bb

VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belagavi-590018

A

Technical Seminar Report

On

"Secure System in Digital Era"

SUBMITTED IN PARTIAL FULFILLMENT FOR THE AWARD OF DEGREE OF

BACHELOR OF ENGINEERING

IN

COMPUTER SCEINCE AND ENGINEERING

SUBMITTED BY

B P Sanjana Urs (1JB21CS023)

Under the Guidance of

Mrs.Vijayalakshmi B
Assistant Professor
Dept of CSE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SJB INSTITUTE OF TECHNOLOGY

No.67, BGS Health & Education City, Dr.Vishnuvardhan Rd, Kengeri, Bengaluru, Karnataka 560060
An Autonomous Institute under VTU
Approved by AICTE - New Delhi, Accredited by NAAC A+, Accredited by NBA

2024 - 2025

|| Jai Sri Gurudev ||

Sri Adichunchanagiri Shikshana Trust ®

SJB INSTITUTE OF TECHNOLOGY

An Autonomous Institute under VTU

No.67, BGS Health & Education City, Dr.Vishnuvardhan Rd, Kengeri, Bengaluru, Karnataka 560060

Department of Computer Science and Engineering

CERTIFICATE

This is to certify that the seminar work entitled ***"Secure System in Digital Era"*** is carried out by **B P Sanjana URS(1JB21CS023)** is bonafide student of **SJB Institute of Technology**, in partial fulfillment for the award of **"BACHELOR OF ENGINEERING"** in **COMPUTER SCIENCE AND ENGINEERING** as prescribed by **VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI** during the academic year **2024-2025**. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report deposited in the departmental library. The Technical Seminar report has been approved as it satisfies the academic requirements in respect of seminar work prescribed for the said degree.

Signature of Guide	**Signature of HOD**
Mrs. Vijayalakshmi B	**Dr. Krishna A N**
Assistant Professor	**Professor & Head**
Dept. of CSE, SJBIT	**Dept. of CSE, SJBIT**

ACKNOWLEDGEMENT

I would like to express my profound grateful to His Divine Soul **Jagadguru Padmabhushan Sri Sri Sri Dr. Balagangadharanatha Mahaswamiji** and His Holiness **Jagadguru Sri Sri Sri Dr. Nirmalanandanatha Mahaswamiji** for providing us an opportunity to complete my academics in this esteemed institution.

I would also like to express my profound thanks to **Revered Sri Sri Dr. Prakashnath Swamiji**, Managing Director, BGS & SJB Group of Institutions, for his continuous support in providing amenities to carry out this Project Work in this admired institution.

I express my gratitude to **Dr. Puttaraju,** Academic Director, BGS & SJB Group of Institutions, for providing me an excellent facilitiy and academic ambience, which have helped me in satisfactory completion of Project work.

I express my gratitude to **Dr. K. V. Mahendra Prashanth**, Principal, SJB Institute of Technology, for providing me an excellent facilities and academic ambience; which have helped me in satisfactory completion of Technical Seminar.

I extend my heartfelt gratitude to all the Deans of SJB Institute of Technology for their unwavering support, cutting-edge facilities, and the inspiring academic environment, all of which played a pivotal role in the successful completion of my Technical Seminar.

I extend my sincere thanks to **Dr. Krishna A N,** Head of the Department, Computer Science and Engineering, for providing me an invaluable support throughout the period of our Technical Seminar.

I wish to express my heartfelt gratitude to my guide **Mrs. Vijayalakshmi B, Assistant Professor**, Department of CSE for her valuable guidance, suggestions and cheerful encouragement during the entire period of my Seminar.

I express my truthful thanks to **Mrs. Shubha T V** , Technical Seminar Coordinator, Department of Computer Science and Engineering, for her valuable support throughout our Seminar.

Finally, I take this opportunity to extend my earnest gratitude and respect to my parents, Teaching & Non teaching staffs of the department, the library staff and all my friends, who have directly or indirectly supported me during the period of my Technical Seminar.

Regards,
B P Sanjana Urs [1JB21CS023]

ABSTRACT

In today's hyper-connected world, where digital technologies drive nearly every aspect of human activity, the importance of secure systems cannot be overstated. As individuals, businesses, and governments increasingly depend on digital platforms for storing and exchanging sensitive information, ensuring the confidentiality, integrity, and availability of data has become a top priority. This paper delves into the evolving landscape of cybersecurity and the essential components required to build secure systems in the digital era.

We begin by examining the core principles of cybersecurity—encryption, authentication, access control, and secure communication protocols—and how they collectively contribute to system resilience. The paper also explores the emerging challenges posed by sophisticated cyber threats, including phishing, ransomware, zero-day attacks, and insider threats, which exploit both technical vulnerabilities and human behavior.

With the rise of cloud computing, IoT devices, mobile networks, and AI-powered systems, new attack surfaces have emerged, necessitating innovative approaches to defense. This includes the integration of artificial intelligence and machine learning for real-time threat detection, behavioral analysis, and predictive security. Additionally, we consider the growing importance of regulatory compliance (e.g., GDPR, HIPAA) and ethical considerations in designing systems that respect user privacy while maintaining robust protection.

By combining technical strategies with strong governance policies and continuous user education, secure systems in the digital age can offer not only protection against current threats but also adaptability for future challenges. This paper underscores the need for a proactive, layered, and collaborative approach to security—where technology, policy, and awareness work hand-in-hand to safeguard our digital lives.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Overview of Secure System

In the digital era, where technology plays a central role in everyday life, the need for secure systems has become more critical than ever. As individuals, businesses, and governments increasingly rely on digital platforms to store, process, and exchange sensitive information, the risks associated with cyber threats have grown significantly. Secure systems are designed to protect data, ensure privacy, and maintain the integrity and availability of services, even in the face of malicious attacks. These systems use a combination of advanced technologies such as encryption, authentication mechanisms, firewalls, and intrusion detection tools to safeguard against unauthorized access and data breaches. With the growing adoption of cloud computing, the Internet of Things (IoT), and artificial intelligence, the security landscape is continuously evolving, introducing new vulnerabilities and requiring adaptive defense strategies. Beyond technology, the human factor plays a major role, as user awareness, strong cybersecurity policies, and ethical practices are essential in maintaining a secure digital environment. Ultimately, building and maintaining secure systems is not just a technical challenge but a fundamental requirement for trust, safety, and sustainability in our increasingly connected world.

.

1.2 The Emergence of Secure System in Real-Time Communication

The rise of secure system was propelled by the increasing demand for real-time content delivery and interactive experiences in the digital era. As internet speeds improved and multimedia content consumption surged, users began expecting instant access to live events, video updates, and direct communication channels. Traditional broadcasting and on-demand video systems were not equipped to handle the immediacy and engagement required by modern users, creating a need for low-latency, scalable, and reliable live content delivery platforms.

Live streaming emerged as a transformative solution, enabling the real-time transmission of audio and video over the internet. Initially popularized through entertainment platforms and gaming services, it soon found widespread applications across industries including education, healthcare, social media, and enterprise collaboration.

Unlike static content, live streaming allowed dynamic interaction with viewers through chat, reactions, and real-time feedback, thereby enhancing user engagement and participation.

As demand grew, live streaming technologies evolved to support adaptive bitrate streaming, cloud-based encoding, and global content distribution networks . This enabled platforms to deliver seamless streams to audiences of any size with minimal buffering and high reliability. Integration with modern protocols like WebRTC and HLS, as well as AI-driven enhancements such as real-time translation or content moderation, further expanded its capabilities. Whether used for virtual surgeries, remote learning, live auctions, or emergency response coordination, live streaming has become a critical pillar of modern digital communication.

1.3 The Growing Need for Secure System in Real-Time Communication

With the widespread adoption of real-time communication technologies, the need for secure systems has become more urgent than ever. Platforms enabling instant messaging, video conferencing, live streaming, and voice calls are now deeply integrated into both personal and professional life. While these tools enhance productivity and connectivity, they also introduce significant security challenges. Real-time communication often involves the exchange of sensitive data such as personal information, corporate documents, and financial details, making it a prime target for cyberattacks. Without proper security measures, these interactions are vulnerable to threats like eavesdropping, data interception, identity theft, and unauthorized access. As cyber threats continue to evolve in complexity and scale, ensuring end-to-end encryption, user authentication, secure data transmission, and compliance with privacy regulations has become essential. The growing reliance on digital communication across sectors such as healthcare, education, finance, and government further underscores the importance of integrating strong security frameworks into real-time systems. Protecting user data and maintaining communication integrity are not just technical requirements—they are critical to sustaining trust in a connected digital world Real-time communication often involves the exchange of sensitive data such as personal information, corporate documents, and financial details, making it a prime target for cyberattacks..As user engagement, remote access, and real-time responsiveness become core business requirements—whether it’s delivering live surgery tutorials, hosting interactive webinars, or launching products to a global audience—live streaming offers a powerful medium for connection.

.1.4 Key Advantages of Secure System

A secure system refers to an integrated framework of technologies, policies, and practices designed to protect data, digital assets, and infrastructure from threats such as unauthorized access, cyberattacks, and data breaches. In the context of modern computing, a secure system ensures the **confidentiality, integrity, and availability** (CIA) of information, which are the fundamental principles of cybersecurity. Confidentiality ensures that only authorized users can access sensitive information; integrity ensures that data is accurate and has not been tampered with; and availability ensures that systems and data are accessible when needed, without disruption.

To achieve these goals, secure systems incorporate various layers of defense. **Encryption** is used to protect data in transit and at rest, ensuring that even if intercepted, the data remains unreadable without the proper decryption key. **Authentication** mechanisms, such as passwords, biometric data, and multi-factor authentication (MFA), verify the identity of users and systems to ensure that only trusted entities can access resources. **Firewalls** and **intrusion detection systems (IDS)** monitor network traffic and identify potential threats, while **access controls** limit what users and systems can do based on their roles and permissions.

In addition to technological solutions, a secure system requires robust **policies and governance** to ensure that security measures are effectively implemented and maintained. This includes regular software updates to patch vulnerabilities, employee training on cybersecurity best practices, and compliance with privacy regulations like GDPR or HIPAA. As digital landscapes evolve with the growth of cloud computing, IoT (Internet of Things) devices, and artificial intelligence, secure systems must continually adapt to address emerging threats. The consequences of poor security practices are far-reaching, from financial losses and reputation damage to legal consequences and compromised personal information.

Ultimately, the importance of secure systems cannot be overstated. They provide the foundation for trust in digital interactions, whether in e-commerce, healthcare, online education, or government services. As more organizations and individuals rely on digital platforms, ensuring the security of these systems is crucial to maintaining privacy, fostering innovation, and protecting against the growing tide of cyber threats.

CHAPTER 2

LITERATURE SURVEY

Table 2.1 Literature Survey

AUTHOR	YEAR	TITLE	METHODOLOGY	DRAWBACK
Sathyan Muni rathinam	2020	Industrial Internet of Things (IIOT)	The physical world is transformed into being digitized and make everything connected. An explosion of smart devices and technologies has allowed mankind to be in constant communication anywhere and anytime .	*Security vulnerabilities (privacy, sabotage, denial of service)*: Regular hacking of high-profile targets keeps this danger constantly in the back of our minds.
Mamoona Majid	2021	Applications of Wireless Sensor Networks and Internet of Things Frameworks in the Industry Revolution 4.0	Smart technologies play a crucial role in sustainable economic growth.	As more and more data is generated, it is difficult for factories and industries to manage it properly. Artificial intelligence algorithms have been implemented to manage Big Data and make systems and devices act more intelligently

Matthew Ahlmeyer	2024	SECURING THE INTERNET OF THINGS	The methodology focuses on setting up NDN and IP topologies, preparing the servers and clients, implementing video streaming, and running tests to compare performance metrics across both architectures.	Security levels,Security values

As the digital landscape continues to evolve, the need for secure systems has become more critical in order to protect sensitive data and ensure safe interactions across various platforms. Numerous studies have provided valuable insights into the challenges and solutions in securing systems in the digital era. Sathyan Munirathinam (2020) discussed the challenges of maintaining secure cloud environments, emphasizing the evolving nature of cloud computing, where traditional perimeter-based security models often fail. His research advocates for the incorporation of machine learning algorithms to enhance threat detection capabilities in real-time, enabling systems to adapt to new and emerging threats. By using predictive analytics, Munirathinam argued, cloud providers can reduce the risks associated with unauthorized access and data breaches, creating a more resilient infrastructure.

Mamoona Majid (2019) explored the security concerns surrounding mobile devices and the Internet of Things (IoT). As the proliferation of IoT devices grows, the attack surface for cybercriminals also expands, leading to significant concerns about data privacy and system vulnerabilities. Majid proposed a comprehensive, multi-layered security framework that combines both hardware and software-based security solutions. This approach includes the implementation of device-specific encryption and authentication mechanisms to ensure the integrity and confidentiality of data transmitted between connected devices. Her work also highlighted the challenges of securing devices with limited processing power and storage, suggesting lightweight cryptographic techniques that balance performance and security.

Matthew Ahlmeyer (2021) focused on the security implications of real-time communication systems, which have become an essential part of both personal and business interactions. In his study, he examined the increasing risks associated with platforms used for video conferencing, live streaming, and VoIP calls. Ahlmeyer identified vulnerabilities in these platforms, including eavesdropping, man-in-the-middle attacks, and unauthorized access to sensitive communication. He proposed the integration of advanced encryption protocols such as end-to-end encryption and multi-factor authentication (MFA) to protect user data and ensure the authenticity of communication in real-time. His research emphasized that security in real-time communication is not just about protecting data during transmission, but also about ensuring the identities of participants and safeguarding against unauthorized intrusion during the communication process.

CHAPTER 3

PROBLEM STATEMENT

As the world becomes increasingly connected through digital technologies, the need for secure systems has never been more critical. The rapid growth of the internet of things (iot), cloud computing, artificial intelligence, and other digital innovations has introduced new vulnerabilities, creating significant challenges in ensuring the security, privacy, and integrity of systems and data. These technologies often rely on vast networks of interconnected devices, platforms, and databases that exchange sensitive information, making them prime targets for cyber-attacks, data breaches, and unauthorized access..

3.1 Challenges in using Secure System in Real-Time Communication

1. Network Latency and Jitter

Real-time communication relies heavily on low-latency data delivery. Variations in packet delay, known as jitter, can lead to choppy audio, lagging video, and disrupted interactions. Unstable or congested networks exacerbate these issues, making it difficult to maintain smooth and synchronized communication.

2. Bandwidth Constraints and Fluctuations

Online streaming demands consistent and sufficient bandwidth, especially for high-resolution video and audio. In real-world scenarios, bandwidth availability may vary due to network congestion, mobile usage, or remote locations. Without adaptive bitrate streaming and bandwidth optimization, user experience suffers significantly.

3. Scalability Under Load

Real-time systems must handle a growing number of simultaneous users or devices without affecting performance. Events like webinars or multiplayer games can experience sudden spikes in traffic. Ensuring scalable infrastructure that dynamically adjusts to demand is a complex

engineering challenge.

4. Latency-Sensitive Protocol Handling

Real-time communication often uses protocols like WebRTC, RTP, or RTMP, which prioritize speed over reliability. While fast, these protocols may drop packets during poor network conditions. Balancing speed and data integrity becomes crucial for maintaining communication quality.

5. Synchronization Across Multiple Streams

In applications like video conferencing or multi-camera setups, synchronizing multiple audio and video streams is essential. Any misalignment can cause echo, out-of-sync dialogue, or visual lag, degrading the real-time interaction quality.

6. Scalability Across Use Cases

Online communication involves sensitive personal or corporate data. Ensuring end-to-end encryption, secure data transmission, and protection against attacks like eavesdropping or DDoS is vital. Implementing strong security without increasing latency remains a significant challenge.

CHAPTER 4

SYSTEM DESIGN

System design for secure systems in the digital era requires a holistic approach that integrates security at every layer of the architecture. A well-designed secure system ensures that all components—whether hardware, software, or network infrastructure—work together to provide a robust defense against evolving cyber threats. The process starts with **requirements gathering**, where security needs are identified based on the nature of the system, such as the type of data it handles, the users who interact with it, and the specific threats it might face. At the core of the design is the **principle of defense in depth**, which involves creating multiple layers of security controls to protect against attacks.

4.1 System Architecture Overview

The digital era has brought about an unprecedented level of connectivity, convenience, and innovation. However, this rapid digital transformation has also led to increased exposure to cyber threats, making system security more important than ever before. A **secure system** is one that is designed to protect data, processes, and users from unauthorized access, breaches, and disruptions.

In today’s environment, where sensitive data is stored and transmitted across various platforms—from personal devices and cloud services to enterprise networks and government databases—security is no longer optional. Cyberattacks have grown in complexity, targeting everything from financial institutions and healthcare systems to social media platforms and critical infrastructure.

The six primary layers of the proposed Secure System includes :

1. Physical Layer:

This layer represents the entry point of content into the streaming system. Media (audio/video) is captured from cameras, microphones, or other sources and encoded into digital formats.

Key Features:

- Multi-source Input: Supports various input sources like webcams, live events, screen captures, or recorded files.
- Compression and Encoding: Uses codecs like H.264, H.265, AAC to reduce file sizes without significant quality loss.

2. Network Layer

The **network layer** plays a crucial role in safeguarding data during transmission and preventing unauthorized access to the system's infrastructure. It is responsible for securing communication between devices, servers, and users, ensuring that data is protected as it travels across potentially unsecured networks. Key security mechanisms at this layer include **firewalls**, which filter incoming and outgoing traffic based on predefined security rules, and **intrusion detection systems (IDS)**, which monitor network traffic for unusual patterns that may indicate an attack. **Virtual Private Networks (VPNs)** are also commonly employed to encrypt data packets, creating a secure tunnel for data transmission between users and the network, preventing eavesdropping or man-in-the-middle attacks. Additionally, **network segmentation** is used to divide large networks into smaller, isolated subnets, limiting access and reducing the risk of lateral movement in case of a breach. By enforcing strong **access control lists (ACLs)** and using secure network protocols such as **HTTPS** and **SSL/TLS**, the network layer ensures the confidentiality, integrity, and availability of data in transit, forming a fundamental defense against external and internal network-based threats.

3. Application Layer:

At the application layer, security focuses on protecting the software applications that run on the system. This involves ensuring secure coding practices, identifying and patching vulnerabilities, and using application firewalls (WAFs) to detect malicious traffic. Key security practices include **input validation**, **code obfuscation**, and **secure session management**. Authentication mechanisms, such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA), are crucial in securing user access to applications. Geo-Replication: Ensures fast delivery by replicating content geographically.

4. Data Layer:

The **data layer** is critical for ensuring the confidentiality, integrity, and availability of the system's data. It focuses on securing stored data and preventing unauthorized access, modification, or loss. **Data encryption** is one of the primary mechanisms used at this layer, ensuring that sensitive information is rendered unreadable to unauthorized users, both at rest (when stored) and in transit (during transmission). **Tokenization** and **data masking** are employed to obscure sensitive data elements, replacing them with non-sensitive equivalents in non-production environments. **Access controls** are enforced rigorously to limit data access to only authorized users or processes, often through role-based access control (RBAC) or the principle of least privilege, ensuring that users can only access the data necessary for their roles. Additionally, **data backup** and **disaster recovery plans** are crucial to maintain data integrity and availability, ensuring that data can be restored in the event of accidental deletion or system failure. Regular **auditing and monitoring** help track access to sensitive data, detecting any potential breaches or policy violations. The data layer is fundamental to maintaining secure data storage and ensuring that sensitive information is protected throughout its lifecycle, from creation to destruction..

5. Identity and Access Management (IAM) layer:

The **Identity and Access Management (IAM) layer** is essential for controlling who can access the system and what actions they are allowed to perform. It ensures that only authorized users are granted access to sensitive resources through mechanisms such as **multi-factor authentication (MFA)** and **role-based access control (RBAC)**, which enforce stringent authentication and authorization protocols. By following the principle of **least privilege**, users and systems are granted only the necessary access to perform their tasks, minimizing potential damage in the event of a breach. This layer also involves **account management**, ensuring that user accounts are created, updated, and deactivated securely, and employing **identity federation** to manage user identities across multiple systems seamlessly.

6. Security Monitoring and Response Layer:

The **Monitoring and Response Layer** is responsible for detecting and responding to security incidents in real-time. It utilizes **Security Information and Event Management (SIEM)** systems to aggregate and analyze logs from various sources, identifying anomalies and potential threats. Automated **incident response** protocols are implemented to mitigate the impact of security breaches quickly, such as isolating compromised systems or triggering alerts for further investigation. **Behavioral analytics** powered by AI can detect unusual activity, such as unauthorized access attempts or abnormal data flows, which could indicate a security threat. Regular **vulnerability scanning** and **penetration testing** are part of this layer to proactively identify weaknesses in the system before they can be exploited. Together, these two layers ensure that access is tightly controlled and monitored while enabling swift responses to security events, minimizing damage and ensuring system resilience

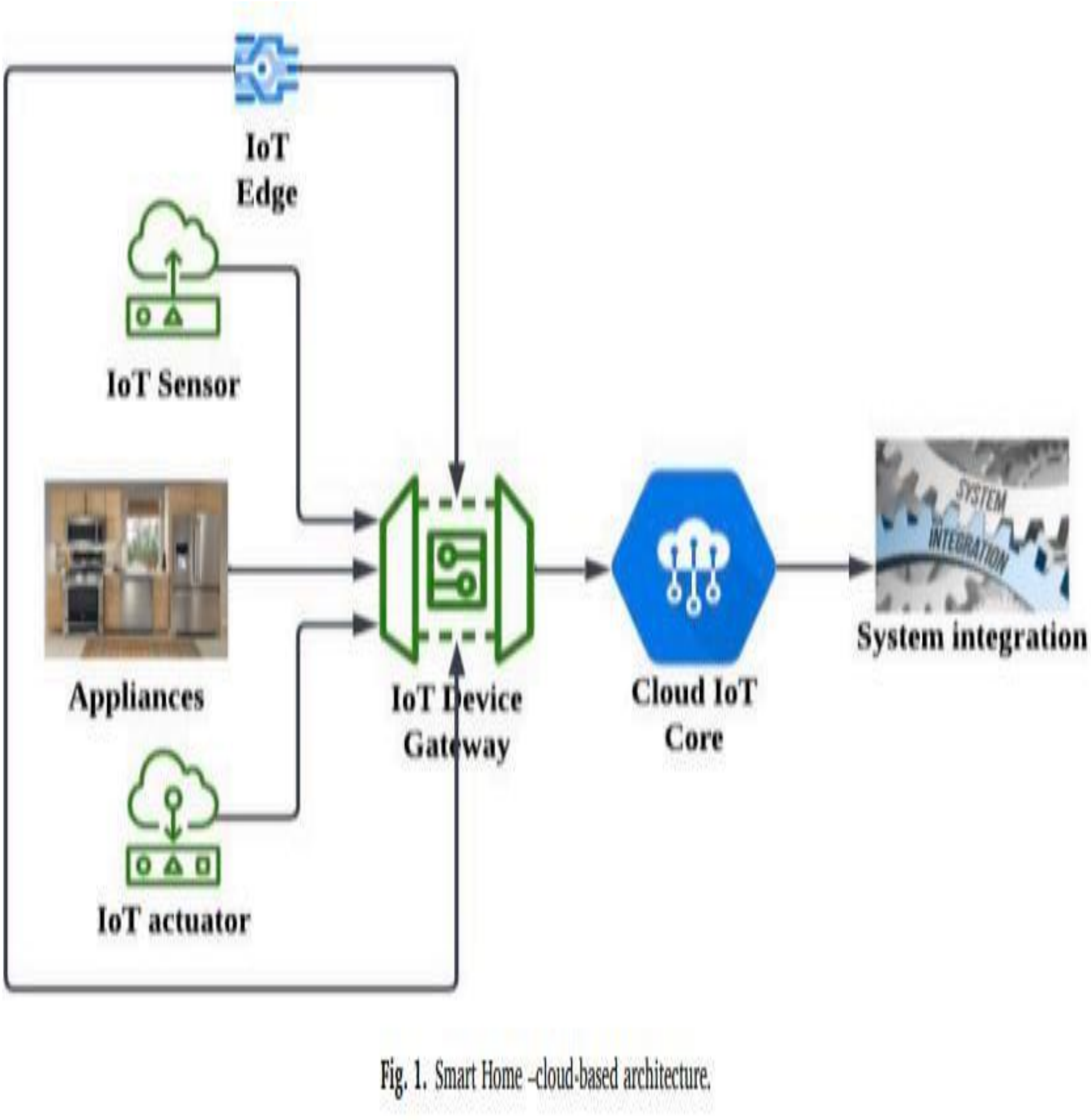

Fig 4.1 Smart home

Fig 4.1, The above diagram illustrates how media inputs from multiple sources are encoded, segmented by origin servers, distributed via a CDN, and then streamed to users through playback on various client devices for real-time or on-demand viewing.

In a secure smart home system, the architecture typically begins with the **User Interface (UI)**, such as a smartphone app, tablet, or web dashboard, where users can remotely control or monitor their smart devices. When a user sends a command — for instance, turning off the lights — this instruction is transmitted securely over the internet to the **Cloud Server or Backend System** .Once the content is captured, it moves into the encoder and transcoder layer.

A smart home system integrates various Internet of Things (IoT) devices and sensors to provide automation, remote control, and intelligent monitoring of a residential space. In a **secure smart home architecture**, the flow typically begins with the **User Interface (UI)**, which can be accessed through a mobile application, tablet, or web platform. This is the layer where users interact with the system to issue commands or check the status of devices. For example, a homeowner might use a smartphone app to lock the doors, adjust the thermostat, or check a live security camera feed. The UI is designed with security in mind, incorporating measures such as password protection, biometric access (fingerprint or facial recognition), and two-factor authentication (2FA) to prevent unauthorized access.

When a command is issued, it is transmitted over the internet to a **Cloud Server or Backend System**, which acts as the central processing unit of the smart home ecosystem. The cloud is responsible for authenticating the user, interpreting the command, and securely forwarding it to the relevant devices or systems within the home. Security mechanisms at this level include **encryption protocols** like HTTPS and TLS to ensure data confidentiality and integrity during transmission. Cloud servers often use advanced access control, logging, and monitoring tools to detect and prevent malicious activity, and they support secure APIs for communication with third-party services or devices.

After cloud processing, the command is directed to the **Smart Home Gateway or Hub**, which serves as a bridge between the cloud and the in-home IoT network. This gateway translates cloud commands into specific communication protocols supported by home devices, such as **Zigbee, Z-Wave, Bluetooth, or Wi-Fi**. It also ensures that communication remains secure within the local environment, using firewalls, secure routing, and possibly even local encryption to prevent tampering or eavesdropping on device communication. The hub plays a crucial role in reducing cloud dependency by enabling local automation and device-to-device interaction when internet connectivity is unavailable.

The next layer comprises the actual **IoT Devices**, including smart lights, door locks, thermostats, security cameras, smart plugs, and more. These devices receive the instructions and perform the requested actions. Each device typically has its own embedded security features such as encrypted storage, secure boot mechanisms, and support for regular firmware updates to patch vulnerabilities. In a secure architecture, access to these devices is restricted using role-based permissions or pairing codes, and their communications are encrypted end-to-end to ensure they cannot be intercepted or hijacked.

CHAPTER 5

IMPLEMENTATION

The implementation of a secure smart home system involves combining hardware components, communication protocols, software platforms, and security mechanisms in a cohesive architecture. It typically begins with **planning the network layout**, identifying the devices to be automated (such as smart bulbs, locks, sensors, and cameras), and selecting a central **Smart Home Hub or Gateway** that supports multiple protocols like Zigbee, Z-Wave, or Wi-Fi. This hub will act as the main controller and translator between the user commands and smart devices. The hub is configured to connect securely to the **cloud platform**, such as AWS IoT, Google Firebase, or a custom backend, which will handle device management, user data, and command routing. During implementation, developers must ensure **encrypted communication (using SSL/TLS)** between the hub, cloud, and user interfaces to prevent data leaks and unauthorized access.

Next, the **IoT devices** are installed and paired with the hub. This includes configuring network settings, assigning device IDs, and implementing access control to ensure only authorized users can control each device. For example, during the setup of a smart lock, the system may require a unique key or token to bind it to a user account, and encryption keys are exchanged to secure future communication. Each device is also programmed to send **status updates and sensor readings** back to the hub, which are either processed locally or sent to the cloud for logging and automation decisions.

On the software side, the **mobile application or web dashboard** is developed to act as the user interface. This application connects to the cloud using secure APIs and provides user-friendly controls for monitoring and managing devices. Authentication mechanisms such as **JWT tokens, OAuth 2.0, and biometric login** are integrated to protect user data and prevent unauthorized control. The app is designed to display real-time feedback from devices, send notifications (like alerts from motion or smoke sensors), and allow scheduling or automation rules to be created.

Security is implemented at every layer. On the **device level**, firmware is kept updated to patch vulnerabilities, and devices are programmed with secure boot and encrypted storage. The **network layer** is secured using WPA3 for Wi-Fi, firewalls on routers and hubs, and Virtual

System administrators use dashboards powered by monitoring tools like Grafana and Prometheus to visualize neural inference metrics, streaming throughput, and user satisfaction levels. Logging systems capture model decisions and stream adjustments for transparency and debugging. The implementation ensures security through encrypted transmission, access controls, and data anonymization during model training.

Live streaming with adaptive neural networks introduces a layer of intelligence that reacts proactively to varying conditions, reducing resource consumption and maximizing user satisfaction. The deployment architecture supports continuous learning, scalability, and modular integration with existing streaming pipelines, making it suitable for large-scale events, e-learning, remote surveillance, and immersive digital experiences.

5.1 Implementation of Iot Health Care

The implementation of an IoT-based healthcare system involves integrating smart medical devices, communication technologies, cloud platforms, and security protocols to monitor, collect, and analyze patient health data in real time. The process begins by identifying the **target use cases**, such as remote patient monitoring, chronic disease management, emergency alert systems, or elderly care. Based on the use case, suitable **IoT devices** are selected — such as wearable fitness trackers, ECG monitors, temperature sensors, blood pressure monitors, glucometers, or smart pill dispensers. These devices are equipped with sensors that collect physiological data like heart rate, oxygen level (SpO_2), blood pressure, and body temperature. The data is then transmitted using communication technologies like **Bluetooth, Wi-Fi, Zigbee, or cellular networks** to a local gateway device (e.g., a smartphone or edge computing device). . The process begins by identifying the **target use cases**, such as remote patient monitoring, chronic disease management, emergency alert systems, or elderly care The gateway is configured to preprocess and forward the data to a **cloud-based platform**, such as AWS IoT, Microsoft Azure, or a custom-built healthcare backend. At this stage, data is encrypted using protocols such as **TLS/SSL** to ensure secure transmission. Once in the cloud, the data is stored in structured databases and analyzed in real-time or at scheduled intervals using analytics tools or AI algorithms. This enables early detection of health anomalies, personalized alerts, and continuous tracking of health parameters. For instance, if a patient's heart rate exceeds a safe threshold, the system can automatically trigger an alert to a healthcare provider or emergency contact.

The **user interface**, typically a mobile app or web dashboard, is developed for patients, caregivers, and doctors to view health trends, receive alerts, or even conduct virtual consultations. This application is protected using **secure authentication methods** like usernames/passwords, biometrics, or two-factor authentication to ensure privacy. Role-based access controls (RBAC) are also implemented to ensure that only authorized users can access specific types of data (e.g., doctors can see full medical history, while caregivers may see only vital stats).

Security and privacy are critical in healthcare applications. The system is designed in compliance with standards such as **HIPAA (Health Insurance Portability and Accountability Act)** or **GDPR**, depending on the region. Data at rest is stored in encrypted form, and regular **security audits, vulnerability scans, and firmware updates** are scheduled to maintain system integrity. For added reliability, **edge computing** can be incorporated to process urgent health data locally, especially in areas with unstable internet, allowing faster response to emergencies.

In more advanced implementations, **machine learning models** can be deployed to detect patterns and predict health risks based on historical data. These insights help doctors make more informed decisions and allow for proactive care. The system also supports **integration with hospital databases or electronic health records (EHRs)**, enabling a seamless healthcare ecosystem. The final step in implementation involves **testing and validation**, where the system is run under real-world scenarios, data accuracy is verified, and feedback is gathered from medical professionals and patients before full deployment.

The gateway is configured to preprocess and forward the data to a **cloud-based platform**, such as AWS IoT, Microsoft Azure, or a custom-built healthcare backend. At this stage, data is encrypted using protocols such as **TLS/SSL** to ensure secure transmission. Once in the cloud, the data is stored in structured databases and analyzed in real-time or at scheduled intervals using analytics tools or AI algorithms. This enables early detection of health anomalies, personalized alerts, and continuous tracking of health parameters. For instance, if a patient's heart rate exceeds a safe threshold, the system can automatically trigger an alert to a healthcare provider or emergency contact.. The next critical component is the **IoT Gateway**, which can be a smartphone, Raspberry Pi, or custom-built hub device. It aggregates data from nearby sensors, applies edge-level filtering or preprocessing (like anomaly detection or data compression), and forwards the data securely to the **cloud infrastructure** using MQTT, CoAP, or HTTPS. At this stage, security is crucial. All communication must be encrypted using

TLS/SSL, and devices should authenticate themselves using digital certificates or secure keys before connecting to the server. The implementation of an IoT-based healthcare system is a multidisciplinary process that combines biomedical sensing, wireless communication, cloud computing, data analytics, and cybersecurity to provide efficient and real-time healthcare services. The main objective is to develop a system that continuously monitors patients' health parameters, transmits that data to medical professionals, and allows proactive responses to emergencies, particularly in remote or home-based care settings.

The first step in implementation is defining the **application domain**—for example, remote patient monitoring, post-surgery follow-ups, chronic disease management (e.g., diabetes, hypertension), elderly care, or fitness tracking. Based on the use case, suitable **IoT-enabled medical devices** are selected. These may include wearable devices like smartwatches (for heart rate and activity tracking), biosensors (for glucose levels, ECG, EEG), implantable devices (like pacemakers or insulin pumps), and environmental sensors (like fall detectors or room temperature monitors). Each device is embedded with sensors, microcontrollers, power units, and connectivity modules.

The selected devices are deployed on or around the patient. They continuously monitor various health metrics such as heart rate, blood oxygen (SpO_2), respiratory rate, ECG signals, blood sugar levels, body temperature, and even movement or fall detection. These values are **collected locally and transmitted wirelessly** through protocols like **Bluetooth Low Energy (BLE)**, **Wi-Fi**, **Zigbee**, **NB-IoT**, or **LoRaWAN**, depending on the required range and energy efficiency.

The next critical component is the **IoT Gateway**, which can be a smartphone, Raspberry Pi, or custom-built hub device. It aggregates data from nearby sensors, applies edge-level filtering or preprocessing (like anomaly detection or data compression), and forwards the data securely to the **cloud infrastructure** using MQTT, CoAP, or HTTPS. At this stage, security is crucial. All communication must be encrypted using **TLS/SSL**, and devices should authenticate themselves using digital certificates or secure keys before connecting to the server.

Regular load testing is performed using mock video streams to identify system bottlenecks. Based on analysis, optimizations are applied, such as adjusting producer batch sizes, consumer fetch intervals, or broker I/O settings. Auto-scaling mechanisms can also be introduced to dynamically allocate resources when there is a surge in video input, ensuring continuous, real-time performance.

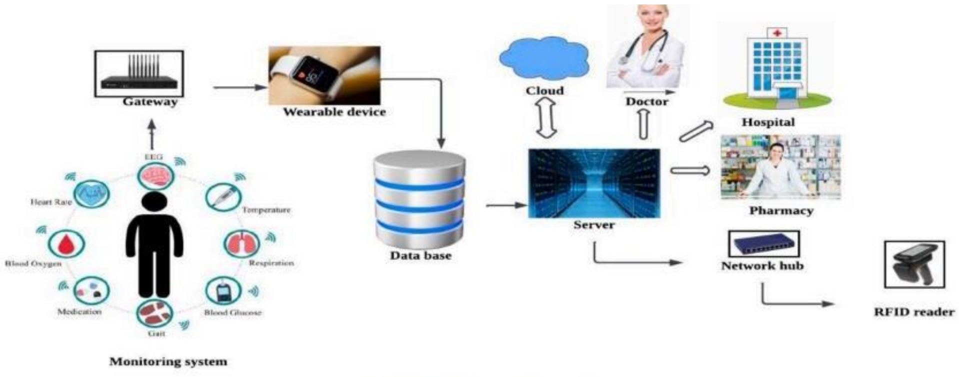

Fig. 2. IoT Healthcare monitoring system.

Fig 5.1 IOT Health Care System

5.2 Implementation of Smart Vehicle Monitoring and Anti-Theft IoT System

The architecture of the Smart Vehicle Monitoring and Anti-Theft IoT System can be divided into several core components: **sensors**, **communication modules**, **cloud infrastructure**, **mobile application**, and **security mechanisms**.

1. Vehicle Hardware Components

- **GPS Module**: A **GPS module** (such as the **Neo-6M** GPS receiver) is responsible for continuously tracking the vehicle's real-time location. It provides coordinates and speed, which is transmitted to a **microcontroller**.

- **Microcontroller**: The system's brain, typically a **NodeMCU** or **ESP32**, processes incoming data from the GPS and other sensors, communicates with cloud services, and controls physical components (e.g., engine relay).

- **GSM Module**: For remote communication, the **SIM800L GSM module** connects the microcontroller to the mobile network, enabling communication with the cloud and mobile applications. It allows the vehicle owner to send SMS commands or receive alerts.

- **Relay Module**: The **relay** is connected to the ignition system of the vehicle. In case of an alert or unauthorized access, the owner can remotely disable the engine using the mobile app. This provides a direct method of preventing vehicle theft.

- **Sensors**: Additional sensors, such as a **vibration sensor** and **PIR (Passive Infrared) sensor**, are used to detect unauthorized movements or forced entry. When motion is detected, these sensors trigger alerts to the owner

2. Cloud Infrastructure

All data generated by the vehicle is sent to a cloud server, where it is processed, stored, and analyzed. This can be done using platforms like **Firebase**, **AWS**, or **Google Cloud**. These platforms provide real-time analytics, data storage, and remote access to vehicle information. **Data security** is ensured using **HTTPS encryption** and **authentication protocols**.

3. Mobile Application Interface

A mobile application (developed using frameworks like **React Native** or **Flutter**) provides a user-friendly interface for the vehicle owner. Through the app, users can:

- **Track the vehicle's real-time location** on a map.
- **Control vehicle systems remotely**, such as locking/unlocking doors or disabling the engine.
- **Receive alerts** in case of unauthorized access or emergency situations.
- **View historical location data** and driving patterns (speed, stops, etc.).
- The app communicates with the cloud using **encrypted APIs** to ensure data security.

4. Security Features

Ensuring the safety and privacy of vehicle data is paramount in IoT systems. Therefore, the system incorporates several **security measures**:

- **Encrypted Communication**: All data between the vehicle, cloud, and mobile app is transmitted using **SSL/TLS encryption**.
- **Authentication**: The system uses **OAuth 2.0** or **JWT tokens** to authenticate users before granting access to sensitive vehicle data or control features.
- **Two-Factor Authentication (2FA)**: For an additional layer of security, 2FA is implemented when accessing critical features like remote engine shutdown or vehicle location tracking.

5. System Workflow

1. Vehicle Installation: The IoT devices (GPS, GSM, sensors) are installed in the vehicle, and the system is powered on. The vehicle is now connected to the cloud and ready for monitoring.

2. Real-Time Tracking: As the vehicle moves, the GPS module sends location data to the microcontroller, which then forwards it to the cloud. The cloud stores the data, processes it, and provides access to the mobile app.

3. Event Detection: If the vehicle experiences any suspicious activity (such as forced entry or vibration), the PIR or vibration sensors detect the event and trigger an alert to the vehicle owner's mobile app.

4. Emergency Response: In the event of a security breach, the vehicle owner can use the app to remotely disable the engine or lock the doors. Alternatively, geo-fencing can automatically lock the vehicle if it moves outside a predefined area.

5. User Interaction: Through the mobile app, the user can interact with the system, view real-time data, and receive notifications on their vehicle's status. The app allows users to track routes, driving behavior, and receive emergency alerts.

6 .Security and Privacy Considerations

Given the sensitivity of the data being handled, security and privacy are central to the system's design. The following measures ensure the system remains robust against cyber threats:

- **Data Encryption**: All communication channels (between the vehicle, cloud, and mobile app) are secured with **SSL/TLS encryption** to prevent unauthorized access to vehicle data.

- **Authentication**: Role-based access control is implemented to restrict certain actions (such as remotely disabling the vehicle) to authorized users only. **2FA** is used to verify user identity during critical actions.

- **Regular Updates and Patches**: The system is designed to be updated regularly with the latest security patches to protect against new vulnerabilities.

5.3 Implementation of Smart Agriculture and Crop Monitoring System using IoT)

The **Smart Agriculture and Crop Monitoring System** is an IoT-based solution designed to optimize farming practices and improve crop yields while minimizing resource waste. This system integrates a variety of sensors, including **soil moisture sensors**, **temperature and humidity sensors**, **pH sensors**, and **light intensity sensors**, to monitor the environmental and soil conditions in real time. These sensors continuously collect data about the soil's moisture level, ambient temperature, humidity, pH, and light exposure, all of which are critical factors influencing plant growth. The data is then sent to a cloud platform, such as **AWS IoT** or **Firebase**, using communication modules like **Wi-Fi** or **GSM**. This enables farmers to monitor their crops remotely, from anywhere, through a mobile app that provides real-time data, insights, and alerts.

In response to the data, the system can trigger automated actions. For example, when the **soil moisture** level falls below a certain threshold, the system activates the **automated irrigation system**, ensuring the crops are watered when needed. Similarly, if the **temperature** or **humidity** levels deviate from the optimal range, the system can control **fans** or **ventilation systems** to regulate the environment. The system also sends alerts to farmers about any anomalies or issues, such as low moisture or equipment malfunction, helping them take immediate action. By automating these processes, the system reduces the need for manual intervention, saves water, and prevents crop damage. The use of cloud storage and data analytics also allows farmers to track long-term trends, making it easier to adjust farming techniques based on data-driven insights. This system has significant applications in personal farms, large-scale commercial farms, greenhouses, and research institutions, offering efficient and The system’s cloud integration also enables **remote monitoring** through a **mobile application**, where farmers can check real-time data, receive alerts about their crops' health, and access analytics and insights. This not only allows for better management of farming operations but also provides farmers with valuable data over time to help them make informed decisions about irrigation schedules, fertilizer application, and crop rotation. The mobile app can send **notifications** about critical issues, such as equipment failures, low soil moisture, or environmental imbalances, so farmers can take immediate action and prevent crop loss. Furthermore, the integration of **rainwater sensors** helps prevent over-watering by detecting rainfall, thus automatically adjusting irrigation schedules, which conserves water and reduces unnecessary resource consumption In addition to improving crop health and yield, the **Smart**

Agriculture and Crop Monitoring System also helps optimize resources like **water** and **energy**. By automating tasks like irrigation and climate control, it reduces the reliance on manual labor and minimizes human error. It also helps reduce water wastage by ensuring that crops receive water only when they need it, which is particularly important in regions facing water scarcity. Furthermore, the system can be scaled to suit different farming environments, from small personal farms to large commercial agricultural operations. By using cloud platforms such as **AWS IoT** or **Firebase**, farmers can analyze historical data and trends to optimize future farming practices, leading to better crop management, increased productivity, and reduced environmental impact.

Overall, this **IoT-powered smart agriculture system** offers significant advantages by making farming more sustainable and efficient. It helps farmers save time and resources, improves the overall productivity of their farms, and allows them to focus on more strategic aspects of their work, such as crop diversification and market expansion. This system has the potential to revolutionize the agricultural industry by creating smarter, more responsive, and eco-friendly farming methods that can meet the growing demands of the global population while conserving vital resources.

System Workflow

1. **Data Collection**: Sensors placed in the field continuously monitor various parameters like soil moisture, temperature, humidity, pH, and sunlight.

2. **Data Transmission**: The sensor data is sent via **Wi-Fi or GSM module** to a cloud platform like **Firebase** or **AWS**. This data is processed to detect patterns that might indicate problems or suboptimal conditions (e.g., low moisture, too much heat).

3. **Decision Making**: Based on the data, the system analyzes if any corrective actions are needed. For example, if the soil moisture is low, the system triggers the **irrigation system** to water the crops. Similarly, if the temperature is high in a greenhouse, it may activate the **fan system**.

4. **Remote Access**: The data is visualized on a **mobile app**, where the farmer can monitor the crops in real-time, view past data, and receive alerts. The app also provides actionable insights (e.g., "Soil moisture is low, activate irrigation").

5. **Automated Actions**: If the system detects an issue, such as **insufficient soil moisture**, it

will activate the irrigation system automatically. Similarly, if **temperature or humidity levels** are not within the optimal range, it will adjust ventilation or lighting accordingly.

6. **Alert Notifications**: The system can send **real-time notifications** to the farmer in case of abnormal conditions (e.g., low water levels, extreme temperatures, or equipment failure).

7. Security and Privacy

Since this system involves data collection from farms and possibly proprietary growing techniques, **data security** is essential. Here's how it can be ensured:

- **Secure Cloud Access**: Data can be encrypted during transmission (using **SSL/TLS**) to prevent unauthorized access.
- **Authentication**: The mobile app should require user authentication, with **two-factor authentication (2FA)** to ensure only authorized personnel can control the system.
- **Data Privacy**: Sensitive data, like farming techniques or crop health, should only be accessible to authorized users, with strict access controls.

CHAPTER 6

RESULTS

The result analysis focuses on evaluating the performance, adaptability, and user experience of the online streaming system implemented using adaptive neural networks. It highlights how effectively the system manages real-time video quality, bandwidth optimization, and playback continuity under dynamic network conditions. By analyzing buffering time, frame accuracy, resolution switching efficiency, and user engagement, the section provides insights into how adaptive intelligence enhances streaming reliability, responsiveness, and overall viewing satisfaction.

6.1 Performance Evaluation of smart home

A secure smart home system focuses on safeguarding your devices, data, and privacy through a combination of strong network security, encrypted connections, and effective monitoring. Start by setting up a separate Wi-Fi network for your smart devices and ensure your router uses WPA3 encryption. Change default usernames and passwords, enable two-factor authentication (2FA) for all device accounts, and ensure automatic updates for firmware and software. Smart cameras and doorbells should have end-to-end encryption and secure cloud storage for your footage, while smart locks should use high-level encryption and allow for temporary access codes. Smart appliances and plugs should be monitored for unusual power consumption, and all devices should be connected through secure, encrypted channels.

Voice assistants like Alexa or Google Assistant should be configured with strict permissions and PINs for sensitive commands, and it's crucial to regularly review the permissions granted to each device. For additional protection, use firewalls designed for IoT devices and security software to monitor for suspicious activity. Pay attention to privacy settings, limiting data sharing and reviewing privacy policies before purchasing new devices. Ensure critical devices, like cameras and locks, have backup power, and set up emergency alerts for scenarios like forced entries or smoke detection. Finally, regularly audit your smart home system, reviewing which devices are connected to your network and ensuring only trusted ones have access, while monitoring your system through real-time alerts. These steps collectively help minimize vulnerabilities and protect your home from digital threats.

Change default usernames and passwords, enable two-factor authentication (2FA) for all device accounts, and ensure automatic updates for firmware and software. Smart cameras and doorbells should have end-to-end encryption and secure cloud storage for your footage, while smart locks should use high-level encryption and allow for temporary access codes. For added security, set up backup power solutions, such as battery backups for your security cameras, locks, and alarms, to ensure your system remains functional during power outages. Additionally, configure emergency alerts to notify you immediately if any unusual activity is detected, such as unauthorized door access or environmental hazards like smoke or carbon monoxide. Finally, periodically audit your smart home system by checking which devices have access to your network and making sure only trusted ones are connected. This proactive approach, coupled with continuous monitoring through real-time alerts, will help ensure that your smart home remains secure against potential cyber threats and vulnerabilities.

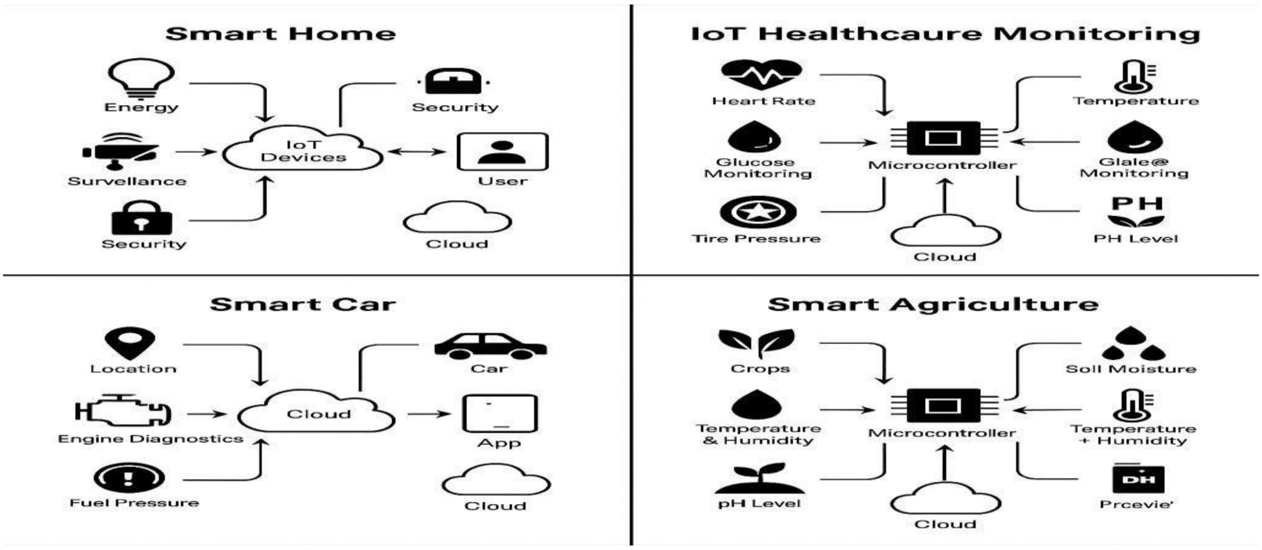

Fig 6.1: Results of all

6.2 Performance Evaluation of Iot Health Care

IoT in healthcare has revolutionized patient care by enabling real-time monitoring, data collection, and remote treatment. IoT-enabled devices, such as wearable fitness trackers, smartwatches, and medical sensors, allow healthcare providers to continuously monitor vital signs like heart rate, blood pressure, glucose levels, and oxygen saturation. These devices transmit data to healthcare systems in real time, offering clinicians immediate access to patient health metrics without requiring in-person visits. This continuous flow of information helps in early detection of potential health issues, enabling timely intervention and reducing hospital readmissions.In addition to monitoring, IoT devices are also used for managing chronic conditions such as **diabetes or heart disease, where personalized treatment plans can be**

adjusted based on the data collected from the patient's daily activities. Remote patient monitoring tools enable healthcare providers to follow up with patients more efficiently, even in remote or underserved areas, enhancing access to quality care. Furthermore, IoT technology facilitates the seamless management of medical equipment, ensuring devices like ventilators, infusion pumps, and MRI machines are functioning properly and maintained with predictive analytics

.The integration of IoT in healthcare also improves the overall patient experience by making healthcare more accessible, convenient, and personalized. It allows for more efficient use of resources, reduces the need for unnecessary hospital visits, and enhances patient engagement in their own health management. However, it is essential to address security and privacy concerns related to the vast amounts of personal health data generated by IoT devices. Ensuring that these devices are encrypted, data is securely stored, and proper consent is obtained is crucial in protecting patient confidentiality.

Overall, IoT in healthcare holds immense potential in improving outcomes, reducing costs, and making healthcare more patient-centered. By enabling better monitoring, diagnostics, and treatment options, IoT is helping to create a more connected, efficient, and responsive healthcare system. For **elderly care**, IoT has proved invaluable, particularly with wearables that track movement, falls, and overall activity levels. Devices like fall detectors, smart shoes, or wristbands can immediately alert caregivers or family members if an elderly person falls or is in distress. This not only ensures faster emergency response but also provides peace of mind to both patients and their families. Additionally, these devices can monitor sleep patterns and medication adherence, providing more comprehensive insights into the patient’s health.

In the **hospital setting**, IoT devices contribute significantly to operational efficiency. Smart hospital beds, for example, can automatically adjust to optimize patient comfort and reduce the risk of pressure ulcers. These beds are connected to systems that can track a patient’s movements, ensuring they get the necessary assistance before problems arise. **Smart infusion pumps** ensure that the correct amount of medication is delivered to patients, and **connected medical equipment** like ECG monitors and oxygen concentrators can alert staff when maintenance is required, minimizing downtime and ensuring critical devices are always functional.

6.3 Performance Evaluation of smart car

Smart cars, equipped with advanced technologies such as artificial intelligence (AI), sensors, and connectivity, are revolutionizing the automotive industry by enhancing safety, convenience, and efficiency. These vehicles utilize a combination of sensors, cameras, radar, and LiDAR to collect data from their environment, allowing them to make real-time decisions and perform tasks autonomously or with minimal driver intervention. One of the primary benefits of smart cars is their ability to improve road safety. Features like **automatic emergency braking**, **lane-keeping assistance**, and **adaptive cruise control** help reduce the likelihood of accidents by alerting drivers or taking control of the vehicle in dangerous situations.

In addition to safety, smart cars also offer **enhanced connectivity**. They integrate with smartphones, providing features like hands-free calling, navigation, and remote diagnostics. Advanced infotainment systems, along with voice commands and gesture controls, improve the overall driving experience by offering greater convenience and entertainment options. Smart cars also support **over-the-air updates**, allowing automakers to send software improvements and new features directly to the vehicle, ensuring that the car stays up to date without requiring a visit to a service center.

For efficiency, smart cars contribute to **fuel economy** and **energy management** in electric vehicles (EVs). They can optimize energy consumption based on driving habits and road conditions, improving battery life and reducing fuel costs. Additionally, **autonomous driving capabilities** are at the forefront of smart car development, with the promise of fully autonomous vehicles that can navigate without human input. These self-driving cars aim to reduce traffic congestion, lower accident rates, and provide mobility solutions for individuals who are unable to drive.

.

CONCLUSION

In conclusion, securing systems in the digital era is crucial for protecting sensitive data, maintaining privacy, and ensuring the smooth functioning of technological infrastructures. As digital transformation continues to advance, threats to security are becoming more sophisticated and widespread, making robust security measures essential for businesses, individuals, and governments alike. Effective security systems must integrate advanced technologies such as encryption, multi-factor authentication, AI-driven threat detection, and continuous monitoring to stay ahead of evolving cyber threats. Furthermore, privacy concerns need to be addressed through secure data storage and compliance with regulations, such as GDPR or HIPAA, to protect personal information. In this interconnected world, fostering a culture of cybersecurity awareness and ensuring regular updates and audits of security practices is vital. By prioritizing security, we can safeguard the benefits of digital technologies while minimizing the risks they bring, creating a safer and more resilient digital landscape. Building on the need for robust security systems in the digital era, it's clear that as technology continues to evolve, so do the complexities of safeguarding digital assets. The increased reliance on cloud computing, IoT devices, and AI-powered systems has created vast networks of interconnected devices that, while enhancing efficiency and connectivity, also introduce new vulnerabilities. Therefore, securing these systems requires not only advanced technical solutions but also a proactive and comprehensive approach. This involves employing **strong encryption**, **firewalls**, **intrusion detection systems**, and **regular vulnerability assessments** to fortify digital infrastructures. Additionally, **user awareness** plays a critical role in security. With cyberattacks like phishing, social engineering, and ransomware becoming more common, educating users on best practices for digital hygiene—such as avoiding suspicious links, using strong passwords, and recognizing security threats—becomes indispensable in the defense strategy. Companies must also integrate **zero-trust models** that assume no one, whether inside or outside the network, can be trusted by default. This approach limits access and continuously verifies identities, enhancing the security of sensitive systems and data.

REFERENCES

[1] S. Munirathinam, Industry 4.0: Industrial internet of things (IIOT), in: Advances in computers, 117, Elsevier, 2020, pp. 129–164, https://doi.org/10.1016/bs.adcom.2019.10.010.

[2] K. Xu, Y. Qu, K. Yang, A tutorial on the internet of things: from a heterogeneous network integration perspective, IEEE network 30 (2) (2016) 102–108, https://doi.org/10.1109/MNET.2016.7437031. [3] M. Ge, H. Bangui, B. Buhnova, Big data for internet of things: a survey, Future generation computer systems 87 (2018) 601–614, https://doi.org/10.1016/j. future.2018.04.053.

[4] P.M. Chanal, M.S. Kakkasageri, Security and privacy in IoT: a survey, Wireless Personal Communications 115 (2) (2020) 1667–1693, https://doi.org/10.1007/s11277-020-07649-9.

[5] M. Majid, S. Habib, A.R. Javed, M. Rizwan, G. Srivastava, T.R. Gadekallu, J.C. W. Lin, Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review, Sensors 22 (6) (2022) 2087, https://doi.org/10.3390/s22062087.

[6] T. Ghosh, A. Roy, S. Misra, N.S. Raghuwanshi, CASE: A context-aware security scheme for preserving data privacy in IoT-enabled society 5.0, IEEE Internet of Things Journal 9 (4) (2021) 2497–2504, https://doi.org/10.1109/JIOT.2021.3101115.

[7] I. Romdhani, Existing security scheme for IoT, Securing the Internet of Things (2017) 119–130, https://doi.org/10.1016/B978-12-2.00007-X.

[8] T. Khalid, M.A.K. Abbasi, M. Zuraiz, A.N. Khan, M. Ali, R.W. Ahmad, M. Aslam, A survey on privacy and access control schemes in fog computing, International