ENHANCING SECURITY OF CLOUDBASED IoT SYSTEMS THROUGH NETWORK ACCESS CONTROL (NAC)

MCS

By

Awais Khan
00000325140

Submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfillment of the requirements for the degree of MS in Information Security

May 2023

Declaration

I hereby declare that no portion of the work presented in this thesis has been submitted in support of another award or qualification either at this institution or elsewhere.

____

Awais Khan

Dedication

I dedicate this thesis to Almighty Allah, my source of inspiration, wisdom, knowledge, blessing, and understanding.

I also dedicate this thesis work to my parents, siblings, better half and daughter who have been a constant source of encouragement and support during this challenging task.

I also dedicate this thesis to my teachers and those whose good examples taught me to work hard for a thing I aspire to achieve.

Abstract

To bring comfort to human life, reliance on smart devices has increased exponentially. In this digital era, millions of IoT devices are interconnected to store, process, and communicate information with each other. Presently, IoT devices are being used regularly in healthcare, education, agriculture, transportation, smart homes, smart cities and defense forces, etc. The use of these devices is, however, strained due to limited resources in terms of storage, computation, and processing. Therefore, resource-intensive encryption algorithms cannot be effectively utilised to ensure the security of information. To overcome the limitations, cloud computing as a resource-rich technology may be integrated with IoT devices to maximize output and utility. However, many security concerns arise after the amalgamation of cloud computing and IoT devices. This study proposes a novel approach, i.e., NAC, to provide robust access control and authorization mechanism for cloud-based IoT systems that can also mitigate multiple threats to cloud-based IoT systems. This study presents a three-layered architecture, i.e., IoT devices layer, authentication layer, and cloud computing layer. A novel solution NAC has been used on the authentication layer and cloud layer (as per organization size and requirement) to enhance the security of a cloud-based IoT system. Our proposed solution provides access control mechanism to cloud-based IoT systems that can also minimize the chances of multiple attacks that are faced by cloud-based IoT systems.

Acknowledgments

I express my deepest gratitude to my supervisor, Dr. Shahzaib Tahir Butt, for his countless hours in reflecting, reading, encouraging, guidance and continuous support throughout this journey. It was a great privilege and honor for me to work and study under his supervision. His vision, dynamism, prompt response and valuable suggestions make it possible to complete this tedious task in due course of time. His suggestions helped me to improve my problem-solving capabilities and research skills.

I would like to extend my gratitude to co-supervisor Dr. Fawad Khan and committee members Dr. Hassan Tahir and Dr. Mir Yasir Umair for their support and recommendations, which improved this research study.

I am very thankful to College of Signals and National University of Sciences and Technology for providing me the opportunity to polish my research skills and contribute to the betterment of society.

I am also very thankful to the organization and individuals who participated in this research study directly or indirectly to implement and test the proposed idea.

Finally, I would like to extend my acknowledgment and gratitude to all who have been directly or indirectly involved in this research study and provided me with valuable suggestions to improve and complete my research work on time.

Thank you all.

Table of Contents

List of Figures

List of Tables

Acronyms

IoT	**Internet of Things**
NAC	**Network Access Control**
DDOS	**Distributed Denial of Service**
LEAs	**Law Enforcement Agencies**
AV	**Antivirus**
SIEM	**Security Information and Event Management**
PC	**Personnel Computer**
AC	**Air conditioner**
IT	**Information Technology**
IBM	**International Business Machines**
CSP	**Cloud Service Providers**
CSC	**Cloud Service Consumer**
SAAS	**Software as a Service**
PAAS	**Platform as a Service**
IAAS	**Infrastructure as a Service**
AWS	**Amazon Web Services**
NIST	**National Institute of Standards and Technology**
IEEE	**Institute of Electrical and Electronics Engineers**
EAP	**Extensible authentication protocol**
PPP	**Point-to-Point Protocol**
VPN	**Virtual Private Network**
AES	**Advanced Encryption Standard**
RSA	**Rivest–Shamir–Adleman**
EHR	**Electronic Health Record**
CIA	**Confidentiality, Integrity, and Availability**
SLA	**Service-Level Agreement**
CLI	**Command Line Interface**
AAA	**Authentication, Authorization and Accounting**
BV	**Business Value**
POT	**Probability of occurrence of threat**

Chapter 1

Introduction

1.1 Overview

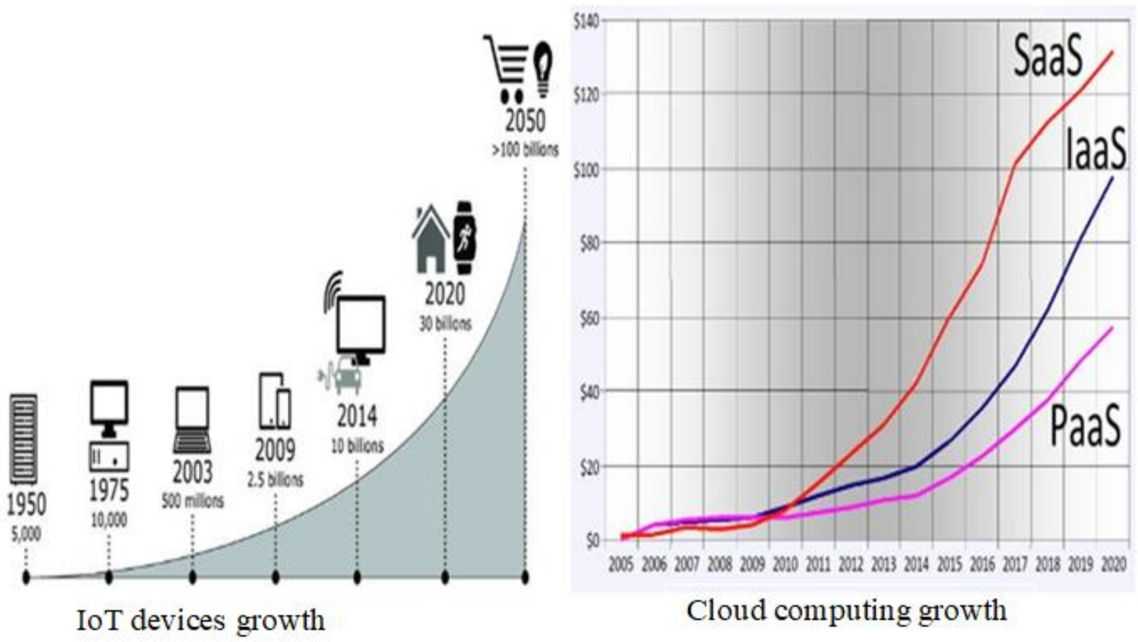
IoT is an emerging technology that is growing rapidly due to the automation of industries, including government and private sectors. In an IoT echo system, millions of devices are interconnected to store, process and communicate valuable information for real-time monitoring and decision-making [23]. It is further highlighted that IoT devices have limited storage, processing and computation resources. These devices often store and process sensitive data and information. However, due to IoT devices' storage and computation limitations, heavy security encryption cannot be effectively implemented on these devices for data security.

Cloud is an environment that guarantees the on-demand availability of data and resources. Further, cloud computing presents a pool of unlimited virtualized resources that end nodes can easily access and utilize. Therefore, to minimize computation and storage overhead, IoT devices are integrated with cloud computing, considered resource-rich infrastructure. By doing this, the resource limitation issues of IoT devices may be resolved up to the maximum level. On one side, this technological amalgamation brings comfort to human life and enhances the efficiency of IoT devices. On the other side, since the cloud operates in the public domain, this revolution becomes a potential threat to the security and privacy of data generated by IoT devices. Therefore, many security concerns arise due to cloud computing and IoT integration. Many researchers have contributed to the secure integration of cloud computing and IoT devices. However, there are rare evidences where access control, along with the minimization of many threats, is addressed in a single study. In this study, a novel solution, NAC has been proposed that can provide access control mechanism to cloud-based IoT systems. Furthermore, in addition to access control, the proposed solution can mitigate multiple threats to cloud-based IoT systems by integrating the same with third parties security solutions like Firewall, SIEM, AVs, and NIARA.

It is pertinent to mention that number of IoT devices connected to the internet was over 10 billion as per report published by “DataProt” in 2021. Similarly, there will be over 25 billion IoT connections by 2025, according to “GSMA Intelligence.” Furthermore, according to “Business Insider,” it is predicted that there will be 41 billion IoT devices by 2027.

According to “Cybercrime magazine,” the stored data on cloud will be over 100 zettabytes in 2025. A zettabyte is approx. equal to billions of terabytes (trillion gigabytes).

IoT and cloud computing growth estimated by Capra *et al*. [41] is given in figure 1.



IoT devices growth

Cloud computing growth

Figure 1: IoT devices and cloud computing growth [41]

1.2 Motivation and Problem Statement

To make people's lives easier, reliance on smart devices has increased exponentially [24]. Smart devices have limited resources in terms of processing and storage [25]. Therefore, heavy encryption algorithms cannot be effectively utilised on these devices to secure data. A viable solution is to integrate IoT devices with cloud computing, which is a resource-rich environment that guarantees the on-demand availability of data and resources. Presently, many Government and private sectors like health, transportation, agriculture, smart cities, LEA, etc., use cloud computing to process and store their IoT-generated data. Similarly, by integrating IoT devices and cloud computing, the attack vector is increased for the attackers. Leakage of such sensitive data can lead to damage on the organizational level or national level.

There is an exhaustive list of threats/ attacks to cloud-based IoT systems, such as unauthorized access, malicious node intrusion, account hijacking, DOS/DDOS, phishing attack, virus injection and information leakage. Researchers have provided mechanisms for access control that may or may not mitigate multiple threats that are faced by cloud-based IoT systems. However, the literature reveals that researchers have provided security solutions for a few threats/attacks. There is rare evidence where extensive minimization of many threats and access control is addressed in a single study. Therefore, a solution is required to provide robust access control to cloud-based IoT systems. In addition to access control, the solution must be capable enough to mitigate multiple threats faced by cloud-based IoT systems.

The proposed solution uses a novel technology NAC at the authentication layer and cloud layer (optional as per requirement and size of organization), which can provide a robust access control mechanism to cloud-based IoT systems that can also minimize the chances of multiple attacks faced by cloud-based IoT systems.

1.3 Research Objectives

Following are the main objectives of this research Study.

- To analyze the existing literature on the security of cloud-based IoT systems and their efficacy, considering all threats that are faced by cloud-based IoT systems.
- To propose a solution that can provide access control to cloud-based IoT systems and enhance the security of data by minimizing the chances of multiple cyber-attacks on cloud-based IoT systems.
- To demonstrate and test our proposed idea in a lab environment. Our lab environment will comprise of NAC solution, cloud/ Server PC, Switch, and devices (PCs/IoT devices/Laptops) to validate the proposed idea.

1.4 Scope of Research

The main focus of this research is to provide access control mechanism along with mitigation of a few threats to cloud-based IoT Systems. In this study, the authors used cloud infrastructure, NAC solution, switch, 3 x Cameras and 1x PC to implement and test the proposed idea in a real environment. Further, the proposed idea can mitigate many threats to cloud-based IoT systems if an organization has the access license, onboard license and on-guard license for the NAC solution. In this study, the NAC solution with only an access license has been implemented to produce the results. It is highlighted that the access control mechanism and mitigation of few threats to cloud-based IoT systems can be achieved using the Access License of NAC. However, to mitigate many threats to cloud-based IoT systems, there is a requirement for Onboard and on-guard licenses of NAC solution. It is pertinent to mention that mitigation of many threats to cloud-based IoT systems could not be simulated due to the unavailability of Onboard and on-guard licenses for testing the purposed in the lab.

1.5 Contribution

The following contributions are made through this study.

- This thesis proposes a strong access control and authorization mechanism that can enhance the security and privacy of IoT data in cloud-based IoT environment. A novel NAC solution has been proposed for the authentication and authorization of IoT devices in cloud-based IoT environment.
- The existing threats are studied and keeping these threats under consideration, the proposed solution is analyzed. The proposed solution is simple to implement and can provide access control to cloud-based IoT systems and mitigate multiple threats that are faced by cloud-based IoT systems.

1.6 Significance of Research

Pakistan is undergoing through digitization of various Govt and Private sectors including military and LEAs. Moreover, IoT is an emerging technology used in different govt and private sectors to bring automation and real-time analysis of processes. These IoT devices generate a considerable amount of data in a millisecond. With the passage of time, processing and storing such a massive amount of digital data would be a challenge for Govt and private sectors due to the limited storage and computation processing of IoT devices. Therefore, organizations are shifting their services to cloud infrastructure in order to get the benefit of unlimited resources of the cloud.

Presently, many organizations and even Pakistani citizens use cloud services for their day-to-day business activities [26]. Cloud computing has unlimited resources in terms of computation, processing and storage. Therefore, data generated by IoT devices deployed in different Govt and private Sectors can be stored and processed on the cloud side.

It is pertinent to mention that confidential data is transferred from IoT devices to the cloud which needs proper security mechanisms to ensure confidentiality, integrity and availability of the data. Therefore, the security of such type of sensitive information is considered paramount. The proposed solution provides access control mechanism to cloud-based IoT systems and can minimize cyber-attacks on cloud-based IoT infrastructure.

1.7 Thesis Organization

The thesis is structured as follows:

- **Chapter 1** covers the introduction part of the thesis that enlightens/highlights the problem statement, research objectives, thesis scope, and its contribution.
- **Chapter 2** is dedicated to essential concepts that cover introduction to IoT, cloud computing and NAC.
- **Chapter 3** covers the research methodology that explains how the research is carried out.
- **Chapter 4** covers various threats that are faced by cloud-based IoT systems.
- **Chapter 5** covers existing literature regarding access control mechanisms and the security of cloud-based IoT systems. This chapter also highlights the limitation of the existing literature.
- **Chapter 6** presents the threat modeling that assists the authors in identification of assets, threats against each asset, rating these threats and mitigation strategies in cloud-based IoT systems.
- **Chapter 7** describes the implementation of the proposed idea in real cloud-based IoT environment. The implementation tools used to establish a cloud-based IoT environment for testing have been presented/ illustrated in this chapter.
- **Chapter 8** concludes the reporting part of the research/ thesis and proposes a future research direction. Figure 2 shows the thesis structure.

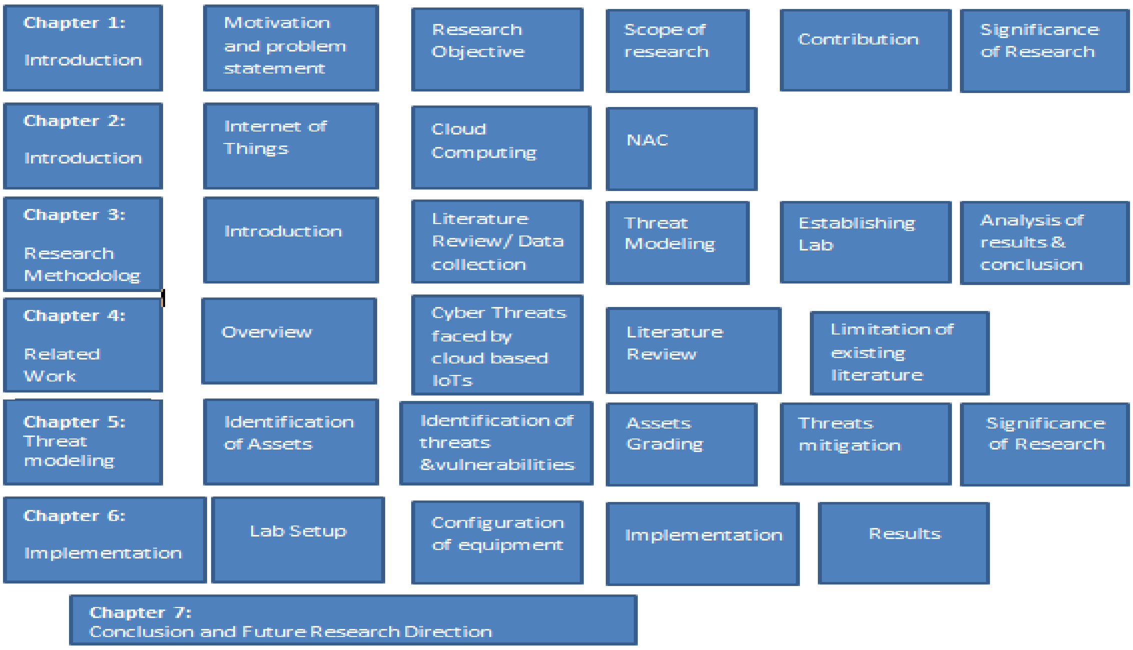

Chapter 1: Introduction
Motivation and problem statement
Research Objective
Scope of research
Contribution
Significance of Research
Chapter 2: Introduction
Internet of Things
Cloud Computing
NAC
Chapter 3: Research Methodolog
Introduction
Literature Review/ Data collection
Threat Modeling
Establishing Lab
Analysis of results & conclusion
Chapter 4: Related Work
Overview
Cyber Threats faced by cloud based IoTs
Literature Review
Limitation of existing literature
Chapter 5: Threat modeling
Identification of Assets
Identification of threats &vulnerabilities
Assets Grading
Threats mitigation
Significance of Research
Chapter 6: Implementation
Lab Setup
Configuration of equipment
Implementation
Results
Chapter 7: Conclusion and Future Research Direction

Figure 2: Thesis Structure

Chapter **2**

Preliminaries

2.1 Introduction

This chapter presents key technologies, i.e., IoT, cloud computing, NAC, importance of IoT and cloud computing, integration of IoT and cloud computing, and the associated security concerns. This chapter also covers the advantages and disadvantages of IoT and cloud computing. Further, cloud computing service models and deployment models have also been discussed. The last part of this chapter covers NAC and its working methodology that can make readers able to understand these technologies and their associated issues.

2.2 IoT

IoT is a system of interrelated devices and people connected to the internet to transfer and receive data from one device to another [27] [29]. Smart home is the best example of IoT. In a smart home environment, home appliances like AC, doorbells, thermostats, fire detectors, water heaters, and security alarms can be interconnected through the internet to share data with users over the internet. When things like door locks, cars, tea maker, cameras, AC and heaters are connected to the internet, this platform is called IoT. For example, if your alarm goes on in the morning, the IoT system opens the window blinds, turns on the coffee machine and turns on the water heater, which is fascinating. Another real-time example is if you want that your room must be chilled before you reach your room, then you can turn on your AC from your office using IoT.

Furthermore, if you want that tea must be ready prior you reach home; this can also be possible using the IoT platform. Even you can lock/unlock the doors of your home from a remote location as per your requirement. Moreover, based on mobile location, locking and unlocking of a user's home can be performed using IoT devices. This platform provides easy tracking, controlling appliances and monitoring things installed at your home. In short, we can say that IoT is shaping the way we live or lives.

IoT devices are being used to resolve many real-world issues, including but not limited to traffic jamming, economic growth, safety and security of the public, smart homes, agriculture, smart cities and health sector [29]. Currently, IoT devices are being used by military commanders to collect battlefield information in advance to move troops accordingly. Moreover, military and LEAs use IoT devices for inventory management, target recognition, autonomous reconnaissance, transportation, etc.

Another best scenario is where IoT can be deployed for real-time information collection, analysis of information, monitoring of the current status of activities and decision making. Suppose a patient is at home and the current patient status is monitored by a monitoring system using sensors fitted on the patient body [30]. All patient information is stored in the cloud. Suppose any abnormality in a patient's body, like an increase in heartbeat or excretion of fluids, is observed. The same is communicated to the cloud for storage and the cloud is further connected to the hospital. Information related to patient will be passed on to the hospital. Doctors at hospital can know about the patient's previous history and current status without physically examining him. Doctors can identify what problem the patient has and even send an ambulance to the patient location to bring the patient back to the hospital.
Meanwhile, doctors can make ready operation theater, medicine and other requirements to treat patients promptly before they arrive at the hospital. The same brings transparency and reduces many efforts to treat patients without delay. Figure 3 shows cloud-based healthcare information system.

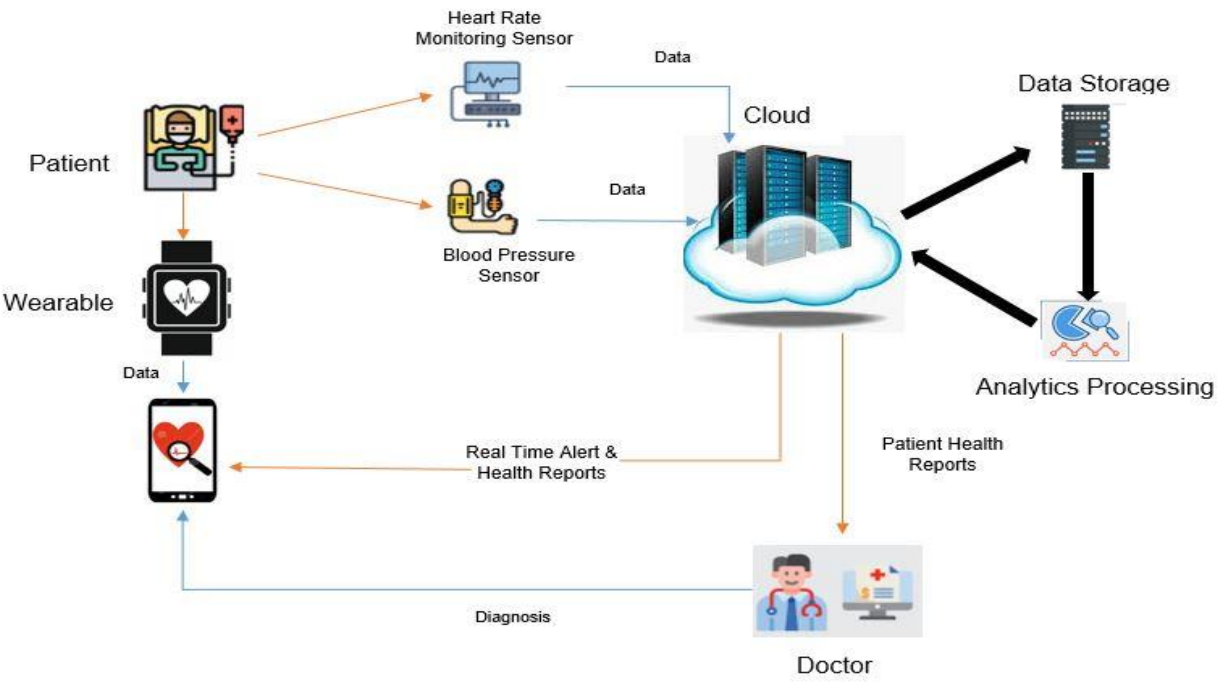


Figure 3: Healthcare system based on cloud-based IoT

The integration of IoTs with cloud computing, machine learning and AI is a way for new exciting innovations [28]. It is pertinent to mention that the manufacturer has kept the security of IoT devices as the least priority. Therefore, organizations put efforts into making the security of IoT devices harder by implanting various third parties security solutions during the deployment in actual environment. On one side, IoT devices bring ease and revolution to human life. However, on the other side, many security concerns are associated with IoT devices, like hackers can use IoT light bulb for massive cyber-attacks. Therefore, more attention should be given to security and privacy before deploying IoT devices in organizations.

In the context of IoT devices, hardware can be classified into two main components i.e. general devices and sensing devices. General devices are the main component of the data hub and information exchange which is connected by wired or wireless interface. Home appliances are typical examples of such devices. On the other side, the sensing devices include sensors and actuators. They measure humidity, temperature, light intensity etc. These IoT devices are connected to the network through gateways. These gateways collect information from sensors and devices and transfer the same to the cloud. Pictorial representation is given in figure 4.

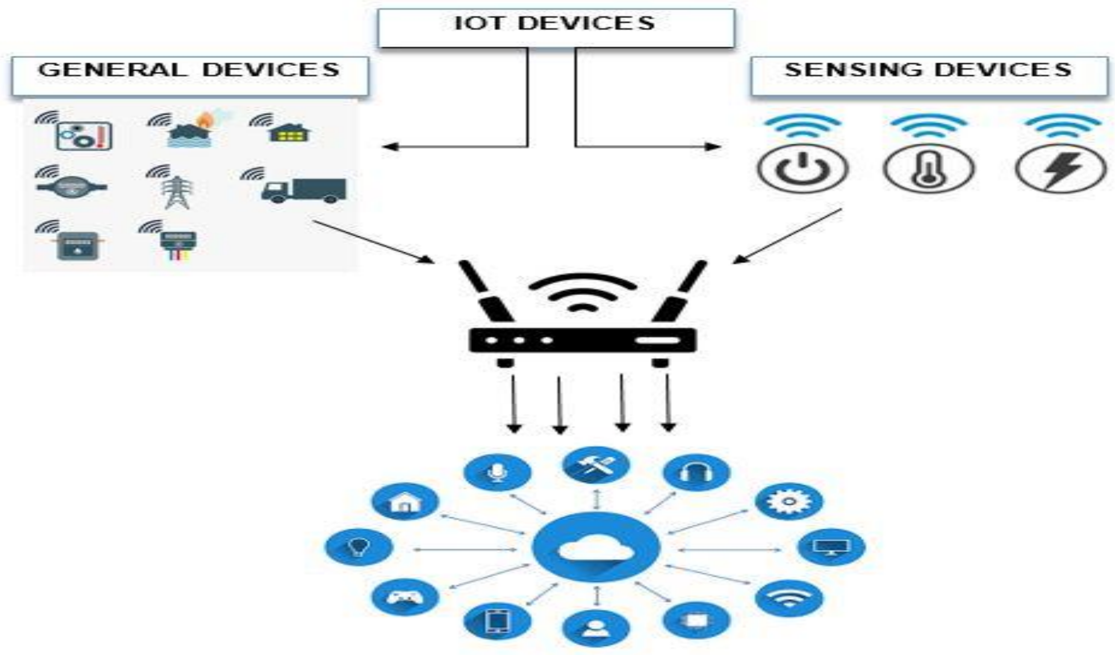


Figure 4: Hardware classification of IoT

In a cloud-based IoT environment, end device management is essential. End devices generate massive data, so we should know which data comes from which device. Suppose we send signal to the cloud to power on AC; a security mechanism/ secure channel must restrict unnecessary and malicious traffic from moving on the network toward the cloud. There is a requirement to ensure data security during transit from device to cloud and vice versa. If an organization does not know which data is coming from which device, this is considered system/ platform failure.

End point management helps us to manage devices, end point identity, meta data and overall life cycle involved. It helps us to identify from which device data is coming and what action is required to be undertaken.

2.2.1 <u>Advantages and disadvantages</u>

IoT devices have multiple advantages, including but not limited to the following:

- Minimize human efforts
- Save time and money
- Efficient utilization of resources
- Improving the quality of life,
- Better monitoring of human appliances connected to IoT network,
- Ability to access information from anywhere

With the advantages mentioned above, the following are some disadvantages associated with IoT devices:

- Lack of security and privacy
- An easy target for attackers due to lack of built-in security
- Lack of memory
- Lack of processing
- Lack of storage
- Complexity
- Increasing unemployment
- Technology takes control of our life
- Compatibility

2.3 Cloud Computing

Cloud computing presents a pool of unlimited virtualized resources that end users can easily access and utilize [31]. It also guarantees the on-demand availability of data and resources to end users. Further, Cloud Computing is the delivery of computing services to the customer including servers, storage, databases, networking, software, analytics and intelligence over the internet.

Currently, organizations are shifting/ storing their data on the Cloud, which can lower the operating cost, infrastructure cost, Technical HR cost and maintenance/troubleshooting cost of organizations because organizations only pay for services they are using. The other issue associated with maintaining/ keeping own IT infrastructure for data storage and processing is upscaling and downscaling, which increases organizations' expenditure.

It is pertinent to mention that a considerable amount of data is generated by organizations on a daily basis to run their daily business routine. This data is either stored on local premises or on the cloud. If an organization opts for local data storage, the cost of IT infrastructure, Monitoring of IT assets and trained HR along with dedicated space are required. This creates unnecessary burdens on organizations and deviates from the organization's main objective and business. The alternate solution to store and process their data is on a cloud which guaranty the on-demand availability of data and resources when and where required. Therefore, organizations prefer to store data in the cloud. So we can say that in this modern and digital era, organizations, IoTs and cloud computing is interconnected. Major cloud services providers in the market are Amazon web services, Google cloud platform, Digital Ocean, IBM cloud, Micro soft azure and Terre mark. Figure 5 shows the features of cloud computing.

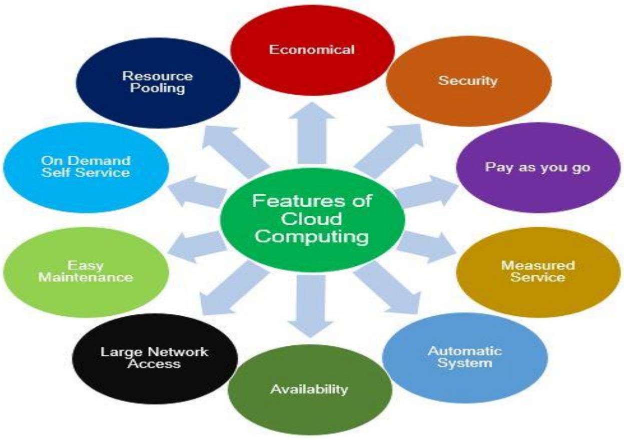


Figure 5: Features of cloud computing

CSPs offer different service models as per company/ user requirements. It is highlighted that these requirements (security, storage, cost, processing, privacy etc.) vary from organization to organization. The detail of the cloud service models is as under:

2.3.1 Cloud Computing Service Models

CSPs offer cloud computing services in three different service models [32]. Each service model fulfills a unique set of company business requirements. Figure 6 shows a pictorial representation of cloud computing service models.

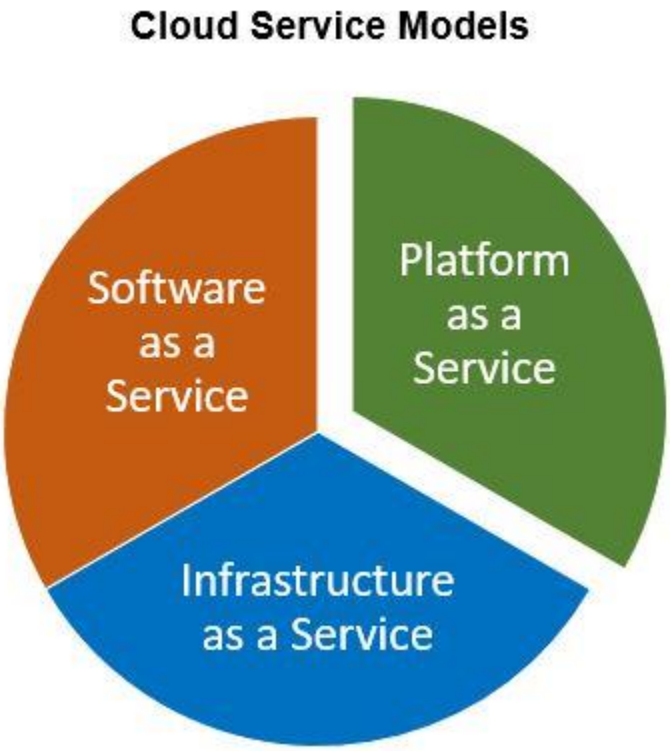


Figure 6: Cloud Service Models

2.3.1.1 SAAS

SAAS is a cloud computing service model that delivers services and applications over the internet, as shown in Figure 7. In this model, the CSPs undertake maintenance of hardware and software. Control of the end user is restricted, and the end user can only access the required service hosted on Cloud infrastructure. Organizations that only required specific service/

services over the internet usually opted for this model because the same reduces cost (pay as per use) of hardware and software maintenance. End users usually use this service. Some benefits of the SAAS model are as under:

- It can be scaled up and scaled down
- SAAS is a platform-independent solution. We can use android, MAC, windows etc., to access services.
- Accessible to users anytime and anywhere.
- It reduces time as we can use applications directly from a browser.
- Examples are drop box, office 365 and Gmail etc.

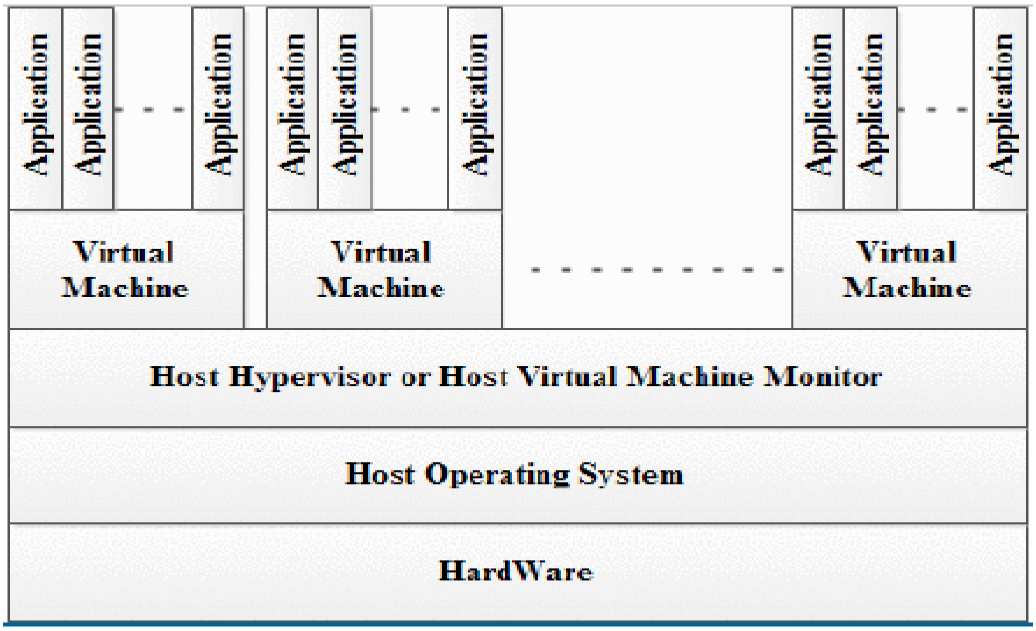


Figure 7: SAAS architecture implemented using virtualization [13]

2.3.1.2 PAAS

PAAS service model provides platform and environment (run time environment) to developers for building applications and services over the internet. The same also provides development and deployment tools to developers that are required to develop applications and services. PAAS gives more control to the user as compared to SAAS. In this model, a user does not have any control over cloud computing infrastructure. Further, no control over cloud infrastructure including network, servers, OS, or storage, is provided to the user. The user has only control over the deployed application and configuration setting. Developers usually use this service. Some benefits of the PAAS model are as under:

- It can be scaled up and scaled down
- Cost-effective (Pay as per use)
- No need to purchase expensive servers, software and storage
- The vendor manages software (license, update etc.)
- Examples are force.com, Google app engine, windows azure

Figure 8 depicts the various services (green box and arrow) offered by PaaS to CSC. The remaining services are applications and data that are considered the responsibility of CSCs.

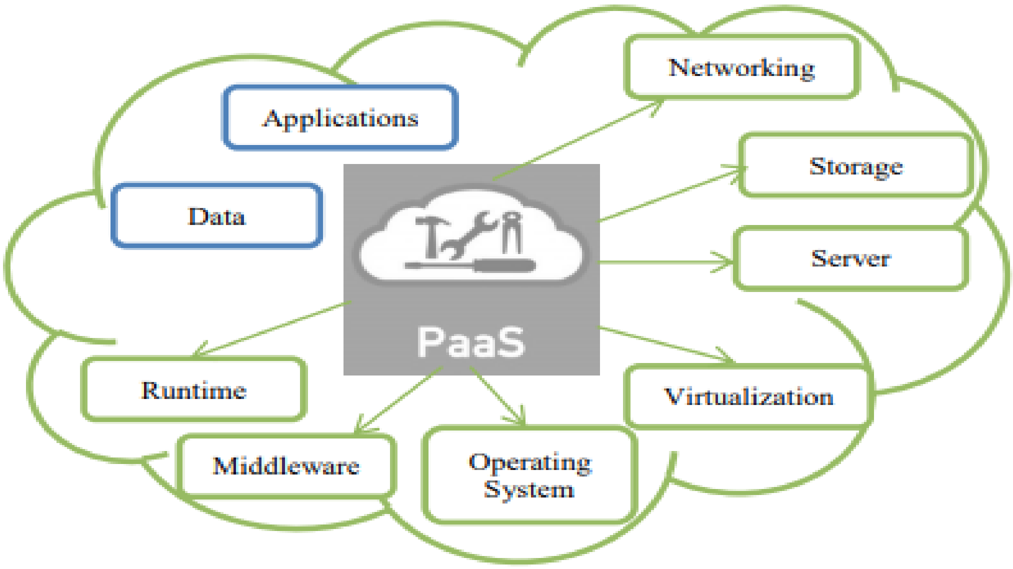


Figure 8: PaaS architecture [13]

2.3.1.3 IAAS

IAAS service model provides complete infrastructure, including underlying operating system, networking, servers and storage etc., for developing applications. The same provides access to essential resources in cloud environments such as virtual machines, virtual storage, etc. In this model, users have complete control over resources. System administrators and network architects use this model. Some benefits of this model are as under:

- Complete control over computing resources through administrative access to virtual machines
- Can scale up and scale down
- Cost-effective (Pay as per use)
- Examples are Google cloud, IBM Cloud, Oracle cloud infrastructure and AWS (AWS—Compute—EC2)

Figure 9 shows the services (the red box and arrow) offered by IaaS to CSC. In this service model, CSP provides resources shown in red boxes to CSC. The remaining services are considered CSC's responsibility.

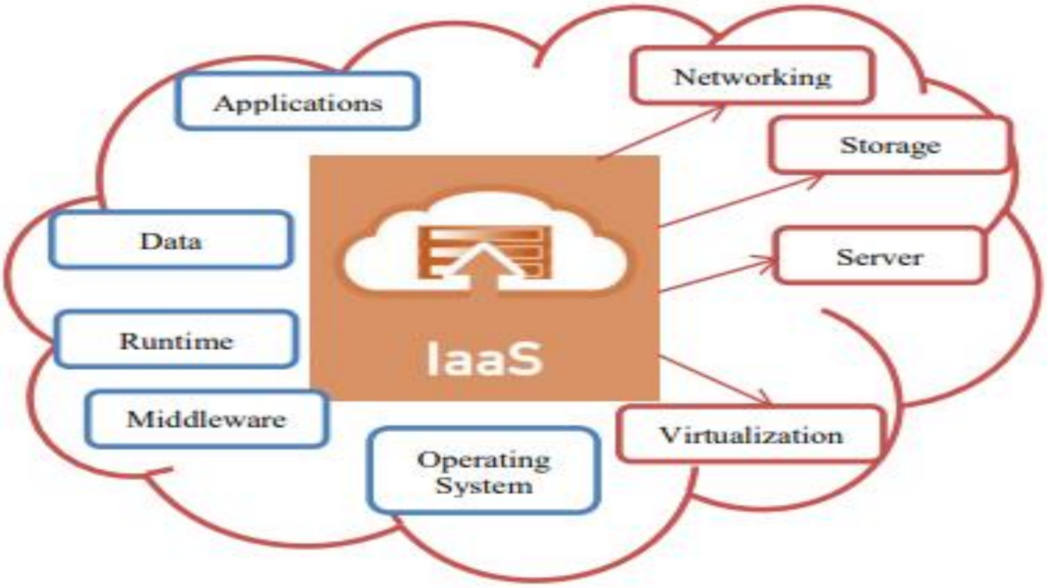


Figure 9: IaaS architecture [13]

2.3.2 Cloud Deployment Models

According to NIST, there are four cloud deployment models i.e. public cloud, private cloud, community cloud and hybrid cloud [33][34]. The cloud deployment model defines how much data organizations want to store and who has access to the cloud infrastructure. The selection of a cloud deployment model before shifting to cloud infrastructure is considered essential for any organization. The cloud deployment model defines the location of a server you are using and the controlling authority of cloud infrastructure. Figure 10 shows cloud deployment models.

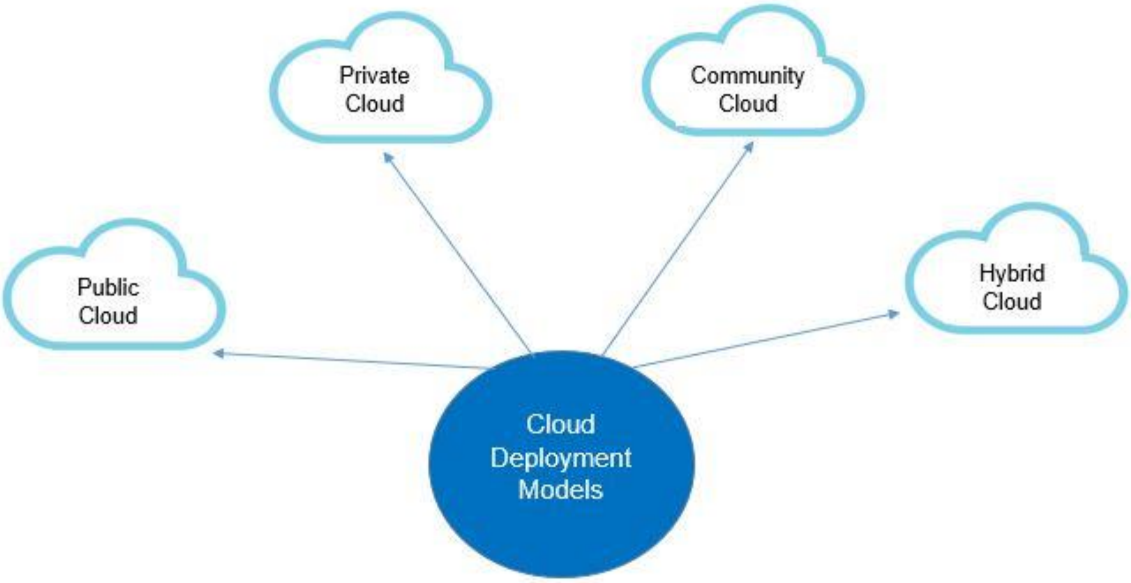


Figure 3: Cloud deployment models

2.3.2.1 Public Cloud

The public cloud is available to all users for storing and accessing information (system and services etc.) over the internet, as shown in Figure 11. It is less secure and less customizable as compared to other deployment models. In this type of cloud, the infrastructure is controlled and managed by entities (CSPs) that provide services and not by end users. The public cloud is based on a multi-tenancy concept i.e. resource is shared amongst multiple users.

Some advantages include but are not limited to the following:

- Maintained by the third party
- Location independent
- High scalability (as Gmail provides 15 GB space. The same can be increased as per organization requirement)
- Cost-effective (Pay as per use)
- Examples are Google drive, drop box etc.

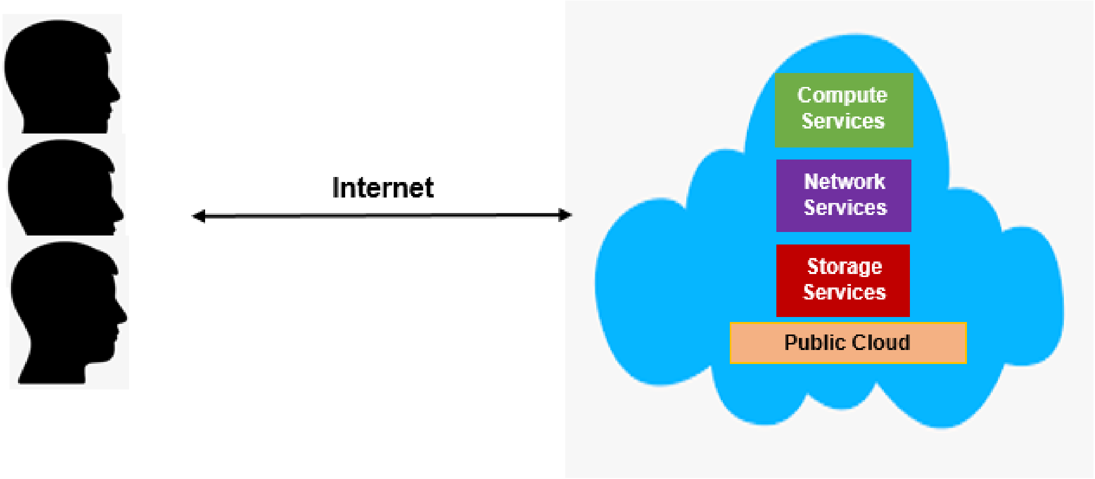


Figure 11: Cloud deployment models

2.3.2.2 Private Cloud

The private cloud belongs to a specific organization and services are only accessible within an organization. The organization or a third-party service provider manages the private cloud. Organization that wants greater control over data and resources usually opt for private cloud. Private cloud is customizable and is generally used by sensitive organizations including military and LEAs. Figure 12 shows private cloud computing.

Advantages

- High security: Information does not flow out of the organization
- Data Privacy: Only legitimate users can access data
- More customizable: can be customized as per company requirement
- Supports legacy systems

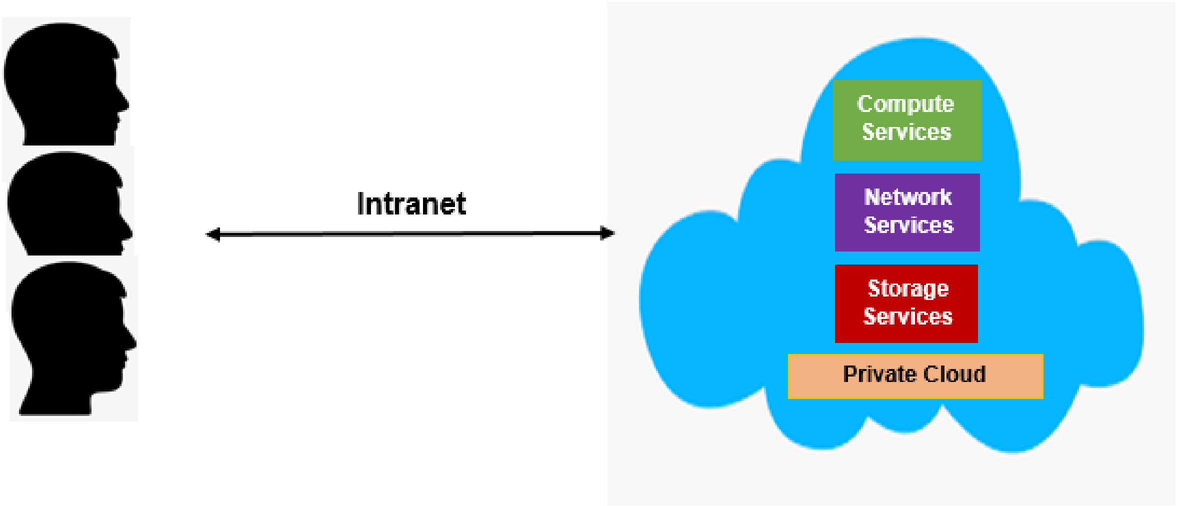


Figure 12: Private cloud

2.3.2.3 Community Cloud

The community cloud facilitates multiple organizations belonging to a community to share resources and information with each other. Community cloud is considered the best choice for a department like police department within a country and universities collaborating in a specific area of research etc. It is pertinent to mention that access to community cloud is restricted to a community only. Figure 13 describes the pictorial representation of the community cloud.

Advantages

- Cost-effective: community cloud is shared by multiple organizations or communities
- Security: provide better security compared to the public cloud
- Shared resources: Allow to share resources with multiple organizations or communities
- Collaboration and information sharing: viable solution for sharing information and collaboration amongst multiple organizations or communities.

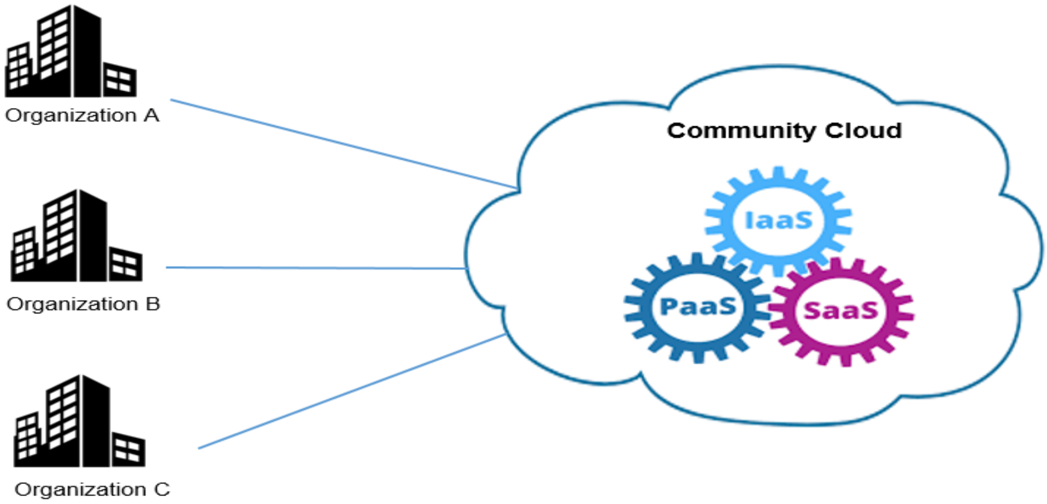


Figure 13: Community cloud [17]

2.3.2.4 **Hybrid Cloud**

In a hybrid cloud, the public cloud, private cloud and on-premises IT infrastructure are combined to achieve a single, cost-effective and flexible infrastructure, as shown in figure 14.
If an organization requires both public and private cloud features in parallel, then a hybrid cloud is considered the best choice. Critical and sensitive activities are performed on the private cloud, whereas normal/noncritical activities are to be performed on public cloud. For example, if an organization wants to show some non-critical information to general public, it will use the public cloud. Similarly, if they want to hide sensitive information from general public, then the same will be processed on public cloud. Some advantages of hybrid cloud are as under:

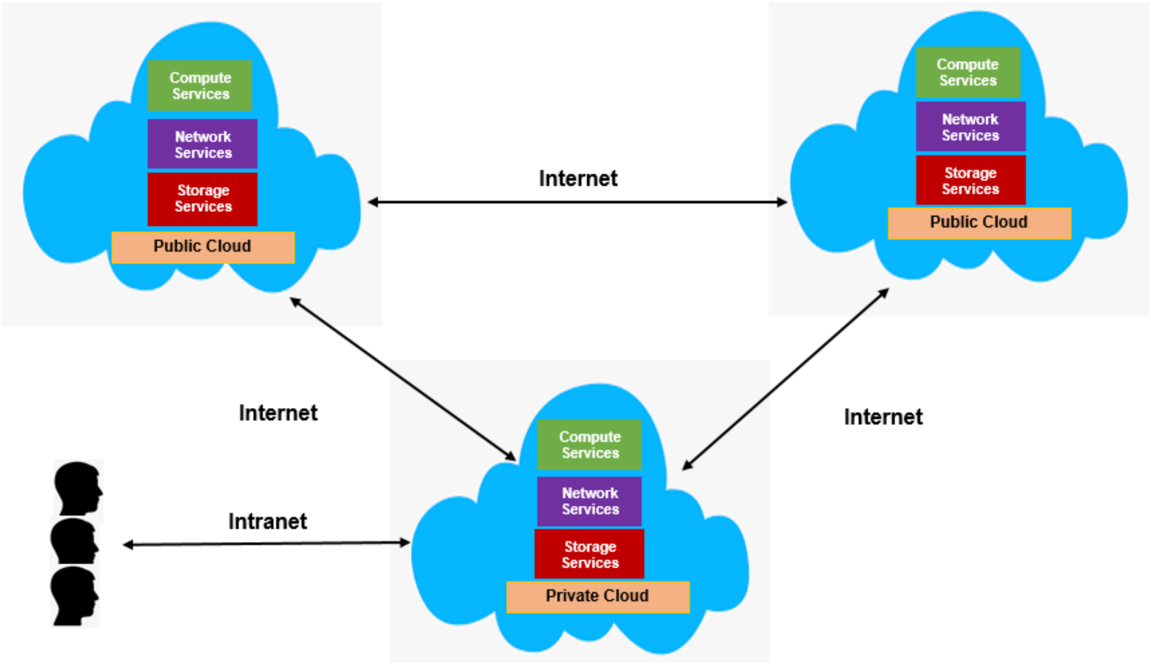


Figure 14: Hybrid cloud

Advantages

- Scalability: Increase or decrease of IT resources as per requirement.
- Security: Provide better security compared to public cloud.
- Low cost as compared to private cloud
- Flexibility: Cloud computing enables organizations to scale up/ down storage and other resources per their requirement.

2.4 NAC

NAC allows organizations to prevent unauthorized devices from accessing network resources, ensures that all connected devices are identified, classified, and authorized, and provides policy-based access control to achieve the maximum level of cyber security. IoT devices, whether deployed in manufacturing, health sector, or any other organization including LEA and defense, are overgrowing and work as supplementary entry points for attackers to penetrate company-sensitive networks. NAC can reduce these risks by applying defined profiling and access policies for various device categories. Furthermore, NAC can be integrated with third parties security solutions like Firewall, SIEM, AVs, and NIARA to detect threats and provide remedial actions.

In the IoT context, cyber attackers are aware of the growing and vulnerable nature of IoT devices, which organizations and manufacturers give little attention during design and development [35]. Therefore, attackers design and launch sophisticated attacks against organizations backbone networks and information systems using IoT devices [36]. NAC has certain benefits including but not limited to controlling unauthorized end nodes entering the organization's network, restricting applications and resources from unauthorized users, detecting any malicious activity in the network and providing a timely response. NAC also permits third parties (contractors, vendors, partners, guests) to access the organization network as required. However, their access can be controlled and restricted. NAC can generate reports covering malicious network activities for different decisions.

In this digital world, it is challenging for the network administrator to identify malicious nodes entering the organizational network. Therefore, NAC is a suitable solution to control and restrict any malicious node joining the organization's network. Only those legitimate devices will be permitted to enter network that fulfills network and organization requirements.

It is pertinent to mention that NAC is unlike a firewall. A firewall only provides perimetric security/ protection; however, NAC monitors and controls all activities inside a company network. For example, a firewall can stop an attacker from Russia to enter a network in Pakistan. Contrary to this, NAC can prevent and restrict attackers from malicious activities inside your organization.

It may also be highlighted that NAC is not a complete security solution. However, it is considered the central part of an organizational security plan that can strengthen the security of networks and information systems. Furthermore, NAC is not considered a replacement for a firewall but it has been observed that most data breaches and information theft occur behind firewalls. Therefore, NAC plays significant role in multi-layered security. Clearpass, Genians, Forescout, FortiNAC etc. are a few examples available in the market.

2.4.1 NAC Architecture

NAC can be deployed either in pre-admission or post-admission mode.

2.4.1.1 Pre-admission

In pre-admission mode, NAC acts like a gatekeeper and verifies each device before accessing the network. NAC verifies credentials, attributes and compliance with organizational policies of the requesting device and grants or denies access subject to verification of said prerequisites. In this mode, NAC blocks any rough or malicious devices that NAC does not recognize as per the organization's policy.

2.4.1.2 Post-admission

In post-admission mode, NAC inspects devices and restricts them for what they are permitted to do**.** The same can be done by placing users into specific VLANs and restricting them to specific applications/ services. Post-admission mode can also log network operations for analysis and auditing to verify compliance with organizational policies and standards.

It is pertinent to mention that all NAC solutions have a pre-admission mode, while all NAC does not have post-admission feature. Organizations must decide whether they need pre-admission NAC or pre-admission NAC plus post-admission NAC.

2.4.2 Internal working of NAC

2.4.2.1 802.1X-based

IEEE 802.1X is the IEEE standard to authenticate devices before joining an organization network. It ensures network security and access control for end-point devices. Primarily the available NAC solutions are based on IEEE 802.1X standard. It is pertinent to mention that 802.1X provides access control mechanism (accept/ reject) to the device subject to verification of credentials. 802.1X can be used for both wired and wireless communication.

The device's credential is forwarded to NAC (Radius Server) through a switch during the NAC verification process. Upon receipt of credentials by NAC (radius server), the same is verified and requesting device is either granted access or denied to join the company network.

802.1X uses EAP (extensible authentication protocol) that can support number of authentication mechanisms such OTPs, Security Certificates and public key authentication. EAP is a framework that provides extensibility for authentication mechanism for secure network access technologies like IEEE 802.1X-based wireless access, IEEE 802.1X-based wired access and PPP connections such as VPN.

The main disadvantage of NAC-based 802.1X is that all switches installed in the organization should be upgraded to support 802.1X.

NAC may be endpoint-based or network based. In endpoint-based NAC, software (agent) must be installed in all connected devices such as PCs, laptops etc. The agent collects device information and sends it to the NAC policy server. The drawback of endpoint-based NAC is that agents do not work on all end devices and operating systems such as smartphones, printers, IoT etc. However, this limitation up to a certain extent can be overcome by using a browser-based dissolvable agent.

Network-based NAC relies on network scans for the discovery of connected devices. Information about the connected devices is gathered and shared with the NAC policy server. This method is a viable solution for networks comprising nodes that do not support agents.

2.5 Integration of IoT with Cloud Computing

The IoT allows billions of devices to connect, communicate and share information, bringing ease and comfort to human lives [18]. Currently, a high rise has been observed in the deployment of IoT devices in health sector, agriculture sector, transportation, smart homes, smart cities, critical industries, military and LEA etc. As already mentioned in this study, the use of these devices is, however, strained due to limited resources in terms of storage, computation, and processing. Therefore, heavy encryption for information security and analysis/processing of information at IoT nodes is difficult to be processed. To overcome the limitations, cloud computing as a resource-rich technology may be integrated with IoT devices to maximize output and utility, as shown in figure 15. However, many security concerns like malicious node intrusion, virus injection, authentication issues, hijacking etc. arise after the amalgamation of cloud computing and IoT devices.

These security concerns, like authentication and mitigation of threats, have been addressed in this research study.

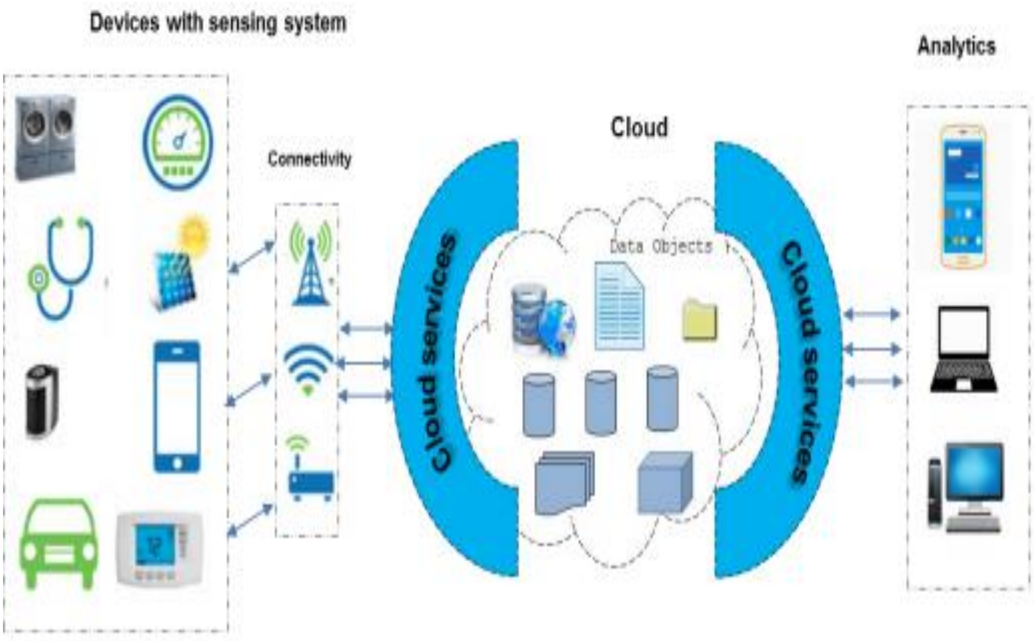


Figure 15: Cloud-based IoT environment [42]

2.6 How NAC can enhance the security of cloud-based IoT infrastructure

NAC provides access control, visibility and compliance to organization policies and standards that ensure the security of information and network infrastructure of organizations. A NAC solution can grant network access to only compliant devices and deny network access to noncompliant nodes. Noncompliant devices are placed in a quarantined area or granted only restricted access to resources, thus keeping malicious nodes away from the company network.

In this study, the NAC solution has been used for securing cloud-based IoT environment. A NAC solution has been used for the authentication of IoT devices prior to accessing cloud infrastructure. The proposed solution can provide access control to cloud-based IoT systems and mitigate multiple threats that are faced by cloud-based IoT systems.

Devices that intend to join network will pass through the NAC solution. NAC will either grant or deny access requests of the device to network after verification of credentials and device profile as shown in figure 16. Moreover, NAC solution with an on guard license verifies the client's health status before joining the network. Updated AV on device, default password, latest patches, etc., is checked by NAC on guard before joining network.

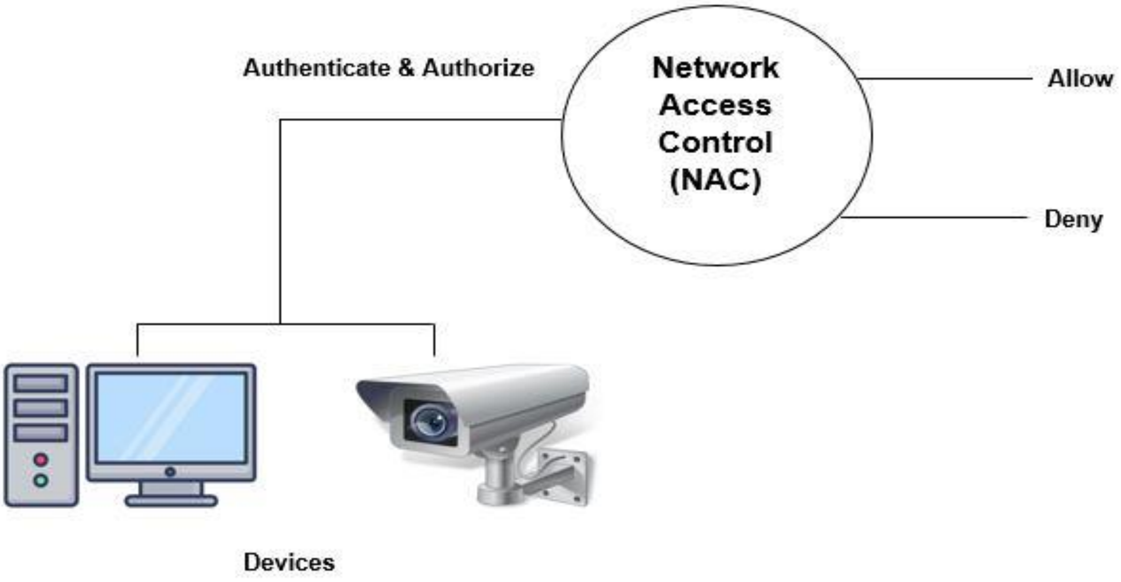


Figure 16: Access control by NAC

2.7 Summary

Detail of essential concepts/ technologies (IoT, cloud computing, and NAC) has been covered in this chapter. This chapter informs readers about the technologies being used/ discussed in this study. The next chapter will cover the research methodology adapted throughout this study.

Chapter 3

Research Methodology

3.1 Introduction

This chapter covers the research methodology adopted in this research study. All components involved in this research, including but not limited to the literature review, threat modeling, equipment used, establishing lab environment and testing the proposed solution, etc., have been mentioned in this chapter.

The objective of this study is to enhance the security of cloud-based IoT systems by providing a robust access control mechanism that can also mitigate multiple threats faced by cloud-based IoT systems. Furthermore, the study's objective has been verified by implementing the proposed idea in a real cloud IoT-based environment. Figure 17 shows the process followed in conducting the research.

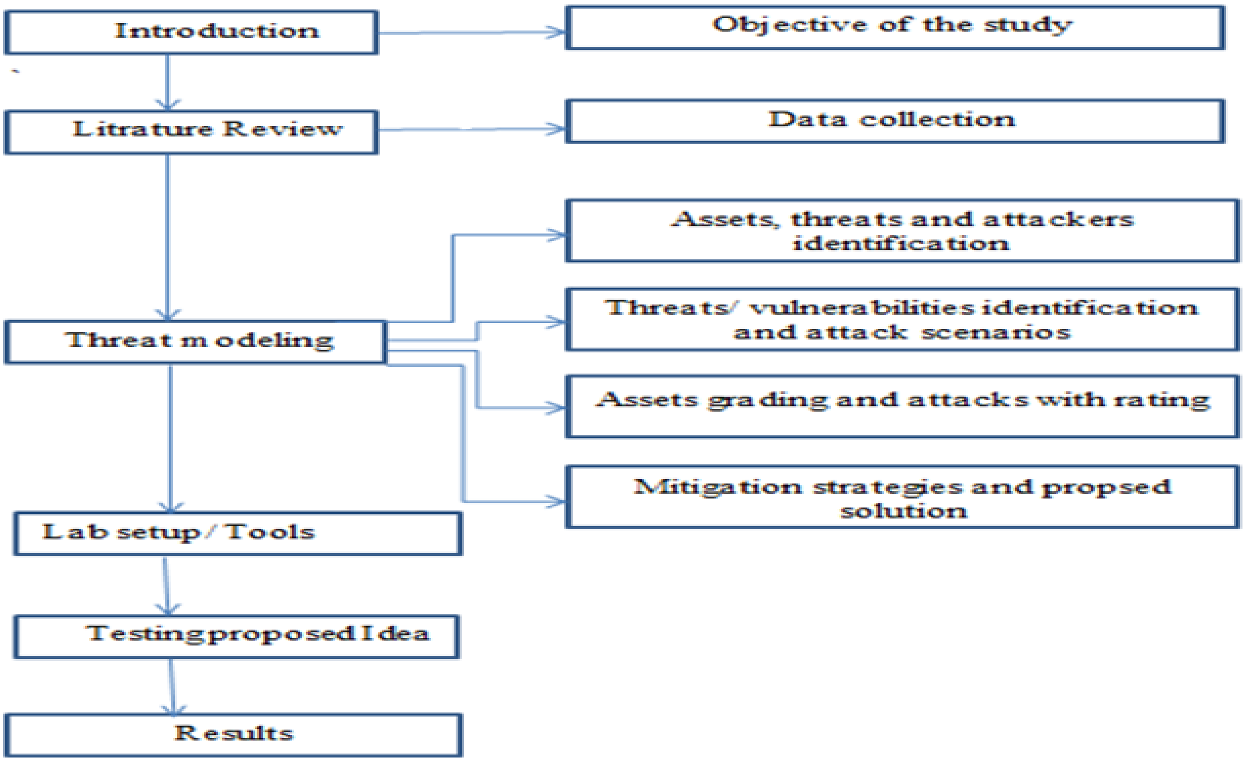

Introduction
Objective of the study
Litrature Review
Data collection
Assets, threats and attackers identification
Threat modeling
Threats/ vulnerabilities identification and attack scenarios
Assets grading and attacks with rating
Mitigation strategies and propsed solution
Lab setup / Tools
Testing proposed Idea
Results

Figure 17: Research process

3.2 Literature Review - Data collection

A thorough literature review has been conducted to identify such areas in cloud-based IoT systems that need more focus and attention. Different research studies regarding the secure integration of cloud computing and IoT have been studied. Furthermore, literature review regarding challenges and security concerns arises after the integration of cloud computing and IoT has been carried out. Finally, the author has chosen the area "access control mechanism" for further research which is considered the most vulnerable area in cloud-based IoT systems. Moreover, it has been deduced from existing literature that there is a requirement to extend existing research on access control mechanisms regarding the security of cloud-based IoT. Based on studying existing literature, the authors proposed a novel solution that can be used to provide an access control mechanism to cloud-based IoT systems. The proposed solution can also mitigate multiple threats that cloud-based IoT s systems face. The thesis written by the authors is based on scientific research papers, online material, journals, etc.

Based on the literature review, an analysis was carried out to identify the main concepts, terminologies, resources and mechanisms used by other researchers. This information extracted from existing literature has been used to propose an alternate solution for enhancing cloud-based IoT security. The following steps were involved while reviewing the literature [21]:

a. Keyword identification for the topic.

b. List creation of terms for searching.

c. Information gathering related to the topic in search engines, online research papers, databases, etc.

d. Modification of list of terms and repetition of step c.

3.3 Threat modeling

Threat modeling is considered essential to further deep dive and get knowledge about all threats that cloud-based IoT systems may face. We usually hear manufacturer claim that their product is secure. However, there is a requirement to justify and verify the claim made by the vendor, which is considered hard. Before claiming a system's security, identification of all threats to the system is very important. Listing all threats and their severity may help researchers to propose a suitable solution for the issue [22].

In order to conduct the research smoothly and enhance the security of cloud-based IoT systems, threat modeling has been carried out. The following have been identified that assist the authors in proposing a suitable solution that enhances the security of cloud-based IoT systems.

- Asset identification
- Actors
- Attackers
- Threat and vulnerabilities identification
- Attack scenarios
- Asset grading
- Attacks grading
- Mitigation strategies

Considering all threats, the researchers have proposed a solution that provides access control mechanism to cloud-based IoT systems, which can also mitigate multiple threats.

3.4 Establishing Lab (Equipment Used)

The authors' claim to enhance the security of cloud-based IoT systems by providing access control and mitigating multiple threats has been validated in the lab environment. The following tools/equipment were used in the lab.
Cloud infrastructure

- Switch
- NAC solution with access license
- IP Camera 1
- IP Camera 2
- IP Camera 3
- Laptop
- PC

It is highlighted that the proposed solution was tested in the account of the devices mentioned above in different scenarios (explained in the implementation phase).

3.5 Analysis of the result

After establishing the lab environment like cloud-based IoT, the proposed solution is tested for Cameras (1,2, and 3), laptop, and PC. It has been observed that the proposed idea is working fine, and the claim is found valid. The results are included in the implementation chapter of this thesis document.

3.6 Summary

This chapter covers an overview of all activities undertaken to conduct this study. In this chapter, the research methodology that has been adopted is highlighted. The next chapter covers threats to cloud-based IoT systems.

Chapter 4

Related Work

4.1 Overview

In recent years, organizations have shifted their businesses, data and applications to cloud infrastructure [16]. Resultantly, cloud-based IoT systems become more lucrative for cyber attackers. Cloud computing can be used in cloud-based IoT Systems to store and process IoT data. It is pertinent to mention that cloud computing is a resource-rich infrastructure that guarantees on-demand and timely access to services and data to users and organizations. Therefore, to overcome IoT storage and processing limitations, Cloud computing is considered a viable solution for storing and processing considerable amounts of data produced by IoT devices. Figure 18 shows some common cyber-attacks that are faced by cloud-based IoT systems:

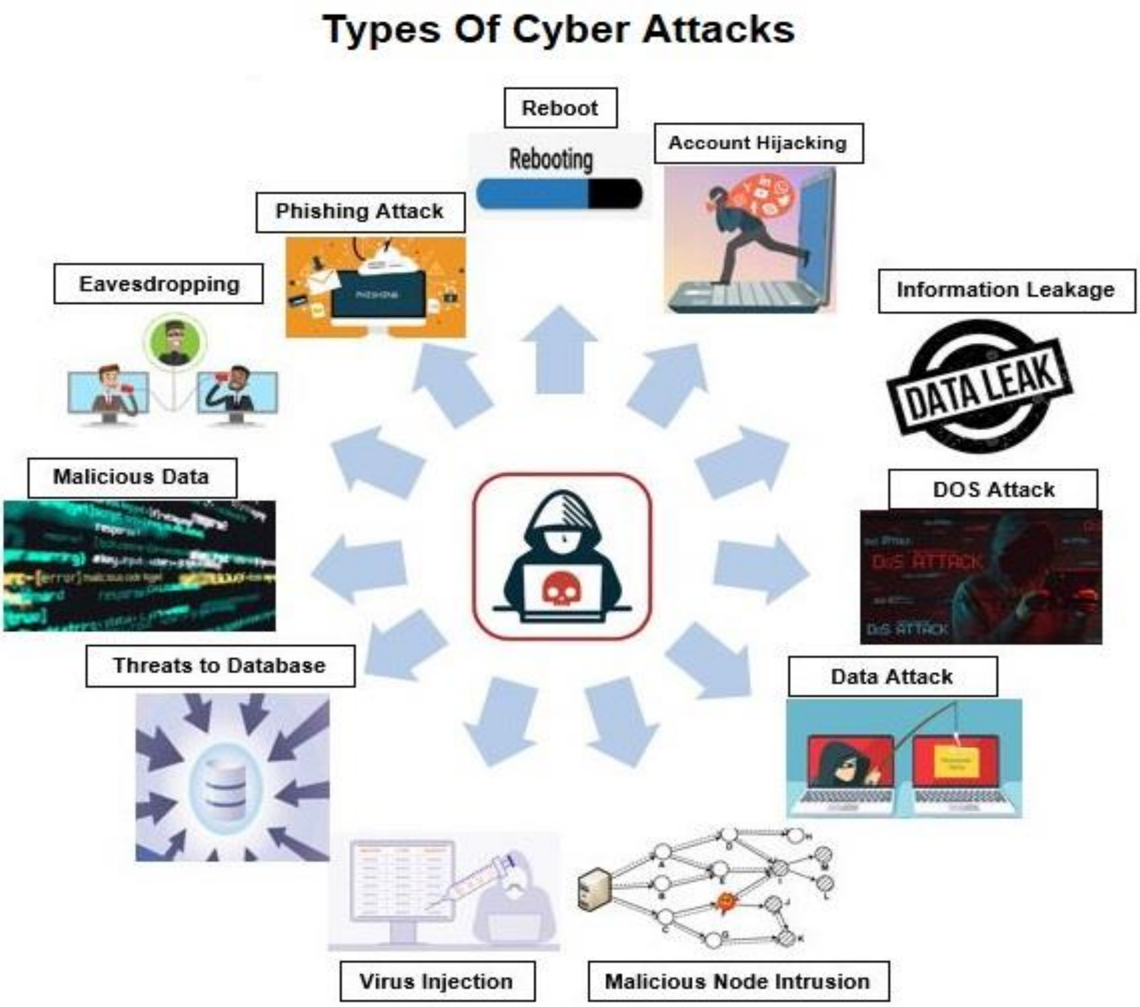


Figure 18: Types of cyber threats to cloud-based IoT systems

4.2 Cyber Threats to cloud-based IoT system

4.2.1 Account Hijacking

Account Hijacking is a type of cyber-attack in which an employee or organization's cloud account (credentials) is stolen/ hijacked by the attacker. The attacker can use these stolen credentials of cloud account to launch another intensive cyber-attack that may lead to potential data breach/ damage on organization and national levels. Moreover, this stolen credential is used by the attacker for any malicious activity that may result in confidential and personnel information leakage [19]. It is estimated that 2 million accounts have been attacked with account hijacking. One of the well-known account hijacking attack was launched against the New York Times online version. In this phishing attack, an email was received by a reseller of Melbourne IT and he was fooled into entering his account credentials. The attacker obtained account credentials and entered the Melbourne IT infrastructure. The attacker redirected the NYT website traffic to the Syrian website and used the same to spread favorable information about the Syrian conflict.

4.2.2 DOS Attack

DOS attack against IoT systems is the most prevalent and is very simple to execute. This kind of attack in a cloud-based IoT environment is considered very harmful, making resources like information, hardware, applications and services unavailable to legitimate users [20]. The attacker sends many requests to the server machine or application; therefore, legitimate traffic becomes challenging for the machine or application to process. The same leads to Denial of service to other incoming legitimate requests. Figure 19 shows graphical representation of DOS/DDOS attack. Week-configured nodes in a cloud-based IoT system may help the attacker to launch such attacks.

Denials of Service attacks are usually launched to restrict legitimate users from accessing IoT, Cloud Services and other computer-based services. For organizations and network administrators, detection and mitigation of DOS attack is challenging. Fig 19 depicts a graphical representation of the DOS attack.

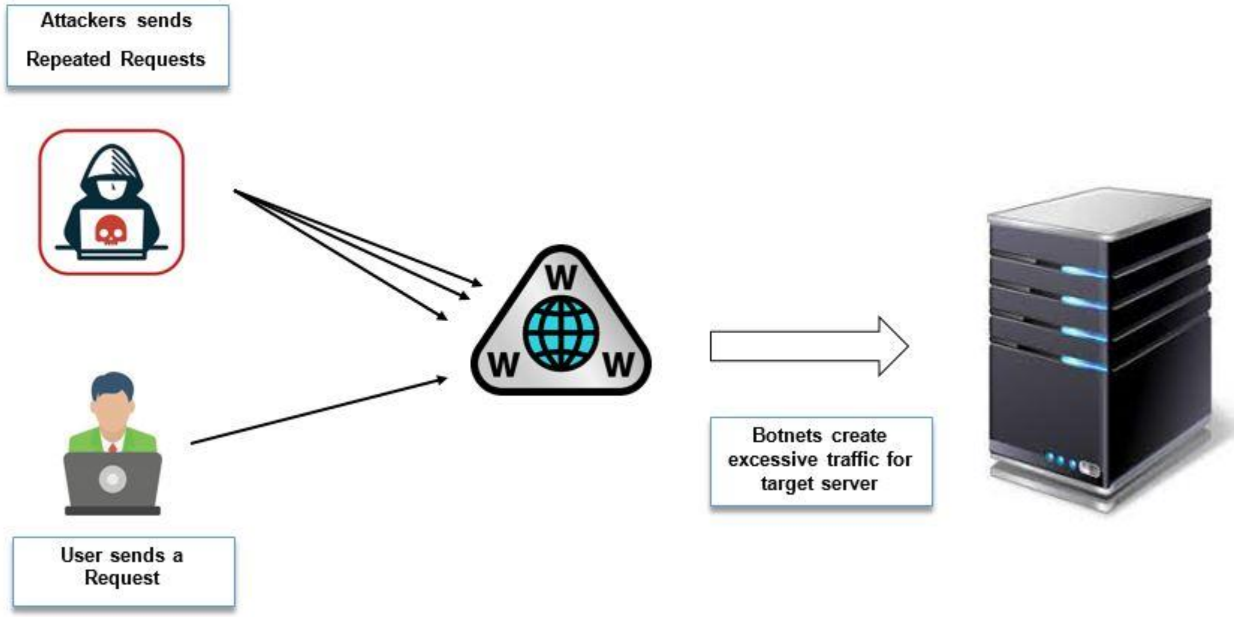

Attackers sends Repeated Requests
W
W
W
Botnets create excessive traffic for target server
User sends a Request

Figure 19: DOS/DDOS attack

4.2.3 Malicious node intrusion / capturing

In a cloud-based IoT environment, IoT devices are more susceptible/ vulnerable to various cyber-attacks [37]. An attacker can capture or replace an IoT device with a malicious node. This new malicious node will seem legitimate but will actually be under the attacker's control. By doing this, an attacker can compromise the whole cloud-based IoT system. The attacker can use the same malicious node for various untoward activities/ attacks.

4.2.4 Virus injection (malicious code injection)

Attackers can inject malicious code into a chip of an IoT device during security patches installation or firmware up gradation [38]. This malicious code forces the IoT node to perform unintended functions or establish communication with the whole cloud-based IoT system.

4.2.5 Malicious data injection attack

If the attacker captures or replaces an IoT node, he can inject incorrect data into the IoT node. By doing this, a false result could be produced. The attacker can also launch DOS/DDOS attack.

4.2.6 Eavesdropping attack

Data generated by IoT nodes are transmitted to the cloud. Therefore, the attacker can capture and eavesdrop on data during transmission.

4.2.7 Reboot attack

Edge devices and IoT nodes are vulnerable to multiple attacks during booting. So, the attacker can launch an attack during the restart process of the node. Therefore, booting must be secured.

4.2.8 Phishing Attack

The phishing attack commonly steals the authentication credentials of IoT nodes or personnel. In this attack, the attacker pretends that he is a legitimate user.

4.2.9 Unauthorized access

In this attack, the attacker gains access to a cloud-based IoT system without authorization and steals sensitive information [39]. Misconfiguration of devices, weak/ share passwords, phishing attack, malware, etc., contribute to unauthorized access. In this attack, the attacker mostly remains undetected while stealing sensitive information.

4.2.10 Data Attack (transit, rest)

IoT nodes transmit data to the cloud; similarly, data is retrieved from the cloud when required by users. The data in transit mode is also prone to cyber-attack. Data at rest is also susceptible to various attacks.

4.2.11 Threats to database

The attacker can target data stored on a cloud Database server. Therefore, Database is susceptible to threats like data breaches and data loss. In this study, database security is considered the responsibility of CSP.

4.2.12 Information leakage

Information leakage is the exposure of sensitive data to unauthorized personnel [40]. Cybercriminals use the same information to launch a successful cyber-attack. Data breaches become possible due to information leakage, mainly if the information contains user credentials. The contributing factors to information leakage are misconfiguration of software settings, obtaining information using social engineering techniques, default passwords, software vulnerabilities, physical theft etc.

4.2.13 Privilege escalation

In most privilege escalation attacks, hackers log in to the system using the ordinary user account and search for flaws in the system that they can exploit to elevate privileges to gain access to the organization's sensitive data. The consequences of privilege escalation are enormous, including company reputation, financial loss, penalty, etc.

4.3 Literature Review

This part of the study will unfold existing literature on secure integration of cloud computing and IoT devices, existing access control mechanisms, threats to cloud-based IoT systems and limitations of the existing literature. Detail of literature review is given below:

Several research studies have been published to ensure the security and privacy of data in cloud-based IoT systems, which are presented as follows.

Stergiou *et al.* [3] surveyed the integration of cloud computing and IoTs with a particular focus on security issues and challenges of both emerging technologies during integration. This paper highlights challenges like heterogeneity, performance, reliability, big data, security and monitoring mechanism. The paper also described the benefits of integrating cloud computing and IoTs, by examining the standard features of both technologies. This paper also highlights how cloud computing improves the performance, utility and out of the IoT devices. Further, a modified double-encryption algorithm model (AES, RSA) has been proposed to secure communication over the network from IoT devices to the cloud. In this modified double encryption algorithm scheme, the strengths of AES and RSA have combined to enhance the performance and security of information. They speed up the key exchange mechanism during communication and data encryption in cloud-based IoT systems.

Li *et al*. [4] devised a framework STRAF (security trust assessment framework) for the security and reputation evaluation of CSPs using cloud security metrics, which can enhance the trust level between CSPs and CSCs. The proposed framework can also be utilized to assess the trustworthiness of CSPs. This study enables CSCs to choose a trusted and secure CSP from multiple CSPs.

Tawabeh *et a*l. [5] proposed a generic and stretched IoT layer model to eliminate all possible security vulnerabilities in cloud-based IoT systems. Many security and privacy issues in IoT systems have been identified and a cloud/edge-supported IoT ecosystem has been implemented and assessed. Moreover, the model can be used with available state-of-the-art security techniques (security certificates, message passing protocol, end-to-end encryption) to neutralize security threats faced by each layer; cloud, IoT and edge. This work also helps organizations to continue implementing policies, end-user awareness, and all involved in secure IoT development.

Bhatt *et al*. [6] proposed ABAC (attribute-based access control) instead of role-based access control to fulfill and strengthen access control requirements in cloud-based IoT systems. In this paper, two use cases i.e. smart homes and smart university car parking systems have been taken as use cases to discuss the proposed access control model.
Bhawiyuga *et al*. [7] have presented a cloud-based software platform that acts as an integration layer between IoT and cloud computing. The authors state that the software platform can handle heterogeneity, communication protocol, security and data management issues faced by cloud-based IoT systems. Furthermore, the proposed software platform has four main components i.e. cloud to device interface, authentication, data management and cloud to user interface. These can overcome challenges like authentication, heterogeneity of network protocols and data management. The authentication component of this platform ensures the legitimacy of the IoT devices.

Wazid *et al*. [8] have proposed a Network Model and Threat Model for authentication in a cloud-based IoT big data environment where only a legitimate user can communicate with IoT devices using common session keys for secure communication. This study discusses security requirements, issues and challenges faced by cloud-based IoT big data environments. Moreover, a comparison of all existing authentication schemes for cloud-based IoT systems is also presented. This study also covers some challenges to be addressed before designing a new authentication scheme.

Abbas *et al*. [9] have proposed FSS (Fog Security Service) for IoT devices to ensure end-to-end security at the fog layer using well-known cryptographic schemes i.e. identity-based encryption and identity-based signature. Using FSS, security services such as authentication, confidentiality and non-repudiation of IoT data can be provided using PKG (private key generator). Moreover, the proposed architecture has been implemented and tested in an OPNET simulator using a single network topology.

Mohanta *et al*. [10] have described security challenges to IoT devices and presented various protocols and applications used in IoT devices. In the paper, different security attacks (layers wise) in IoT systems i.e. malicious node intrusion, Jamming attack, Power analysis attack, etc. have also been highlighted. Furthermore, the authors addressed security issues using ML, AI and Blockchain.

Liu *et al*. [11] proposed two approaches for detecting malicious nodes in network. One is the perception detection approach (PD), in which perception and K means are implemented to compute IoT "trust value" for identifying malicious nodes. In contrast, the other approach is Perception Detection Approach (PDE) with enhancement and this approach detects malicious nodes with a high accuracy rate as compared with other similar methods. In the study, the authors formalized various attacks like Temper attack, replay attack, drop attack and multiple mix attack.

Barbareshi *et al*. [12] have proposed PHEMAP, a mutual authentication scheme based on PUFs (physically unclonable functions) to prevent malicious device intrusion into IoT network. Moreover, salted PHEMAP ensures mutual authentication between a gateway and terminal nodes equipped with PUFs, while Babel chain PHEMAP ensures mutual authentication between two terminals equipped with PUFs.

Hassija *et al*. [13] have classified various IoT applications and highlighted security and privacy issues associated with each class of IoT applications. In the study, security challenges and sources of threats at different layers in IoT applications have also been discussed. Moreover, recommendations have been provided to improve IoT infrastructure to secure communication. In this paper, the authors also proposed the implementation of novel technologies like AI, blockchain, fog computing, and edge computing to enhance the security of IoT devices.

Riad *et al*. [18] proposed a sensitive and energetic access control (SE-AC) mechanism for managing a cloud-based EHR system, including IoT devices. In the study, preserving the privacy of EHR has been achieved using a secure encryption mechanism. The proposed mechanism can handle huge number of end users and empower the patient to control their EHR information.

Riaz *et al*. [15] proposed an access control mechanism for such an environment where all resources are utilized. In the Study, researchers also conducted a detailed survey on proposed access control mechanisms/ access models and conducted a performance analysis of existing techniques for cloud/edge-enabled end nodes. In the study, threats to cloud-enabled IoT systems have been identified and classified/ mapped as threats on the User End, Threats to Cloud/ Fog Computing and threats to the Database. The authors further highlighted that which layer is vulnerable to which threat.

4.4 Limitation of the existing literature

Table 1 shows some weaknesses/ limitations of the existing literature:

S. No	Limitations	Detail
1	In the existing literature, there are rare evidences where the minimization of many threats and access control is addressed in a single study	There is an exhaustive list of threats/Attacks to cloud-based IoT systems. However, the literature reveals that researchers have proposed security solutions for a few threats/ attacks. There are rare evidences where extensive minimization of many threats and access control is addressed in a single study.
2	Achievement of information security through encryption algorithm	Some researchers proposed encryption algorithms to secure data during transmission. As all IoTs have resource limitations; therefore, the implementation of encryption algorithms cannot be effectively in IoT environment and may ultimately affect the performance of cloud-based IoT echo systems.
3	Existing literature is lacking in implementation of Novel solutions	Existing literature is lacking in implementing any novel solution to secure cloud-based IoT systems. In the existing literature, some rare standard terms and methodologies are known to industry and academia. On the contrary, the proposed novel solution in this research paper is known to industry and academia. Therefore, the same can be integrated with cloud-based IoT systems easily. In this current study, researchers propose a novel NAC solution that can be implemented on the authentication and cloud layer (depends on size and remote campuses of organization) to ensure authentication and authorization in cloud-based IoT systems. NAC solution is now mature enough and already implemented in industries for security purposes. Multiple security features of NAC can be used to provide security to cloud-based IoT systems. Organizations can use the proposed idea to achieve strong access control and threat mitigation.

Table 1: weaknesses/limitations of existing literature

4.5 Summary

In this chapter, threats to cloud-based IoT systems have been presented. Further, existing literature regarding the secure integration of cloud computing and IoT, security concerns that arise after integration of cloud computing and IoT, existing proposed access control mechanisms, and limitations of the existing literature has been discussed in this chapter. The next chapter covers threats modeling to identify threats and vulnerabilities faced by cloud-based IoT systems.

Chapter 5

Threat modeling

5.1 Introduction

Threats and vulnerabilities to cloud-based IoT systems have been identified using the threat modeling process. Threat modeling has been conducted to identify potential threats and vulnerabilities faced by cloud-based IoT systems. Furthermore, threat modeling is considered essential to study and identify potential threats and enhance the security of cloud-based IoT systems. Moreover, phase wise approach has been adopted to carry out threat modeling for cloud base IoT.

Threat modeling has been conducted in the following 4 phases.

- **Phase – 1**
  - Asset identification
  - Actors
  - Attackers
- **Phase – 2**
  - Threats and vulnerabilities identification
  - Attack scenarios
- **Phase – 3**
  - Asset grading on criticality bases
  - Attacks and their rating
- **Phase – 4**
  - Mitigation strategies
  - Proposed solution

5.2 Phase – 1

5.2.1 Assets identification

Asset identification is essential for organizations to know about the most critical assets and ensure their security and protection. Assets identification is considered the first line of defense against any threat. All critical assets in cloud-based IoT system have been enlisted in table 2.

S No	Category	Assets Description
1	Hardware	IoT devices
		Application Server machine
		Storage devices
		DB server machines.
		Devices to interface with things (end users)
		Power backup systems (For IoT devices, Server machines, PCs, etc.)
2	Communication (Hardware)	Routers
		Gateways
		Firewalls
		Switches
		Medium (wireless / Ethernet)
3	Applications	DBMS
		OS/ IOS of equipment
		IoT devices applications
		Servers OS
4.	HR	End users (Internal / External)
		Administrators (trusted / untrusted)
		IT Maintenance Staff
5.	Data (Soft copy)	Back up of configurations files of all equipment
		Data in digital form
6.	Data (Hard copy)	Policies
		SLAs

Table 2: Assets identification

5.2.2 Actors

Table 3 shows the actors of cloud-based IoT systems.

S No	Actors
1	End users (Internal / external)
2	Consultants /professionals
3	Trusted Admins / untrusted admin
4	Manufacturers of devices (IoT, Communication Equipment etc.)
5	IT maintenance Staff
6	Attackers

Table 3: Actors

5.2.3 Attackers

Table 4 shows attackers that may access cloud-based IoT systems without authorization.

S No	Attackers	Purpose/ Aim
1	Cyber criminals	Intention is to generate profit by stealing company information or personnel data
2	Hacktivist	To hack something for a cause by promoting political agendas, religious beliefs, or ideology
3	State-sponsored attackers	Cyber warfare, industrial espionage, intellectual property theft, state secrets etc.
4	Insider attackers	Attack that comes from within an organization, either intentionally or accidentally
5	Out sider attack	Attack that comes from outside of the organization
6	Recreational attackers	To get fame and notoriety

Table 4: Attackers

5.3 Phase – 2

In this phase, threats against Hardware, Communication equipment, application and HR involved in a cloud-based IoT environment has been identified and listed.

5.3.1 Threats and vulnerabilities identification

Table 5 shows the threats and vulnerabilities against each component in cloud-based IoT systems.

S No	Category	Threat	Vulnerabilities
1	Hardware	Physical damage	Not placed in a secure environment
		Power drainage	No power backup is available
		Theft	Not placed in secure environment
		Disk Failure	No Raid was implemented
		Virus intrusion	• No AV installed • Usage of USBs and external devices.
		Malicious node intrusion	• No access control mechanism implemented
2	Communication (Hardware)	Unauthorized access	• Weak Passwords / Default passwords. • No access control mechanism implemented • No password change management policy implemented
		Malicious node intrusion	• No access control mechanism implemented
		DOS	• Echo request response allowed • Unused ports are open • No security solution exists that can stop DOS/DDOS attack
		Man in the middle	• Weak Passwords / Default passwords. • No encryption is implemented
		Privilege escalation	• Design flaw • Configuration oversight

3	Application	Misconfiguration	Untrained developers
		Virus intrusion	• AV not installed • Usage of USBs
		Leakage of information	• End users not cleared security wise • The technology used for services may also leak sensitive information • No encryption mechanism implemented • No security solution has been deployed that can identify and monitor data leakage
		Data breaches and data loss	
		Privilege escalation	• Design flaw • Configuration oversight • End users not cleared security wise • No logging monitoring mechanism implemented
		Unauthorized access	• Week passwords • No proper access control mechanism implemented
4	Data (soft and hard)	Un authorized access	• Not password protected
		Physical damage	• Not placed in secure place
		Theft	• Un attendant

Table 5: Threats and vulnerabilities identification

5.3.2 Attack scenarios

Attack scenarios in cloud-based IoT systems include but are not limited to the following.

- In a cloud-based IoT system, if an attacker injects a malicious IoT node into an IoT network. The same can compromise IoT network, edge devices and cloud infrastructure and can be able to launch various attacks.
- In a cloud-based IoT environment, attackers can steal user credentials and behave like legitimate users. The attacker can perform various malicious activities/attacks using the same credentials.
- Design flaws in systems and devices and weak passwords may also invite attackers to gain unauthorized access and perform malicious activities.
- The attacker can also inject viruses /malware into cloud-based IoT systems to steal sensitive information and compromise the cloud-based IoT echo system.
- The attacker can spoof MAC address and IP address of a legitimate machine, assign the same to his machine and start accessing the cloud-based IoT network and resources.

- In cloud-based IoT systems, privilege escalation by a legitimate user cannot be ruled out.
- In cloud-based IoT systems, lack of trust between the client and CSP may also result in the leakage of sensitive information. Further, internal CSP staff may execute malicious intent intentionally or unintentionally, which may lead to sensitive information leakage.

5.4 Phase – 3

5.4.1 Asset grading based on its criticality

In this section, all assets are graded in terms of CIA, impact on business value (BV) and probability of occurrence of threats (POT). It is further highlighted that from the following table, we can infer that the security of hardware, communication, applications, HR, data and information is paramount. Table 6 also indicates that all the included assets must be secured. So, to secure the whole cloud IoT-based echo environment, there is a dire need for a mechanism that counters multiple threats to cloud-based IoT systems.

S No	Category	Assets Description	Criticality in terms of CIA, BV and POT (C+I+A)*BV*POT	Average
1.	Hardware	IoT devices	(3+3+3)*5*0.7= 31.5	12.9
		Application Server machine	(3+3+3)*5*0.1= 4.5	
		Storage devices	(3+3+3)*5*0.4= 18	
		DB server machines.	(3+3+3)*5*0.1= 4.5	
		Devices to interface with things (Users' nodes (end user or consultant))	(3+3+3)*5*0.1= 4.5	
		Power back systems (IoT devices, Server machines and PCs.	(3+3+3)*4*0.4= 14.4	
2.	Communication (Hardware)	Routers	(3+3+3)*5*0.4= 18	18
		Gateways	(3+3+3)*5*0.4= 18	
		Firewalls	(3+3+3)*5*0.4= 18	
		Switches	(3+3+3)*5*0.4= 18	
		Medium (wireless / Ethernet)	(3+3+3)*5*0.4= 18	
3.	Applications	DBMS	(3+3+3)*5*0.4= 18	18
		OS/ IOS of equipment	(3+3+3)*5*0.4= 18	
		IoT devices applications	(3+3+3)*5*0.4= 18	
		Servers OS	(3+3+3)*5*0.4= 18	
4.	HR	End users (Internal / External)	(3+3+3)*5*0.1= 4.5	13.5
		Administrators (trusted / untrusted)	(3+3+3)*5*0.4= 18	
		IT Maintenance Staff	(3+3+3)*5*0.4= 18	

5.	Data (soft copy)	Back up of configurations files of all equipment	(3+3+3)*5*0.1= 4.5	4.5
6.	Data (hard copy)	Policies	(3+3+3)*4*0.1= 3.6	3.6
		SLAs	(3+3+3)*4*0.1= 3.6	

Table 6: Assets grading based on the criticality

Ranges

CIA (1……….5)	where one shows less critical and five shows critical
BV (1………...5)	where one shows less critical and five shows critical
POT (.1, .4, .7, 1)	where (.1) shows low (year or above)
POT (.1, .4, .7, 1)	where (.4) shows medium (once in year)
POT (.1, .4, .7, 1)	where (.7) shows high (within 6 months)
POT (.1, .4, .7, 1)	where (.1) shows low (year or above)
POT (.1, .4, .7, 1)	where (.7) shows low (within 3 months)

5.4.2 Attacks and Rating

Table 7 shows threats against each component involved in cloud-based IoT environment.

S No	Category	Threat	(C+I+A)*BV*POT	Average
1.	Hardware	Physical damage	(0+0+5)*5*.1=2.5	17.5
		Power drainage	(0+0+5)*5*.1=2.5	
		Theft	(5+5+5)*5*.1=7.5	
		Disk Failure	(0+0+5)*5*.4=10	
		Virus intrusion	(5+5+5)*5*.7=52.5	
		Malicious node intrusion	(5+5+5)*5*.4=30	
2.	Communication (Hardware)	Unauthorized access	(5+5+3)*5*.7=45.5	25.81
		Malicious node intrusion	(5+5+5)*5*.4=30	
		DOS	(0+0+5)*5*.4=10	
		Man in the middle	(5+5+3)*5*.4=26	
		Privilege escalation	(5+5+3)*5*.4=26	
		Virus intrusion	(5+5+4)*5*.7=49	
		Leakage of information	(5+0+0)*5*.4=10	
		Data breaches and data loss	(5+0+0)*5*.4=10	

3.	HR	Misuse of privilege	(5+4+0)*5*.7=31.5	33
		Privilege escalation	(4+4+3)*5*.4=22	
		Unauthorized access	(5+5+3)*5*.7=45.5	
4.	Data (soft and hard)	Un authorized access	(5+5+3)*5*.7=45.5	18.5
		Physical damage	(0+0+5)*5*.1=2.5	
		Theft	(5+5+5)*5*.1=7.5	

Table 7: Attacks and rating

5.5 Phase 4

5.5.1 Mitigation strategies

In this study, threats that are faced by cloud-based IoT systems have been identified and graded. In order to enhance the security of cloud-based IoT systems, it reiterated that robust access control mechanism is required that can mitigate multiple threats faced by cloud based IoT systems. It is highlighted that threats repeated against each cloud-based IoT component have been removed/ consolidated in table 8.

S No	Threat	Security responsibility	After implementing the proposed solution
1	Account Hijacking	Can be mitigated using the proposed solution	✓
2	DOS	Can be mitigated using the proposed solution	✓
3	Malicious node intrusion	Can be mitigated using the proposed solution	✓
4	Virus intrusion/ injection	Can be mitigated using the proposed solution	✓
5	Malicious data injection attack	Can be mitigated using the proposed solution	✓
6	Phishing attack	Can be mitigated using the proposed solution	✓
7	Unauthorized access	Can be mitigated using the proposed solution	✓
10	Leakage of information	Can be mitigated using the proposed solution	✓
9	Privilege escalation	Can be mitigated using the proposed solution	✓

11	Physical damage	Organization / CSPs depend on device location	✗
12	Power drainage	Organization / CSPs depends on location	
13	Theft	Organization / CSPs depends on location	
14	Disk Failure	Organization / CSPs depend on premises	

Table 8: Threats mitigated by proposed solution

5.5.2 Proposed solution

This study presents a novel solution that can provide access control mechanism to IoT devices in a cloud-based IoT environment. The same solution is also capable of mitigating/minimizing the chances of multiple attacks faced by cloud-based IoT systems. In the proposed solution, a novel security solution i.e. NAC has been deployed on the authentication layer and cloud layer (if required depending on organization size and offices). Any IoT device that intends to access cloud infrastructure/ IoT network is required to pass through NAC. Furthermore, NAC denies or grants access to the device to access cloud or other IoT devices subject to verification of credential/ profile.

The working mechanism of the proposed solution is as under:

5.5.2.1 Registering devices

All IoT devices and switches are to be registered with NAC (Radius Server). Any IoT Device/ end-user/ professional intending to connect with cloud infrastructure is authenticated by NAC before accessing the cloud. In this proposed architecture, IoT device/ end-user/ professional forward request to switch for accessing cloud services and resources. After registration of devices, various scenarios may exist in a cloud-based IoT environment and NAC will provide authentication in all scenarios as described below:

- In a cloud-based IoT environment, IoT devices require cloud services for storing and processing information. In IoT to cloud scenario, the IoT device forward request to switch for accessing the cloud. Switch forward the IoT device's credentials (MAC address/profile information) to the NAC solution. Further, NAC grants or denies access request of IoT device for the cloud after verifying IoT device credentials/ profile.

- Sometimes, in a cloud-based IoT environment, one IoT device requires input /information from another. In IoT to IoT scenario, the IoT device forwards a request to switch to access another IoT device. Switch forward the IoT device's credentials (MAC address/profile information) to the NAC solution. Further, NAC grants or denies access to requesting IoT device for another IoT device after verifying IoT device credentials/ profile.

- In a cloud-based IoT environment, sometimes end-user or professionals requires information from the cloud. In end-user/ professional to cloud scenario, the end user or professional forwards a request to switch to access the cloud. Switch forward credentials (MAC address/profile information) of end-user/ professional to NAC solution. Further, NAC grants or denies access to end user/ professional for the cloud after verifying end-user credentials/ profile.

- In a cloud-based IoT environment, sometimes end-user or professionals requires information from IoT device. In end-user/ professional to IoT device scenario, end user or professional forward request to switch for accessing the required IoT device. Switch forward credentials (MAC address/profile information) of the end user/ professional to the NAC solution. Further, NAC grants or denies access to end user/ professional for IoT device after verifying end-user credentials/ profile.
- In enterprise-level organizations, having sub-campuses in dispersed locations and deployed NAC in every sub-campus, NAC solution at the cloud layer for the authentication of NACs deployed in sub-campuses may also be considered.
- A draft diagram / high-level view of the proposed solution is given below:

5.6 Threat mitigation by the proposed solution

By implementing the proposed idea in a cloud-based IoT environment, the chances of following threats can be minimized/ mitigated to the maximum level. It is reiterated that the primary purpose of the proposed solution is to provide access control mechanism in cloud-based IoT environment; however, the same can also mitigate multiple threats that are faced by cloud-based IoT systems.

Table 9 shows threats that the proposed solution can mitigate.

S No	Threat	Justification – Threat mitigation by proposed solution
1	Account Hijacking	By implementing our proposed solution, account hijacking attack can be mitigated up to a certain level as the NAC solution authenticates end users prior to joining the network to use network services and resources. Therefore, attackers, despite having user credentials, cannot access network resources and services due to the NAC solution's authentication and verification process. The attacker's request originating from another PC (Not registered with NAC) will be denied at the first tier of security. An attacker may need an authentic machine registered with the NAC solution and a valid credential to compromise the company network for a successful attack. Here, the NAC solution adds a layer of security that can make the attacker's job harder.
2	DOS Attack	By implementing our proposed solution, risk of DOS attack associated with cloud-based IoT systems can be minimized and the attacker job to carry out a DOS attack can be made complex. Primarily, in a DOS attack, the attackers use a compromised node or any other node connected to the network for forwarding lots of requests to the server machine or application that is to be choked. By implementing our proposed solution in a cloud-based IoT network, NAC prevents malicious nodes from entering/joining the company network. Only legitimate devices will be permitted to access network and services; therefore, chances of DOS attacks are minimized. Furthermore, DOS attack can be detected by NAC by integrating it with NIARA etc). Moreover, number of requests generated by the device can be restricted to specified numbers using integration of NAC with third parties vendors. NAC receives logs from third parties vendors like firewall, SIEM etc., analyzes them and

		performs remedial actions. For example, when a device sends requests more than ten times, the same will be notified to the administrator. To summarize the scenario, by implementing our proposed solution, the chances of DOS/DDOS can be minimized by refusing malicious nodes into the network. MAC Spoofing and IP spoofing can be identified using NAC solution's device profiling feature/ attribute. Only those devices or users can communicate with each other/ cloud that has valid MAC addresses. Similarly, integrating third parties security solutions with NAC can detect and prevent DOS/DDSO attack.
3	Malicious node intrusion / capturing	By implementing our proposed solution, intrusion of the malicious node in a cloud-based IoT network is impossible because the MAC address, IP address and other attributes of the machine are validated by NAC (Radius Server) at the Authentication layer. Moreover, the Authentication server can log such malicious nodes and the same remains visible to the NAC operator.
4	Virus injection (malicious code injection)	NAC solution can check the device's health (virus, default passwords, compliance with policies, etc.) before joining the network. Therefore, the NAC solution restricts unhealthy and non-compliant devices from joining the network. With the help of third parties solutions like AVs, firewalls, NIARA, SIEM etc., the intrusion of viruses can be detected and neutralized. Therefore, the proposed solution minimizes the chances of virus intrusion and propagation in the network.
5	Malicious data injection attack	Implementing our proposed solution, only a legitimate device or user can join/ access a specific service and communicate on the cloud-based IoT network. The authentication server will grant permission to only those nodes that have valid MAC and IP addresses following organizational policies. The profiling feature of NAC can detect any abnormal behavior of IoT devices and quarantine the same for further analysis. Moreover, NAC solution can be integrated with third parties security solutions (NIARA, Firewalls, SIEM, and AVs) to detect and prevent any malicious activities
6	Phishing Attack	Every network node is validated by the authentication servers deployed at the authentication layer and cloud layer by verifying its MAC address, IP address and other attributes (device profile). The Attacker despite having a user credential, cannot access network resources because the attacker's request from another machine not registered with the NAC solution will be denied in the verification

		process.
7	Unauthorized access	Implementing our proposed solution, only a legitimate device or user can join/ access a cloud-based IoT network. As already mentioned, the NAC solution can be integrated with third parties vendors like NIARA, Firewall, SIEM and AVs; Therefore, NAC verifies device health and security posture before joining the network. NAC solution can monitor any abnormality like weak passwords, virus intrusion, etc., by analyzing third-party security solutions logs. Furthermore, NAC integrated with NIARA (behavior analytics) can identify any unauthorized malicious intruder. So, NAC has capable of identifying unauthorized access and can provide quick remedial action.
8	Information leakage	The proposed solution provides proper access control and an authorization mechanism to a cloud-based IoT environment, thus lessening the chances of leakage of information. Moreover, NAC can also detect and prevent any information leakage using third-party security services. Furthermore, as already mentioned, NAC can be integrated with AVs, Firewalls, SIEM Solution, and NIARA to detect any anomaly timely and respond. NAC with an on-guard / onboard license can check device health and comply with company policy before joining the network
9	Privilege escalation	By implementing our proposed solution, the NAC component provides access control and authorization mechanism to end users; hence, the NAC's authorization feature restricts users from misusing privileges. Moreover, NAC solution can be integrated with third parties security solutions like AVs, Firewalls, SIEM, NIARA etc. that can assist NAC in the early detection of privilege escalation and other cyber threats.

Table 9: Consolidated threats mitigation by proposed solution

5.7 Summary

In this chapter, threat modeling of cloud-based IoT environment has been carried out. Identification of assets, threats against each asset and its grading based on criticality have been presented in this chapter. The next chapter covers the implementation part of the study.

Chapter 6

Implementation

.

6.1 Objective

The primary objective of this implementation is to verify the access control mechanism provided by NAC solution to IoT devices in cloud-based IoT environment.

6.2 Lab components

To implement the proposed idea in a real environment, following IT infrastructure / Equipment has been used. Figure 20 depicts the implementation setup to validate the proposed idea and results.

a. Cloud infrastructure
b. Switch (Allied Telesis)
c. NAC Solution
d. IP cameras 1
e. IP camera 2
f. IP camera 3
g. Laptop and PC

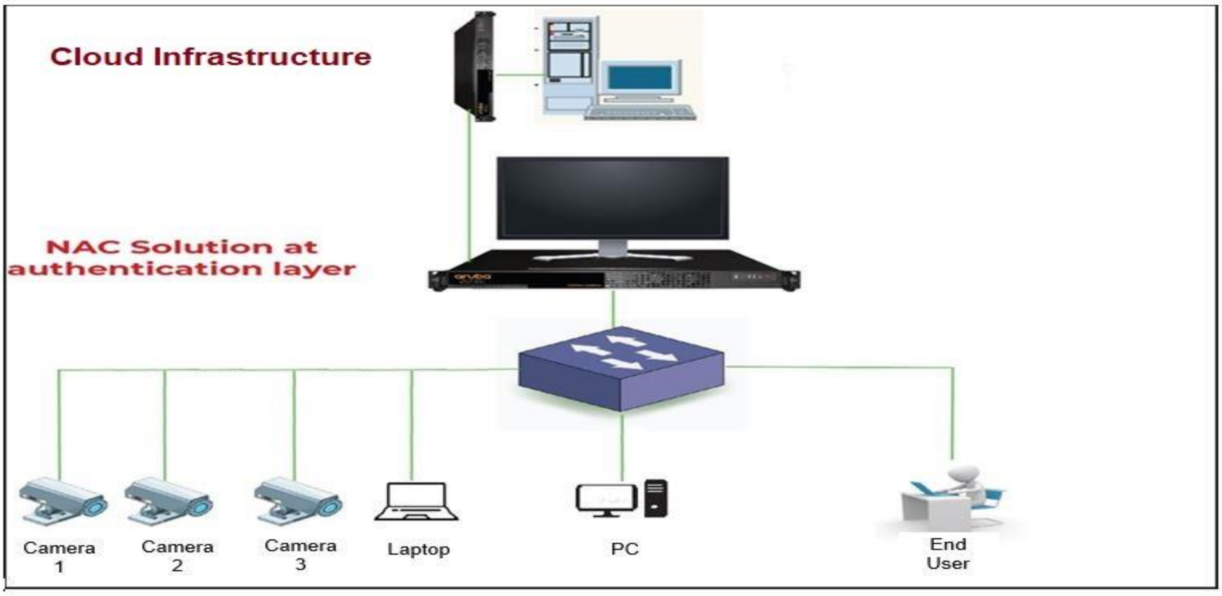


Figure 20: System Architecture Diagram

6.3 Scenarios

The following stepwise approach has been adopted to test the proposed idea in a real-time cloud-based IoT environment. In this regard, the proposed idea has been tested in following scenarios.

a. To verify the access control mechanism provided by NAC to **IP Camera 1** connected to NAC solution via switch, which is further connected to cloud infrastructure. NAC is deployed between switch and Cloud, as shown in figure 21:

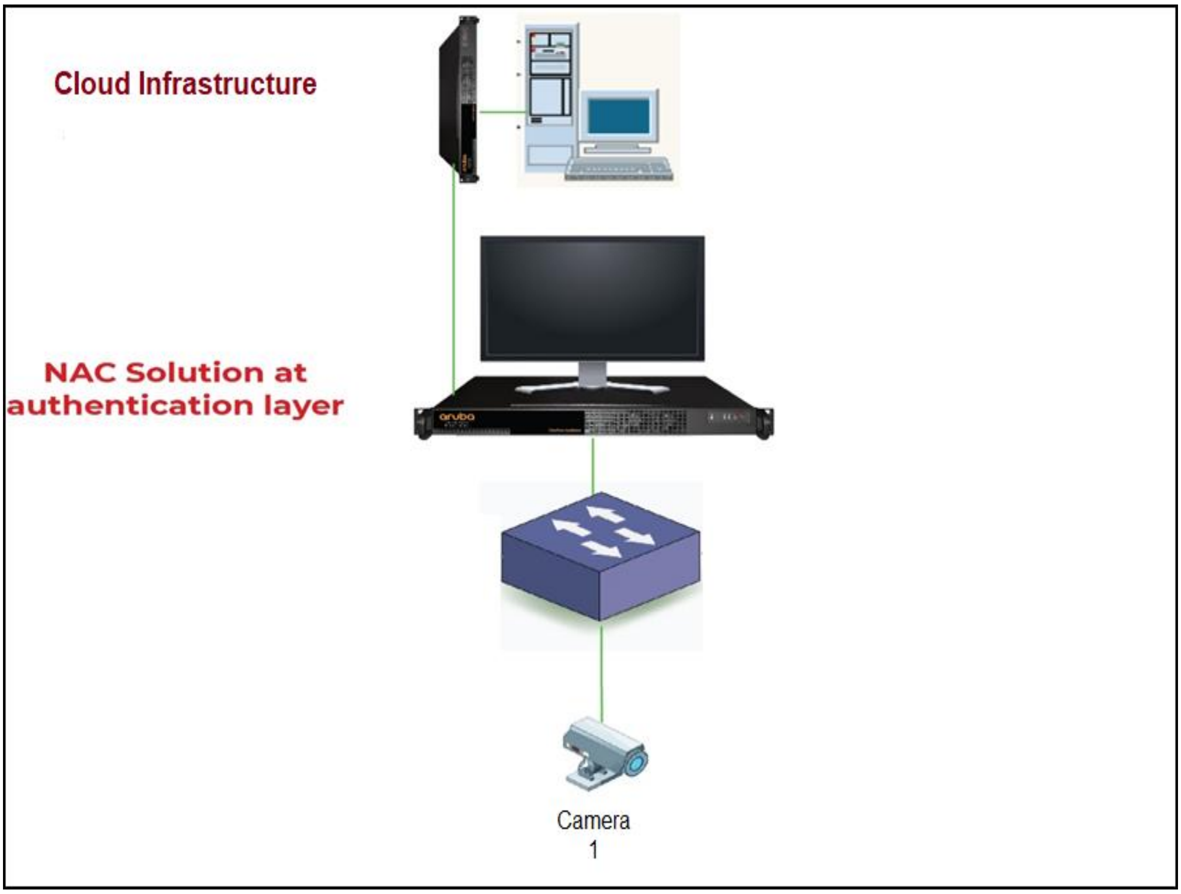


Figure 21: Access Control Mechanism provided by NAC to IP Camera 1

b. To verify access control mechanism provided by NAC to IP Camera 2, connected to the NAC solution via switch, which is further connected to cloud infrastructure. NAC is deployed between switch and Cloud as shown in figure 22.

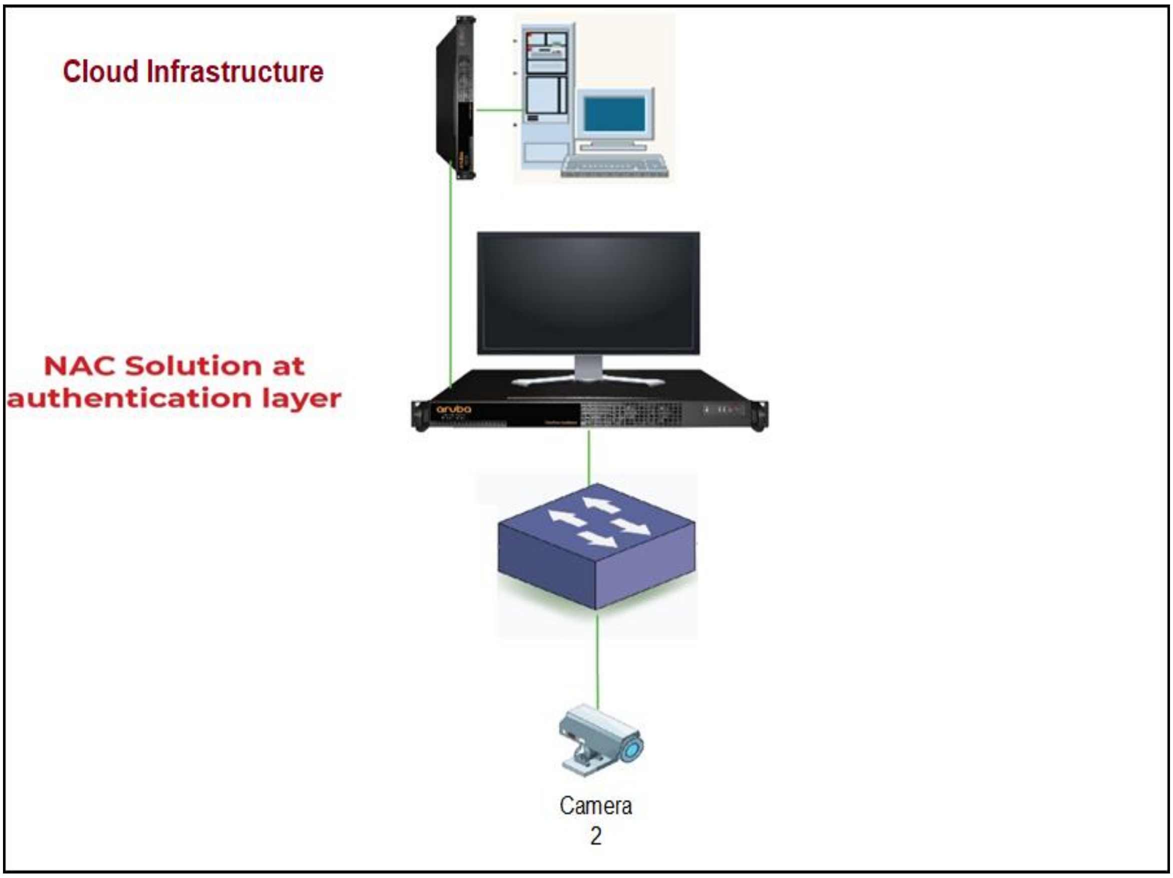


Figure 22: Access Control Mechanism provided by NAC to IP Camera 2

c. To verify access control mechanism provided by NAC to IP Camera 3 connected to the NAC solution via switch, which is further connected to cloud infrastructure. NAC is deployed between switch and Cloud as shown in figure 23.

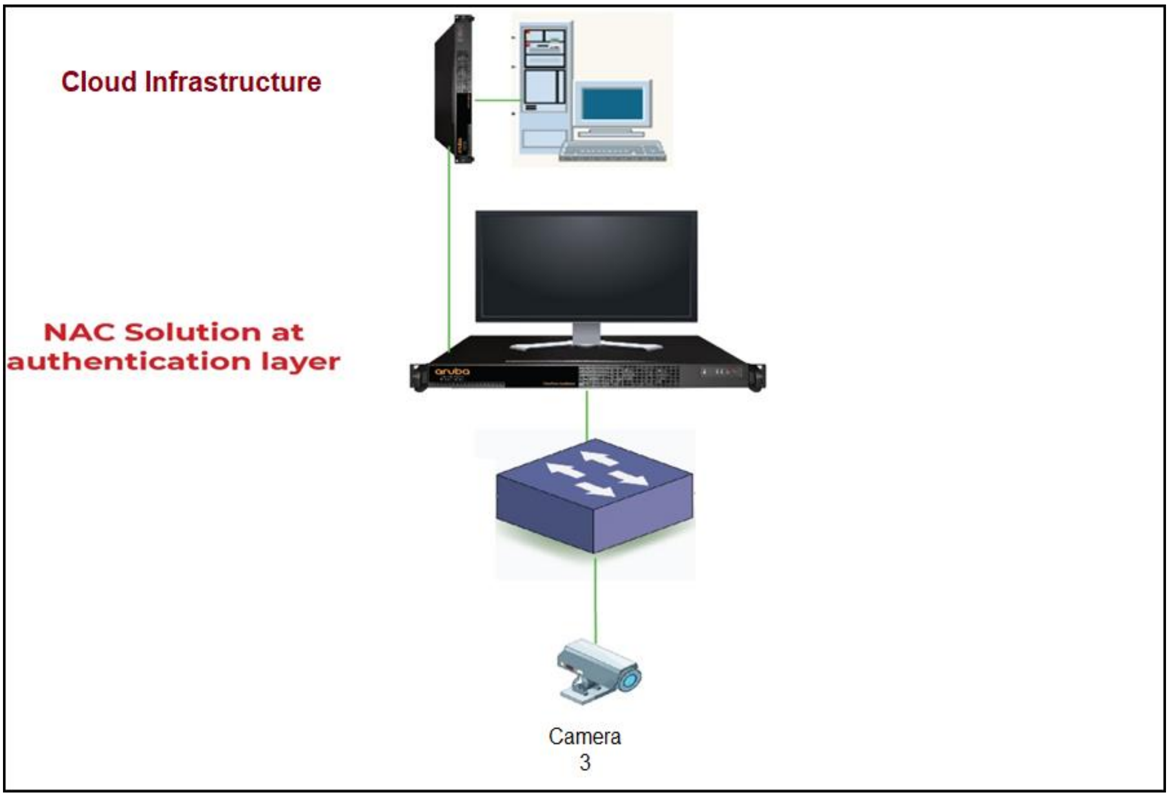


Figure 23: Access Control Mechanism provided by NAC to IP Camera 3

d. To verify access control mechanism provided by NAC to Laptop connected to the NAC solution via switch (Allied Telesis), which is further connected to cloud infrastructure. NAC is deployed between switch and Cloud as shown in figure 24.

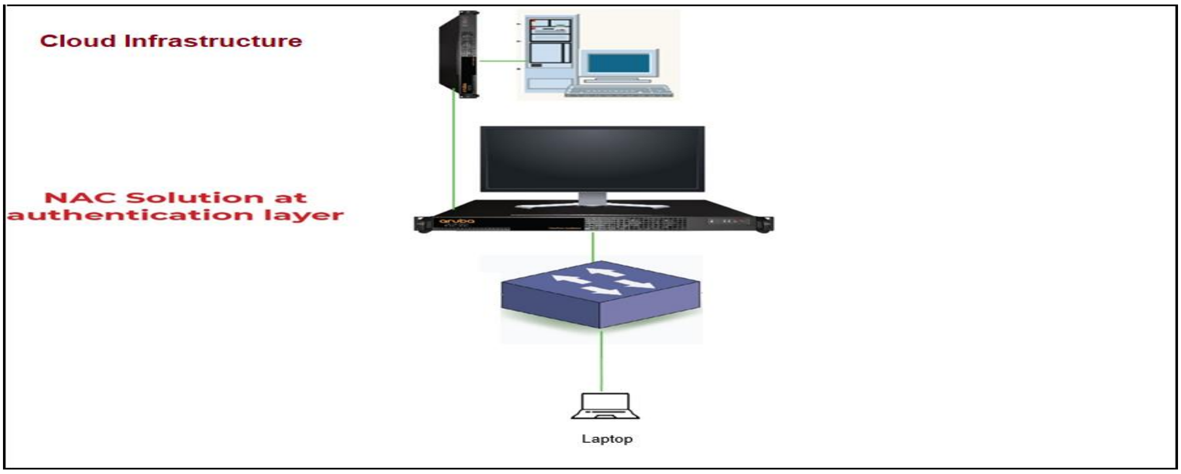


Figure 24: Access Control Mechanism provided by NAC to Laptop

e. To verify access control mechanism provided by NAC to PC connected to the NAC solution via switch (Allied Telesis), which is further connected to cloud infrastructure. NAC is deployed between switch and Cloud as shown in figure 25.

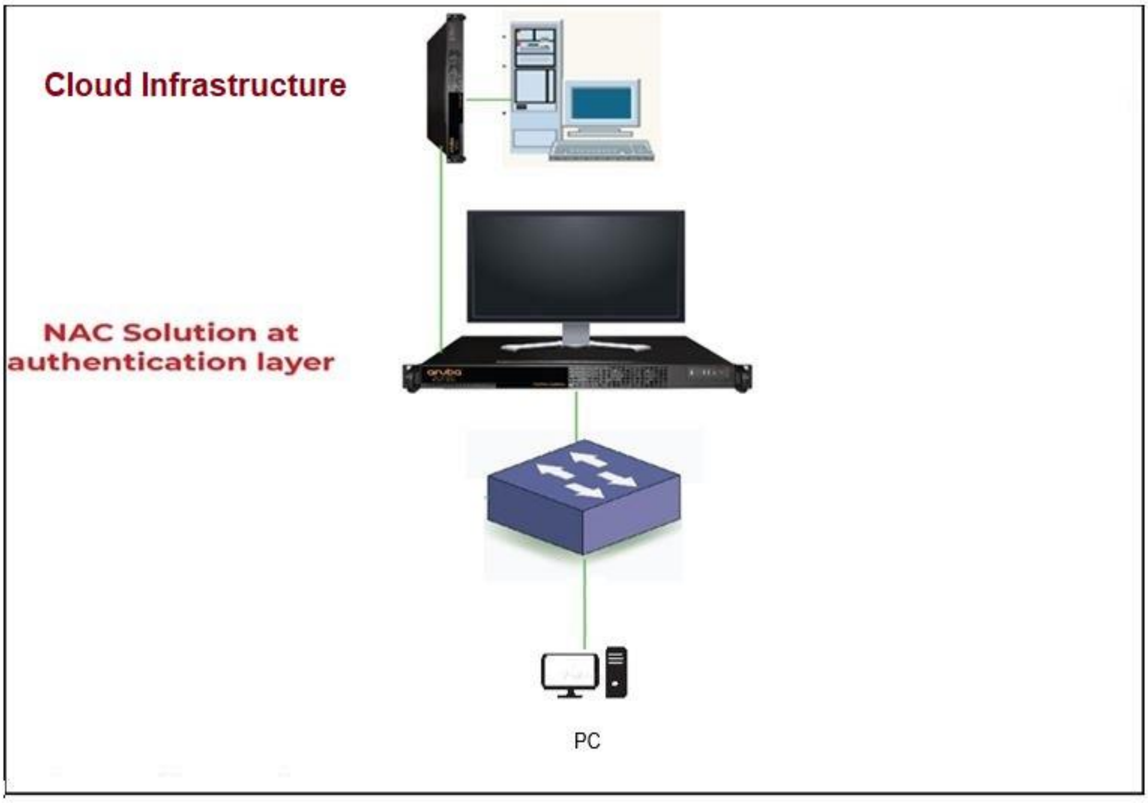


Figure 25: Access Control Mechanism provided by NAC to PC

6.4 Lab Setup

In order to establish a lab environment, configuration of following equipment is considered prerequisite/ essential. All equipment required for testing the proposed idea in a real cloud-based IoT environment is configured as per our requirements.

a. Configuration of Switch

Following features have been configured on the switch. It is pertinent to mention here that switch of any make model/ manufacture can be used to perform the said activity. In this lab environment, we have used Allied Telesis switch. Following are to be configured on switch.

- Radius Server Configuration
- Enabling AAA authentication
- Enable Dot1x / port-based authentication on interfaces

b. Configuration of NAC (Aruba Clear pass)

Following configurations have been undertaken on the NAC solution.

- Integration of switch with NAC
- Integration of devices (Cameras (1, 2, 3), PC, Laptops etc.) with NAC

c. Results (Tabular Form)

Following results have been produced after the implementation of NAC solution, based on under mentioned scenarios in cloud-based IoT system.

- Normal flow of the architecture – without implementing NAC
- Flow of the proposed architecture after NAC implementation – Before registering devices on NAC
- Flow of the proposed architecture – After registering devices on NAC
- Flow of the proposed architecture – After registering Camera 1 and Camera 2 on NAC while Camera 3, Laptop and PC Remained unregister

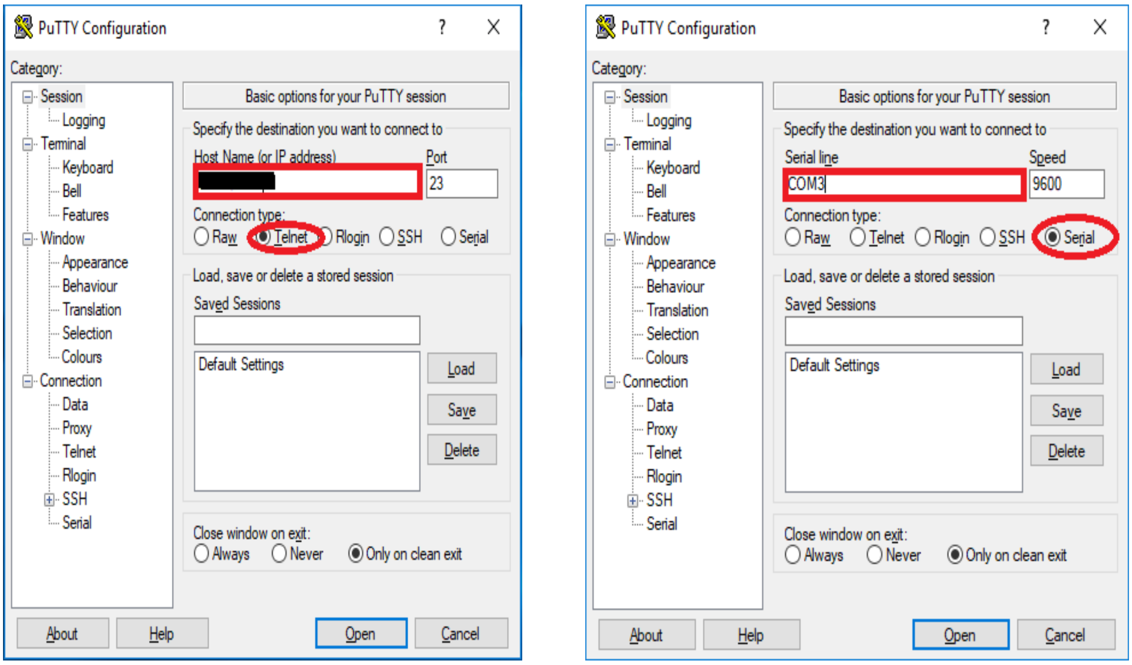
6.5 Detail of the implementation- configuration of devices

As already mentioned, configuration of switch and NAC solution is essential for lab environment to test the proposed idea. Step-by-step configurations of required devices are as under:

6.5.1 Configuration of Allied Telesis switch

Following configuration has been undertaken on switch to prepare lab environment.

a. Access CLI of switch using the putty application via IP address (Telnet) or through console in figure 26.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): [redacted] Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

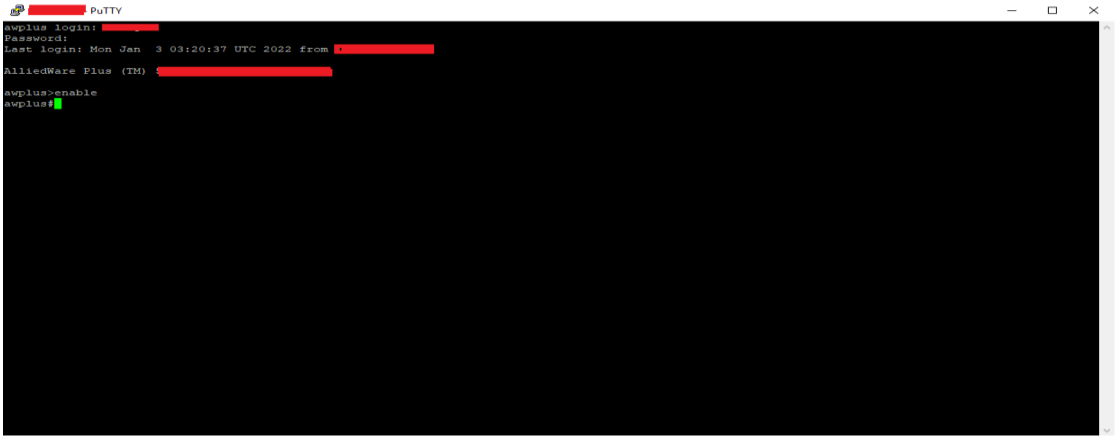
Serial line: COM3 Speed: 9600

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Close window on exit: ○ Always ○ Never ● Only on clean exit

Figure 26: Accessing Switch CLI using Putty application

b. Click on Open button, Switch CLI will be displayed in figure 27.



[redacted] PuTTY

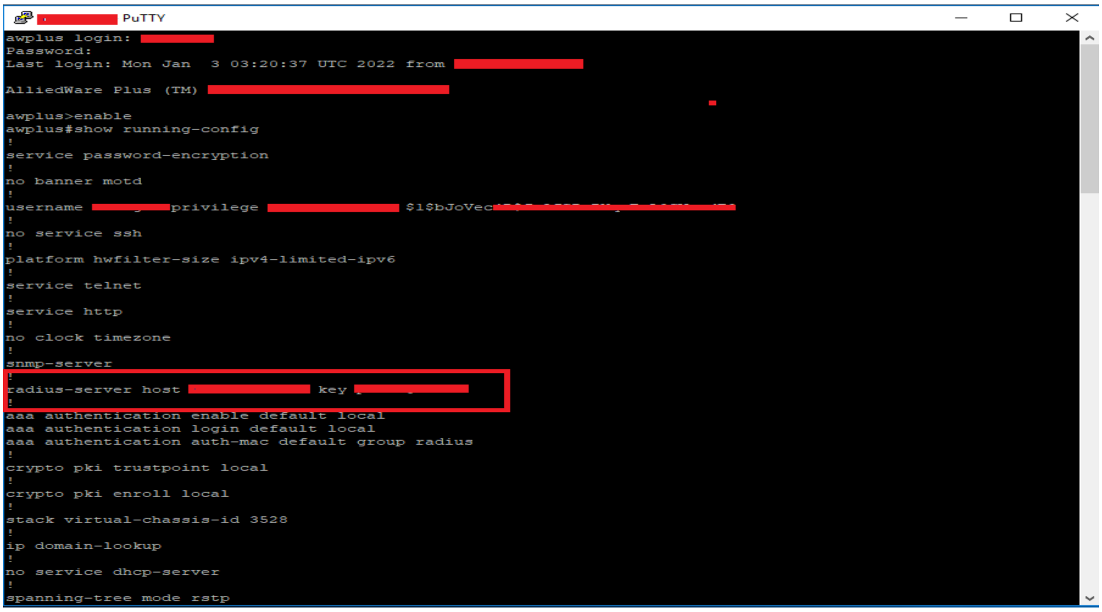
```
awplus login: [redacted]
Password:
Last login: Mon Jan  3 03:20:37 UTC 2022 from [redacted]

AlliedWare Plus (TM) [redacted]

awplus>enable
awplus#
```

Figure 27: CLI mode of the switch

c. Configure the radius Server on switch as shown in figure 28.



[redacted] PuTTY

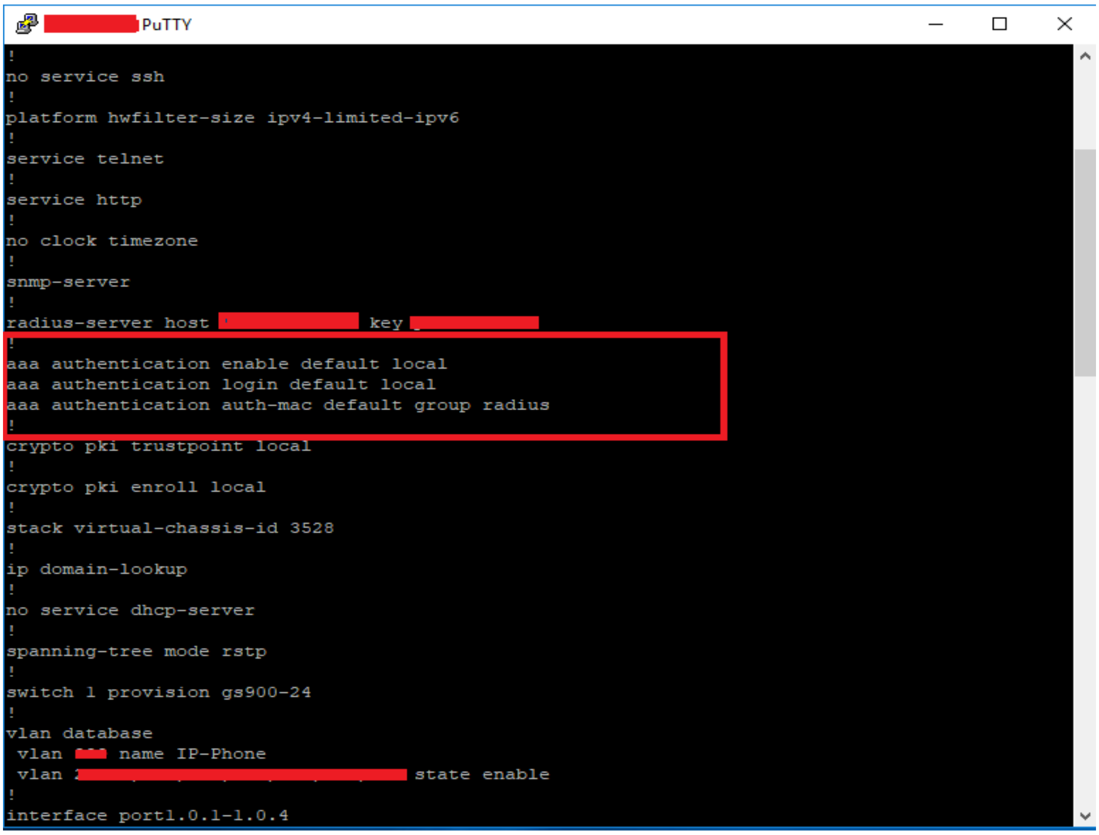
```
awplus login: [redacted]
Password:
Last login: Mon Jan  3 03:20:37 UTC 2022 from [redacted]

AlliedWare Plus (TM) [redacted]

awplus>enable
awplus#show running-config
!
service password-encryption
!
no banner motd
!
username [redacted]privilege [redacted] $1$bJoVec[redacted]
!
no service ssh
!
platform hwfilter-size ipv4-limited-ipv6
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
radius-server host [redacted] key [redacted]
!
aaa authentication enable default local
aaa authentication login default local
aaa authentication auth-mac default group radius
!
crypto pki trustpoint local
!
crypto pki enroll local
!
stack virtual-chassis-id 3528
!
ip domain-lookup
!
no service dhcp-server
!
spanning-tree mode rstp
```

Figure 28: Radius Server configuration on switch

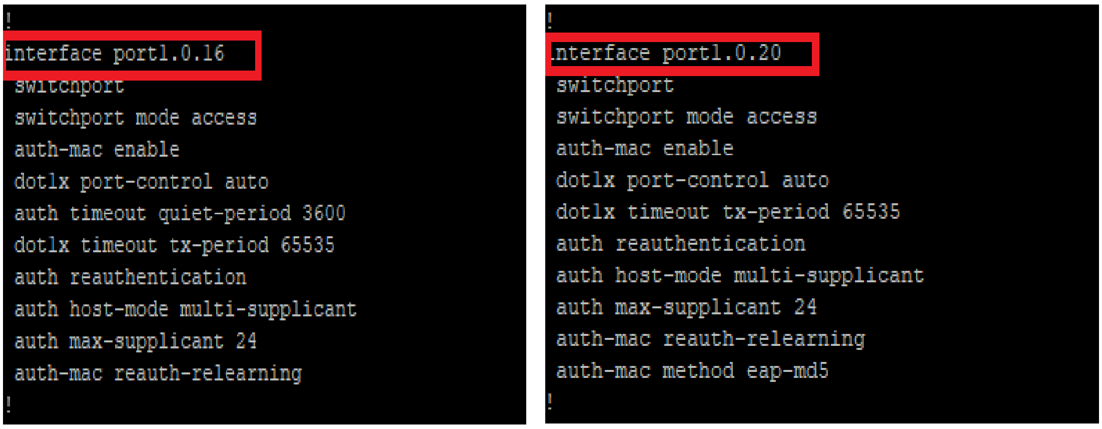
d. Enable AAA authentication on switch in figure 29.



```
!
no service ssh
!
platform hwfilter-size ipv4-limited-ipv6
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
!
radius-server host [redacted] key [redacted]
!
aaa authentication enable default local
aaa authentication login default local
aaa authentication auth-mac default group radius
!
crypto pki trustpoint local
!
crypto pki enroll local
!
stack virtual-chassis-id 3528
!
ip domain-lookup
!
no service dhcp-server
!
spanning-tree mode rstp
!
switch 1 provision gs900-24
!
vlan database
 vlan [redacted] name IP-Phone
 vlan [redacted] state enable
!
interface port1.0.1-1.0.4
```

Figure 29: Enabling AAA authentication on switch

e. Enable Dot1x / port-based authentication on interfaces (port 16 & 20 in this lab) using following command as shown in figure 30.



```
!
interface port1.0.16
 switchport
 switchport mode access
 auth-mac enable
 dot1x port-control auto
 auth timeout quiet-period 3600
 dot1x timeout tx-period 65535
 auth reauthentication
 auth host-mode multi-supplicant
 auth max-supplicant 24
 auth-mac reauth-relearning
!
```

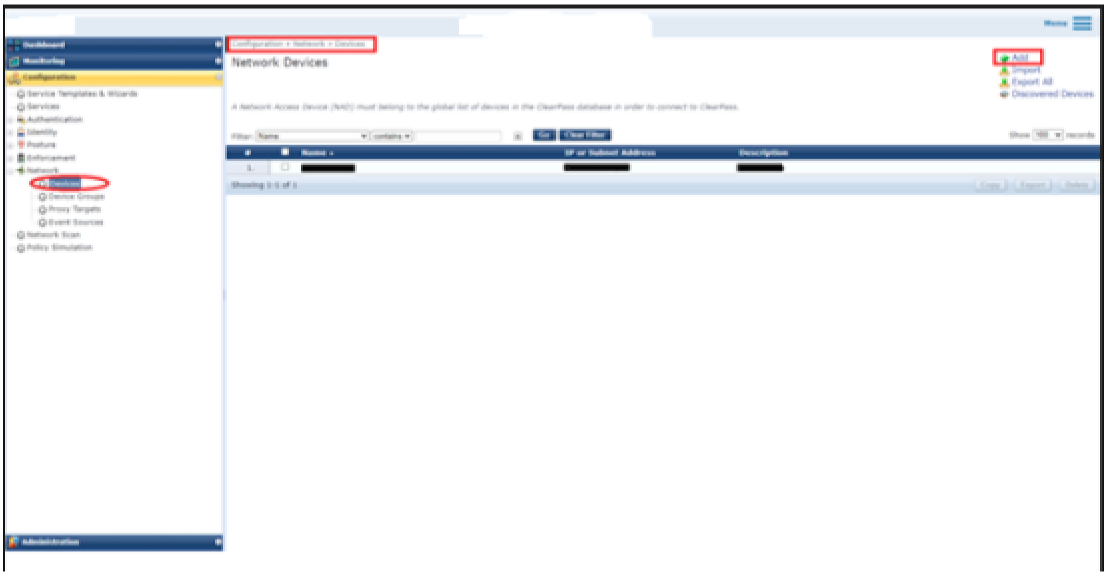
```
!
interface port1.0.20
 switchport
 switchport mode access
 auth-mac enable
 dot1x port-control auto
 dot1x timeout tx-period 65535
 auth reauthentication
 auth host-mode multi-supplicant
 auth max-supplicant 24
 auth-mac reauth-relearning
 auth-mac method eap-md5
!
```

Figure 30: Enabling DOT1x/port-based authentication on switch

6.5.2 Configuration of NAC/ integration of switch with NAC

NAC provides access control to cloud-based IoT environment. Therefore, there is a requirement to integrate the configured switch connected to devices with the NAC solution. The configured switch (already configured) has been added in NAC as shown below:

a. To integrate switch with NAC, go to Configuration » Network » Devices on NAC (Aruba Clear Pass policy manager) as shown in figure 31.



Network Devices

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Filter: Name contains

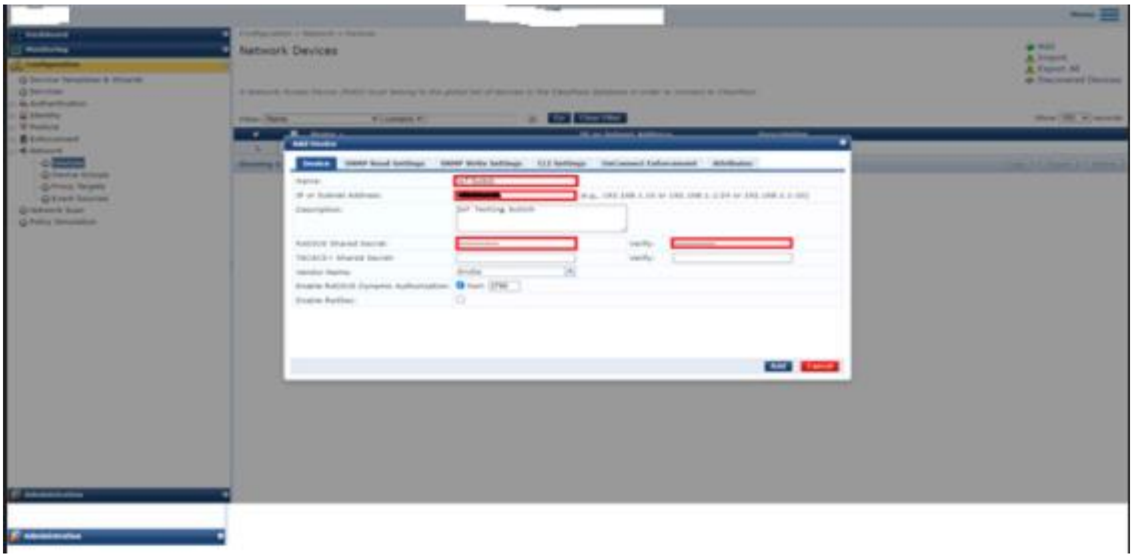
Show 100 records

#	Name	IP or Subnet Address	Description
1	[redacted]	[redacted]	[redacted]

Showing 1-1 of 1

Figure 31: Adding switch in Clear Pass Policy Manager of NAC

b. Now click on Add button, following screen shown in figure 32 will be displayed.



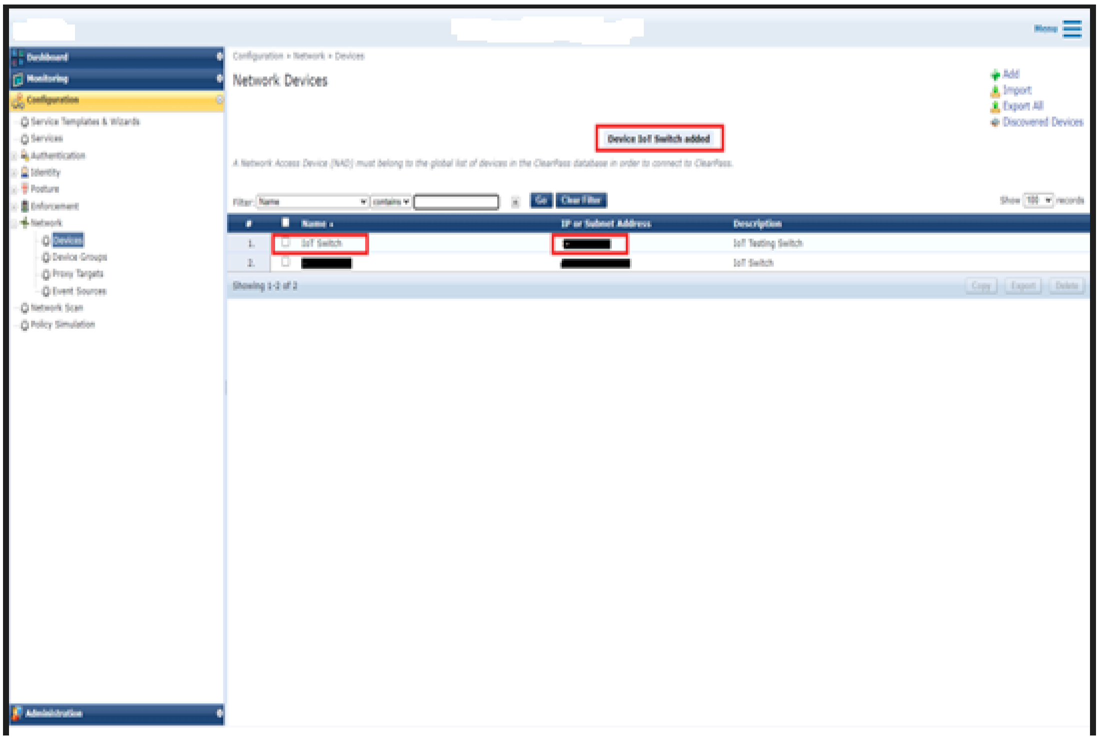
Network Devices

Add Device

Description: IoT Testing Switch

Figure 32: Switch integration with NAC

c. Fill the text boxes and click on Add button, screen shown in figure 33 will be displayed.



Configuration » Network » Devices

Network Devices

Device IoT Switch added

A Network Access Device (NAD) must belong to the global list of devices in the ClearPass database in order to connect to ClearPass.

Filter: Name ▾ contains ▾ Go Clear Filter Show 100 ▾ records

#	□	Name ▴	IP or Subnet Address	Description
1.	□	IoT Switch	[redacted]	IoT Testing Switch
2.	□	[redacted]	[redacted]	IoT Switch

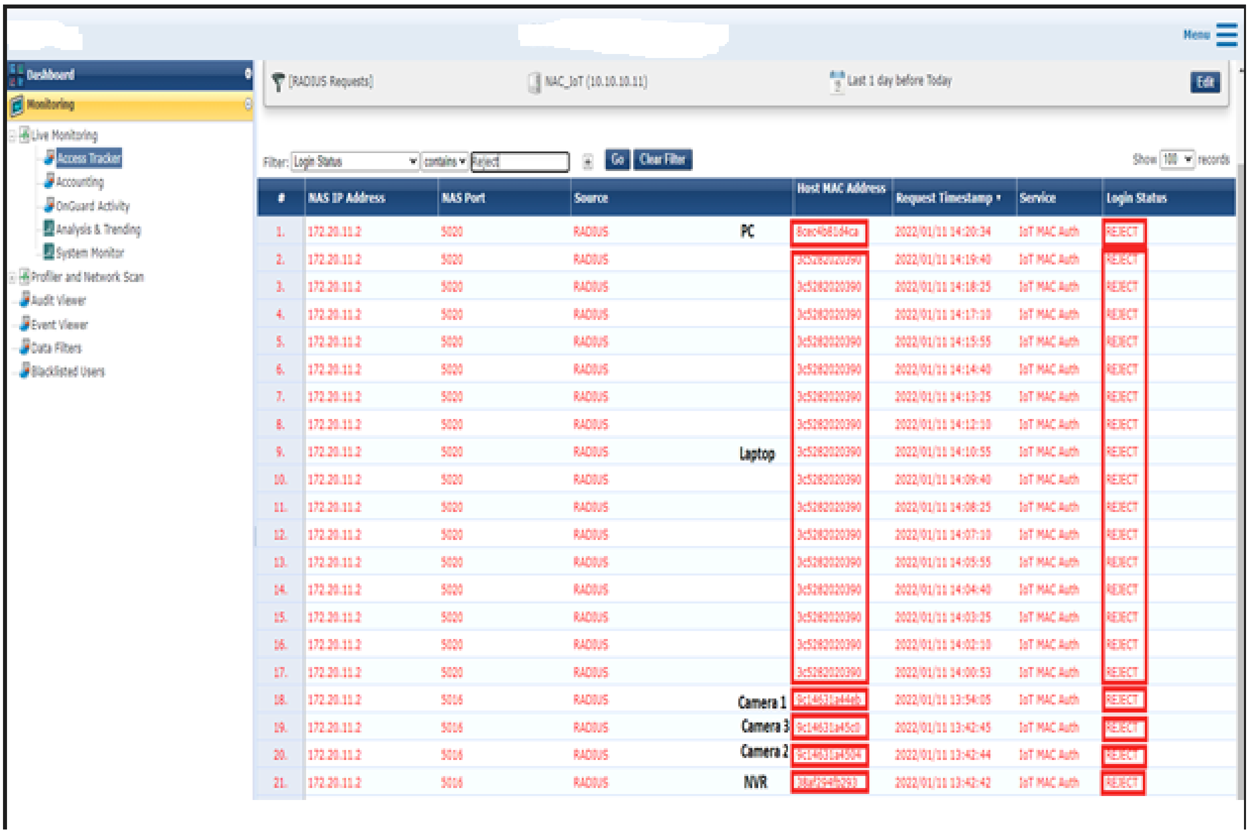
Showing 1-2 of 2 Copy Export Delete

Figure 33: Switch integration with NAC

d. Message will be displayed that **switch Added**, as shown in figure 33. It may be highlighted that you can add switch to a specific group for enforcement of various policies; if you have multiple switches, they can be added using similar way as discussed previously.

6.5.3 Integration of Camera (1, 2, 3), PC and Laptops etc.) with NAC

It is pertinent to mention that initially, all devices will be rejected as shown in figure 34 by NAC because these devices have not been integrated/ added in NAC (static host list).



[RADIUS Requests] NAC_IoT (10.10.10.11) Last 1 day before Today

Filter: Login Status contains Reject

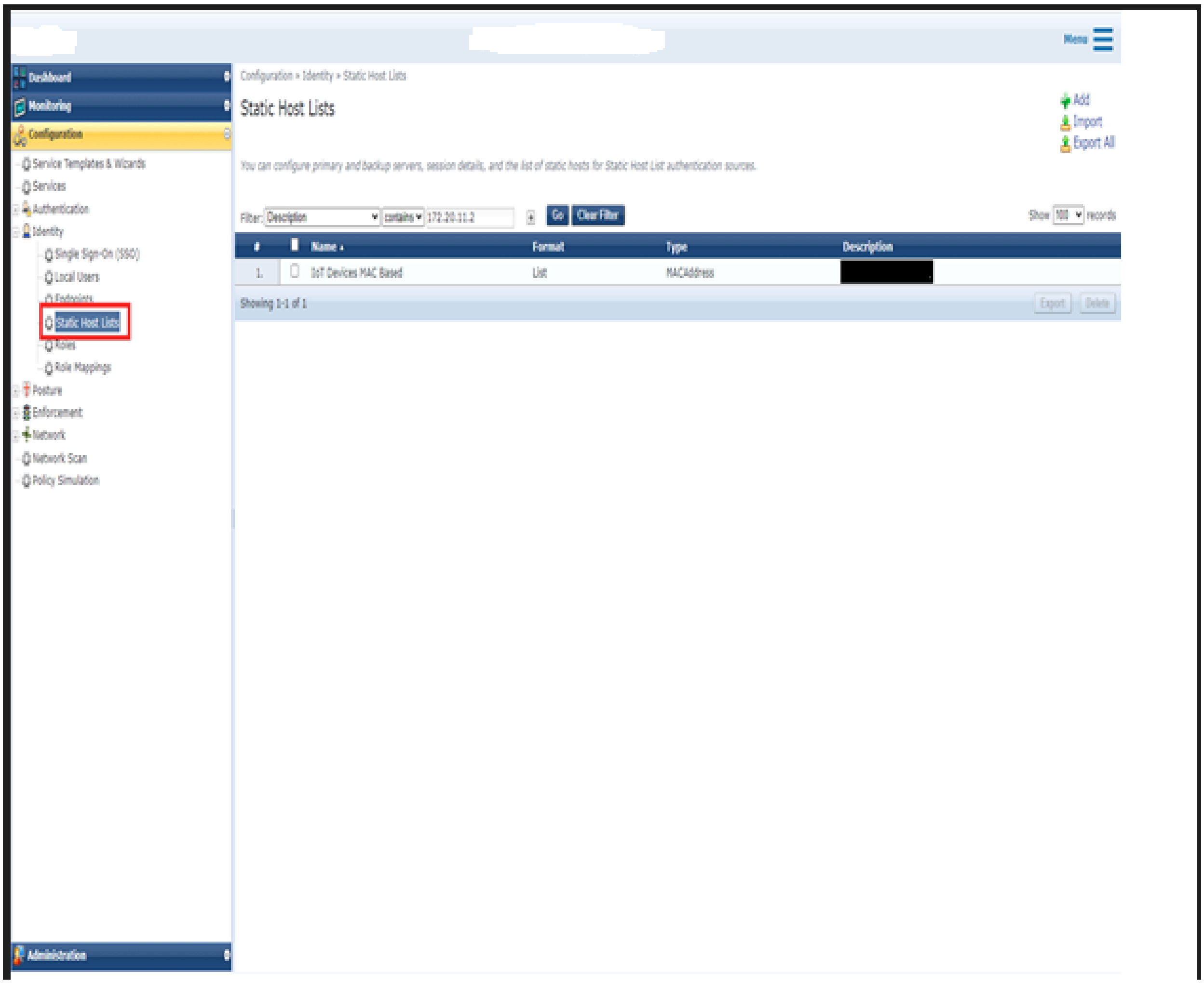
Show 100 records

#	NAS IP Address	NAS Port	Source	Host MAC Address	Request Timestamp	Service	Login Status
1.	172.20.11.2	5020	RADIUS	8cec4b81d4ca	2022/01/11 14:20:34	IoT MAC Auth	REJECT
2.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:19:40	IoT MAC Auth	REJECT
3.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:18:25	IoT MAC Auth	REJECT
4.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:17:10	IoT MAC Auth	REJECT
5.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:15:55	IoT MAC Auth	REJECT
6.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:14:40	IoT MAC Auth	REJECT
7.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:13:25	IoT MAC Auth	REJECT
8.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:12:10	IoT MAC Auth	REJECT
9.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:10:55	IoT MAC Auth	REJECT
10.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:09:40	IoT MAC Auth	REJECT
11.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:08:25	IoT MAC Auth	REJECT
12.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:07:10	IoT MAC Auth	REJECT
13.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:05:55	IoT MAC Auth	REJECT
14.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:04:40	IoT MAC Auth	REJECT
15.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:03:25	IoT MAC Auth	REJECT
16.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:02:10	IoT MAC Auth	REJECT
17.	172.20.11.2	5020	RADIUS	3c5282020390	2022/01/11 14:00:53	IoT MAC Auth	REJECT
18.	172.20.11.2	5016	RADIUS	9c14631a44eb	2022/01/11 13:54:05	IoT MAC Auth	REJECT
19.	172.20.11.2	5016	RADIUS	9c14631a45c0	2022/01/11 13:42:45	IoT MAC Auth	REJECT
20.	172.20.11.2	5016	RADIUS	9c14631a4504	2022/01/11 13:42:44	IoT MAC Auth	REJECT
21.	172.20.11.2	5016	RADIUS	38af294fb293	2022/01/11 13:42:42	IoT MAC Auth	REJECT

Figure 34: Rejection of connected devices (not integrated/added) by NAC

To integrate devices with NAC, following steps have been undertaken.

a. Go to Configuration » Identity » Static Host Lists on NAC ClearPass Policy Manager as shown in figure 35.



Configuration » Identity » Static Host Lists

Static Host Lists

You can configure primary and backup servers, session details, and the list of static hosts for Static Host List authentication sources.

Filter: Description contains 172.20.11.2 Go Clear Filter Show 100 records

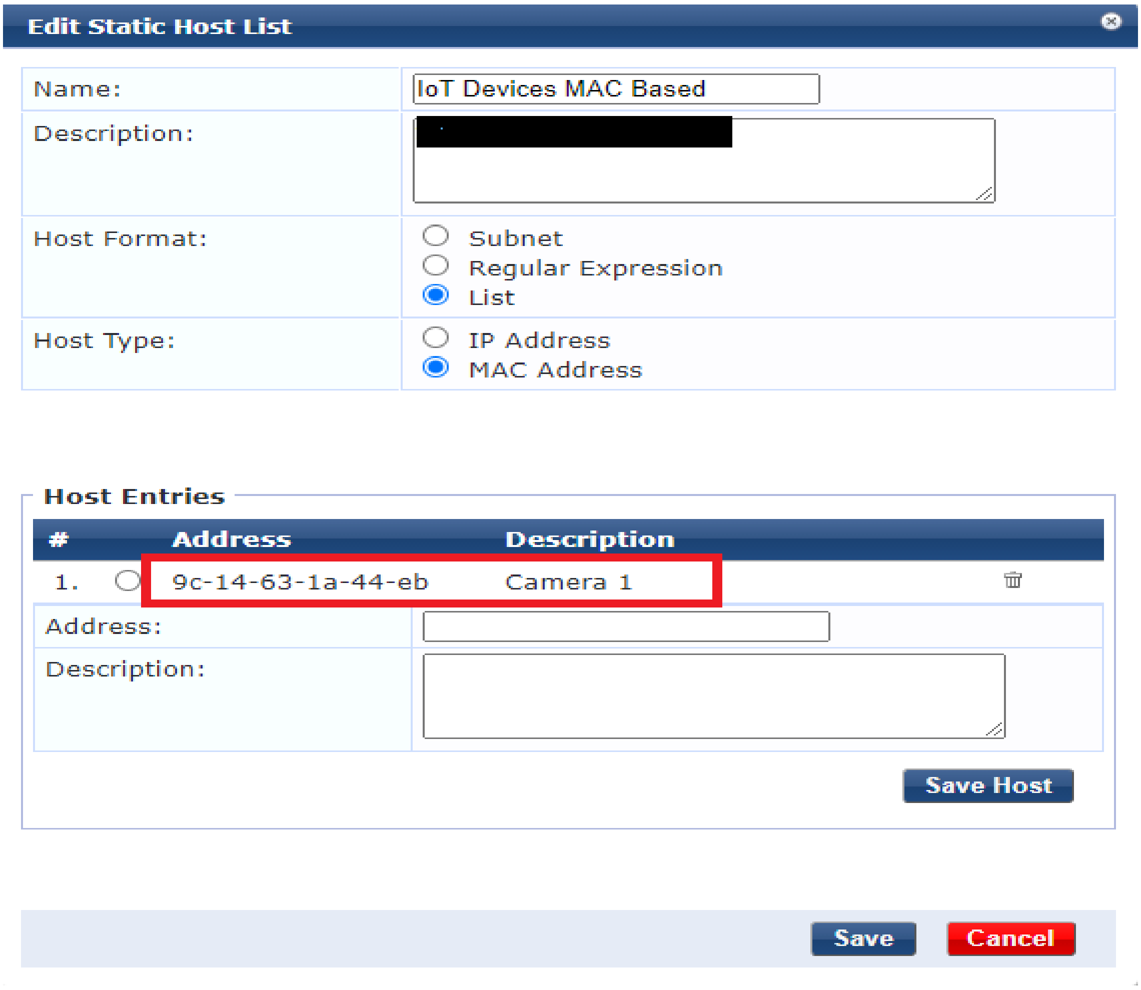
#	Name	Format	Type	Description
1.	IoT Devices MAC Based	List	MACAddress	[redacted]

Showing 1-1 of 1

Figure 35: Devices Integration with NAC

b. **<u>Adding Camera (1, 2, 3), laptop and PC in NAC (Static Host List</u>)**

(i) To Add **Camera 1** in NAC, go to “Configuration » Identity » Static Host Lists “and click on switch as shown in figure 36.



Edit Static Host List

Name:	IoT Devices MAC Based
Description:	[redacted]
Host Format:	○ Subnet ○ Regular Expression ● List
Host Type:	○ IP Address ● MAC Address

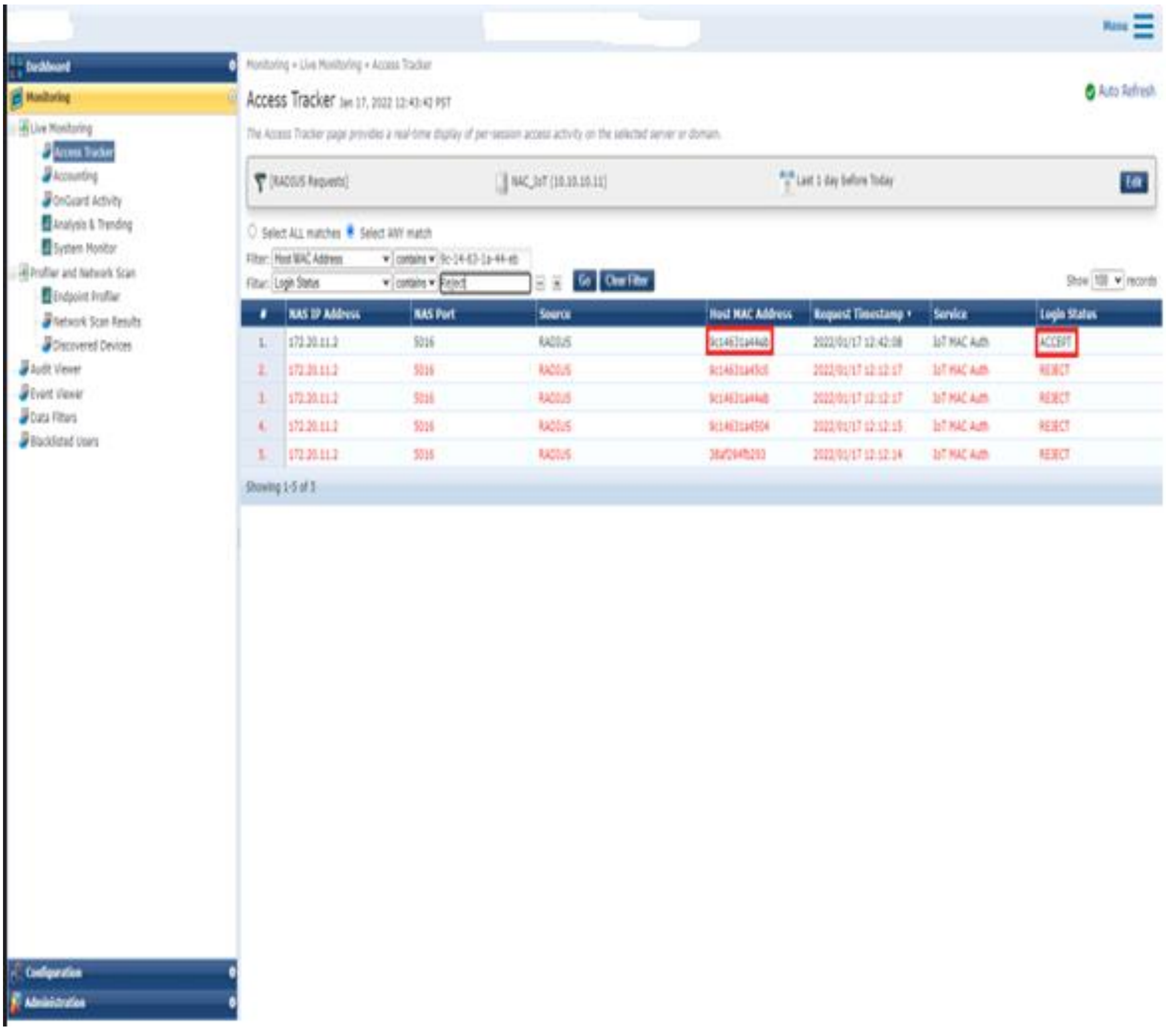
Host Entries

#		Address	Description
1.	○	9c-14-63-1a-44-eb	Camera 1

Address:	
Description:	

Figure 36: Addition of Camera 1 in static host list of NAC

(ii) Adding Camera 1 in NAC, permission will be granted to camera 1, while the remaining devices will be rejected as shown in figure 37.



Monitoring » Live Monitoring » Access Tracker

Access Tracker Jan 17, 2022 12:43:42 PST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[RADIUS Requests] NAC_IoT [10.10.10.11] Last 1 day before Today

○ Select ALL matches ● Select ANY match

Filter: Host MAC Address contains 9c-14-63-1a-44-eb

Filter: Login Status contains Reject

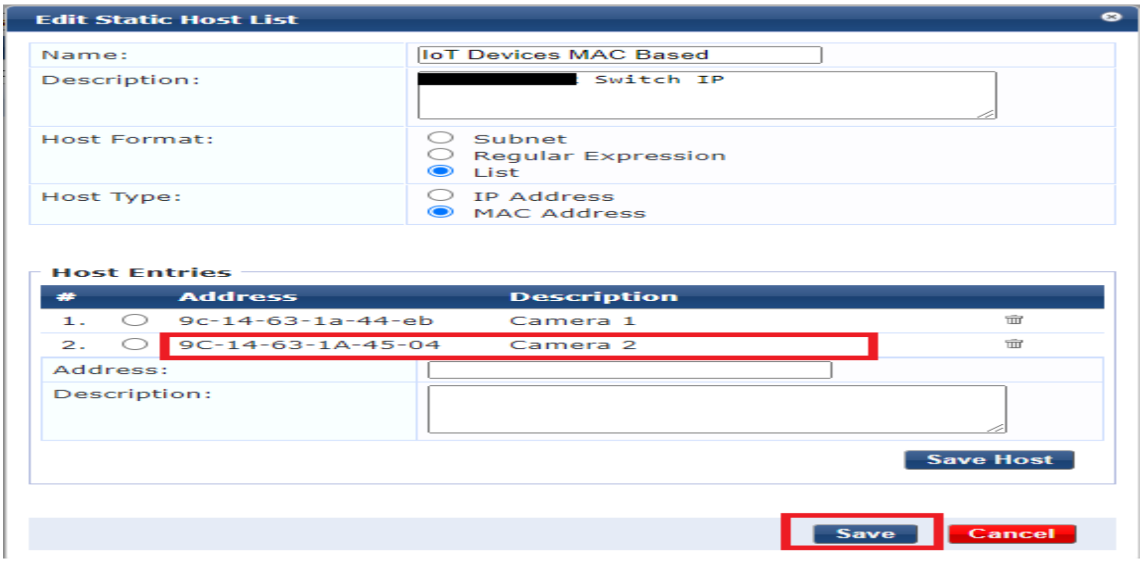
Show 100 records

#	NAS IP Address	NAS Port	Source	Host MAC Address	Request Timestamp	Service	Login Status
1.	172.20.11.2	5016	RADIUS	9c14631a44eb	2022/01/17 12:42:08	IoT MAC Auth	ACCEPT
2.	172.20.11.2	5016	RADIUS	9c14631a45c6	2022/01/17 12:12:17	IoT MAC Auth	REJECT
3.	172.20.11.2	5016	RADIUS	9c14631a44eb	2022/01/17 12:12:17	IoT MAC Auth	REJECT
4.	172.20.11.2	5016	RADIUS	9c14631a4504	2022/01/17 12:12:15	IoT MAC Auth	REJECT
5.	172.20.11.2	5016	RADIUS	38af294fb203	2022/01/17 12:12:14	IoT MAC Auth	REJECT

Showing 1-5 of 5

Figure 37: Authentication of Camera 1 by NAC (access granted)

(iii) To Add Camera 2 in NAC solution, go to “Configuration » Identity » Static Host Lists “and click on switch and Add camera 2 as shown in figure 38.



Edit Static Host List

Name:	IoT Devices MAC Based
Description:	[redacted] Switch IP
Host Format:	○ Subnet ○ Regular Expression ● List
Host Type:	○ IP Address ● MAC Address

Host Entries

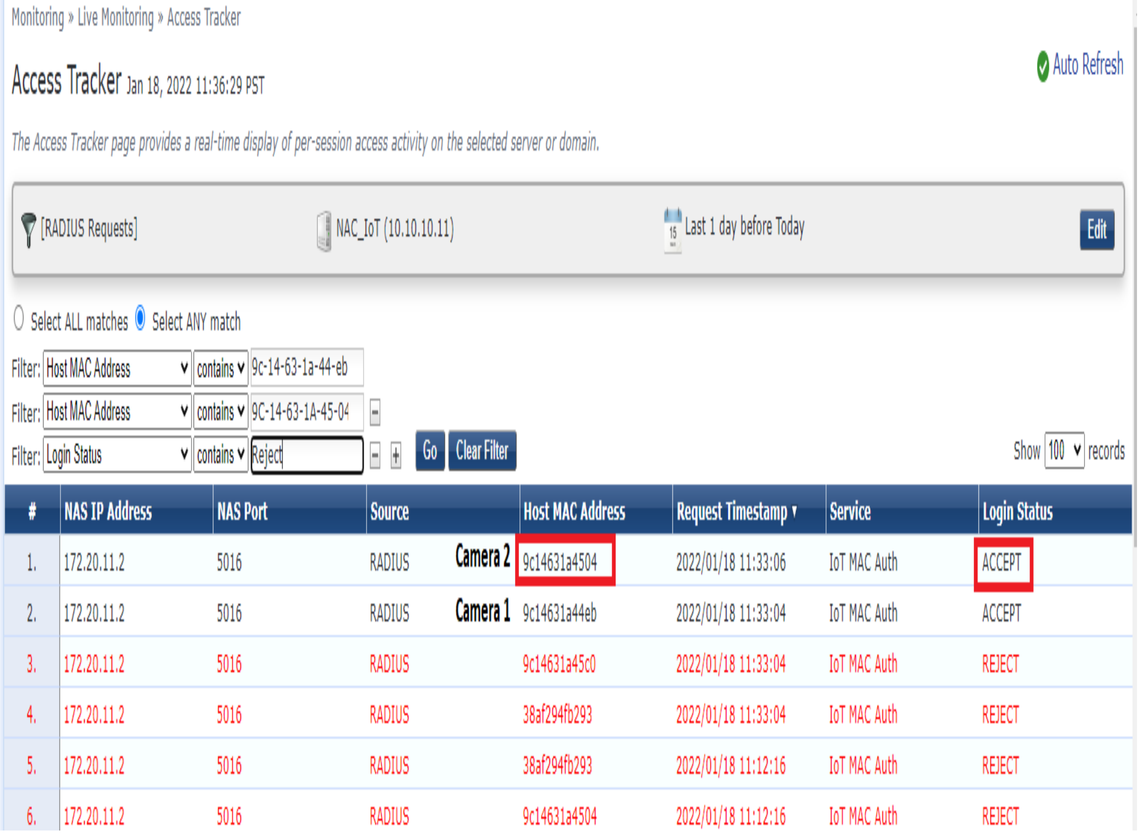
#		Address	Description
1.	○	9c-14-63-1a-44-eb	Camera 1
2.	○	9C-14-63-1A-45-04	Camera 2

Address:

Description:

Figure 38: Addition of Camera 2 in static host list of NAC

(iv) Adding Camera 2 in NAC, permission will be granted to camera 1 and camera 2 because MAC addresses of both have been added in NAC. At the same time, the remaining devices will be rejected as shown in figure 39.



Monitoring » Live Monitoring » Access Tracker

Access Tracker Jan 18, 2022 11:36:29 PST

Auto Refresh

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[RADIUS Requests] NAC_IoT (10.10.10.11) Last 1 day before Today Edit

○ Select ALL matches ● Select ANY match

Filter: Host MAC Address contains 9c-14-63-1a-44-eb

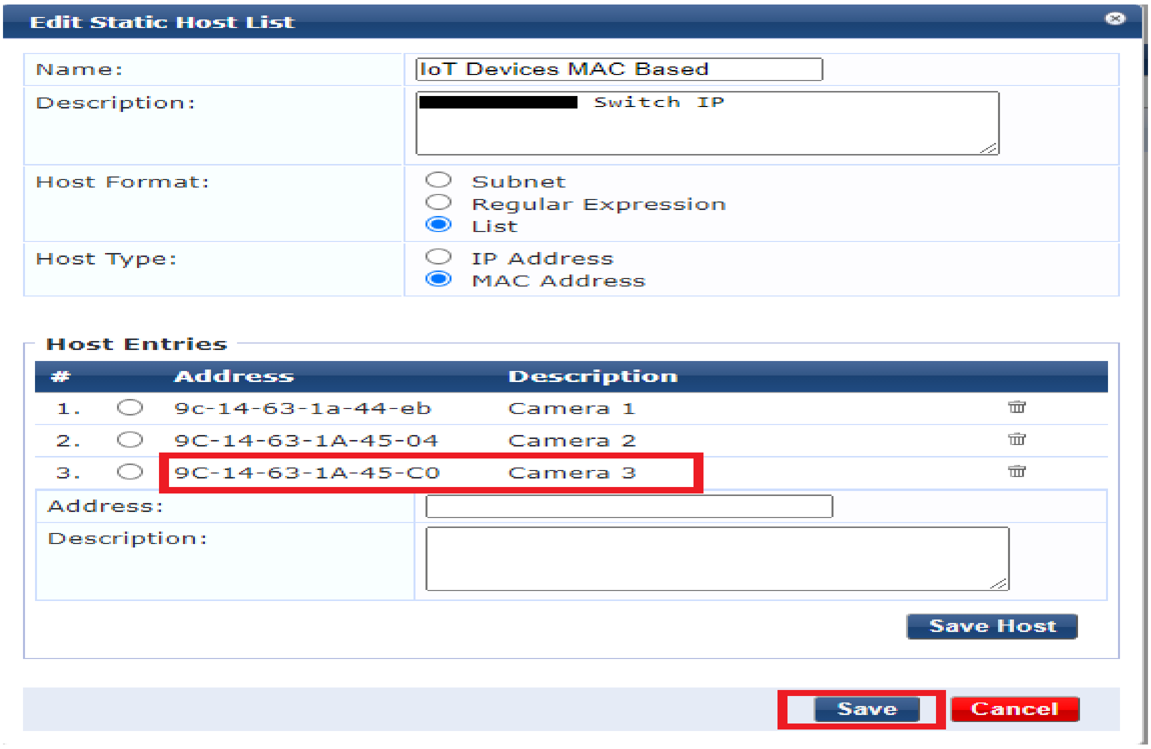
Filter: Host MAC Address contains 9C-14-63-1A-45-04

Filter: Login Status contains Reject

#	NAS IP Address	NAS Port	Source	Host MAC Address	Request Timestamp	Service	Login Status
1.	172.20.11.2	5016	RADIUS Camera 2	9c14631a4504	2022/01/18 11:33:06	IoT MAC Auth	ACCEPT
2.	172.20.11.2	5016	RADIUS Camera 1	9c14631a44eb	2022/01/18 11:33:04	IoT MAC Auth	ACCEPT
3.	172.20.11.2	5016	RADIUS	9c14631a45c0	2022/01/18 11:33:04	IoT MAC Auth	REJECT
4.	172.20.11.2	5016	RADIUS	38af294fb293	2022/01/18 11:33:04	IoT MAC Auth	REJECT
5.	172.20.11.2	5016	RADIUS	38af294fb293	2022/01/18 11:12:16	IoT MAC Auth	REJECT
6.	172.20.11.2	5016	RADIUS	9c14631a4504	2022/01/18 11:12:16	IoT MAC Auth	REJECT

Figure 39: Authentication of Cam 2 and cam 1 by NAC (access granted)

(v) To Add Camera 3 in NAC, go to “Configuration » Identity » Static Host Lists “and click on switch and Add camera 3 as shown in figure 40.



Edit Static Host List

Name:	IoT Devices MAC Based
Description:	[redacted] Switch IP
Host Format:	○ Subnet ○ Regular Expression ● List
Host Type:	○ IP Address ● MAC Address

Host Entries

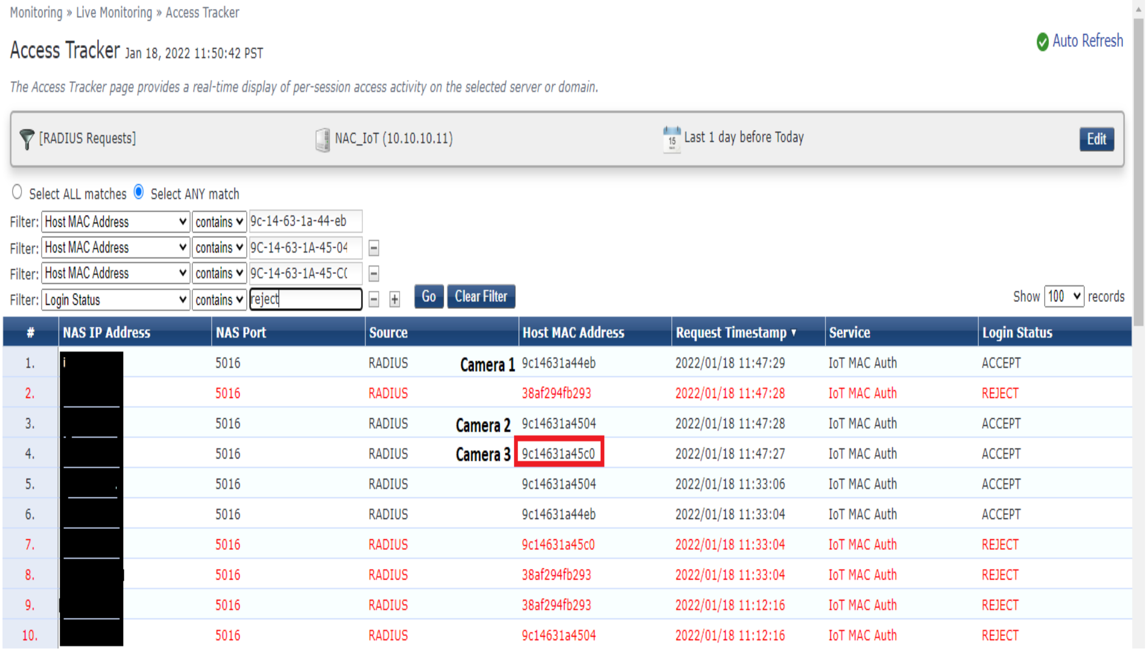
#		Address	Description
1.	○	9c-14-63-1a-44-eb	Camera 1
2.	○	9C-14-63-1A-45-04	Camera 2
3.	○	9C-14-63-1A-45-C0	Camera 3

Address:

Description:

Figure 40: Addition of Camera 3 in static host list of NAC

(vi) Adding Camera 3 in NAC, permission will be granted to camera 1, camera 2 and camera 3 because MAC addresses have been added in NAC. At the same time, the remaining devices will be rejected as shown in figure 41.



Monitoring » Live Monitoring » Access Tracker

Access Tracker Jan 18, 2022 11:50:42 PST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[RADIUS Requests] NAC_IoT (10.10.10.11) Last 1 day before Today

○ Select ALL matches ● Select ANY match

Filter: Host MAC Address contains 9c-14-63-1a-44-eb
Filter: Host MAC Address contains 9C-14-63-1A-45-04
Filter: Host MAC Address contains 9C-14-63-1A-45-C(
Filter: Login Status contains reject

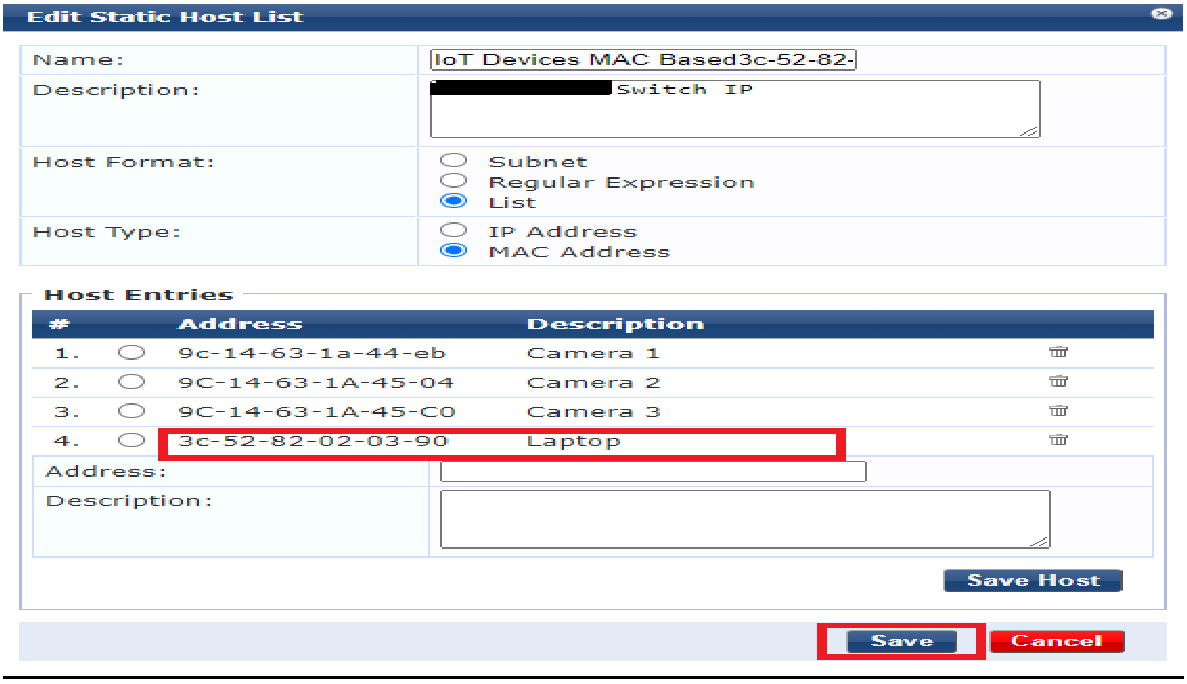
Show 100 records

#	NAS IP Address	NAS Port	Source	Host MAC Address	Request Timestamp ▾	Service	Login Status
1.	[redacted]	5016	RADIUS	Camera 1 9c14631a44eb	2022/01/18 11:47:29	IoT MAC Auth	ACCEPT
2.	[redacted]	5016	RADIUS	38af294fb293	2022/01/18 11:47:28	IoT MAC Auth	REJECT
3.	[redacted]	5016	RADIUS	Camera 2 9c14631a4504	2022/01/18 11:47:28	IoT MAC Auth	ACCEPT
4.	[redacted]	5016	RADIUS	Camera 3 9c14631a45c0	2022/01/18 11:47:27	IoT MAC Auth	ACCEPT
5.	[redacted]	5016	RADIUS	9c14631a4504	2022/01/18 11:33:06	IoT MAC Auth	ACCEPT
6.	[redacted]	5016	RADIUS	9c14631a44eb	2022/01/18 11:33:04	IoT MAC Auth	ACCEPT
7.	[redacted]	5016	RADIUS	9c14631a45c0	2022/01/18 11:33:04	IoT MAC Auth	REJECT
8.	[redacted]	5016	RADIUS	38af294fb293	2022/01/18 11:33:04	IoT MAC Auth	REJECT
9.	[redacted]	5016	RADIUS	38af294fb293	2022/01/18 11:12:16	IoT MAC Auth	REJECT
10.	[redacted]	5016	RADIUS	9c14631a4504	2022/01/18 11:12:16	IoT MAC Auth	REJECT

Figure 41: Authentication of Cam (3, 2 & 1) by NAC (Access granted)

c. Adding Laptop in NAC (Static host List)

(i) To Add Laptop in NAC, go to “Configuration » Identity » Static Host Lists “and click on switch; add Laptop as shown in figure 42



Edit Static Host List

Name:	IoT Devices MAC Based3c-52-82-
Description:	[redacted] Switch IP
Host Format:	○ Subnet ○ Regular Expression ● List
Host Type:	○ IP Address ● MAC Address

Host Entries

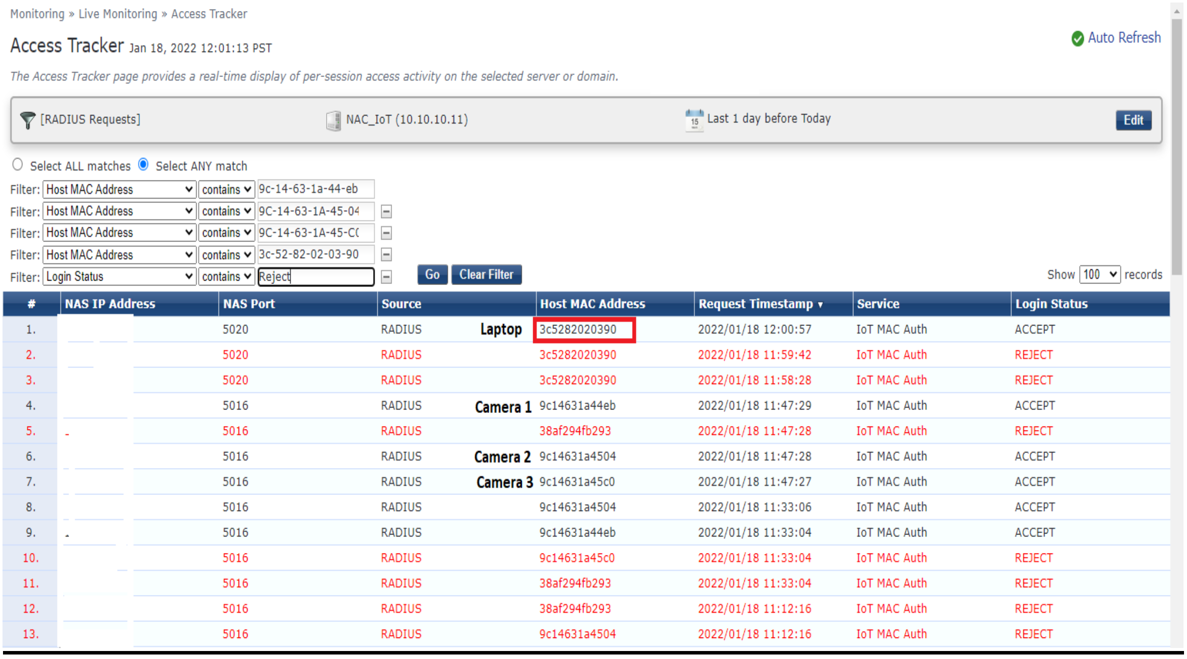
#		Address	Description
1.	○	9c-14-63-1a-44-eb	Camera 1
2.	○	9C-14-63-1A-45-04	Camera 2
3.	○	9C-14-63-1A-45-C0	Camera 3
4.	○	3c-52-82-02-03-90	Laptop

Address:

Description:

Figure 42: Addition of Laptop in static host list of NAC

(ii) Adding laptop in NAC, permission will be granted to Laptop, camera 1, camera 2 and camera 3 because MAC addresses have been added in NAC, while remaining devices will be rejected as shown in figure 43.



Monitoring » Live Monitoring » Access Tracker

Access Tracker Jan 18, 2022 12:01:13 PST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

[RADIUS Requests] NAC_IoT (10.10.10.11) Last 1 day before Today

○ Select ALL matches ● Select ANY match

Filter: Host MAC Address contains 9c-14-63-1a-44-eb
Filter: Host MAC Address contains 9C-14-63-1A-45-04
Filter: Host MAC Address contains 9C-14-63-1A-45-C(
Filter: Host MAC Address contains 3c-52-82-02-03-90
Filter: Login Status contains Reject

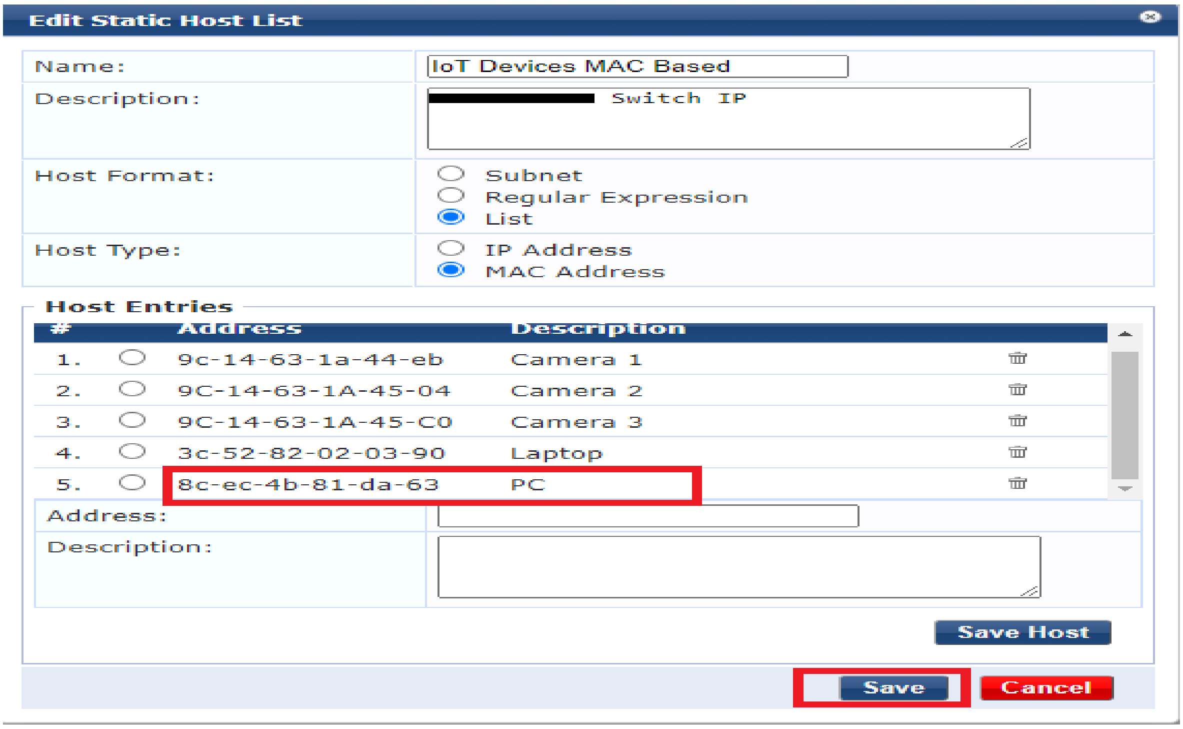
Show 100 records

#	NAS IP Address	NAS Port	Source	Host MAC Address	Request Timestamp ▾	Service	Login Status
1.		5020	RADIUS Laptop	3c5282020390	2022/01/18 12:00:57	IoT MAC Auth	ACCEPT
2.		5020	RADIUS	3c5282020390	2022/01/18 11:59:42	IoT MAC Auth	REJECT
3.		5020	RADIUS	3c5282020390	2022/01/18 11:58:28	IoT MAC Auth	REJECT
4.		5016	RADIUS Camera 1	9c14631a44eb	2022/01/18 11:47:29	IoT MAC Auth	ACCEPT
5.		5016	RADIUS	38af294fb293	2022/01/18 11:47:28	IoT MAC Auth	REJECT
6.		5016	RADIUS Camera 2	9c14631a4504	2022/01/18 11:47:28	IoT MAC Auth	ACCEPT
7.		5016	RADIUS Camera 3	9c14631a45c0	2022/01/18 11:47:27	IoT MAC Auth	ACCEPT
8.		5016	RADIUS	9c14631a4504	2022/01/18 11:33:06	IoT MAC Auth	ACCEPT
9.		5016	RADIUS	9c14631a44eb	2022/01/18 11:33:04	IoT MAC Auth	ACCEPT
10.		5016	RADIUS	9c14631a45c0	2022/01/18 11:33:04	IoT MAC Auth	REJECT
11.		5016	RADIUS	38af294fb293	2022/01/18 11:33:04	IoT MAC Auth	REJECT
12.		5016	RADIUS	38af294fb293	2022/01/18 11:12:16	IoT MAC Auth	REJECT
13.		5016	RADIUS	9c14631a4504	2022/01/18 11:12:16	IoT MAC Auth	REJECT

Figure 43: Authentication of Laptop, Cam (3, 2&1) by NAC (Access granted)

d. Adding PC in NAC (Static host List)

(i) To Add PC in NAC, go to “Configuration » Identity » Static Host Lists “and click on switch. Add PC as shown in figure 44.



Edit Static Host List

Name:	IoT Devices MAC Based
Description:	[redacted] Switch IP
Host Format:	○ Subnet ○ Regular Expression ● List
Host Type:	○ IP Address ● MAC Address

Host Entries

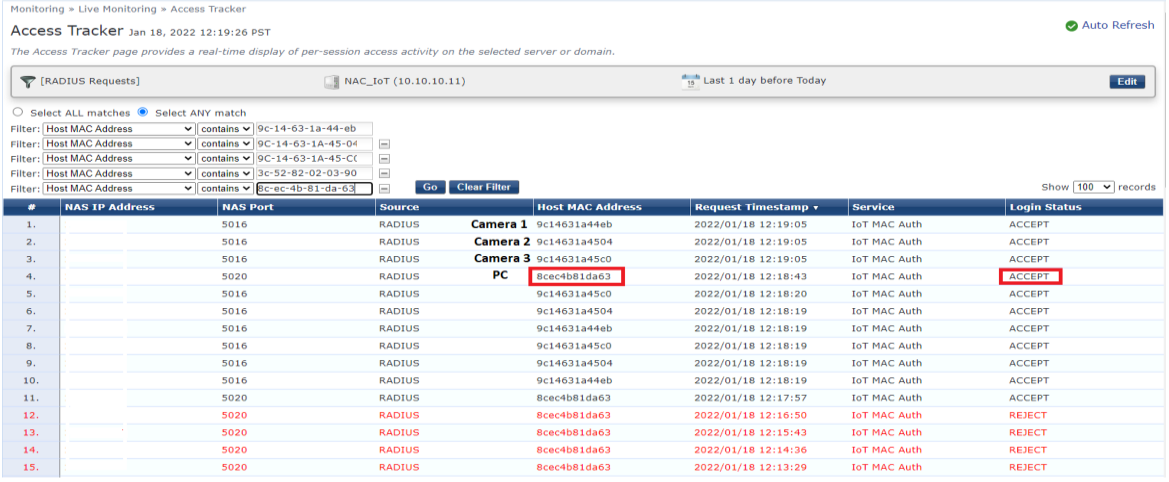
#		Address	Description	
1.	○	9c-14-63-1a-44-eb	Camera 1	🗑
2.	○	9C-14-63-1A-45-04	Camera 2	🗑
3.	○	9C-14-63-1A-45-C0	Camera 3	🗑
4.	○	3c-52-82-02-03-90	Laptop	🗑
5.	○	8c-ec-4b-81-da-63	PC	🗑

Address:

Description:

Figure 44: Addition of Laptop in static host list of NAC

(ii) Adding PC in NAC, permission will be granted to PC, Laptop, camera 1, camera 2 and camera 3 because MAC addresses are added in NAC. At the same time, the remaining devices will be rejected if they try to connect with cloud infrastructure, as shown in figure 45.



Monitoring » Live Monitoring » Access Tracker

Access Tracker Jan 18, 2022 12:19:26 PST

The Access Tracker page provides a real-time display of per-session access activity on the selected server or domain.

○ Select ALL matches ● Select ANY match

Filter: Host MAC Address contains 9c-14-63-1a-44-eb
Filter: Host MAC Address contains 9C-14-63-1A-45-04
Filter: Host MAC Address contains 9C-14-63-1A-45-C(
Filter: Host MAC Address contains 3c-52-82-02-03-90
Filter: Host MAC Address contains 8c-ec-4b-81-da-63

Show 100 records

#	NAS IP Address	NAS Port	Source	Host MAC Address	Request Timestamp ▾	Service	Login Status
1.		5016	RADIUS **Camera 1**	9c14631a44eb	2022/01/18 12:19:05	IoT MAC Auth	ACCEPT
2.		5016	RADIUS **Camera 2**	9c14631a4504	2022/01/18 12:19:05	IoT MAC Auth	ACCEPT
3.		5016	RADIUS **Camera 3**	9c14631a45c0	2022/01/18 12:19:05	IoT MAC Auth	ACCEPT
4.		5020	RADIUS **PC**	8cec4b81da63	2022/01/18 12:18:43	IoT MAC Auth	ACCEPT
5.		5016	RADIUS	9c14631a45c0	2022/01/18 12:18:20	IoT MAC Auth	ACCEPT
6.		5016	RADIUS	9c14631a4504	2022/01/18 12:18:19	IoT MAC Auth	ACCEPT
7.		5016	RADIUS	9c14631a44eb	2022/01/18 12:18:19	IoT MAC Auth	ACCEPT
8.		5016	RADIUS	9c14631a45c0	2022/01/18 12:18:19	IoT MAC Auth	ACCEPT
9.		5016	RADIUS	9c14631a4504	2022/01/18 12:18:19	IoT MAC Auth	ACCEPT
10.		5016	RADIUS	9c14631a44eb	2022/01/18 12:18:19	IoT MAC Auth	ACCEPT
11.		5020	RADIUS	8cec4b81da63	2022/01/18 12:17:57	IoT MAC Auth	ACCEPT
12.		5020	RADIUS	8cec4b81da63	2022/01/18 12:16:50	IoT MAC Auth	REJECT
13.		5020	RADIUS	8cec4b81da63	2022/01/18 12:15:43	IoT MAC Auth	REJECT
14.		5020	RADIUS	8cec4b81da63	2022/01/18 12:14:36	IoT MAC Auth	REJECT
15.		5020	RADIUS	8cec4b81da63	2022/01/18 12:13:29	IoT MAC Auth	REJECT

Figure 45: Authentication of Laptop, Cam (3, 2&1) by NAC (Access granted)

6.6 Results

a. Normal flow of the architecture – without implementing NAC

Table 10 shows normal flow of the architecture. In this architecture, NAC is not implemented so for.

Device Description	NAC implemented	Connectivity permitted	Connectivity denied	Remarks
Camera 1	×	✓	×	Cloud infrastructure has been accessed by Cameras (1, 2, and 3), Laptop and PC because NAC has not deployed for access control.
Camera 2	×	✓	×	
Camera 3	×	✓	×	
Laptop	×	✓	×	
PC	×	✓	×	

Table 10: Normal Flow – without implementing NAC

b. Flow of the proposed architecture after NAC implementation – Before registering devices on NAC

Table 11 shows the flow of the architecture after deployment of NAC. In this architecture, NAC is deployed, but devices are not registered with NAC.

Device Description	NAC implemented	Device registration on NAC	Connectivity permitted	Connectivity denied	Remarks
Camera 1	✓	×	×	✓	NAC rejected all requests initiated by Camera (1, 2, and 3), Laptop and PC to access cloud infrastructure because devices have not been registered with NAC.
Camera 2	✓	×	×	✓	
Camera 3	✓	×	×	✓	
Laptop	✓	×	×	✓	
PC	✓	×	×	✓	

Table 11: Flow after NAC implementation– Before registering devices with NAC

c. Flow of the proposed architecture – After registering devices on NAC

Table 12 shows flow of the proposed architecture after deployment of NAC. In this architecture, NAC is deployed and devices are registered with NAC.

Device Description	NAC implemented	Device registration on NAC	Connectivity permitted	Connectivity denied	Remarks
Camera 1	✓	✓	✓	×	NAC permitted all requests initiated by Cameras (1, 2, and 3), Laptop and PC to access cloud infrastructure because devices have been registered on NAC.
Camera 2	✓	✓	✓	×	
Camera 3	✓	✓	✓	×	
Laptop	✓	✓	✓	×	
PC	✓	✓	✓	×	

Table 12: Flow after NAC implementation– after registering devices with NAC

d. Flow of the proposed architecture – After registering Camera 1 and Camera 2 on NAC and Camera 3, Laptop and PC Remained unregister

Table 13 shows flow of the proposed architecture after deployment of NAC. In this architecture, NAC is deployed. It is highlighted that in this scenario, only camera 1 & camera 2 are registered with NAC. The remaining devices i.e. camera 3, laptop and PC are not registered with NAC.

Device Description	NAC implemented	Device registration on NAC	Connectivity permitted	Connectivity denied	Remarks
Camera 1	✓	✓	✓	×	NAC only permitted requests initiated by Camera (1, 2,3) because both devices are registered with NAC and rejected requests from Laptop and PC to access cloud infrastructure because devices have not been registered on NAC.
Camera 2	✓	✓	✓	×	
Camera 3	✓	✓	✓	×	
Laptop	✓	×	×	✓	
PC	✓	×	×	✓	

Table 13: Registering Camera (1&2) on NAC and leaving remaining devices unregistered

6.7 Summary

In this chapter, the proposed idea has been implemented in real cloud-based IoT environment. This chapter covers establishing lab setup, configuring all participating devices, and analyzing results considering the proposed idea. The last chapter of this study covers conclusion and future work of the study.

Chapter 7

Conclusion and Future Work

7.1 Conclusion and future work

In this study, access control mechanism in cloud-based IoT environment has been presented that can also mitigate multiple threats to cloud-based IoT systems. A novel security solution i.e. NAC has been implemented to restrict/ permit IoT devices to access cloud infrastructure. In this study, security of cloud-based IoT systems has been enhanced through NAC. It is pertinent to mention that researchers have contributed to the secure integration of cloud computing and IoT devices. However, there are rare evidences where access control along with minimization of many threats is addressed in a single study. Furthermore, in addition to access control, the proposed solution can mitigate multiple threats to cloud-based IoT systems by integrating the same with third parties security solutions like Firewall, SIEM, AVs, and NIARA. This study discusses the proposed solution's system architecture, its working methodology, and threats to cloud-based IoT systems.

Implementing the proposed solution in real environment, following has been deduced/ concluded.

- Request from devices recognized/registered with NAC to access cloud infrastructure was permitted to access cloud infrastructure.

- Request from devices not recognized/ registered with NAC to access cloud infrastructure was denied.

- The access control mechanism provided by NAC in a cloud-based IoT system has been verified in a real cloud-based environment and is working fine.

- Solution is considered more suitable for organizations having on-premises cloud. However, organizations using the off-premises cloud can also implement the same as the end users are authenticated before accessing cloud resources.

- Few threats can also be mitigated by implementing the proposed solution.

- Users are authenticated prior to engaging with the cloud. The same allows the organization to monitor and restrict users before connecting to cloud infrastructure.

For future research directions, following is suggested.

- Third parties vendors (As already discussed) like firewalls, AVs, NIARA etc. may be integrated with NAC to simulate threats mitigation and to verify multiple threats mitigation by proposed solution. It is pertinent to mention that in our lab environment, NAC with only access license was available; therefore, we could not simulate/ verify multiple threats faced by cloud-based IoT systems.

- Indigenous application having features of NAC, AV database, behavior analytics for anomaly detection, and device profiling may be designed for organizations using our proposed idea.

- The proposed idea has been verified in on-premises environment. The same may be extended to off-premises cloud-based IoT environment.

Bibliography

[1] J. Pourqasem, “Cloud-based IoT: integration cloud computing with internet of things,” International Journal of Research in Industrial Engineering, vol. 7, no. 4, pp. 482–494, 2018.

[2] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos, “Security and privacy for cloud-based iot: Challenges,” IEEE Communications Magazine, vol. 55, no. 1, pp. 26–33, 2017.

[3] C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, “Secure integration of iot and cloud computing,” Future Generation Computer Systems, vol. 78, pp. 964–975, 2018.

[4] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang and D. Chen, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach," in IEEE Access, vol. 7, pp. 9368-9383, 2019, doi: 10.1109/ACCESS.2018.2890432.

[5] Tawalbeh, Loai & Muheidat, Fadi & Tawalbeh, Mais & Quwaider, Muhannad. (2020). IoT Privacy and Security: Challenges and Solutions. Applied Sciences. 10. 4102. 10.3390/app10124102.

[6] S. Bhatt, L. A. Tawalbeh, P. Chhetri and P. Bhatt, "Authorizations in Cloud-Based Internet of Things: Current Trends and Use Cases," 2019 Fourth International Conference on Fog and Mobile Edge Computing (FMEC), Rome, Italy, 2019, pp. 241-246, doi: 10.1109/FMEC.2019.8795309.

[7] Bhawiyuga, Adhitya & Primanita, Dany & Amron, Kasyful & Pratama, Ocki & Habibi, Moch. (2019). Architectural design of IoT-cloud computing integration platform. TELKOMNIKA (Telecommunication Computing Electronics and Control). 17. 1399. 10.12928/telkomnika.v17i3.11786.

[8] Mohammad Wazid, Ashok Kumar Das, Rasheed Hussain, Giancarlo Succi, Joel J.P.C. Rodrigues, Authentication in cloud-driven IoT-based big data environment: Survey and outlook, Journal of Systems Architecture, Volume 97, 2019, Pages 185-196, ISSN 1383-7621, https://doi.org/10.1016/j.sysarc.2018.12.005.

[9] Abbas N, Asim M, Tariq N, Baker T, Abbas S. A Mechanism for Securing IoT-enabled Applications at the Fog Layer. Journal of Sensor and Actuator Networks. 2019; 8(1):16.

[10] Bhabendu Kumar Mohanta, Debasish Jena, Utkalika Satapathy, Srikanta Patnaik, Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and Blockchain technology, Internet of Things, Volume 11, 2020, 100227, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2020.100227.

[11] Liang Liu, Zuchao Ma, Weizhi Meng, Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks, Future Generation Computer Systems, Volume 101, 2019, Pages 865-879, ISSN 0167-739X, https://doi.org/10.1016/j.future.2019.07.021.

[12] Mario Barbareschi, Alessandra De Benedictis, Erasmo La Montagna, Antonino Mazzeo, Nicola Mazzocca, A PUF-based mutual authentication scheme for Cloud-Edges IoT systems, Future Generation Computer Systems, Volume 101, 2019, Pages 246-261, ISSN 0167-739X, https://doi.org/10.1016/j.future.2019.06.012.

[13] A. S. Rumale and D. N. Chaudhari, "Cloud computing: Software as a service," 2017 Second International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017, pp. 1-6, doi: 10.1109/ICECCT.2017.8117817.

[14] K. Riad, R.Hamza and H. Yan, “Sensitive and Energetic IoT Access Control for managing cloud electronic health records,” in IEEE access, vol. 7, pp. 86384-86393, 2019, DOI: 10.1109/ access.2019.2926354.

[15] A.Riaz, R.Ahmed, A K. Kiani and S.Saleem”Access Control for Fog/ Cloud enabled IoT,” Sept 2019 International Journal of Computer Science and Information Security (IJCSIS) Vol. 17, No.9.

[16] (H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters and G. B. Wills, "Integration of Cloud Computing with the Internet of Things: Challenges and Open Issues," 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (Green Com) and IEEE Cyber, Physical and Social Computing (CPS Com) and IEEE Smart Data (Smart Data), 2017, pp. 670-675, DOI: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.105.)

[17] Bamiah, Mervat & Brohi, Sarfraz. (2013). Exploring the Cloud Deployment and Service Delivery Models.

[18] A. R. Javed, M. Usman, S. U. Rehman, M. U. Khan and M. S. Haghighi, "Anomaly Detection in Automated Vehicles Using Multistage Attention-Based Convolutional Neural Network," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 7, pp. 4291-4300, July 2021, doi: 10.1109/TITS.2020.3025875.

[19] Riaz, S.; Khan, A.H.; Haroon, M.; Latif, S.; Bhatti, S. Big Data Security and Privacy: Current Challenges and Future Research perspective in Cloud Environment. In Proceedings of the 2020 International Conference on Information Management and Technology (ICIM Tech), Bandung, Indonesia, 13–14 August 2020; pp. 977–982.

[20] Ahmed, Waqas & Javed, Abdul Rehman & Baker, Thar & Jalil, Zunera. (2021). Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey. Electronics. 16. 10.3390/electronics11010016.

[21] Arlene G. Fink. Conducting Research Literature Reviews: From Paper to the Internet. Sage Publications, Inc, first edition, April 1998.

[22] Myagmar, Suvda & Lee, Adam & Yurcik, William. (2005). Threat Modeling as a Basis for Security Requirements.

[23] Hassan, Zozo & Ali, Hesham & Badawy, Mahmoud. (2015). Internet of Things (IoT): Definitions, Challenges, and Recent Research Directions. International Journal of Computer Applications. 128. 975-8887.

[24] I. Seth, S. N. Panda and K. Guleria, "IoT based Smart Applications and Recent Research Trends," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 407-412, doi: 10.1109/ISPCC53510.2021.9609484.

[25] X. Li, Q. Wang, X. Lan, X. Chen, N. Zhang and D. Chen, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach," in IEEE Access, vol. 7, pp. 9368-9383, 2019, doi: 10.1109/ACCESS.2018.2890432.

[26] Sheth, Mrs & Bhosale, Sachin & Kadam, Mr & Prof, Asst. (2021). Research Paper on Cloud Computing. 2021.

[27] O. Georgiana Dorobantu and S. Halunga, "Security threats in IoT," 2020 International Symposium on Electronics and Telecommunications (ISETC), 2020, pp. 1-4, doi: 10.1109/ISETC50328.2020.9301127.

[28] S. M. Alrubei, E. Ball and J. M. Rigelsford, "The Use of Blockchain to Support Distributed AI Implementation in IoT Systems," in IEEE Internet of Things Journal, vol. 9, no. 16, pp. 14790-14802, 15 Aug.15, 2022, doi: 10.1109/JIOT.2021.3064176.

[29] S. Y. W. Irene and C.L. Ng, *The Internet-of-Things: Review and research directions*, pp. 3-21, 2016.

[30] G. A. R, Y. P. Singh and N. S. Narawade, "Design Of Fog Computing System For Health Care Applications Based On IoT," 2022 3rd International Conference for Emerging Technology (INCET), 2022, pp. 1-4, doi: 10.1109/INCET54531.2022.9825347.

[31] Sheth, Mrs & Bhosale, Sachin & Kadam, Mr & Prof, Asst. (2021). Research Paper on Cloud Computing. 2021.

[32] S. Gupta, A. Gupta and G. Shankar, "Cloud Computing: Services, Deployment Models and Security Challenges," 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 414-418, doi: 10.1109/ICOSEC51865.2021.9591794.

[33] Mohammad, Ahmad & Aldalabeeh, Ahmad. (2022). Cloud Deployment Models.

[34] B., Patel. (2021). Cloud Computing Deployment Models: A Comparative Study. International Journal of Innovative Research in Computer Science & Technology. 9. 10.21276/ijircst.2021.9.2.8.

[35] Sameer, Ameer. (2020). Internet of Things (IoT) Security. 10.1109/NTICT.2020.P20.

[36] Hezam, Akram & Konstantas, Dimitri & Mahyoub, Mohammed. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Mode. International Journal of Advanced Computer Science and Applications. Vol. 9. 10.14569/IJACSA.2018.090349.

[37] Manjunath V , Devidas Kalaskar, 2020, Cloud Assisted IoT Application’s Security Attacks and their Countermeasures, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 09, Issue 05 (May 2020),

[38] Milosevic, Jelena & Sklavos, Nicolas & Koutsikou, Konstantina. (2016). Malware in IoT Software and Hardware.

[39] Abdulkareem, Nasiba & Zeebaree, Subhi & M.Sadeeq, Mohammed & Ahmed, Dindar & Sami, Ahmed & Zebari, Rizgar. (2021). IoT and Cloud Computing Issues, Challenges and Opportunities: A Review. 1. 1-7. 10.48161/qaj.v1n2a36.

[40] Park, Mookyu & Oh, Haengrok & Lee, Kyungho. (2019). Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective. Sensors. 19. 2148. 10.3390/s19092148.

[41] Capra, Maurizio & Peloso, Riccardo & Masera, Guido & Ruo Roch, Massimo & Martina, Maurizio. (2019). Edge Computing: A Survey On the Hardware Requirements in the Internet of Things World. Future Internet. 11. 100. 10.3390/fi11040100.

[42] Sharma, Sugam & Chang, Victor & Tim, U. & Wong, Johnny & Gadia, Shashi. (2019). Cloud and IoT-based emerging services systems. Cluster Computing. 22. 10.1007/s10586-018-2821-8.