

A project report on

SECURING CLOUD SERVICES IN IoT

Submitted in partial fulfillment for the award of the course

CSE4072 - SECURITY AND PRIVACY IN CYBER PHYSICAL SYSTEMS

by

PRANAV RAJ (19BPS1041)

HANUMAN SAI (19BPS1066)

LAKSHMI MEGHANA (19BPS1068)



SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

July, 2022

DECLARATION

We hereby declare that the thesis entitled “**SECURING CLOUD SERVICES IN IoT**” submitted by us, for the award of the degree of Bachelor of Technology in Computer Science and Engineering, Vellore Institute of Technology, Chennai is a record of bonafide work carried out by us under the supervision of **Dr.Renjith P N**


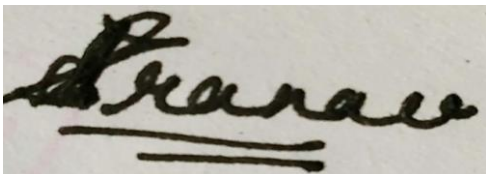
We further declare that the work reported in this thesis has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Place: Chennai

Date: 31st July 2022

Signature of the Candidate

Hanuman Sai. M

A handwritten signature in cursive script, appearing to read "Jleghana", written on a light-colored background.A handwritten signature in cursive script, appearing to read "Dr. Renjith P N", written on a light-colored background.



School of Computer Science and Engineering

CERTIFICATE

This is to certify that the report entitled “**SECURING CLOUD SERVICES USING IoT**” is prepared and submitted by **PRANAV RAJ(19BPS1041),HANUMAN SAI(19BPS1066),LAKSHMI MEGHANA (19BPS1068)** to Vellore Institute of Technology, Chennai, in partial fulfillment of the requirement for the award of the degree of **B.Tech. CSE** programme is a bonafide record carried out under my guidance. The project fulfills the requirements as per the regulations of this University and in my opinion meets the necessary standards for submission. The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma and the same is certified.

Signature of the Guide:

Name: Dr.Renjith P N

Date:

Approved by HOD,CSE cps

Name: Dr. Maheswari R

Date:

(Seal of SCOPE)

ABSTRACT

Connecting various agile thousands of devices over the internet and involving millions of data points, hence all of them need to be secured. Due to its large expanded attack surface, the security and privacy of IoT are noticed as major problems. Attackers might gain access to the network by attacking weakly linked configured IoT devices. Because IoT devices are very closely connected to each other, all a hacker does is targeting one vulnerability for manipulating all the data, making it unusable. Cloud computing and services models and also sheds light on various threats occurring in the cloud computing environment and also highlights the major security issues in different computing services and also lists security metrics that may help customers of the cloud in deciding the security they will have for their data and applications.

ACKNOWLEDGEMENT

It is our pleasure to express with deep sense of gratitude to DR.Renjith P N, Assistant professor senior Grade 2, SCOPE, Vellore Institute of Technology, Chennai, for his constant guidance, continual encouragement, understanding; more than all, he taught us patience in our endeavor. Our association with him is not confined to academics only, but it is a great opportunity on our part of work with an intellectual and expert in the field of cyber physical systems..

In a jubilant mood we express ingeniously our whole-hearted thanks to Dr. Maheswari R, Head of the Department. Computer Science and Engineering, SCOPE, Vellore Institute of Technology, Chennai for her valuable support and encouragement to take up and complete the thesis.

Special mention to Dean, Dr. Ganesan R, Dean, SCOPE, Vellore Institute of Technology, Chennai for spending his valuable time and efforts in sharing their knowledge and for helping us in every aspect.

All teaching staff and members working as limbs of our university prompted the acquirement of the requisite knowledge to finalize our course study successfully. We would like to thank our parents for their support.

It is indeed a pleasure to thank our friends who encouraged us to take up and complete this task. At last but not least, we express our gratitude to all those who have helped us directly or indirectly toward the successful completion of this project.

Place: Chennai

Date:31st july 2022

Pranav Raj,HanumanSai,Lakshmi Meghana

CONTENTS

INTRODUCTION	10
INTERNET OF THINGS	13
DEFINITION OF IoT	13
CLOUD ESSENTIAL CHARACTERISTICS	14
CLOUD SERVICE MODELS	14
CLOUD DEPLOYMENT MODELS	16
IoT NETWORKING OVERVIEW	16
CISCO PACKET TRACER OVERVIEW	17
CISCO PACKET TRACER IoT TECHNOLOGY INTRODUCTION	18
ARCHITECTURE	20
METHODOLOGY	21
SOFTWARE USED	25
LITERATURE SURVEY	26
RESEARCH QUESTIONS	38
CONCLUSION	39
REFERENCES	46

LIST OF ACRONYMS

IoT	Internet of Things
CSP	Cloud Service Provider
WAP	Wireless Access Point
CPS	Cyber Physical Systems

Introduction

The Internet of Things and the Internet of Everything are two words that commonly refer to each other. The new trend is to have small, cheap and always connected devices used to send data to backend cloud applications. This opens up new possibilities and products that companies develop and sell in both industrial and consumer markets.

The aim of this thesis was to create practical cases where students could try, through an IoT simulator, various components based on IoT sensors, network environments where all devices are connected, and backend intelligence where logic and sensor-based data can be collected and analyzed.

The tool selected for the simulations is Cisco Packet Tracer. The main advantage of the tool is the menu of various network components that simulate a real network, the device would then be connected and configured to create a network. In the latest version Cisco introduced IoT capabilities and now it is possible to add smart devices, components, sensors, actuators and also devices that simulate microcontrollers like Arduino or Raspberry Pi to the network. All IoT devices can be run on standard programs or customized by programming with Java, Python or Blockly. This makes Cisco Packet Tracer the ideal tool for creating hands-on IoT simulations.

The aim of this study was to focus on the preparation of four different predefined Cisco packet Tracer scenarios that would help students quickly understand IoT features Tools.

The need for a pre-configured exercise comes from the fact that there were only two classes intended for practical IoT simulations within the study course. These exercises provide a solid foundation for students to extend the simulations as closely as possible to their own business case developed in the previous part of the study. Four simulation environments provide a fully functional network using different Cisco components such as: router, wireless router, switch, cloud internet connection and backend IoT servers. In addition, there are examples of smart IoT in all four simulation devices that are already connected to the local network. Backend logic is also available and programming of these sensors has been created to provide examples to students how to set up more and more complex cases.

For more advanced users and to create more realistic Cisco Packet Tracer cases

it also offers the possibility of lower-leverage IoT simulation using a microcontroller, sensors and actuators. These scenarios do not use the smart devices they are always connected to IoT network, but they replicate the cases where Arduino or Raspberry Pi microcontrollers including cabling and tailor-made programs.

In each of the four simulations, there is one example use case between the sensor and the actuator basic block programming of microcontrollers. The methodology used in the diploma thesis is similar to that used in ordinary business project: demand, development, delivery, feedback and closure.

The starting point of the diploma thesis was the interview and collection of requirements from course instructor on IoT course needs and content. Although the need for practical exercises was clear, the tool, methodology and structure of the simulation were open degree, especially since the IoT course was never part of the degree program before. Other constraints that were kept in mind at the planning stage were be able to structure exercises so that students encounter different skills group to balance networking and programming knowledge. Another limitation that During the interviews, it emerged that the practice blocks were limited to two sessions computer class. The need to have prepackaged simulations was clear. Once the demand part of the project was clarified, the next part was the development an exercise with the Cisco Packet Tracer tool.

The Cisco Packet Tracer tutorial was not fully available or even available, especially for the IoT section. In order to gain initial knowledge of the tool and develop by their creation of simulations, part of the work was to monitor three online Cisco NetAcad courses: Introduction to IoT, Packet Tracer 101 (2016) and Packet Tracer 101 (2017).

These three courses helped to gain a solid overview of the IoT tool and its possibilities it. Another key activity in the development of the thesis was the preparation and documentation of simulations, their construction began by creating specifications and setting up basic networks and then adding smart IoT devices, creating backend intelligence and then adding small microcontroller examples.

Four IoT cases simulate Smart-Homes, in two variants, Smart-Campus and Smart-Industrial. The network layers were created using a combination between a router and a wireless connection routers, switches, backbone connections, 3G antennas and cloud internet connections.

Smart-Home pods simulate a home automation experience where smart IoT devices are connected to a local network to provide automation in the home. Examples of home automations include climate control, alarms and security

events, electricity storage and smart lights.

Smart-Campus simulates a university campus with different network zones where electricity is generated and used by smart devices and security sensors. Smart building access control is also implemented

Smart-Industrial is a power plant simulation that generates and stores electricity through solar panels and wind turbines. So all electricity is produced by smart devices stored and used to power a production chain filled with intelligent sensors and actuators. IoT security features are also introduced in the simulations.

Another basic part of the work was the execution of exercises and performances simulation for students of the Metropolia Internet of Things course. Two sessions were arranged to first briefly introduce the student to the instrument and its abilities, in addition, students were also provided with a small networking exercise to try setting up a basic meshed network using basic components such as: router, switch and simulated PC.

Internet of Things (IoT)

This chapter briefly introduces the Internet of Things (IoT) concept and describes the basic cloud concept, its definition, different types of implementations, and aspects of the IoT network.

Later in this chapter, we will also briefly introduce the Cisco PacketTracer.

Definition of IoT

An industry-wide definition of cloud computing was published by the US National Institute of Standards and Technology (NIST) in 2009, with a revised version published in September 2011:

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, server, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model consists of five basic characteristics, three service models and four deployment models.”

In other words, it defines that access and provision of computing resources should be easy and possible from anywhere. Resources should be scalable, organized in groups, and can be allocated based on requirements with minimal management effort.

The basic characteristics of the Internet of Things according to the definitions are: self-service on demand, wide network access, pooling of resources, rapid elasticity and measurable services.

The three service models are: IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and SaaS (Software as a Service).

The four deployment models are public cloud, community cloud, private cloud, and hybrid cloud.

Cloud Essential Characteristics

The on-demand nature gives cloud users the freedom to provision cloud IT resources independently without human intervention. Deployment is primarily through a self-service portal that allows users to choose computing power, storage capacity, network connectivity, optional software, and more. This property enables the main concepts of "service-based content" and "consumption-driven content". Cloud environment. ..

Broad Access defines that users with heterogeneous access devices need to have most access to cloud services. In fact, users need to be able to connect to services using different types of device devices (PCs, tablets, mobiles), transport protocols, and security technologies. A broad approach allows the service to meet your requirements and requires an additional application programming interface (API).

Resource pooling and multi-tenancy means dynamically allocating IT resources to meet customer needs. Resource allocation should be completely transparent to the end user and independent of where the cloud service is hosted. Resource pooling primarily uses virtualization technology to enable cloud providers to serve multiple customers on the same infrastructure. This is called multi-tenancy. Different tenants have separate resources that allow them to dynamically reserve and release IT resources without being aware of each other's existence.

Rapid resilience is a feature of cloud services that automatically and transparently allocates IT resources to meet the needs of cloud users. The user has the illusion of endless resources. Scaling is typically done using probes and scaling agents that can detect needs and instantly allocate more IT resources such as network, memory, storage, compute, and VMs. This feature is the main reason why cloud services themselves exist.

Cloud Service Models

A Cloud Service Pattern, also known as a Cloud Delivery Pattern, is a collection of pre-packaged combinations of computing resources provided by cloud service providers. These models are specialized according to the needs of the user and

provide a certain degree of freedom of configuration. Three models are included in the NIST cloud definition: IaaS, PaaS, and SaaS.

Infrastructure as a Service, or IaaS, is a cloud model in which a provider provides users with a self-contained computing environment that users can maintain and manage through management tools accessible through the cloud service portal. This computing environment generally refers to hardware, processing capabilities, storage, networking, virtualized servers, operating systems, and more. Unlike other service models, responsibility for managing cloud services rests with cloud consumers. Vendors may offer a set of pre-configured virtual servers to facilitate consumer management operations in the cloud. Cloud providers can also offer IaaS to other cloud providers, who will then build their own services on top of this cloud infrastructure. The advantage of this delivery model is that the customer has full control over the infrastructure; The downside is that customers will need internal IT resources to manage the cloud infrastructure.

Platform as a Service or PaaS generally refers to an "off-the-shelf" platform on which cloud customers can begin developing their own applications. In this delivery model, all IT resources must be deployed, fully configured and "out of the box". The platform also comes with a comprehensive set of application development tools (for example, Google App Engine provides Java and Python-based environments) to track the entire application development lifecycle.

This model typically simplifies the IT management tasks of cloud customers because the underlying infrastructure cannot be managed, however, cloud customers have control over application deployment and installation. configure computer resources to host applications

SaaS, or software as a service model, generally refers to a completely off-the-shelf, pre-packaged environment that cloud customers can use through cloud services. This solution gives customers access to a really quick and simple setup service, and allows the cloud provider to reuse the same cloud product for multiple customers. Cloud users in this model do not have administrative access and control over computing resources, can only make minimal installation changes to the software itself.

Multiplex technologies are used to spread the load across multiple resources, making SaaS a trusted and distributed service. SaaS can be both a "paid" service and a "free" service for users. In the second model, the provider will obtain revenue from commercial advertising or the resale of statistical information about service users.

Over the past year, a large number of more specialized service models have been introduced, mainly focusing on specific services. Examples: Storage as a service, Database as a service, Security as a service, Processing as a service, Testing as a service, Integration as a service, etc. In addition, a combination of cloud delivery models can also be offered to customers. , such as IaaS in addition to PaaS can provide cloud users with SDK software that also provides a high level of resource management compared to a PaaS-only scenario.

Cloud Deployment Models

The deployment model is the basis of the NIST definition and describes the owner, scale, and who has access to cloud infrastructure. The definition includes four models: private cloud, public cloud, community cloud, and hybrid cloud.

A private cloud is an infrastructure owned and accessed by a single organization. The cloud itself can be hosted on both local and third-party equipment. Private businesses can use a private cloud to centralize their IT environment or extend on-premises services in a cloud solution managed by a third party. In this scenario, the cloud consumer is also the cloud provider, and the in-house IT department can assume the specific provider role. IT resources can also be considered cloud resources if they are available remotely. Private clouds have a large amount of physical space and usually require a capital investment.

Public Cloud is a public cloud environment owned and hosted by a third party company acting as a cloud service provider. It is generally available to the general public and is probably free. Because data is hosted “off-the-shelf” and the service is made available to a wide audience, security issues arise in the public cloud and potentially accessible via untrusted networks.

The community cloud deployment model is similar in concept to the public cloud, but access is restricted to a specific set of organizations with common requirements. The infrastructure may be owned by third parties or owned by community members. Access to parties outside the community is generally prohibited.

Hybrid cloud is the latest deployment model defined by NIST and usually represents a combination of different deployment models.

IoT Networking Overview

Specifically for IoT, the most common types of networks range from Bluetooth to traditional wireless local area networks (WLANs), cellular networks, and next-generation low-power networks (LPWAN). There is currently no network standard in the IoT industry, however, few technologies have a clear advantage over others.

WLAN and Bluetooth technologies are by far the most common type of consumer network on the market today. Both operate in the unlicensed radio frequency range, both offer good transfer rates, and both require relatively inexpensive receivers. The drawback, however, is that they have obvious scale limitations that make them unlikely to be the primary choice for use in large-scale IoT applications. The range is really limited to a few tens of meters in the WLAN and a few meters for the Bluetooth connection.

Since industrial IoT applications aim to work primarily with devices distributed over a wide area, there is often poor cellular network coverage and this will require severe power management. Strictly to extend battery life, Low Power Wide Area Network (LPWAN) technology is evolving in IoT.

LPWAN is a network that combines technologies to achieve low-speed, robust, long-range communications with battery-powered sensors that are geo-located over a wide area. The three most important LPWAN technologies are LoRaWAN, SigFox, and Narrowband IoT.

Cisco Packet Tracer Overview

Cisco Packet Tracer is a Cisco proprietary cross-platform tool that allows students to create networks and simulate IoT without the need for pre-existing hardware or networks.

This tool is free, works on major operating systems, and can be downloaded from the Cisco NetAcad site for all students and teachers with a valid NetAcad account.

This tool has been made available to all students taking Cisco courses over the years and was originally designed to assist with hands-on exercises for students attending Certified courses. of the Cisco Network Associated (CCNA). At the time

of this writing, the latest version available is 7.1.

In fact, this tool provides a complete set of hardware and cabling that allows students to configure a basic network into a very complex one, allowing them to learn how to program Cisco devices via command line interface (CLI). It also teaches how to troubleshoot network related problems as the tool also includes practical debugging features.

Starting with version 7.0, Cisco has also included IoT features in the tool, allowing students to practice configuring IoT devices and IoT automation. The same version also provides low-level IoT simulation using a tablet computer (SBC) and a sensor.

Cisco Packet Tracer IoT Technology Introduction

This chapter mainly focuses on IoT tool functions and provides only a brief overview of network components. The focus of the course is IoT, not networking, so all four IoT simulations have a pre-configured network that allows IoT students to focus more on IoT aspects.

In all four IoT simulations, network devices are the backbone of connecting IoT devices, allowing them to interact with each other.

Each simulation has a dedicated grid layout, but the basic components are similar across examples. True wireless routers, switches, and routers are often used to form the basis of a network.

In the image below, which can be viewed as an example of the different routers offered by Cisco Packet Tracer, the main difference to consider when placing the device in the simulation are hardware limitations. may be included with the device in terms of the number of available ports, the ability to change the network interface, the number of expansion slots, etc. A complete list of switches, servers, PCs and laptops is also available in tool.



Figure - List of routers in Cisco Packet Tracer

In special cases, like the two Smart Home examples, simulation of an Internet connection is also used. This connection is designed to emulate a standard Internet Service Provider (ISP) connection, giving homeowners the ability to connect remotely to their home network from an external network such as a corporate office or mobile network. In the second Smart Home simulation, the ISP is also used to connect home devices to the IoT backend intelligence, as IoT functions are provided as a service.

In addition, in the Smart Industry case and one of the Smart Home cases, 3G networks were also deployed. Additional components such as cell towers and backend servers are needed to keep the network running. Leveraging mobile networks has brought more flexibility in connecting IoT devices to the network. Since the configuration is very simple and there are no limitations, the range and number of connected devices is the same as in a real WLAN.

Once the network device is placed in the emulation, the next step is to configure it. Cisco Packet Tracer offers two options: configure the device through the user interface or through the command line interface (CLI). When using the CLI method, you must use Cisco-specific commands and use actual device logic. Configuration via a more intuitive user interface, requires no knowledge of Cisco commands, but limits the number of parameters that can be set.

Depending on the different installations, different types of cables have been used to connect network devices, such as copper straight wire, copper crossover cable, and optical fast Ethernet cable. The sample microcontroller also uses a custom IoT cable.

As shown in the figure below, Cisco Packet Tracer offers several wiring options, but one important feature is the automatic cabling option. When selected, the tool automatically selects the correct cable to connect the two network interfaces



Figure - List of available cables in Cisco Packet Tracer

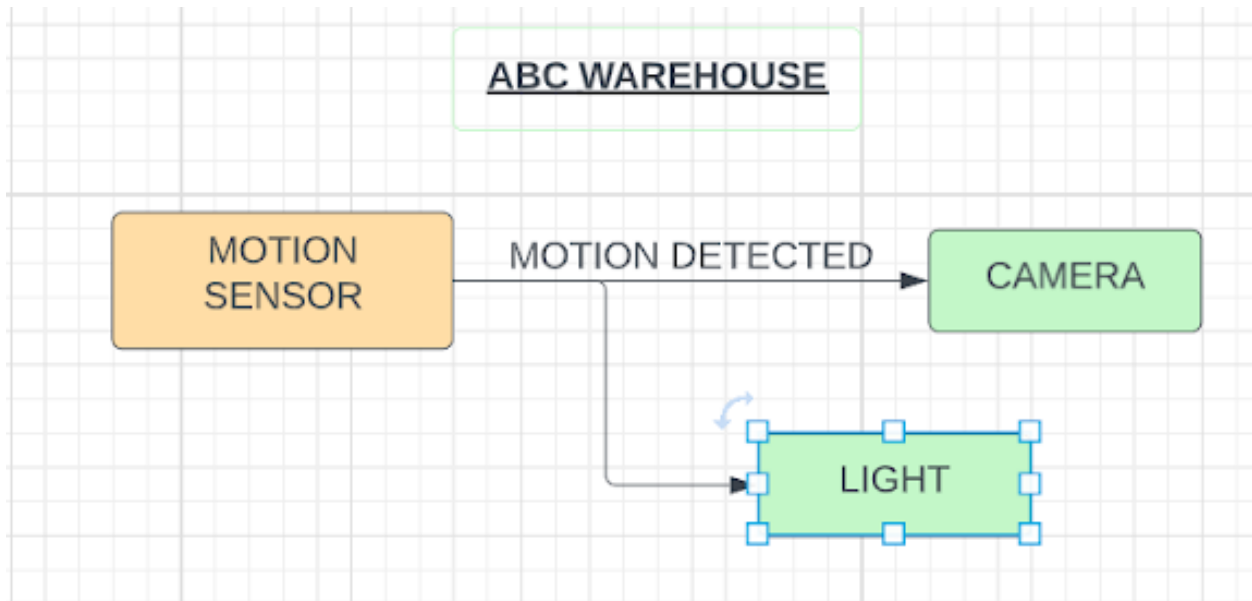
The physical layers and network components have been present in Cisco Packet Tracer for many years, the real addition to the tool's ability to simulate IoT environments is the introduction of IoT devices.

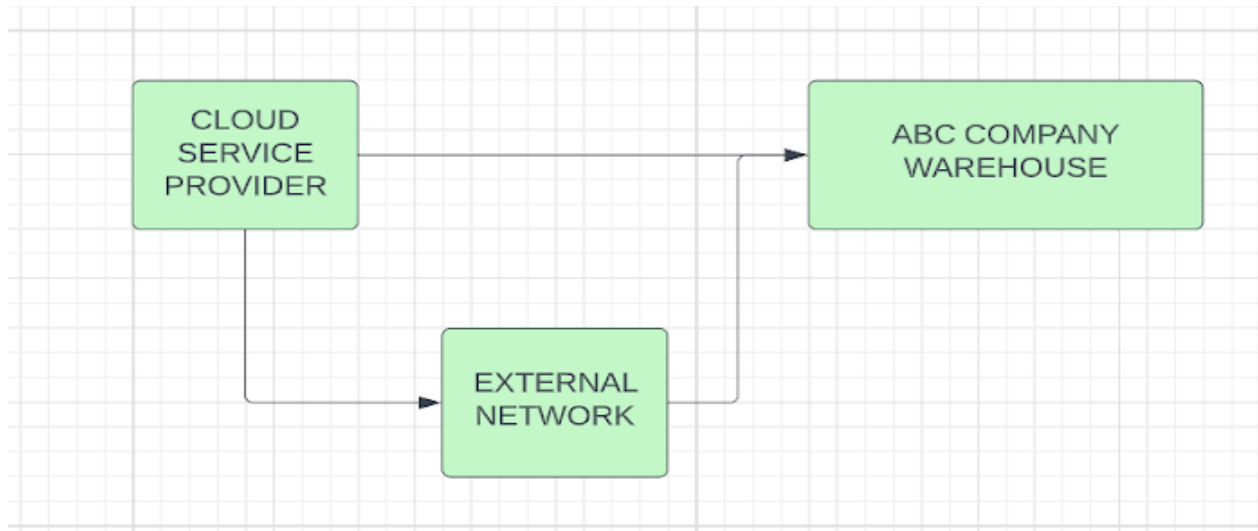
The main categories are: smart devices, sensors, actuators and microcontrollers. The image below is a sample list of smart home devices that can be added to the IoT simulation.



Figure - List of smart device

ARCHITECTURE





METHODOLOGY

1 . Register IoT Devices to the Registration Server

Add a user to the registration server www.registrar1.pka with a strong password:

1. Use a PC in the WH office. Under Desktop tab, open Web Browser, type www.registrar1.pka and select Go. The Registration Server Login window displays.
2. Click Sign up now and create your own account with a strong password (ensure a password is at least 8 characters long with combination of capital characters, lower case characters, and numbers).
3. What is your username and password? _____

Register IoT devices to the registration server:

1. Within the warehouse, click on Motion Detector. Under the Config tab, select Remote Server in the IoT Server section. Enter www.registrar1.pka as the server address and click Connect. Enter

the username/password you just created.

2. Does Motion Detector appear in the registration server? _____

3. Repeat steps 1 and 2 to register the Light, Webcam, and Trip Sensor.

2. Add Conditions in the Registration Server

You will add conditions in the registration server so that when either the Motion Detector or Trip Sensor is

activated, the directed light and the webcam are turned on.

Log in to the registration server using the username/password you created.

Do you see four IoT devices listed? _____

Click Conditions and add following three conditions:

1. Name it LightsOn1, if MD status On is true, then set Directed Light status to On AND set CAM status On to true.

2. Name it LightsOn2, if TS status On is true, then set Directed Light status to On AND set CAM

status On to true.

3. Name it LightsOff, if both MD status On is false AND TS status On is false, then set Directed Light status to Off AND set CAM status On to false.

4. Test the conditions.

Hold the ALT key and move the mouse over Motion Detector. Are Directed Light and Webcam turned on?

3. Configure Strong Authentication to Network Devices

You will configure strong authentication for a wireless connection on the WH gateway device:

1. Within the warehouse, click on the WH Gateway device. Under the Config tab, Wireless option,

set the SSID to WhGateway1, set Authentication to WPA2-PSK with Pass Phrase as IoTWh001.

Leave Encryption Type as AES.

2. Click on the Laptop. Under the Config tab, Wireless0 option, set the SSID to WhGateway1, set

Authentication to WPA2-PSK with Pass Phrase as IoTWh001. Leave Encryption Type as AES.

On the warehouse router, configure a banner to display a warning message for unlawful access.

Although a banner message is not a security measure by itself, it may function as a deterrence to intruders. Set an encrypted password to enter the Exec mode. Set up a local user account for the console line and remote access.

1. Click the Warehouse 2911 router, then click the CLI tab and enter these commands:

```
Warehouse> enable
```

```
Warehouse# config terminal
```

```
Warehouse(config)# banner login %Login with valid password%
```

```
Warehouse(config)# banner motd %Authorized Access Only! Unauthorized access is  
subject to Federal Prosecution.%
```

```
Warehouse(config)#
```

2. Set a secure Exec mode password:

```
Warehouse(config)# enable secret AbcWh001
```

```
Warehouse(config)# exit
```

3. Set a local username for the console line and VTY lines access:

```
Warehouse# configure terminal
```

```
Warehouse(config)# username WhAdmin secret AbcLine001
```

```
Warehouse(config)# line console 0
```

```
Warehouse(config-line)# login local
```

```
Warehouse(config-line)# exit
```

```
Warehouse(config)# line vty 0 4
```

```
Warehouse(config-line)# login local
```

```
Warehouse(config-line)# end
```

```
Warehouse#
```

4. Configure Access Lists to Restrict Traffic between ABC Company IoT devices and the Cloud Service Provider Network

On the warehouse router, configure and apply access list 10 to allow traffic from only the DNS server

and the registration server to enter the ABC Company warehouse IoT devices network:

```
Warehouse# configure terminal
```

```
Warehouse(config)# access-list 10 permit host 172.18.1.5
```

```
Warehouse(config)# access-list 10 permit host 209.165.201.5
```

```
Warehouse(config)# interface g0/2
```

```
Warehouse(config-if)# ip access-group 10 out
```

```
Warehouse(config-if)# end
```

```
Warehouse#
```

On the Cloud Service Provider router, configure and apply an access list 110 to allow traffic from only

the ABC Company warehouse IoT devices network to access the registration server:

```
CSP# configure terminal
```

```
CSP(config)# access-list 110 permit ip host 209.165.200.226 host 209.165.201.5
```

```
CSP(config)# access-list 110 deny ip any host 209.165.201.5
```

```
CSP(config)# access-list 110 permit ip any any
```

```
CSP(config)# interface g0/0
```

```
CSP(config-if)# ip access-group 110 out
```

```
CSP(config-if)# end
```

CSP#

In the ACL 110, why is the warehouse router interface IP address selected as the source in the ACL 110?

5. Configure Secure Web Communication to the Web Server in the Cloud Service Provider Network

The ABC Company uses the web server in the cloud service provider for part of its operation.

Configure the web server in the cloud service provider network to be accessed only via HTTPS:

1. Click CSP Svr, then click the Services tab.
2. Click HTTP on the left pane. Make certain that HTTP is off and HTTPS is on.

6. Testing

From the laptop in the warehouse network, access the registration server. Trigger either the motion

detector or trip sensor, and observe the action of the directed light and webcam

From PC1 or PC2, open the web browser. Can it access the registration server? No.

From PC1 or PC2, open the web browser. Can it access the web server 209.165.201.3 via HTTP?

From PC1 or PC2, open the web browser. Can it access the web server 209.165.201.3 via HTTPS?

SOFTWARE USED

CISCO PACKET TRACER: Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface.

Literature survey

S. No	Objective/Theme	Research problem	Conclusion and discussion
1.	<p>Data is being transferred by internet based enabled things to communicate among themselves and data contains precious information. However, this new world built over the Internet is prone to various challenges in the perspective of security and privacy. In this article, the main challenges of acquisition and privacy and the techniques useful to prevent them were mentioned.</p>	<p><i>The challenges and security issues have been addressed.</i> They are:</p> <ul style="list-style-type: none"> • Divergency and heterogeneity • Performance of computations, storage and communications • Steadfastness • Transportation, access and processing problems might be created by big data • Surveillance <p><i>Privacy solutions that were defined:</i></p> <ol style="list-style-type: none"> 1.Data Segmentation. 2.Bewilderment. 3.Unionization. 4.Sticky Policy. 5.Trusted Platform Module 6.IAM 	<p>An individualized review of Internet-based computing has been given in this paper. Mainly, the relationships, similarities and differences between IoT, CC, CoT were examined, in addition to their architectures and enabling technologies. And also, to secure computing, potential privacy and security issues that could affect the convincingness of the system.</p>
2.	<p>Cloud computing and IoT are two different technologies. Cloud computing helps IoT succeed. This paper mainly limelight the data collection and data accessing methods of IoT services integrated with cloud services.</p>	<p>This paper addressed the attacks on IoT device level and IoT application data and established an architecture for integrating internet of things with cloud services. And the key points of maintaining security over the IoT data by properly configuring network infrastructure and gateways in the cloud.</p>	<p>The combination of cloud computing and IoT will allow us to use new monitoring services and powerful sensory data processing. However, Using IoT with the cloud may lead to new problems.</p>
3.	<p>Resolving the security challenges faced by the users when using IoT devices in cloud computing. Considering the security</p>	<p><i>Surveillance Challenges observed in Internet of Things</i></p> <ol style="list-style-type: none"> 1.There are lack of updates and insufficient testing 	<p>This research helps in creating the minimal cybersecurity standards especially to those owned and controlled by the government.</p>

	challenges in this paper will help us in identifying the original source of the issues and helps in finding strategies that can solve them.	<p>2. Home invasion</p> <p>3. The lack of user knowledge about the security of the internet of things.</p> <p><i>Blueprint of responding to insecure IoT device</i></p> <p>1. Using strong passwords and changing them regularly.</p> <p>2. By locally storing the data and files thus creating a backup.</p> <p>3. Avoiding the components of Universal Plug & Play.</p> <p>4. Using a Secondary Network</p> <p>5. Periodically updating the IoT devices.</p>	By understanding the vulnerabilities that might occur in various devices, there will be more strategies focused at bringing order to the security chaos of IoT devices.
4.	This paper entrenches main issues that are believed to have long-term impact in security and privacy of IoT and cloud computing, on the basis of documented problems and described weaknesses.	<p><i>Steps recommended to mitigate risks</i></p> <p>1. Ensure good governance, risk handling and compliance processes work well.</p> <p>2. Monitoring operational and business processes</p> <p>3. Manage persons associated with it, roles and identities</p> <p>4. Ensure proper encryption and protection of information and data</p> <p>5. Applying suitable confidentiality policies</p> <p>6. Assessing the security benefits for cloud applications</p> <p>7. Ensure cloud networks are properly configured and connections are secured.</p> <p>8. Periodically evaluating security controls on physical infrastructure and facilities</p>	The technology related to Internet of Things (IoT) assumes that identical technology and underlying network devices can work automatically and smartly. Even if the security experts observed all the security concerns linked to wearable technology, people are more willing to become too used to this kind of automation. Either way, it may be the hope of an average consumer who relies on such sorts of devices that tech experts will close and correct the various loopholes around IoT and cloud technology as soon as possible.
5.	<p><i>The manifesto of this paper is:</i></p> <p>A deliberative survey on</p>	This paper consigned the Challenges and Limitations in the point of Cloud Computing	This paper described cloud architectures, deployment models, and common

	<p>cloud-based IoT architecture, services available, configurations, and security models.</p> <p>There are 4 major categories in Cloud security i.e., data or info, network and service, applications used, and security issues involving people.</p> <p>Latest advancements in cloud-based service attacks have been noticed.</p> <p>And the limitations have been described in the machine learning and deep learning perspective.</p>	<ol style="list-style-type: none"> 1. Confidentiality, Availability and Integrity. 2. Application security aspects 3. challenges like COVID 19 situations 4. computation resources might be limited. 5. classification of security issues 6. obsolete and outdated laws. 7. Improper security and privacy policies 	<p>cyber-attacks. Security issues in the cloud have been divided in four categories and shown the associated issues in each category.</p> <p>Various challenges in cloud computing that need to be solved soon. The challenges addressed are the limitations that were there in the Artificial intelligence and Deep Learning domain in cloud computing.</p>
6.	<p>The main ambition is cloud computing and services models and also sheds light on various threats occurring in the cloud computing environment and also highlights the major security issues in different computing services and also lists security metrics that may help customers of the cloud in deciding the security they will have for their data and applications.</p>	<p>This paper amplifies certain versatile Deployment Models and Computing Services, Security Threats in Cloud Security, Issues in Different Cloud Computing Services and Cloud Security Assessment Metrics</p>	<p>In this paper, a metric-based model for security assessment of cloud services, where important security metrics were calculated and taken into account to decide about what type of data they could move to the cloud.</p>
7.	<p>This paper pertinently is a literature survey on the process of integrating IoT devices with cloud. Beginning with the analysis and understanding the starting points of both IoT and Cloud Computing, their relationship with each other has been discussed detailing what is currently leading to their integration.</p>	<p><i>Issues related to IoT security and privacy</i></p> <p>By connecting various agile thousands of devices over the internet and involving millions of data points, hence all of them need to be secured.</p> <p>Due to its large expanded attack surface, the security and privacy of IoT are noticed as major problems. Attackers might gain access to the network by attacking weakly linked configured IoT</p>	<p>The combination of cloud computing and IoT's combination is observed as the next big leap in today's internet world. Various versatile and new applications coming from the integration of this 2 are paving way for newer platforms for business as well as research. There is a hope that this combination paves the way for a new platform for the innovation of multi-networking and open services platform for users</p>

		<p>devices. Because IoT devices are very closely connected to each other, all a hacker does is targeting one vulnerability for manipulating all the data, making it unusable.</p>	
8.	<p>The experiments were conducted using a designed dataset of security metrics and also a real web service dataset of people has shown that the proposed framework of trust assessment can effectively evaluate the trustworthiness of a given cloud service when outperformed other numerous trust assessment methods.</p>	<p>In this paper, the system model that handles two assessment models, likely the security model for assessment and the reputation assessment model has been described. The security assessment model mainly focuses on the elements and components containing the method of security-based trust assessment. The reputation model mainly describes the weight factors that are helpful to mitigate the common cyber-attacks affecting the reputation assessment results.</p>	<p>An innovative trust estimation framework for cloud service models (named STRAF) that integrates its security and respectability. This framework can enhance the context of security of the cloud-based IoT via trustworthy cloud services. It also focuses on CSCs in assessing the trustworthiness of the models related to cloud services by the functionally equal CSPs and selecting the very most trustworthy one from the group that is the one to deploy the cloud service on.</p>
9.	<p>Based on a common generalized architecture of cloud services with IoT, the chances of testing security and privacy needs of cloud services from the user perspective are assessed. The proposed framework is used to assess the cloud services offering IoT like providers Amazon, Microsoft, Google and Thing Speak.</p>	<p>In this paper, A common generalized architecture of IoT cloud services is given and specified the important elements of the architecture for IoT cloud services.</p> <p>The tests for security and privacy requirements were also proposed in. And evaluation of the mentioned IoT cloud services on the basis of the framework proposed was described and discussed.</p>	<p>The test cases pretended were applied to the cloud providers of IoT like Amazon AWS IoT, Microsoft Azure, GCP and Thing Speak It also summarizes the results. The test can either be completely filled, partially filled with limitations or not fully filled. Here, mainly the results of those tests which are partially filled or not at all fulfilled are explained and discussed.</p>
10	<p>This paper surveys the problems of security that are specific to the IoT cloud concepts, this is the first paper of its kind. This paper also shows off the background of research on security and</p>	<p>Based on the security and privacy challenges prescribed in this paper, it is common that security problems about the IoT cloud led to a new set of security challenges from the currently emerging usage of the technology</p>	<p>In general, the purpose of this literature survey paper was to include an outline to sum up the up-to-date studies and contributions on cloud computing and IoT and its significance in our environment</p>

	<p>privacy related to cloud and internet-based things, this paper also discusses the challenges in security of IoT cloud, and later gives security solutions in the described literature.</p>	<p>ensample. This new updated set of security challenges might become tougher to deal with for integrating IoT technology with the cloud. Despite of some security solutions in the literature, there still exist a few problems those deserve the attention of the community for the safety</p>	<p>and recommend suitable research directions and real-world issues regarding the integration of IoT and cloud computing and their security.</p>
11.	<p>The paper uses Cisco packet tracer version 7.2, which consists of four sub-categories of smart things – home, smart city, industrial and energy network, to design an IoT-based control system for a fertilizer plant. Packet tracking also consists of boards - microcontrollers (MCU-PT) and single-board computers (SBC-PT), as well as actuators and sensors. The model enables flexible communication options between things – machines, databases and HMI (Human Machine Interfaces). Implementing an IoT system brings finer process control as operating conditions are monitored online and broadcast to all stakeholders in real-time for faster resolution of deviations.</p>	<p>Designing and implementing Internet of Things (IoT) systems requires platforms with smart things and components. The two dominant architectural approaches for developing IoT systems are the mashup and model-based approaches. Mashup approaches use existing services and are especially suitable for less critical, personalized applications. Web development tools are widely used in mashup approaches. Model-based techniques describe the system at a higher level of abstraction, leading to very expressive modeling of systems</p>	<p>The developed model focuses on three processing facilities; steam production, equipment for the production of nitric acid and ammonium nitrate. Key process parameters are saturated steam temperature, fuel flow rates, CO and SOx emissions, converter head temperature, NOx emissions, neutralization temperature, solution temperature and evaporator vapor pressure. Parameters must be monitored to ensure quality, safety and efficacy. A use case, physical layout, network layout, IoT layout, configuration and simulation interfaces were developed through Cisco's packet tracing platform.</p>
12.	<p>The aim of this research is to come up with a simulation of smart devices that can be controlled by the end user's smart device remotely, and then show a concept called a smart home. Utilization of Cisco Packet Tracking Simulated smart home and IoT</p>	<p>Technology plays a key role in all of today's daily activities. One of these needs is to create a smart home that controls traffic and turns off electronic devices via a smartphone. This implementation can be effectively implemented using package tracking software that includes IoT features to</p>	<p>The simulation results show that the smart objects can be connected to the home portal and the objects can be successfully monitored, which leads to the idea of real implementation</p>

	devices are monitored.	control and simulate a smart home. IoT technology can be applied to many real-life problems, such as: homework, treatment, campus, office, etc. In this paper, we focus on a safe home system that includes devices such as: air conditioner, alarm, lighting, and door. The garage is one of the daily problems	
13.	Cloud computing provides a flexible architecture where data and resources are dispersed at various locations and are accessible from various industrial environments. Cloud computing has changed the using, storing, and sharing of resources such as data, services, and applications for industrial applications. The findings of the proposed research include the following: we present a comprehensive survey of enabling cloud-based IoT architecture, services, configurations, and security models; the classification of cloud security concerns in IoT into four major categories (data, network and service, applications, and people-related security issues), which are discussed in detail; we identify and inspect the latest advancements in cloud-based IoT attacks	During the last decade, industries have rapidly switched to cloud computing for having more comprehensive access, reduced cost, and increased performance. In addition, significant improvement has been observed in the internet of things (IoT) with the integration of cloud computing. However, this rapid transition into the cloud raised various security issues and concerns. Traditional security solutions are not directly applicable and sometimes ineffective for cloud-based systems. Cloud platforms' challenges and security concerns have been addressed during the last three years, despite the successive use and proliferation of multifaceted cyber weapons. The rapid evolution of deep learning (DL) in the artificial intelligence (AI) domain has brought many benefits that can be utilized to address industrial security issues in the cloud.	we identify, discuss, and analyze significant security issues in each category and present the limitations from a general, artificial intelligence and deep learning perspective; we provide the technological challenges identified in the literature and then identify significant research gaps in the IoT-based cloud infrastructure to highlight future research directions to blend cybersecurity in cloud.
14.	The main goal of interaction and cooperation between things and objects that are transmitted through wireless	Mobile Cloud Computing is a new technology that refers to an infrastructure where data storage and processing takes place	We combine the two technologies mentioned above (i.e., Cloud Computing and IoT) to explore the commonalities

	<p>networks is to fulfill the goal that has been set for them as a combined whole. In addition, there is rapid development of both technologies, Cloud Computing and Internet of Things, in the field of wireless communications. In this post, we present a survey of IoT and Cloud Computing, focusing on the security issues of both technologies.</p>	<p>outside of mobile devices. Another latest technology is the Internet of Things. The Internet of Things is a new technology that is rapidly developing in the field of telecommunications. More specifically, IoT is related to wireless telecommunications.</p>	<p>and discover the benefits of their integration. In conclusion, we present the contribution of cloud computing to IoT technology. Thus, it shows how Cloud Computing technology improves the functionality of the Internet of Things. Finally, we explore the security challenges of integrating IoT and Cloud Computing.</p>
15.	<p>The Internet of Things (IoT) provides a new paradigm for the development of heterogeneous and distributed systems and is increasingly becoming a ubiquitous computing service platform. However, due to the lack of sufficient computing and storage resources dedicated to processing and storing huge volumes of IoT data, it tends to adopt cloud-based architecture to solve resource problems. limitations. A number of challenging security and trust concerns have therefore emerged in the context of the cloud-based IoT. For this purpose, a new trust evaluation framework for the security and reputation of cloud services is proposed.</p>	<p>The security-based trustworthiness evaluation method uses cloud-specific security metrics to evaluate the security of a cloud service. In addition, the cloud service quality feedback evaluation is used in the reputation-based trustworthiness evaluation method to evaluate the reputation of the cloud service.</p>	<p>. Experiments conducted using a synthesized security metrics dataset and a real-world web service dataset show that our proposed trust evaluation framework can effectively and efficiently assess the trustworthiness of a cloud service while outperforming other trust evaluation methods. This framework enables the trust evaluation of cloud services to ensure the security of the cloud IoT context through the integration of security and reputation based trust evaluation methods.</p>
16.	<p>Over the years, with the rapid development of distributed computing, parallel computing, grid computing, network storage, and virtual system technology, computing resources have become larger, more abundant, cheaper, and</p>	<p>Service providers are divided into infrastructure companies that manage cloud systems and lease resources based on pricing models, and provider companies that lease resources from infrastructure companies to provide services to</p>	<p>The Internet of Things (IoT) allows the user to connect billions of intelligent machines and exchange information, monitor and manage services that include home automation systems, related to healthcare, agriculture, security</p>

	<p>more accessible than ever before. The improvement of the information technology (IT) industry and the influx of digital technologies devices to the market have increased the demand for computing and storage resources. In this context, a brand new computing model known as cloud computing was suggested. In this mode, resources (including networks, computing, storage, and applications) are made available to customers for on-demand access at any time.</p>	<p>customers. Due to Due to the maturity of the cloud computing generation and its advantages of low cost, easy access to information, rapid deployment, data backup and automated software integration, the cloud is widely used.</p>	<p>surveillance, energy grid or important infrastructure management and manipulation of IoT is another current approach. In which the boundaries between artificial and real environments are always constrained by the dynamic digitization of physical systems equipped to provide value-added services for mobile devices</p>
17.	<p>The Internet of Things is gradually turning into a ubiquitous computing service that needs huge volumes of data storage and processing. However, due to the characteristics of resource limitation, self-organization, and short-range communication in the Internet of Things (IoT), it always adapts to the cloud for external storage and computation. This integration of IoT with the cloud introduces a number of unknown security issues for data at rest.</p>	<p>Cloud computing provides highly scalable and flexible computing and storage resources on a pay-per-use basis. Cloud computing services for computing and storage are becoming increasingly popular, and many organizations are now moving their data from their own data centers to cloud storage providers (CSPs)</p>	<p>In this paper, we conduct an analytical study to explore the challenges and strategies adapted by Cloud Computing to facilitate the secure migration of IoT applications to the cloud.</p>
18.	<p>The Internet of Things has transformed the way things are done in the world of computing. This is why the integration between cloud computing and IoT devices is essential, as the amount of data produced by IoT devices requires a proper and secure</p>	<p>Privacy is even more important in a world where our well-being could be threatened by unsecured data. Therefore, the Internet of Things in cloud computing must always ensure the security and privacy of users.</p>	<p>This research paper addressed issues such as security and strategies that can be used in IoT in cloud computing. The findings indicate that there are major security issues and threats that still need to be addressed. Design the architecture and make changes to the current</p>

	storage as well as a processing system. Still, security concerns remain more important as people share a wide range of cloud computing resources across their devices in many ways		software to achieve this goal. This paper discusses several security challenges faced by IoT in cloud computing, especially regarding threats to users' privacy and cybersecurity
19.	Cloud computing provides a flexible architecture where data and resources are dispersed in different locations and accessible from different industrial environments. Cloud computing has changed the use, storage and sharing of resources such as data, services and applications for industrial applications. Over the past decade, industries have rapidly moved to cloud computing for more comprehensive access, lower costs, and higher performance. In addition, significant improvement has been observed in the Internet of Things (IoT) field due to the integration of cloud computing. However, this rapid move to the cloud has raised various security issues and concerns	Traditional security solutions are not directly applicable and sometimes ineffective for cloud systems. The challenges and security issues of cloud platforms have been addressed over the past three years, despite the gradual use and proliferation of multifaceted cyber weapons. The rapid development of deep learning (DL) in the domain of artificial intelligence (AI) has brought many advantages that can be used to solve industrial security problems in the cloud.	The conclusions of the proposed research include the following: we present a comprehensive exploration of cloud-enabled IoT architecture, services, configurations and security models; classifying IoT cloud security issues into four main categories (data, networks and services, applications, and people-related security issues), which are discussed in detail; we identify and review the latest advances in cloud IoT attacks; we identify, discuss, and analyze significant security issues in each category and present limitations from a general, artificial intelligence, and deep learning perspective; we provide the technological challenges identified in the literature and then identify significant research gaps in IoT-based cloud infrastructure to highlight future research directions on how to bridge cybersecurity in the cloud.
20.	The major goal of this article is to enable organizations to securely store IoT data in the cloud by utilizing various access control policies and cryptographic ideas	The largest and most pressing concern is cloud storage security. In many cases, data generated by IoT devices is more sensitive or critical to the enterprise. When enterprises employ cloud storage, they are concerned about cloud security. This article highlights some of the security challenges that plague the	It solves the security concerns associated with cloud storage. The technique demonstrated allows an enterprise to safely upload IoT data to a public cloud while storing organizational information on a private cloud. The developed

		cloud, as well as the solutions that ensure the organization's data housed on the cloud is safe.	method is extremely efficient during message encryption and decryption. The developed system is beneficial in a variety of commercial enterprises, where data is collected from IoT devices and job capabilities are split based on the user's role in the business. Data from IoT devices is securely uploaded to cloud storage using AES and RSA cryptographic algorithms
21.	The primary goal of this work is to use blockchain to secure a service provisioning mechanism for IoTs. also to introduce cloud nodes to manage the validity status of edge service providers. The reputation of an edge node is seen as a service rating given by end users. and to use the smart contract to check the validity condition of the edge servers.	The adoption of devices that support cloud computing and edge transparent computing increased the data exchange and service provisioning capabilities of resource- constrained devices. However, present solutions are incapable of dealing with network security issues. The creation of blockchain technology solves security challenges by giving the features of openness, decentralization, and tamper proof system.	They introduced blockchain technology in this study to safeguard IoT devices from malicious edge servers. The usage of smart contracts ensures the integrity of edge servers. Service codes generated by edge servers are also validated by IoT devices.
22.	The aim is to secure cloud computing environments used in IoT. The main objective is to applied the Knapsack method to encrypt our ENPKES keys to enrich high security in cloud system	Misconfigurations and other security issues in the cloud can have major consequences for the IoT ecosystem. If the cloud lacks security measures such as authentication and encryption, access restrictions and the integrity of data exchanged between endpoints are compromised.	They used an ENPKES approach in this research, which utilized a Diophantine equation and RSA public keys to perform three stages of encryption and two stages of decryption. With an appropriate key size, it may achieve high strength and security to secure their valuable data.
23.	Classification of security vulnerabilities highlights problems, solutions and open research problems	The issue of assuring resilience in IoT networks was approached by developing protocols and a network management system. Faults in IoT networks might arise as a result of network	They classified and described state-of- the-art work done in assuring security in IoT networks in this study. Efforts in privacy providing, lightweight cryptographic framework, safe

		<p>attacks or energy depletion. There have been several efforts to address errors, most of which have failed to take into account the resource constraints of IoT devices.</p>	<p>routing and forwarding, robustness and resilience management, denial of service detection, and insider attack detection are all thoroughly explored. Privacy is critical in IoT, especially because the properties of such networks differ from those of traditional Internet networks. This paper identifies and discusses such challenges and requirements.</p>
24.	<p>Categorize major IoT system attacks based on attack objects and map them to one or more architectural layers;</p>	<p>Leakage of data in any IoT-based application .Users' privacy may be violated as a result. As a result, in order to prevent such issues while simultaneously allowing for flexibility . The work has developed a blockchain-based searchable encryption mechanism for sensitive data exchange EHRs.</p> <p>The actual EHRs are hosted in public cloud servers under this arrangement, while an index for a complicated logic formula is used to calculate each EHR.</p>	<p>With the rise of IoT, the research community has become aware of a number of security flaws ranging from attacks on devices to attacks on data in transit. Furthermore, the widespread deployment of IoT in industry has established IIoT as a distinct study subject. The strong linkage of the physical and virtual worlds via intelligent systems has increased the vulnerabilities of Industrial IoT-based systems. As a result, during the surveying of IoT particular security challenges and solutions, with a special emphasis on IIoT, are described in this study.</p>
25.	<p>Internet-enabled "things" can interact with each other by sending data providing valuable information. However, this new world built on the Internet is prone to a range of security and privacy issues. The primary security and privacy concerns, as well as solutions for preventing them,</p>	<p>The difficulties and security concerns have been handled. They are as follows: Heterogeneity • Computational, storage, and communication performance • Reliability</p>	<p>This article provides a thorough examination of Internet-based computing. The relationships, similarities, and differences between IoT, CC, and CoT, as well as their designs and supporting technologies, were primarily explored. In addition, to safe computing, possible privacy and security problems that might affect system</p>

	were discussed in this article.		effectiveness.
26.	IoT and cloud computing are two distinct technologies. Cloud computing contributes to the success of IoT. This study focuses mostly on data collecting and data access strategies for IoT services that are connected with cloud services.	This research addressed IoT device level and IoT application data threats and proposed a framework for connecting the internet of things with cloud services. And the need of securing data over IoT data by securely managing network infrastructure and cloud gateways	The combination of cloud computing and IoT will allow us to use new monitoring services and powerful sensory data processing. However, Using IoT with the cloud may lead to new problems.
27.	Resolving the security issues that users face while utilizing IoT devices in cloud computing. Considering the security concerns in this article will assist us in understanding the root cause of the problems and in developing solutions.	<i>Security Challenges observed in Internet of Things</i> -There are lack of updates and insufficient testing Home invasion. The lack of user knowledge about the security of the internet of things.	This research contributes to the development of basic cybersecurity requirements, particularly for those owned and managed by the government. Understanding the vulnerabilities that may exist in diverse devices will allow additional techniques to be developed to bring order to the security explodes of IoT devices.
28.	The goal of this article was to effectively turn the IoT Security Framework into the Reliable IoT Sensor to Cloud Ecosystem	It addresses the Insecure Web Interface is one of the security challenges and consequences of IoT. Improper Authentication/Authorization, Insecure Network Services, Poor Transport Encryption, Privacy Concerns Insecure Cloud Interface, Insecure Mobile Interface, and Insecure Web Interface. Limited Security Configurability	Before designing a safe network architecture and ecosystem, the approach of integrating all security requirements was adopted.

RESEARCH QUESTIONS

R1. What are the challenges of security and privacy associated with IoT?

Insufficient and improper data protection, including communication and storage. The most habitually happening concerns in procuring the data of IoT applications are mostly because of insecure communications and improper data storage. One of the specific challenges for IoT privacy and security is that poorly secured devices could be used to access confidential data.

R2. How the IoT is being impacted by the security issues present in the cloud?

Similar security flaws and misconfigurations in the cloud might cause severe damage to the IoT ecosystem to which the cloud belongs. Access controls and the data sent between the endpoints are prone to threats if the cloud doesn't have security features like encryption and authentication.

R3. What are the top 5 security concerns about IoT in the cloud?

- Vulnerabilities. Vulnerabilities are a big problem that constantly trouble users
- Escalated and frequent cyberattacks. ...
- Malware induction.
- Information theft, data theft and unknown exposure to unknown users
- Device mismanagement, malfunction and misconfiguration.

R4. How is security provided by the IoT cloud?

Some Secure networking protocols like the message-passing protocol, and enabling point-to-point encryption and handling security certificates are crucial for overall cloud security. Cloud providers like aws, GCP offer certificates and private security keys for the users, which should be generated individually for each IoT device.

R5. How are cloud services related and important to IoT?

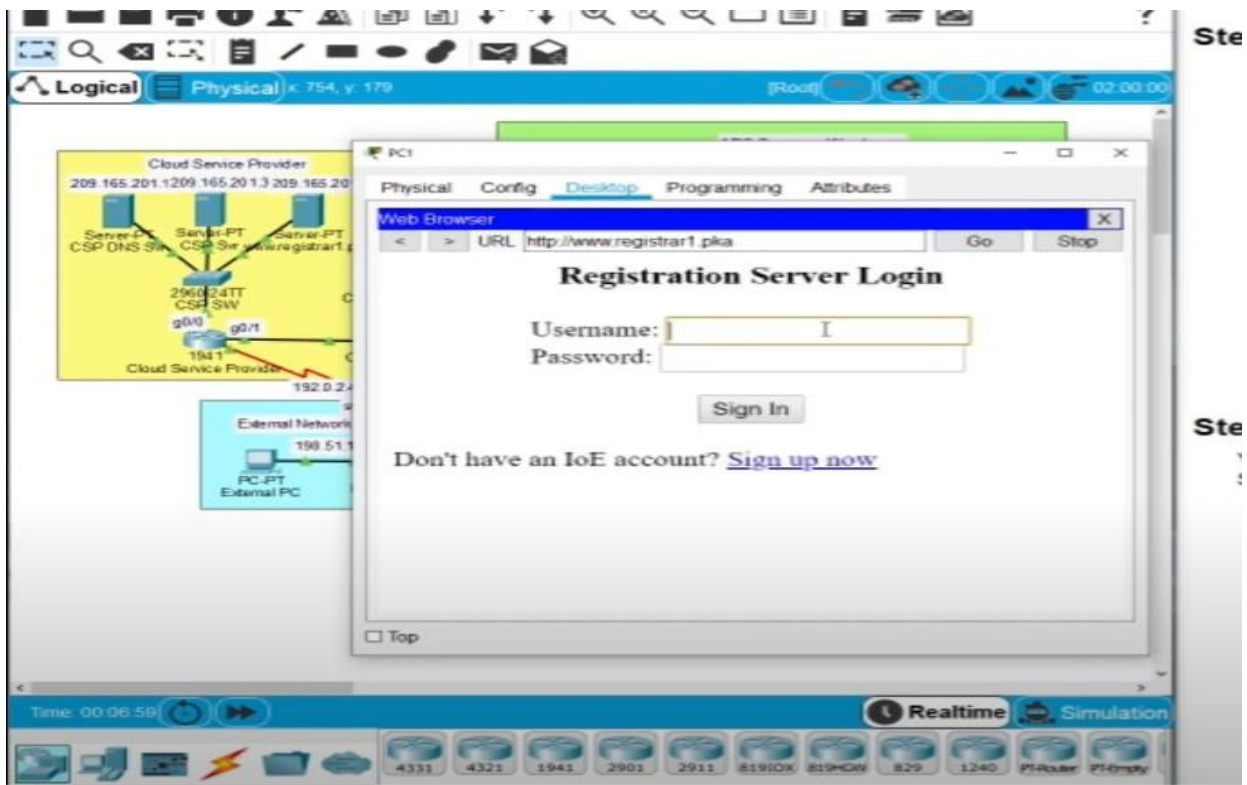
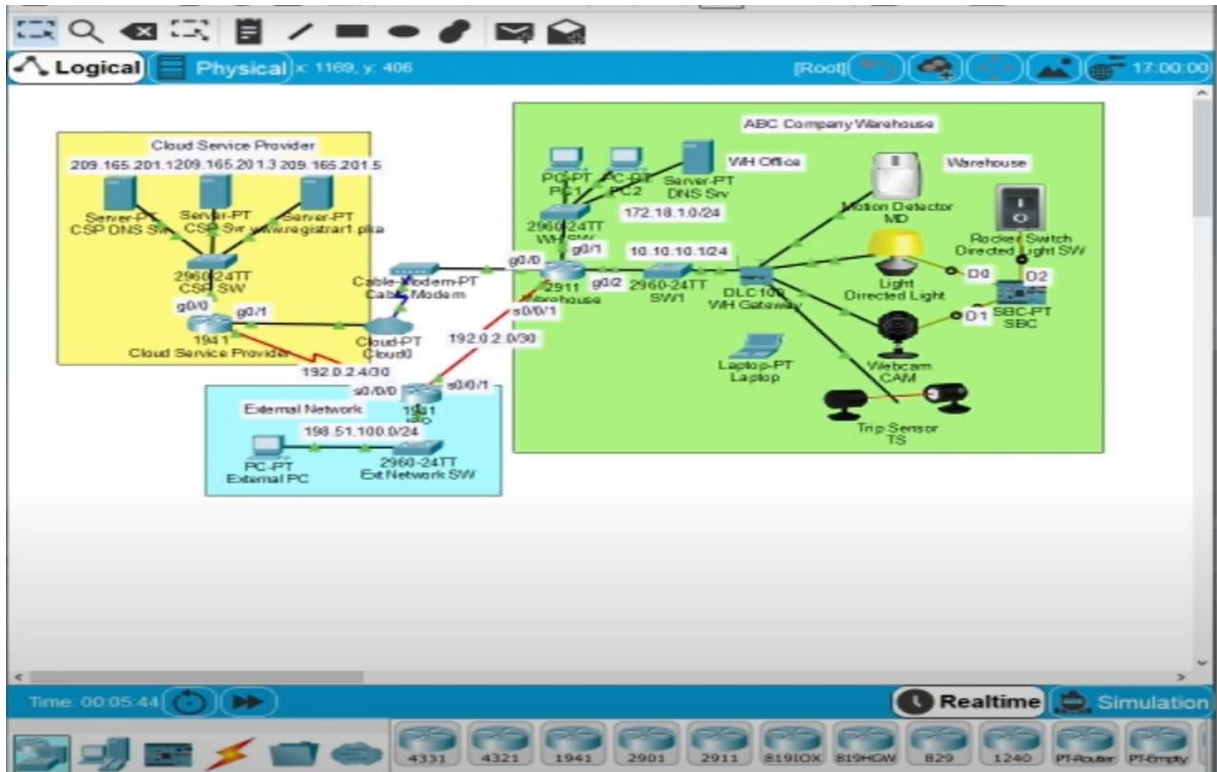
cloud IoT provides such cloud services that connect the IoT devices to other devices and cloud services. Cloud with IoT usually provides device software that helps in connecting IoT devices with cloud IoT-based services.

Conclusion & Future Work

Based on a common generalized architecture of cloud services with IoT, the chances of testing security and privacy needs of cloud services from the user perspective are assessed. The proposed framework is used to assess the cloud services offering IoT like providers Amazon, Microsoft, Google and Thing Speak. A deliberative survey on cloud-based IoT architecture, services available, configurations, and security models. There are 4 major categories in Cloud security i.e., data or info, network and service, applications used, and security issues involving people. Latest advancements in cloud-based service attacks have been noticed. And the limitations have been described in the machine learning and deep learning perspective. Resolving the security challenges faced by the users when using IoT devices in cloud computing. Considering the security challenges in this paper will help us in identifying the original source of the issues and helps in finding strategies that can solve them.

Appendix

SCREENSHOTS OF THE IMPLEMENTATION



Physical Config **Desktop** Programming Attributes

Web Browser
 < > URL: <http://www.registrar1.pka/conditions.html> Go Stop

IoT Server - Device Conditions Home | Conditions | Editor | Log Out

Actions		Enabled	Name	Condition	Actions
Edit	Remove	Yes	Fanoff	PTT0810C8I6 Status is 0	Set PTT0810B5ZI Status to 0
Edit	Remove	Yes	Fan1	PTT0810C8I6 Status is 1	Set PTT0810B5ZI Status to 1
Edit	Remove	Yes	Fan2	PTT0810C8I6 Status is 2	Set PTT0810B5ZI Status to 2
Edit	Remove	Yes	LightsOn1	MD On is true	Set Directed Light Status to On Set CAM On to true
Edit	Remove	Yes	LightsOn2	TS On is true	Set Directed Light Status to On Set CAM On to true
Edit	Remove	Yes	LightsOff	Match all: • MD On is false • TS On is false	Set Directed Light Status to Off Set CAM On to false

Add

File Edit Options View Tools Extensions Help

Packet Tracer 7.1

Step 1 - Register IoT Devices to the Registration

Logical Physical x 824, y 455 [Root]

Cloud Service Provider
 209.165.201.1209.165.201.3 209.165.201.5
 Server-PT CSP DNS Srv Server-PT CSP Srv Registrar1.pka
 2960-24TT CSP SW
 g0/0
 1941 Cloud Service Provider
 192.0.2.4/30
 Cloud PT (Cloud)

External Network
 192.0.2.4/30
 PC-PT External PC 2960-24TT Ext Network SW
 g0/0/1

ABC Company/Warehouse
 PC-PT PC-2 Server-PT DNS Srv
 172.18.1.0/24
 2960-24TT WH SW
 g0/0/1
 10.10.10.124
 2911 g0/0 2960-24TT SW1
 10.10.10.124
 VM Office
 Motion Detector MD
 Light Directed Light
 Webcam CAM
 Trip Sensor TS
 Laptop-PT Laptop
 VM Gateway

PC1

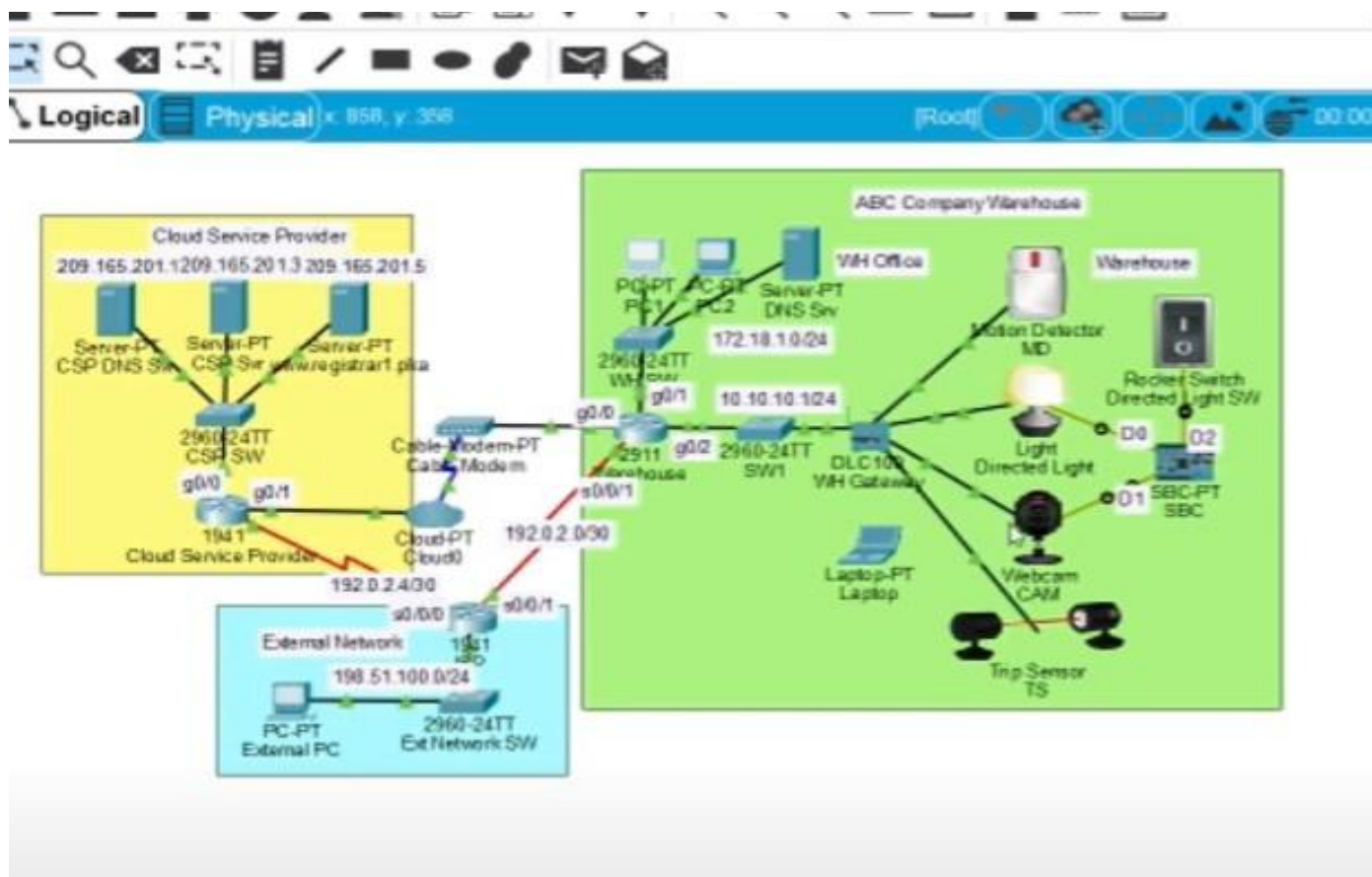
Physical Config **Desktop** Programming Attributes

Web Browser
 < > URL: <http://www.registrar1.pka/home.html> Go Stop

IoT Server - Devices Home | Conditions | Editor | Log Out

- MD (PTT08107BK8) Motion Detector
- Directed Light (PTT0810L8JJ) Light
- CAM (PTT08104132) Webcam
- TS (PTT0810JWY7) Trip Sensor

Top



```

Warehouse>
Warehouse>enable
Warehouse#conf term
Enter configuration commands, one per line. End
with CNTL/Z.
Warehouse(config)#banner login %Login with valid
password%
Warehouse(config)# banner motd %Authorized Access
Only! Unauthorized access is subject to Federal
Prosecution.%
Warehouse(config)#enable secret AbcWh001
Warehouse(config)#exit
Warehouse#
%SYS-5-CONFIG_I: Configured from console by console

Warehouse#
Warehouse#
Warehouse#
  
```


Warehouse(config)# access-list 10 permit host 209.165.201.1209.165.201.5

Warehouse(config)# interface g0/2

Warehouse(config-if)# ip access-group 10 out

Port	Link	VLAN	IP Address	IPv6 Address	MAC Address
GigabitEthernet0/0	Up	--	209.165.200.226/30	<not set>	0030.A378.3B01
GigabitEthernet0/1	Up	--	172.18.1.254/24	<not set>	0030.A378.3B02
GigabitEthernet0/2	Up	--	10.10.10.254/24	<not set>	0030.A378.3B03
Serial0/0/0	Down	--	<not set>	<not set>	<not set>
Serial0/0/1	Up	--	192.0.2.2/30	<not set>	<not set>
Vlan1	Down	1	<not set>	<not set>	0060.47D7.29B0

Hostname: Warehouse

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet

CSP# configure terminal

CSP(config)# access-list 110 permit ip host 209.165.201.1209.165.201.5

CSP(config)# access-list 110 deny ip any host 209.165.201.1209.165.201.5

CSP(config)# access-list 110 permit ip any any

CSP(config)# interface g0/0

CSP(config-if)# ip access-group 110 out

CSP(config-if)# end

CSP#

In the ACL 110, why is the warehouse router interface IP address ACL 110?

File Edit Options View Tools Extensions Help

Logical Physical X:776, Y:214 [Root]

Cloud Service Provider

209.165.201.1209.165.201.3 209.165.201.5

Server-PT CSP DNS Svr

Server-PT CSP Svr

Server-PT Svr

2960-24TT CSP SW

g0/0

g0/1

Cloud Service Provider

194.1

Cloud-PT (Cloud)

192.0.2.4/30

g0/0/0

g0/0/1

External Network

198.51.100.0/24

PC-PT External PC

2960-24TT ExtNetwork SW

ABC Company Warehouse

Warehouse Office

Warehouse

PC-PT PC1

PC-PT PC2

Server-PT DNS Svr

172.18.1.0/24

2960-24TT Warehouse SW

g0/0

g0/1

2511 Warehouse

g0/0/1

2960-24TT SW

g0/0/2

DLC100 Warehouse

Laptop-PT Laptop

Webcam CAM

Tri-P Sensor TS

Light Directed Light

Robot Switch Directed Light SW

g0/0

g0/1

g0/2

g0/3

g0/4

g0/5

g0/6

g0/7

g0/8

g0/9

g0/10

g0/11

g0/12

g0/13

g0/14

g0/15

g0/16

g0/17

g0/18

g0/19

g0/20

g0/21

g0/22

g0/23

g0/24

g0/25

g0/26

g0/27

g0/28

g0/29

g0/30

g0/31

g0/32

g0/33

g0/34

g0/35

g0/36

g0/37

g0/38

g0/39

g0/40

g0/41

g0/42

g0/43

g0/44

g0/45

g0/46

g0/47

g0/48

g0/49

g0/50

g0/51

g0/52

g0/53

g0/54

g0/55

g0/56

g0/57

g0/58

g0/59

g0/60

g0/61

g0/62

g0/63

g0/64

g0/65

g0/66

g0/67

g0/68

g0/69

g0/70

g0/71

g0/72

g0/73

g0/74

g0/75

g0/76

g0/77

g0/78

g0/79

g0/80

g0/81

g0/82

g0/83

g0/84

g0/85

g0/86

g0/87

g0/88

g0/89

g0/90

g0/91

g0/92

g0/93

g0/94

g0/95

g0/96

g0/97

g0/98

g0/99

g0/100

g0/101

g0/102

g0/103

g0/104

g0/105

g0/106

g0/107

g0/108

g0/109

g0/110

g0/111

g0/112

g0/113

g0/114

g0/115

g0/116

g0/117

g0/118

g0/119

g0/120

g0/121

g0/122

g0/123

g0/124

g0/125

g0/126

g0/127

g0/128

g0/129

g0/130

g0/131

g0/132

g0/133

g0/134

g0/135

g0/136

g0/137

g0/138

g0/139

g0/140

g0/141

g0/142

g0/143

g0/144

g0/145

g0/146

g0/147

g0/148

g0/149

g0/150

g0/151

g0/152

g0/153

g0/154

g0/155

g0/156

g0/157

g0/158

g0/159

g0/160

g0/161

g0/162

g0/163

g0/164

g0/165

g0/166

g0/167

g0/168

g0/169

g0/170

g0/171

g0/172

g0/173

g0/174

g0/175

g0/176

g0/177

g0/178

g0/179

g0/180

g0/181

g0/182

g0/183

g0/184

g0/185

g0/186

g0/187

g0/188

g0/189

g0/190

g0/191

g0/192

g0/193

g0/194

g0/195

g0/196

g0/197

g0/198

g0/199

g0/200

g0/201

g0/202

g0/203

g0/204

g0/205

g0/206

g0/207

g0/208

g0/209

g0/210

g0/211

g0/212

g0/213

g0/214

g0/215

g0/216

g0/217

g0/218

g0/219

g0/220

g0/221

g0/222

g0/223

g0/224

g0/225

g0/226

g0/227

g0/228

g0/229

g0/230

g0/231

g0/232

g0/233

g0/234

g0/235

g0/236

g0/237

g0/238

g0/239

g0/240

g0/241

g0/242

g0/243

g0/244

g0/245

g0/246

g0/247

g0/248

g0/249

g0/250

g0/251

g0/252

g0/253

g0/254

g0/255

g0/256

g0/257

g0/258

g0/259

g0/260

g0/261

g0/262

g0/263

g0/264

g0/265

g0/266

g0/267

g0/268

g0/269

g0/270

g0/271

g0/272

g0/273

g0/274

g0/275

g0/276

g0/277

g0/278

g0/279

g0/280

g0/281

g0/282

g0/283

g0/284

g0/285

g0/286

g0/287

g0/288

g0/289

g0/290

g0/291

g0/292

g0/293

g0/294

g0/295

g0/296

g0/297

g0/298

g0/299

g0/300

g0/301

g0/302

g0/303

g0/304

g0/305

g0/306

g0/307

g0/308

g0/309

g0/310

g0/311

g0/312

g0/313

g0/314

g0/315

g0/316

g0/317

g0/318

g0/319

g0/320

g0/321

g0/322

g0/323

g0/324

g0/325

g0/326

g0/327

g0/328

g0/329

g0/330

g0/331

g0/332

g0/333

g0/334

g0/335

g0/336

g0/337

g0/338

g0/339

g0/340

g0/341

g0/342

g0/343

g0/344

g0/345

g0/346

g0/347

g0/348

g0/349

g0/350

g0/351

g0/352

g0/353

g0/354

g0/355

g0/356

g0/357

g0/358

g0/359

g0/360

g0/361

g0/362

g0/363

g0/364

g0/365

g0/366

g0/367

g0/368

g0/369

g0/370

g0/371

g0/372

g0/373

g0/374

g0/375

g0/376

g0/377

g0/378

g0/379

g0/380

g0/381

g0/382

g0/383

g0/384

g0/385

g0/386

g0/387

g0/388

g0/389

g0/390

g0/391

g0/392

g0/393

g0/394

g0/395

g0/396

g0/397

g0/398

g0/399

g0/400

g0/401

g0/402

g0/403

g0/404

g0/405

g0/406

g0/407

g0/408

g0/409

g0/410

g0/411

g0/412

g0/413

g0/414

g0/415

g0/416

g0/417

g0/418

g0/419

g0/420

g0/421

g0/422

g0/423

g0/424

g0/425

g0/426

g0/427

g0/428

g0/429

g0/430

g0/431

g0/432

g0/433

g0/434

g0/435

g0/436

g0/437

g0/438

g0/439

g0/440

g0/441

g0/442

g0/443

g0/444

g0/445

g0/446

g0/447

g0/448

g0/449

g0/450

g0/451

g0/452

g0/453

g0/454

g0/455

g0/456

g0/457

g0/458

g0/459

g0/460

g0/461

g0/462

g0/463

g0/464

g0/465

g0/466

g0/467

g0/468

g0/469

g0/470

g0/471

g0/472

g0/473

g0/474

g0/475

g0/476

g0/477

g0/478

g0/479

g0/480

g0/481

g0/482

g0/483

g0/484

g0/485

g0/486

g0/487

g0/488

g0/489

g0/490

g0/491

g0/492

g0/493

g0/494

g0/495

g0/496

g0/497

g0/498

g0/499

g0/500

g0/501

g0/502

g0/503

g0/504

g0/505

g0/506

g0/507

g0/508

g0/509

g0/510

g0/511

g0/512

g0/513

g0/514

g0/515

g0/516

g0/517

g0/518

g0/519

g0/520

g0/521

g0/522

g0/523

g0/524

g0/525

g0/526

g0/527

g0/528

g0/529

g0/530

g0/531

g0/532

g0/533

g0/534

g0/535

g0/536

g0/537

g0/538

g0/539

g0/540

g0/541

g0/542

g0/543

g0/544

g0/545

g0/546

g0/547

g0/548

g0/549

g0/550

g0/551

g0/552

g0/553

g0/554

g0/555

g0/556

g0/557

g0/558

g0/559

g0/560

g0/561

g0/562

g0/563

g0/564

g0/565

g0/566

g0/567

g0/568

g0/569

g0/570

g0/571

g0/572

g0/573

g0/574

g0/575

g0/576

g0/577

g0/578

g0/579

g0/580

g0/581

g0/582

g0/583

g0/584

g0/585

g0/586

g0/587

g0/588

g0/589

g0/590

g0/591

g0/592

g0/593

g0/594

g0/595

g0/596

g0/597

g0/598

g0/599

g0/600

g0/601

g0/602

g0/603

g0/604

g0/605

g0/606

g0/607

g0/608

g0/609

g0/610

g0/611

g0/612

g0/613

g0/614

g0/615

g0/616

g0/617

g0/618

g0/619

g0/620

g0/621

g0/622

g0/623

g0/624

g0/625

g0/626

g0/627

g0/628

g0/629

g0/630

g0/631

g0/632

g0/633

g0/634

g0/635

g0/636

g0/637

g0/638

g0/639

g0/640

g0/641

g0/642

g0/643

g0/644

g0/645

g0/646

g0/647

g0/648

g0/649

g0/650

g0/651

g0/652

g0/653

g0/654

g0/655

g0/656

g0/657

g0/658

g0/659

g0/660

g0/661

g0/662

g0/663

g0/664

g0/665

g0/666

g0/667

g0/668

g0/669

g0/670

g0/671

g0/672

g0/673

g0/674

g0/675

g0/676

g0/677

g0/678

g0/679

g0/680

g0/681

g0/682

g0/683

g0/684

g0/685

g0/686

g0/687

g0/688

g0/689

g0/690

g0/691

g0/692

g0/693

g0/694

g0/695

g0/696

g0/697

g0/698

g0/699

g0/700

g0/701

g0/702

g0/703

g0/704

g0/705

g0/706

g0/707

g0/708

g0/709

g0/710

g0/711

g0/712

g0/713

g0/714

g0/715

g0/716

g0/717

g0/718

g0/719

g0/720

g0/721

g0/722

g0/723

g0/724

g0/725

g0/726

g0/727

g0/728

g0/729

g0/730

g0/731

g0/732

g0/733

g0/734

g0/735

g0/736

g0/737

g0/738

g0/739

g0/740

g0/741

g0/742

g0/743

g0/744

g0/745

g0/746

g0/747

g0/748

g0/749

g0/750

g0/751

g0/752

g0/753

g0/754

g0/755

g0/756

g0/757

g0/758

g0/759

g0/760

g0/761

g0/762

g0/763

g0/764

g0/765

g0/766

g0/767

g0/768

g0/769

g0/770

g0/771

g0/772

g0/773

g0/774

g0/775

g0/776

g0/777

g0/778

g0/779

g0/780

g0/781

g0/782

g0/783

g0/784

g0/785

g0/786

g0/787

g0/788

g0/789

g0/790

g0/791

g0/792

g0/793

g0/794

g0/795

g0/796

g0/797

g0/798

g0/799

g0/800

g0/801

g0/802

g0/803

g0/804

g0/805

g0/806

g0/807

g0/808

g0/809

g0/810

g0/811

g0/812

g0/813

g0/814

g0/815

g0/816

g0/817

g0/818

g0/819

g0/820

g0/821

g0/822

g0/823

g0/824

g0/825

g0/826

g0/827

g0/828

g0/829

g0/830

g0/831

g0/832

g0/833

g0/834

g0/835

g0/836

g0/837

g0/838

g0/839

g0/840

g0/841

g0/842

g0/843

g0/844

g0/845

g0/846

g0/847

g0/848

g0/849

g0/850

g0/851

g0/852

g0/853

g0/854

g0/855

g0/856

g0/857

g0/858

g0/859

g0/860

g0/861

g0/862

g0/863

g0/864

g0/865

g0/866

g0/867

g0/868

g0/869

g0/870

g0/871

g0/872

g0/873

g0/874

g0/875

g0/876

g0/877

g0/878

g0/879

g0/880

g0/881

g0/882

g0/883

g0/884

g0/885

g0/886

g0/887

g0/888

g0/889

g0/890

g0/891

g0/892

g0/893

g0/894

g0/895

g0/896

g0/897

g0/898

g0/899

g0/900

g0/901

g0/902

g0/903

REFERENCES

- 1.** Privacy and Security in Internet-based Computing: Cloud Computing, Internet of Things, Cloud of Things: a review, Syrine Sahmima , Hamza Gharsellaoui Cloud of Things, International Conference on Knowledge Based and Intelligent Information and Engineering Systems
- 2.** Data Access and security in Cloud integrated IoT, L.Mohan Assistant Professor, Dept. of CSE Chirstu jyothi Institute of Technology & Science jangaon, India
- 3.** Security challenges and strategies for the IoT in cloud computing, S.Vijaya Laxmi Assistant Professor, Dept. of CSE Chirstu jyothi Institute of Technology & Science jangaon, India.
- 4.** Security Ecosystem in IoT & Cloud, Pokuri Rajani, Parupally Anuja Reddy Department of Computing Science and Engineering, G Narayanamma Institute of Technology & Science Hyderabad, India
- 5.** Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey, Waqas Ahmad Aamir Rasool, Thar Baker, Abdul Rehman Javed and Zunera Jalil
- 6.** Security Issues in IoT and Cloud Computing Service Models with Suggested Solutions, Dinesh Kumar Saini, Punit Gupta and Krishan Kumar.
- 7.** A Comparative study of cloud computing through IOT, Manoj Chopra, Vijay Dhote Assistant Professor, IES College, INDIA
- 8.** Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service,XIAO LAN , NING ZHANG,XINGSHU CHEN(Member, IEEE), AND DAJIANG CHEN ,
- 9.** Security of IoT Cloud Services - A User-Oriented Test Approach, Martin Bohm,Diederich Wermser,Ina Schiering.
- 10.** The Security Challenges in Cloud IoT- A Review, Lakshmi sri surya, Data Scientist & Department of Information Technology, California, USA
- 11.** Bokefode, J. D., Bhise, A. S., Satarkar, P. A., & Modani, D. G. (2016). Developing a secure cloud storage system for storing IoT data by applying role based encryption. Procedia Computer Science, 89, 43-50.Rana, S.S., Kumar, S. and Thakur, M.J.,GET A BITE: The charity-based application through which people can donate food, books and clothes to needy people.
- 12.**Rehman, M., Javaid, N., Awais, M., Imran, M., & Naseer, N. (2019, December). Cloud based secure service providing for IoTs using blockchain. In 2019 IEEE Global Communications Conference (GLOBECOM) (pp. 1-7). IEEE. Mejia, G., Argueta, C.M., Rangel, V., García-Díaz, C., Montoya, C. and Agudelo, I.I., 2015, July. Food donation: An initiative to mitigate hunger in

the world. In 2015 Meeting Urban Food Needs (MUFN) Programme, July 1, 2015, Rome, Italy.

13. Thirumalai, C., Mohan, S., & Srivastava, G. (2020). An efficient public key secure scheme for cloud and IoT security. *Computer Communications*, 150, 634-643.

14. Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal of Computer Networks and Communications*, 2019.

15. Sengupta, J., Ruj, S., & Bit, S. D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. *Journal of Network and Computer Applications*, 149, 102481. Don, V.S.A.A., Loke, S.W. and Zaslavsky, A., 2018, February. IoT-Aided Charity: An Excess Food Redistribution Framework. In 2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU) (pp. 1-6). IEEE.

16. Sahmim, S., & Gharsellaoui, H. (2017). Privacy and security in internet-based computing: cloud computing, internet of things, cloud of things: a review. *Procedia computer science*, 112, 1516-1522. Mandal, K., Jadhav, S. and Lakhani, K., 2016. Food Wastage Reduction through Donation using Modern Technological Approach: Helping Hands. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 5(4).

17. Mohan, L. Data Access and security in Cloud integrated IoT.

18. Surya, L. (2016). Security challenges and strategies for the IoT in cloud computing. *International Journal of Innovations in Engineering Research and Technology* ISSN, 2394-3696.

19. Rahman, A. F. A., Daud, M., & Mohamad, M. Z. (2016, March). Securing sensor to cloud ecosystem using internet of things (iot) security framework. In *Proceedings of the International Conference on Internet of things and Cloud Computing* (pp. 1-5).