Security Issues in IoT, Cloud and their Convergence

Kota Aakash[1], Syed Muqthadar Ali[2]

[1]Graduate Student pursuing Bachelor of Technology in Computer Science Engineering, CVR College of Engineering,Ibrahimpatnam, Mangalpalli.Kota.aakash15@gmail.com

[2]Senior Assistant Professor,Department of CSE, CVR College of Engineering, Ibrahimpatnam, Mangalpalli.

Abstract

For any technology to provide an effective and secure technology as per International Standards of Organization (ISO), need to adhereto the security requirements such as Confidentiality, Integrity, Authentication, Availability and Authorization.

IoT came a long way from initial stage's and became intangible part of human life making the life of people better and comfortable. IoT is used in various fields such as agriculture, manufacturing, healthcare, smart homes, smart cities and military. IOT is mainly interconnection of physical devices such as sensors etc, technology and networking without human intervention. With the low manufacturing cost of sensors and advent of technology, IOT invaded in all parts of life. However, this generates lots of data to be processed, shared and analyzed.

Here, the cloud technology comes into picture. The cloud technology reduces stress on resources for organizations enabling storing and accessing the data, data processing etc in cloud so that more and more IoT can be brought to the consumers or end users. However, this brings a whole lot of security concerns.This review paper highlights the security concerns faced by both technologies individually and when the two technologies are converged their mitigation techniques.

Introduction

The Internet of Things is made up of various technologies, networks, and sensors. In the 1980s, students at Carnegie Mellon to avoid unnecessary trips to the vending machine decided tomodify a Coca-Cola vending machine, to track its contents remotely popularly known as an "internet coke machine,". This was the first time the idea of incorporating sensors and intelligence into physical objects was addressed. However, the technology was difficult, and there was only so much that could be done. A computer scientist named Kevin Ashton is credited with coining the phrase "Internet of Things" in 1999.

Kevin Ashton, a British technology pioneer, was one of the co-founders of MIT's Auto-ID Center. This centre created a global standard system for radio frequency identification and other sensors.The Internet of Things (IoT) is a system that connects the Internet to the physical world through sensors. A sensor is any device that collects information and delivers it to a data collection facility, such as a data warehouse, database, or log server. While working for Procter & Gamble, Ashton devised the notion of embedding radio-frequency identification (RFID) chips into products to trace their movement through a supply chain. Temperature, humidity, and dock-to-dock travel times would be reported back to the company's headquarters for further investigation. You will also be able to track the costs involvedin delivering each food

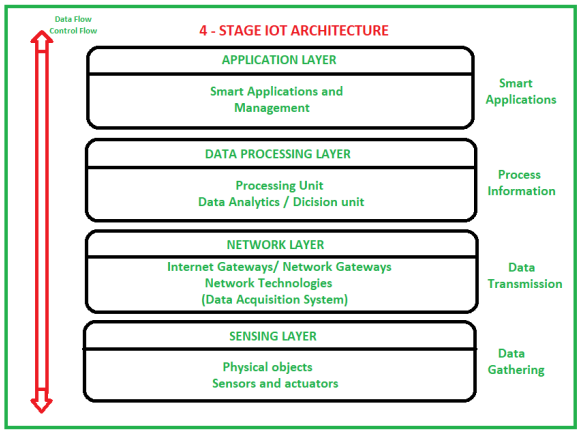
eISSN 1303-5150

product or container to the consumer with better precision.

In general, An IoT ecosystem components are web-enabled smart devices that use embedded systems such as CPUs, sensors, and communication hardware to autonomously collect, send, and act on data acquired from the surroundings in which they are located. Connecting to an Internet of Things gateway or another edge device enables IoT devices to exchange sensor data with one another. The data is then analyzedeither by uploading to the cloud or locally. These devices will occasionally talk with other linked devices and act on the information they get from one another. Individuals can interact with the devices in a variety of ways (for example, to set them up, give them instructions, or get data), but the devices do the majority of the work without human intervention.

IoT Architecture

The IoT architecture model might actually vary greatly depending on the implementation. In order to accommodate a variety of network applications, it needs to be open enough and use open protocols. In this section, we will talk about the four-layer architecture paradigm for the Internet of Things.



Sensing layer/Perception Layer: The sensing layer, also known as the perception layer, is the lowest layer in the IoT architecture and is responsible for gathering data from the physical world using a variety of tools such as actuators, sensors, RFIDs, GPS, IR, and other devices.

Network Layer : The analogue data that was collected from the sensing devices is converted into digital form at the network layer before being delivered through the distributed networks. Data acquisition systems (DAS), gateways to the Internet, and other networks are part of Network layer.

Data Processing Layer : It is obvious from the name of the layer, "Data Processing" that this layer is in charge of processing the data.After being analysed andprocessed, the data is stored so that it can be used by a variety of software programmes.

Application layer: This layer offers a platform to help end users to access the data that the Data Processing layer has processed for use in industrial, agricultural, health care, consumer, and other applications. In addition to this platform, the end users can also access the data that was processed by the data processing layer.

Internet of Things (IoT) frameworksare provided many organisations which allow smart devices to connect and communicate with one another without difficulty in a secure setting thus making it possible for smart devices to perform a wide range of data operations, including multi-dimensional analysis, transformation, and aggregation, as well as to visualise their operations in a way that is appropriate for the businessas per their requirement and budget. Several of them are listed below:

• Google's Brillo/Weave, which combines an Android-based operating system for the development of embedded low-power

eISSN 1303-5150

devices with weave, an IOT-oriented communication protocol;

• Amazon Web Services (AWS) by Amazon;

• Arm Mbed by Arm Microcontrollers;

• Microsoft Azure by Microsoft;

• Calvin by Ericsson;

Protocols in IoT

IoT devices typically connect to the internet through the IP(Internet Protocol) stack. IoT protocols are typically divided into 3 groups viz.,

Connectivity protocols: IoT objects are connected with each other and implemented on data link and physical layers of IoT stacking.
Eg: RFID, Blue tooth based, Wi-Fi based and ZigBee based.

CommunicationProtocols: used to exchange messages between IoT objects and implemented on application layer and transport layers of IoT stack.
Eg : TCP and UDP protocols and

Network Protocols: responsible for routing the packets received from transport layer.
Eg : Routing protocol (RPL)

Security threats at Different layers and their mitigation techniques

The Internet of Things (IoT) is a rapidly evolving technology that is revolutionising how individuals and organisations interact with the physical world as well as among themselves. This is being made possible by breakthroughs in low-cost and low-power sensor technology, the development of 5G services, and new technologies such as cloud computing, data analytics, machine learning, and artificial intelligence. However, there are a number of limitations in the subsystems, including cost, power, energy consumption, and lifetime. Because of the rapid development of heterogeneous devices and the combination of these devices, the Internet of Things ecosystem is vulnerable to attacks on its many technologies and future capacities. As a result, a comprehensive security framework that protects all Internet of Things assets from threats is critical to the system's effective operation.

A succinct overview of the security threats that each layer must deal with, as well as the remedies that must be implemented.

When discussing the possible hazards offered by the Internet of Things (IoT), we will always focus entirely on software vulnerabilities and internet hacking attempts, avoiding the prospect of unauthorised access to physical equipment.

Perception Layer/Hardware Layer: The perception layer deals with the physical environment and collects all data from physical world with the use of sensor nodes and other devices like Bluetooth, GPS, Zigbee, RFID tags and readers, and so on, which are fairly popular but limited to PANs (Personal Area Networks).

This layer's Internet of Things devices communicate with one another locally via non-IP networks and with the internet via smart gateways. Internet of Things devices are created in compact form with limited computing resources and minimal energy consumption and usually function in unprotected and occasionally hostile surroundings. As a result, IoT devices are extremely vulnerable, and hackers and vandals can simply exploit them to obtain

eISSN 1303-5150

access to networks. The following is a list of the most common attacks on the hardware components and protocols of IoT devices in general.

Physical damage: The IoT objects and devices can be physically damaged by an attacker, resulting in network damage. This is distinct from node tempering.

Node tempering: Node tempering is a method of cyberattack that causes damage by physically sending and receiving entire nodes or by totallydestroying the sensor node in order to obtain access to the critical information that is contained in the node and alter it. Extraction of cryptographic keys, alteration of operating system or the firmware, and the modification of circuits are some of them.

Jamming of node in Wireless sensor network (WSN): Jammers are used to obstruct any signals or communications sent between the nodes.

Malicious Node Injection: In this attack method, the attacker inserts a malicious node between two legitimate nodes in the IoT network in an effort to gain unauthorised access often known as "Man in the Middle attack". The attacker will have control over all of the data in this attack, and as a result, has control over the entire network.

Social Engineering Attack : The users of IOT system are exploited physically by the attacker to get sensitive information from them.

Malicious Code Injection: Insertion of malicious Code into a node or object of IoTtotake over control of IoT system.

Sleep deprivation attack/outage: Many Internet of Things devices operate on disposable batteries in hostile environments without an Internet connection. To prolong the battery's life, the sleep routine functions and other processes are carried out. These batteries are the target of the attackers, who either shut off their power source or significantly drain it by keeping the node active.

Tag cloning: When various devices in an Internet of Things system are given tags, the system becomes visible and vulnerable to physical attacks. The user will be unable to differentiate between the original material and copies generated by a cybercriminal by capturing these tags.

RFID RF Interference: In this type of assault, radio frequencies are used to emit a lot of noisy signals in order to interfere with radio frequency identification (RFID) transmission.

Unauthorized Access to the tags: If the RFID system does not have a strong authentication method, an attacker can access any tag without authorization and have complete access to the information stored there.

Timing attack: To improve data security and prevent unauthorised access, the Internet of Things devices are provided with encryption keys. In this kind of attack, the attacker can get the encryption key by calculating the time taken to complete the encryption procedure.

Eavesdropping Attack: Due to memory restrictions subjected to compact size of IoT devices, no encryption technique is used throughout the transmission process (i.e., from user to tag or tag to user and vice versa). Therefore, eavesdropping and accessing it allows an attacker to obtain sensitive information. In an RFID system, for example, tags and readers connect to each other wirelessly and communicate with

eISSN 1303-5150

one another without any form of human intervention; as a result, there is a chance that their communication could be eaves dropped.

Spoofing: Spoofing is an attack where a malicious tag impersonates a legitimate tag to eavesdrop in on a communication between two tags and obtain sensitive data.

Replay attacks: In replay attacks, the adversary alters or modifies the signals that are sent between users and tags in order to spoof the signals and obtain the sensitive data for later use.

Mitigation Techniques

Securing the physical design is likely to be successful in resolving the bulk of the physical layer threats. Hardware-based security, which may include a removable security element or an embedded and integrated Security element into the host system on chip, serves as a natural starting point for the implementation of IOT protocols and procedures, and provides elegant and efficient solutions to a variety of problems, such as data masking (encryption), device identification and authentication key generation, random number generation, secure storage of sensitive data, secure boot, and side channel protection. Hardware-based security is also a good starting point for implementing IOT standards and procedures.

The four most typical types of hardware-based risks are illustrated below: 1) A brute-force attack 2) Fuzzing assaults 3) Row hammer attack , and 4) Side channel attacks

Network layer

This layer functions as a mediator in the transmission of data for data management through communication protocols between the physical devices and networks. As a result, ensuring that data transport is reliable and secure is of utmost importance. The attacker does not need to be physically close to the network of IoT systems; rather, they only need to focus on the network of IoT systems.

Denial of Service: DOS stands for "Denial of Service," and it describes how the adversary assaults the network of IoT devices by transmitting a large amount of traffic data thereby, preventing the user from accessing their resources over the network.

Man in the Middle: An attack known as "Man in the Middle" occurs when an opponent intercepts the communication channel between two nodes while data is being transmitted. This allows the adversary to gain access to confidential data that is being transmitted between the nodes by managing and monitoring the network.

Attack by SelectiveForwarding: The attacker chooses which packets to be forwarded / transmitted thereby causing disruptions in the routing path. A denial-of-service (DOS) attack is also a possibility of such an assault.

Sink Hole Attack: In this kind of attack, a malicious node is inserted, showing that it is a beneficial route or a created path to persuade many nodes to divert their packets through it like a sink hole, preventing the transmission of packets rather than sending them to their destination. When combined with another assault, this attack will be extremely damaging to the network.

Sybil attack: An attack known as a Sybil attack occurs when a hostile entity attempts to use many identities within the same

eISSN 1303-5150

network. It asserts that it holds identification for a significant number of nodes. The primary objective of this assault is to circumvent the redundancy procedures used in scattered data storage.

Worm hole attack: This type of attack disrupts both the topology of the network and the traffic on it. This attack can be made by establishing a private channel in the network between the two attackers, and the relocating of bits from their original location in the network where there is a link with low to extremely low latency.

Hello floods attack: When newly connected devices join the network send broadcast packets, known as "hello" message. The attacker in this attack will pretend to be a neighbouring node and send a hello message to multiple other nodes, which will result in a jamming attack and directly cause a block in the channel of the network. This can be accomplished by a single malicious node, and it will result in the blockage of the entire network since it generates so much traffic.

Black Hole attack: The black hole attack, as its name suggests, is one that is intended to drag all data packets towards the malicious node that is advertising itself as the shortest way to the destination.

Mitigation Techniques

We can say that the network layer is vulnerable to attacks from both the inside and the outside, but these vulnerabilities can be mitigated using cryptography and IDS (intrusion detection system) techniques.

Cryptography is a very powerful and effective tool for protecting against external assaults, yet it is incapable of detecting and preventing internal attacks. This is due to the fact that cryptography is unable to identify attackers who possess legal keys but act in a malicious way. For instance, the use of cryptography in network security makes it vulnerable to attacks that target network performance, such as denial of service (DoS) assaults, as well as resource attacks, such as jamming. As a result, the use of cryptography by itself cannot guarantee the network's complete safety. It is necessary to have an intrusion detection system in order to monitor any malicious behaviour that may occur within the network and to take preventative measures against it at an early stage.

The idea behind intrusion detection systems (IDS) is to analyze all of the data collected from a network in order to look for tell-tale signals of an assault or intrusion, then either raise an alert and notify the anomaly. IDS monitors the data based on a variety of criteria, including the amount of time that passes between two consecutive messages, the frequency with which the messages are sent, the sender's identification, the length of the delay, any changes to the payload, any modified packets, any lost packets, and the amount of energy that is used.

Layer for the Processing of Data:

Within this layer, data is stored, analysed, and processed, and it is also where the majority of security assaults and threats take place. Only attacks that are somewhat common will reach this stratum.

Data loss caused by partnerships with third parties: PaaS stands for "Platform as a Service," and it refers to a type of cloud computing platform in which a third party provides the necessary software and hardware resources. When sensitive data is stolen from a third-party vendor or when their systems are exploited to access and steal sensitive information housed on your systems, this is referred to as a breach that involves a third party.

eISSN 1303-5150

Theft of data: Data from Internet of Things devices is stored remotely in data centres, where it is not under the oversight of the holders of the data. Additionally, data may be stored in a variety of data centres located in a variety of locations around the world. It is possible for data modification attacks, data loss attacks, data exposure attacks, and data leakage attacks to occur when there are no secure methods of processing, storing, or sending data.

SharedResources: Sharing resources involves the utilisation of common technologies such as virtualization and cloud orchestration. Sharing resources enables cloud providers and customers to decrease their capital investment, operational expenditure, and total cost of ownership. Therefore, attackers might inflict severe damage on a large number of users of the cloud by taking advantage of flaws in any aspect of these systems. Hackers may be able to take control of virtual machines and even the host computer if the hypervisor has vulnerabilities that they can exploit. Shared resources allow hackers to have unrestricted access to the host computer in the event that a virtual machine is able to escape their control.

Threats to the underlying infrastructure: In platform as a service, the developers do not have access to the lower layer, and the responsibility for the security of this layer lies with the service provider. This is done with the intention of preserving the integrity of an Internet of Things application.

Assaults from the inside: Legitimate cloud users having harmful thoughts on organisation have several options available to them when it comes to arranging attacks or leaking data in cloud systems. etc.

Mitigation Techniques

Some of the methods that are used for security measures at the data processing layer: web application software, encryption, fragmentation redundancy scattering (FRS) (data is divided and stored in several fragments of storage in servers), and so on. Because the fragments include no information that could be valuable, the risk of data theft is significantly reduced. Homomorphic encryption and Hyper Safe: (Hyper Safe prevents memory pages from being changed and enables the restriction of pointer indexes, which prevents monitored data from being written intopointerindexes.)

ApplicationLayer:

Attacks made using software to cause damage to the system's resources. Attacks could be based on online apps, the operating system, or the firmware.

Denial-of-Service:-As part of a denial-of-service attack, malicious code is injected into the system in order to prevent authorised users from communicating with the application layer.

Malicious Code injection: Injection of harmful code refers to the process by which an attacker inserts malicious code into a system in order to steal or manipulate data.

Phishing Attack : By hacking email , phone or social media account an attacker can access sensitive data such as login credentials and credit card information

Trojan Horses, Worms, spyware and Viruses : An attacker can compromise the system of an IoT device by inserting malicious software with a variety of different effects, such as viruses, Trojan horses, worms, and spyware.

eISSN 1303-5150

Mitigation Techniques

The most crucial aspects of this layer are the authentication and integrity checks. Encryption, access control lists (ACLs) for maintaining incoming and outgoing traffic, and monitoring access requests from a large number of users within the system are some of the countermeasures that can be taken. Other countermeasures include intrusion detection, firewalls, and antivirus software.

Cloud Introduction

Cloud computing technology dates back to the 1960s and was previously only available on mainframe systems. However, through time, it grew into what is now known as the cloud. The technology itself, is a combination of several technologies such as virtualization, clustering, and grid computing, among others, is offered at affordable rates to corporate customers, thereby reducing the maintenance expense run an internal data center. Businesses have begun to embrace cloud computing due to the multiple benefits it provides, such as cost savings, reliability, agility, the ability to rapidly deploy new technologies, elasticity, and scalability, among others. Because of the surge in popularity of 5G internet services, the adoption of cloud computing has skyrocketed.

Cloud Computing Deployment models

The following are the three primary deployment models available for use with cloud computing:

Private Cloud: private cloud is one that is managed by a single firm behind the firewall of that company's own data centre and is only accessible to that company's users or the company itself. The operating and capital costs are substantial, but it provides a higher level of data protection and control over the data.

Public Cloud:The public cloud, as its name implies, serves a vast number of persons or organisations, and the services it offers can be accessed on demand and are invoiced on a pay-per-use basis. Despite the fact that both the operational and data costs are low, this provides no data security.

Hybrid Cloud:The phrase "hybrid cloud" refers to the integration of multiple clouds that are linked together using industry-standard technologies to allow for the exchange of data and applications regardless of who owns them or where they are located. This will give participating organisations an advantage over the applications in terms of flexibility and control, while also supporting them in overcoming the constraints they currently face.

Community Cloud: As the name implies, this is for several organisations with similar interests, and each member of the community gets free access to all data and applications hosted on the cloud.

Aside from these deployment technologies, which are commonly used in line with the requirement and necessity, many more deployment methods are developed for a range of uses by a variety of clients. Businesses in the present era are both dynamic and complex, and as a result, enterprises must be capable of dealing with spikey workloads, various apps, and more data in order to interact with consumers, partners, and companies that collaborate. Because corporations must find a balance between flexibility, agility, security, innovation, and speed, which is not possible with a single type of cloud deployment, organisations are choosing to deploy several clouds or hybrid cloud solutions. A virtual

eISSN 1303-5150

private cloud, sometimes known as a VPN, is one example of this. Because virtual private networks (VPNs) connect multiple resources, the public cloud can be used in a private setting.

Cloud Computing Service Delivery Models

Software as a Service (SaaS): SaaS is also known as "on-demand software," and it is the top layer of the service model network that allows end users to access the services that are made available to them by cloud service providers without having to install any software on their own devices. SaaS is also known as "Software as a Service." SaaS raises new security concerns, including a vulnerability to new malware and phishing attacks, in addition to the potential exposure of client data. These concerns are in addition to the fact that SaaS offers many advantages, such as being cost-effective, one-to-many (an application that is shared by many users), having fewer software and hardware requirements, etc.

Platform asa Service: Platform as a Service or PaaS, is the name given to the intermediate layer of a service-model network. This layer comprises anything from an operating system and a database management system to a programming environment and more. In a nutshell, it is a comprehensive development and deployment environment that is hosted in the cloud and comes with resources that allow you to deliver everything from straightforward cloud-based applications to complex enterprise software that is enabled by cloud computing.

PaaS operates on a pay-as-youuse basis while simultaneously lowering associated costs for resources. The customer and the cloud service provider each bear some degree of responsibility for the cloud's level of security. The PaaS customer is responsible for ensuring the safety of the platform's software, records, and user access. The PaaS provider is responsible for the protection of both the operating system and the physical infrastructure.

IaaSor infrastructure as a service: IaaS refers to the innermost or bottom layer of the service model network. This is where cloud providers provide bare infrastructure on demand, such as storage, networks, processing power, and an operating system. The client can deploy any operating system or software according to his requirements and pay only for the resources they are using without worrying about the infrastructure underneath. In its most basic form, we can say that IaaS is based on virtualization technology.

The cloud technology, while beneficial to the expansion of businesses thanks to the many services it offers, has also given rise to a great number of security concerns. These concerns include security threats and attacks, which are catastrophes for both service providers and service consumers and which need to be addressed in the appropriate manner. Because of the vast size involved as well as the fact that the resources owned by cloud providers are completely diverse, distributed, and virtualized. Traditional security techniques, such as identity, authorization, and authentication, are no longer sufficient for protecting cloud computing environments as they currently exist. The migration of mission-critical applications and sensitive data to environments hosted in the cloud presents a significant challenge for businesses that are expanding beyond the data centre networks they have under their control. A provider of cloud solutions is required to accommodate and ensure that all of their customers use the same level of

eISSN 1303-5150

security and privacy controls over their applications and services, as well as meet their security-level agreements and demonstrate compliance to auditors. In addition, these customers are required to comply with the requirements of the provider.

Cloud computing has a number of advantages over more conventional means of computing, but there are also a number of risks that users face that prevent them from taking advantage of these advantages. The generally recognised dangers and attacks are mentioned below, along with the preventative measures that can be taken and the types of services that come under attack.

Cloud Computing and Its Potential Security Risks

So, what exactly is a threat? Vulnerability can be purposely exploited, or it might be exploited unintentionally. A threat is something that can gain access to, hurt, or remove an asset by exploiting a vulnerability. Threats can come in the form of anything, including natural calamities like floods, storms, and tornadoes; an employee inadvertently accessing erroneous information; spyware, virus, and adware companies; or the actions of an employee who is acting maliciously. There are many potential breaches of security, but the following list only includes ones that have been mostly acknowledged and unanimously agreed upon.

Loss of Data: The data for a cloud computing network is kept in several separate data centres that are in various parts of the world. Data security can be breached in a variety of ways, including by alteration and deletion of the data, as well as by natural disasters like floods and fires.

Data breaches: Data breaches occur when suitable authentication and permission procedures are lacking, which can result in the disclosure of sensitive information to those who are not authorised to view it. This can happen when there is a lack of appropriate authentication and authorization techniques.

Hijacking of an account or service: If an attacker is able to acquire access to login credentials, he can change the data (create, change, and delete) to his own advantage. It is possible to achieve this goal by using the credentials to set up fictitious accounts or services.

APIs, orapplication programming interfaces, that are not encrypted: Interfaces for application programming are what connect customers of cloud services to the suppliers of cloud services. APIs are standards and protocols, and if they are not adequately secured, they can lead to unauthorised access to networks, limited monitoring and logging capabilities, and other difficulties.

Insufficient due diligence: This can occur When corporations rush into employing services provided by delivery service providers without having appropriate information about the cloud models and the activities that are related to them, this is an example of inadequate due diligence. (A lack of comprehension regarding the way in whichthe system functions.)

Misusing cloud services: It also known as "abusing cloud services," is characterised by unethical and possibly illegal behaviour on the part of the consumer. As a result of low-cost infrastructure, abundant resources, and relaxed registration requirements, spammers, criminals, and other undesirable users now have a far easier time maintaining their anonymity online. Because of this, they

eISSN 1303-5150

were able to accomplish their mission of attacking the system.

Shared Technology Issues: In a framework with multiple tenants, issues can arise due to the usage of shared technology (a widely used architecture to create SAAS applications). Virtualized hypervisors have security vulnerabilities, making it possible for malicious users to acquire unauthorised access to and control over legitimate user virtual machines.

In addition to these threats, there are otherless severe threats, such as the loss of governance, the acquisition of a cloud provider, the failure of isolation, data segregation, compromised servers, and regulatory compliance, among others.

Mitigation Techniques

Regular backups, protecting data while it's in transit, data monitoring, encryption techniques, proper authentication and authorization techniques, security audits, a proper understanding of security policies and service level agreements (SLA), and the implementation of robust application programming interfaces (API) are some of the ways that these security threats can be mitigated to some extent.

Security Attacks in Cloud Computing

The use of cloud computing leaves businesses and individuals open to security risks.
Attack, we mean an un authorised activity that was carried out on a system intentionally. Depending on the manner in which the system resources are being influenced, attacks are classified into active attack or passive attack. Listed below are some of the more noteworthy assaults that have taken place:

Injection attacks utilising the Structured Query Language (SQL):The attacker inserting malicious code into the standard SQL code in order to gain unauthorised access to a database and obtain sensitive information about the user. Injection attacks can be prevented by enforcing strong passwords and encrypting sensitive data. The SQL server is able to access the data that the hackers have uploaded to the website, and it handles this data as though it belongs to the users. This makes it possible for the attacker to gain a deeper understanding of the operation of the website and, therefore, to make changes to the website.

Cross-Site Scripting Attacks: It is also known as XSS Attacks, take place when an adversary injects malicious code into a user's web page with the intention of diverting the user to the adversary's website in order to access sensitive data. It can be done in two ways reflected XSS(immediately reflects back malicious code to the user and hence does not store it permanently)., or stored XSS, which permanently saves malicious code into a resource held by the web application.

Phishing Attacks: An attacker conducting a phishing attack will use a cloud service to modify a web link to divert the user's attention to a false link. Because of this, the attacker has the ability to take over the user's account and gain access to sensitive information.

Domain Name Server (DNS) : When a user tries to visit a server by calling its domain name, but instead of being routed to the domain he requested, he is forwarded to some other malicious code, an attack against

eISSN 1303-5150

a domain name server (DNS) occurs. This takes place in the event of a DNS attack, in which the attacker makes use of DNS to convert the user's domain name into an IP address in order to acquire access to the user's private data.

Attacks Conducted by a Man Positioned in the Middle (MITM): An attack is said to be (MITM) when an adversary makes an attempt to intervene in an ongoing discussion with the purpose of injecting false information in order to get access to sensitive information that is being shared.

DOS Attacks: A denial-of-service assault (also known as a DOS attack) makes a network or machine inaccessible to users by repeatedly sending data packets to the servers that are the target of the attack. Because these data packets are delivered without changing the nodes, data pockets, or decrypting encrypted data, they occupy the bandwidth of the network and take up the resources of the target servers.

Distributed denial of service (DDOS) attack:The server that is being targeted is bombarded with many packets coming from multiple networks that have been compromised in the past. As a result, the target server is unable to process the requests that are being delivered to it. The amount of traffic generated is greater than DOS attack

Reused IP address Attack : This attacks make use of IP addresses that have been used in the past .When a person connects to a network for the first time, that user is given a unique IP address that is assigned to each node of the network. When a user logs off of a network, the IP address that was previously associated with that user is made available to be used by a different user. It is possible for the new user to access the data of the previous user since the address remains retained in DNS caches.

Zombie Attack: An attack known as a "zombie attack" takes place when the virtual machines (VMs) belonging to a victim are inundated with a large number of requests sent from other VMs on the network in a relatively short amount of time. This type of attack can result in a denial of service (DOS) or a distributed denial of service (DDOS).

Sniffer attacks: Sniffer attacks are when an attacker launches a series of programmes that let a host collect flowing packets in an Ethernet network by putting the host's network interface card (NIC) into malicious code.

Wrapping Attack: When a user makes a request for a virtual machine (VM) through a web server, the server will generate a SOAP message that will contain information that is based on XML. This message will then be transmitted between the browser and the server. The XML-based information is digitally signed with signature values before the user and the server engage in any kind of communication with one another. The adversary will first make a copy of the SOAP message as it is being translated, and then they will send the copied message to the server while pretending to be a legitimate user. The attacker will be able to gain access to the cloud service and execute malicious code because ofthis.

Cookie poisoning: When the information contained within cookies is changed in such a way that it no longer carries the sensitive credential information related to the user's data, this type of attack is referred to as "cookie poisoning." A hacker could exploit this vulnerability to gain access to the user's data.

eISSN 1303-5150

CAPTCHA breaking attacks: It is common practise to put individuals through the CAPTCHA test in order to differentiate human beings from computers (and harmful programmes) on the internet.

Google Hacking Attacks: The Google search engine is used in Google Hacking Attacks often referred to as Google Dorking tests, in order to identify security flaws in the configuration settings. This enables the hacker to obtain knowledge about the target that they aim to attack .

HypervisorAttacks:The hypervisor allows server virtualization by logically assigning and separating the server's physical resourcesmaking it possible for multiple operating systems to run simultaneously on a single piece of hardware, and hence also known as the "Virtual Machine Manager" (VMM). It enables a guest operating system to operate as though it is the only one in charge of hardware while it is running on a virtual machine, without the guest operating system being aware that other guests are sharing the hardware with it. "Hypervisor attack" is the term used to describe what happens when a guest operating system executes malicious code on the host system. The objective of this assault is to seize complete control of the host system and block access to any other guest operating systems that could be present.

Mitigation Techniques

Using the appropriate mitigation techniques, such as avoiding the incorporation of dynamically generated SQL into the code, sanitizing and validating the code, employing active content filtration and content-based data leakage prevention technology, ensuring that the Secure Sockets Layer (SSL) configuration is accurate, utilising anti-malware software, ensuring that the DNS security measures are accurate, employing appropriate Intruder Detection Systems (IDS), and Sniffer detection techniques , encryption methods, implementation of backup policies to avoid issues with data recovery using secure hypervisor with proper monitoring and VM isolation.

Security Threats towards convergence of Cloud and IoT: Internet of Things devices produce an enormous volume of data, which then needs to be processed and analysed before a conclusion can be reached on anything. The term "cloud" refers to a server that is housed in a central location and is responsible for storing a variety of computer resourcesto be accessed whenever is required. The Internet of Things generate vast amounts of data, which need to be transported across the internet in a timely and pleasant manner. Cloud computing offers a path that meets these requirements.

Prior to the development of the technology known as "cloud computing," the bulk organization's data was kept on its own private servers locally. Because of this, a considerable amount of the company's resources had to be allocated toward storage and maintenance, which reduced the possibility that the technology might be expanded to include additional users and nodes. Since the introduction of cloud computing, there has been a discernible reduction in the level of stress that is being placed on the resources that are now accessible. Not only does cloud technology make it possible to store and access data, applications, and services through the internet, but it also offers a number of benefits that are not available with the more conventional approach to managing a company's affairs. Scalability, dependability, and accessibility are just a few of the benefits that can be cited in this context.

eISSN 1303-5150

Despite the fact that this is the case, a new model that has been given the name "IoT Cloud" has been developed as a result of the convergence of Internet of Things technology and cloud computing. This model possesses a number of additional qualities, such as the capability to react quickly, to be ubiquitous, and to adapt. IoT developers are able to remotely perform tasks on IoT devices. Some examples of these tasks include analysing the current status of their assets, reviewing the specifications of those assets, configuring and reconfiguring those assets, commanding and updating those assets, and extracting any kind of statistics, values, or settings.

Because of the vast number and variety of devices that are being monitored and managed, cloud security configurations take on an even more significant level of importance when it comes to the Internet of Things (IoT). Assaults on devices that are connected to the internet of things have the potential to open the door to stepping stone attacks and enable access to network or cloud resources, as well as the other way around. Inadequate security on the level of Internet of Things devices or the IOT gateways has the potential to cause insecure connectivity and dataflow towards the cloud, which has repercussions for the overall security of the ecosystem. Inadequate security on the level of IoT gateways also has the potential to cause insecure connectivity and dataflow towards the cloud.

Connecting: The Internet of Things (IoT) must handle a wide array of scopes, hardware, operating systems, and network communication protocols. This is necessary since IoT applications span from smart homes to smart industries. The Internet of Things can be characterised by its ability to connect to and communicate with a wide variety of distinct devices and components in order to make it easier for businesses to make a profit. Implementation of an appropriate communication protocol should be considered one of the most crucial things to do in order to achieve this objective. A communication protocol is a set of rules that explains how two or more components of a system are expected to interact with one another. The protocol may also describe how the components of the system may interact with other systems.

Confidentiality : An increase in the number of connections and nodes inside an Internet of Things network that has been badly constructed increases the risk that the network may be hacked, which can be detrimental to users' privacy. For instance, if a healthcare system is adequately structured, it will be simpler for patients and medical personnel to monitor their health conditions and make significant decisions in the face of an emergency situation. However, if it were to fall into the hands of businesses that are primarily concerned with commerce, such as insurance companies, it may create a big risk. This is because businesses like these typically deal with financial transactions. In a similar vein, smart agriculture, when correctly implemented, will be beneficial to farmers. On the other hand, if it were to slip into the hands of groups with a commercial goal, such as producers of fertilisers and pesticides, it would pose a significant risk.. Hence, the system of the Internet of Things needs to be robust enough to adjust to any environment.

Integrity: The Internet of Things produces enormous quantities of data each and every single second. Loss of data and breaches in data security are the primary sources of concern, and they can be brought about either by natural disasters (such as floods, earthquakes, and fires) or by the corporatization of data. To ensure that no data is ever lost, cloud service providers are

eISSN 1303-5150

mandated to maintain several copies of the data at all times and store these copies in many locations.

Interoperability: When the Internet of Things (IoT) was merged with cloud technology, it provided a gateway for numerous technologies in various areas, making people's lives better and easier. However, it also resulted in a significant increase in the number of potential security risks, all of which to be addressed before normal operations need can be resumed. Interoperability refers to the capacity of different technologies to collaborate effectively. In order to find a workable solution to the issue of interoperability, cloud service providers, also known as CSPs, have multiple avenues open to them to work together and form alliances. The following are the ones that stand out as the most important among them:

Federated Clouds: When cloud service providers (CSPs) come to an agreement with one another and establish a trust boundary, this results in the formation of federated clouds. Federated clouds make it possible to scale resources and create backups in the event of an emergency.

Hybrid Clouds : The bridging of trust barriers among CSPs in hybrid clouds makes it possible for applications to select resources and services from a range of clouds all at the same time. This is made possible by the hybrid cloud's architecture.

Conclusion

In this paper, we evaluate and assess the security features of the Internet of Things (IoT) and cloud computing, as well as the security challenges that arise when these two technologies are combined, as well as some possible mitigation strategies. When all of the challenges are considered, the Internet of Things (IoT) and cloud computing both have different advantages and can be viewed as potential pathways for the future of information and communication technology. Information processing for Internet of Things applications must take place in the cloud. IoT features and services can be added to the cloud, or cloud services can be integrated into IoT offerings. These are the two key intersections of the two main domains.

However, as the number of Internet of Things devices grows, so does the volume of data generated by these devices; as a result, relying on any central organisation, such as cloud computing, becomes impractical. Traditional cloud computing is incapable of resolving difficulties in the Internet of Things that are crucial for making vital judgments in industries such as telemedicine, health centres, vehicle-to-vehicle communication, and security departments, to name a few. These issues include time sensitivity and connectivity. Two newly created technologies have entered the picture, each of which is capable of delivering the benefits of cloud computing while also adapting to the specific needs of IoT devices. Computing at the edge and computing in the fog are two distinct concepts.

REFERENCES

[1] N. Amara, H. Zhiqui, and A. Ali, “Cloud Computing Security Threats and Attacks with Their Mitigation Techniques,” in *Proceedings - 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2017*, Jul. 2017, vol. 2018-January, pp. 244–251. doi: 10.1109/CyberC.2017.37.

[2] K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security

eISSN 1303-5150

issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1–13, 2013, doi: 10.1186/1869-0238-4-5.

[3] Sri Shakthi Institute of Engineering and Technology, Institute of Electrical and Electronics Engineers. Madras Section, All-India Council for Technical Education, and Institute of Electrical and Electronics Engineers, *2020 International Conference on Computer Communication and Informatics : January 22-24, 2020, Coimbatore, India*.

[4] H. Akram Abdul-Ghani, D. Konstantas, and M. Mahyoub, "A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model," 2018. [Online]. Available: www.ijacsa.thesai.org

[5] A. Wahab Ahmed, M. Muhammad Ahmed, O. Ahmad Khan, and M. Ali Shah, "A Comprehensive Analysis on the Security Threats and their Countermeasures of IoT," 2017. [Online]. Available: www.ijacsa.thesai.org

[6] B. Shukla *et al.*, *2017 6th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions) : September 20-22, 2017, venue, Amity University Uttar Pradesh, Noida, India*.

[7] Institute of Electrical and Electronics Engineers, Association for Computing Machinery, Calif. IEEE/ACM International Conference on Computer-Aided Design 2014.11.02-06 San Jose, and Calif. ICCAD 2014.11.02-06 San Jose, *IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2014 2-6 Nov. 2014, San Jose, CA*. IEEE, 2014.

[8] F. van den Abeele, J. Hoebeke, I. Moerman, and P. Demeester, "Integration of Heterogeneous Devices and Communication Models via the Cloud in the Constrained Internet of Things," *Int J Distrib Sens Netw*, vol. 2015, 2015, doi: 10.1155/2015/683425.

[9] S. Rashmi, S. Roopashree, and V. Sathiyamoorthi, "Challenges for convergence of cloud and IoT in applications and edge computing," in *Challenges and Opportunities for the Convergence of IoT, Big Data, and Cloud Computing*, IGI Global, 2021, pp. 17–36. doi: 10.4018/978-1-7998-3111-2.ch002.

eISSN 1303-5150