **Virtual Spying:** Connected Internet of Things gadgets often have upgraded versions of virtual personal assistants like Alexa or Siri. They are paid to take notes and listen to you. Many companies, though, don't have a clear strategy for putting virtual assistant data to use.

   Personal assistants are a constant source of anxiety because to the risk that they would reveal trade secrets or leak critical information, damaging the company's standing in the eyes of consumers.

XI. PRIVACY – PRESERVING IOT: METHODS & APPLICATIONS

In the last decade, the Internet of Things (IoT) has become a highly influential sector of the tech industry. The simple and automatic way in which it provides vital services to consumers by detecting the environment has drawn the attention of the technology sector. The total number of sensors and devices that make up the IoT network and make the service possible. Although it has many benefits because to its widespread application in areas such as automatic home appliance management, healthcare monitoring, and transportation control, it also has serious security and privacy concerns. Every IoT node is a data generator. It reveals private information about the user's actions. Therefore, preventing the disclosure of such details is crucial. An additional critical concern is the means by which IoT data is stored. A reliable authentication and access control system is required to safeguard the information. Insightful discoveries can be made using the IoT data collected for academic and research purposes. Data analysis that does not first remove identifying or private information could compromise individuals' confidentiality. Since this is sensitive information, it must be protected before being presented to researchers. Users' privacy can be protected throughout the data processing lifecycle, from initial data capture through final analysis. Since the identity of the user and IoT nodes may be concealed, anonymous data collecting methods have become increasingly common. The data collected by IoT devices is often kept in a cloud storage service. Many encryption methods exist which can be used to protect data while it is being stored. For secret analysis and retrieval of data, homomorphic encryption methods are used.

1. **IoT Security Requirement Applications**

   - **Home Automation Using Iot:** In order to track usage and conserve energy, smart homes (SH) are fitted with various sensors and RFID. In the Internet of Things, devices communicate with one another over wireless connections to build networks and exchange data via so-called edge networks. Daily power consumption and other user behaviors are tracked by the home automation system. This kind of information is extremely private and must be kept secret. Therefore, it is crucial to create a home automation system that effectively protects users' privacy. Protecting the identity, location, and routine activities of its users, a privacy-focused home automation system does just that.

   - **Health Care and IoT:** Wearable sensors, a smart pillbox, a smart bed, and other IoT health care apps are used to remotely monitor the health of the patients. As it gathers data on patient health, there are a number of security and privacy issues. IoT devices use cloud-based or fog-based systems to store health information. Applications for patient healthcare should collect user data in an anonymous manner and should delete any sensitive health-related data. Such privacy-protected data is a valuable resource for medical systems and illness diagnostics. Therefore, it is now required to create health care applications with privacy in mind.

   - **IoT in the Cloud and Fog:** The combination of cloud computing and the Internet of Things is referred to as cloudIoT. Data from IoT sensors is gathered and stored in the cloud by cloud-based IoT systems. The cloud provides the IoT system with a variety of services, including data storage, service, compute, and more. It lessens the need for processing on Internet-of-Things gadgets. Fog computing is an offshoot of cloud computing that goes by another name: edge computing. When it comes to the underlying infrastructure, fog computing is distinct from cloud computing. Fog computing refers to an architecture where intelligent edge devices communicate with the cloud. Having fog nodes at the network's periphery reduces the load on cloud servers and boosts accessibility. Fog nodes are the building blocks of fog-enabled IoT systems; they are responsible for routing, data gathering, and data aggregation. Then, the information is uploaded to the cloud.

   - **Blockchain IoT:** Another cutting-edge technology utilized in transactions and interactions is blockchain. Blockchain for IoT applications can speed up transactions, save computing costs, and increase device confidence. The use of blockchain in IoT offers a mechanism for synchronizing data across tens of thousands of IoT devices. A large number of IoT devices cannot be synchronized using the traditional client-server model.

2. **IOT Privacy-Preserving Methods:** Many encryption and anonymization strategies can prevent a compromise in privacy in an IoT system. Scholarly and scientific investigations may make use of the anonymized data.

   Many methods for protecting users' anonymity within an Internet of Things infrastructure are outlined here. These methods include homomorphic encryption, multi-party computation, trustworthy third-party computation, and anonymization techniques.

3. **Internet of Things Anonymization Methods:** With the process of information aggregation, sensitive data that is stored on Internet of Things nodes is protected. Nonetheless, other issues develop, such as delays in computing, erroneous findings, software defects, and so on. There is a proposal for a public aggregation mechanism that can be verified. First, the data from the untrusted nodes are gathered using this method, and then the data are aggregated. With the tuple methods that have been presented, it is possible for the public to verify the reliability of the data. In spite of this, certain data owners have been excluded from participation in this plan.

   The Internet of Things (IoT) proposes a technique for anonymously collecting raw data with no central authority to be trusted. With this setup, the data is not aggregated nor is any noise introduced; rather, it is provided in its purest form for the analysis to extract the most value possible. When data is combined with that of other group members, it becomes unintelligible to any one person, effectively masking their identity and protecting their privacy. As well as reducing computational capacity, removing a source of trust removes a relationship between the data and the person who provided it.

   We propose a medical IoT node where patient data can be stored anonymously while still being traceable. Patients' privacy is protected by a sophisticated encryption method called attribute-based encryption (ABE). Using a policy based on the matching of keywords, it restricts access to patient information. A trusted authority, medical nodes, and a cloud platform make up the proposed system concept. This approach imposes a relatively significant computational cost.

   For IoT-driven applications, an anonymous authentication mechanism is introduced. To protect users' privacy and prevent their actions from being traced back to them, the protocol is completely decentralised. To address the concerns of both data owners and data collectors, an anonymous protocol has been developed. To ensure confidentiality, the protocol implemented Shamir's secret sharing mechanism. This protocol has been criticised for being ill-thought-out and ill-secured. Bypassing the authentication system and fooling the data collectors is possible if an adversary can pose as a legitimate user.

   In the Internet of Things, location privacy is always a hot topic when it comes to services that rely on users' precise whereabouts. A sham method for protecting the location secrecy of Internet of Things (IoT) devices is presented. They have studied the attack method and created a system for protecting users' location privacy using entropy. It is built to withstand collusion and inference assaults while requiring as little processing power as possible. Up until it reaches k-anonymity, it uses a greedy strategy to pick the dummy site.

4. **Multi-Party Computation in the Internet of Things:** OppNet tracks node locations. It uses a history table to determine the optimum route from sender to receiver node. History table leaks private data. In proposes privacy-preserving history-based routing. It protects OppNet identity and location. It sends messages anonymously using multiparty computation. It trades computation for security and privacy. IoT-based smart metering systems collect user data regularly.

User privacy is at danger. A smart grid advanced metering infrastructure protocol uses fully homomorphic encryption (FHE) and secure multiparty computing (MPC) to preserve user privacy. This solves FHE's excessive fragmentation and MPC's message complexity. Pseudorandom number generators calculate the share privately, protecting users' privacy.

5. **IoT Homomorphic Encryption:** Due to IoT security, fog orchestration addresses response time and service delivery. Fog orchestration customises the network to give the intended service with privacy and security options. ABE and HE are used to protect data privacy with low latency and power consumption in IoT devices.

An anonymous privacy-preserving data aggregation approach for fog augmented IoT systems protects sensitive data. This pseudonym technique provided anonymity and authenticity. Data aggregation uses Paillier algorithm for privacy. Real-time communication and resource-limited devices benefit from this system. Smart grids cannot use this approach.

To enable Internet of Things (IoT) applications in smart cities, we apply a context-aware privacy protecting approach to the SDN paradigm. Data packet flows over the network are monitored to manage privacy breaches. When the SDN controller detects particularly sensitive information in the network, it splits that information in half. The data is split in two and sent, initially over a VPN and then via a secure channel in the network.

In order to prevent hackers from gaining access to private information stored in IoT devices, a privacy-preserving IoT architecture is proposed. Access to private information is monitored and managed using a homomorphic encryption technique. Because of the data aggregation to appendices, no private information is exposed to potential hackers or attackers. It's a system that ensures confidential data transfer from beginning to end. The system is also tested for how quickly queries are processed. The data generated by IoT devices is analysed by cognitive IoT to draw useful conclusions. Yet, truth finding methods ensure the reliability of the collected data. Designing truth finding so that privacy is not compromised is crucial. In order to protect the personal information of users of fog-based IoT devices, a framework called LPTD is presented. This framework uses the Paillier cryptosystem and the one-way hash chain techniques to stop the privacy violation from occurring. In addition to stopping the introduction of erroneous data, it also facilitates the finding of the truth while requiring less time and effort from the involved computers and networks.

6. **IoT Independent Verification Service:** Trusted anonymous server-based privacy preserving trajectory system for mobile IoT devices preserves users' location privacy by satisfying spatial k-anonymity for group snapshot queries. It prevents location-based service provider inference attacks and protects user location privacy. Circular secure locations are suggested for continual queries. The optimal average nearest neighbour algorithm keeps people apart and hides their real locations.

Data privacy and granular control over access can be achieved with an attribute-based encryption approach and a decentralised, multi-authority access control mechanism. Therefore, the proposed strategy employs this technique to create an anonymizing and cryptographically sound authentication mechanism for the attributes. The decryption computation was outsourced, reducing the computational load.

XII. CONCLUSION

Although IoT cybersecurity is a global topic that is rising, engineers should use a comprehensive strategy to IoT security to protect their IoT project implementations.

From the beginning of the process of creating an Internet of Things (IoT) component, security must be a top concern. Protecting the Internet of Things requires multiple layers of security, including those at the device, gateway, cloud, application, and communication levels.

REFERENCES

[1] Aqeel M., Ali F., Iqbal W. M., Rana A. T., Arif M., Auwul R. M., 2022. A Review of Security and Privacy Concerns in the Internet of Things (IoT), Hindawi Journal of Sensors, Volume 2022, Article ID 5724168

[2] Langley et al argue that IoE is an expanded and broadened version of IoT by throwing people, business and other processes into the mix. They describe IoE as 'a network of connections between smart things, people, processes, and data with real-time data/information flows between them.' See David Langley, (2021) 'The Internet of Everything: Smart Things and their Impact on Business Models' Journal of Business Research, Vol. 122, pp853 – 863.

[3] Olumide Babaloa, Internet of Things (IoT): Data Security and Privacy Concerns under the General Data Protection Regulation (GDPR), (2021), AIRCC Publishing Corporation

[4] Q. D. Ngo, H. T. Nguyen, V. H. Le, and D. H. Nguyen, "A survey of IoT malware and detection methods based on static features," ICT Express, vol. 6, no. 4, pp. 280–286, 2020

[5] M. Khalid, Mohsin Murtaza, Mostafa Habbal, Study of Security and Privacy Issues in Internet of Things, 2020, 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)

[6] M. R. Naqvi, M. W. Iqbal, S. K. Shahzad et al.,"A concurrence study on interoperability issues in IoT and decision making based model on data and services being used during interoperability," Lahore Garrison University Research Journal of Computer Science and Information Technology, vol. 4, no. 4, pp. 73–85, 2020

[7] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," Future Generation Computer Systems, vol. 108, pp. 909–920, 2020.

[8] L. A. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: challenges and solutions," Applied Sciences, vol. 10, no. 12, p. 4102, 2020

[9] N Alhalafi and Prakash Veeraraghavan, Privacy and Security Challenges and Solutions in IOT: A review, 2019, International Conference on Smart Power & Internet Energy Systems

[10] G. S. Hukkeri and R. H. Goudar, "IoT: issues, challenges, tools, security, solutions and best practices," International Journal of Pure and Applied Mathematics, vol. 120, no. 6, pp. 12099–12109, 2019

[11] Owais Ahmed, (2019) 'Internet of Things (IoT) A Review' International Journal of Research in Engineering Application & Management, Vol. 4, No. 10, p2454.

[12] K. M. Sadique, R. Rahmani, and P. Johannesson, "Towards security on Internet of Things: applications and challenges in technology," Procedia Computer Science, vol. 141, pp. 199–206, 2018.

[13] Jari Porras, et al, (2018) 'Security in the Internet of Things- A Systematic Mapping Study' Proceedings of the 51st Hawaii International Conference on System sciences.

[14] This is the integration of cloud computing and IoT. See D. Vaishnavi, (2018) 'Towards Cloud of Things from Internet of Things' International Journal of Engineering & Technology, Vol. 7 No. 4, p112-116.

[15] AlemColakovic and MesudHadzialic, (2018) 'Internet of Things (IoT). A Review of Enabling Technologies, Challenges and Open Research Issues' (2018) Computer Networks, Vol. 114, pp17-39.

[16] D. Palmer, Mirai botnet adds three new attacks to target IoT devices, May 2018, [online] Available: https://www.zdnet.com/article/miraibotnet-adds-three-new-attacks-to-target-iot-devices/.

[17] R.Vignesh and 2A.Samydurai, “Security on Internet of Things (IOT) with Challenges and Countermeasures”, 2017, IJEDR, Volume 5, Issue 1, pp417-423.

[18] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey", 2017 International Conference on I-SMAC (IoT in Social Mobile Analytics and Cloud) (I-SMAC), 2017.

[19] J. Lin, W. Yu, X. Y. Nan Zhang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture Enabling Technologies Security and Privacy and Applications", IEEE Internet of Things Journal, vol. 4, no. 5, Oct. 2017.

[20] Husamuddin Mohammed, Mohammed Qayyum, Internet of Things: A Study on Security and Privacy Threats, 2017, The 2nd International Conference on Anti-Cyber Crimes (ICACC) organized by IEEE.

[21] S. G. H. Soumyalatha, “Study of IoT: understanding IoT architecture, applications, issues and challenges,” International Journal of Advanced Networking & Applications, vol. 478, 2016.

[22] J. Clark, What is the Internet Of Things?, November 2016, [online] Available: https://www.ibm.com/blogs/internet-of-things/whatis-the-iot/.

[23] Koien M. G., Abomhara M., 2014. Security and privacy in the Internet of Things: Current status and open issues.

[24] https://www.briskinfosec.com/blogs/blogsdetail/Security-and-Privacy-in-IoT,

[25] Gwyneth Iredale; https://101blockchains.com/security-and-privacy-in-iot/