International Journal of
Image Processing and Pattern Recognition

ISSN: 2456-6985
Volume 11, Issue 2, 2025
July–December
DOI (Journal): 10.37628/IJIPPR

https://journalspub.com/journal/ijippr

Review IJIPPR

A Review of Real-Time Human Detection

Eshwar Gopad[1], Rohan Bihari Jangid[1], Riya Sandeep Salvi[1], Mahesh Sunil Belhekar[1]

Abstract

The real-time human detection and counting system leverages deep learning and computer vision to detect individuals, classify gender, and estimate age from live video feeds or CCTV footage. Implemented using flask as a lightweight web framework, the system manages user authentication, detection control, and real-time result display. A Python-based detection script operates asynchronously, ensuring smooth execution, while results – including counts of males, females, and total individuals – are stored in a JSON file for persistence and retrieval. Our project addresses the growing demand for accurate crowd monitoring solutions, particularly in high-traffic environments like shopping malls and public spaces. Using the YOLO V8 model for human detection and Deep SORT for object tracking, the system maintains precise tracking and counting of individuals. TensorFlow optimizes performance on GPU, enabling real-time processing with enhanced speed and accuracy. To ensure adaptability, the system tackles environmental challenges such as varying lighting conditions, camera angles, and low-resolution imagery. Advanced techniques, like frame differencing and histogram of oriented gradients, improve detection accuracy, while an expectation–maximization model enhances people's localization in minimal-movement scenarios. Beyond security and surveillance, this project has significant applications in retail analytics and crowd management, aiding businesses in optimizing space utilization and improving operational efficiency. Extensive testing demonstrates the system's high accuracy under diverse conditions, establishing it as a reliable tool for modern automation and real-time monitoring needs. By integrating state-of-the-art deep learning techniques, our system presents a scalable and robust solution for intelligent human detection and analytics in dynamic environments.

Keywords: People counting, human detection, real-time tracking, deep learning, YOLOv3, computer vision, TensorFlow, crowd management

INTRODUCTION

Overview of People Counting

People counting is an essential technology used to estimate the number of individuals entering and exiting specific areas. This capability is crucial across multiple industries, including video surveillance, urban planning, resource management, and customer profiling. By accurately tracking foot traffic, organizations can enhance security, optimize space utilization, and make data-driven decisions. In the retail sector, real-time people counting enables businesses to analyze customer visit patterns, leading to better inventory management and targeted marketing strategies. Similarly, restaurants can use this data to predict peak hours, improve customer service, and optimize staffing. Additionally, with the increasing adoption of Online-to-Offline (O2O) services, businesses now integrate people counting technologies to connect digital interactions with physical store visits, allowing them to offer personalized services and promotions.

***Author for Correspondence**
Eshwar Gopad
E-mail: eshwargopad@gmail.com

[1]Student, Department of Computer Engineering, RD's Shree Chhatrapati Shivajiraje College of Engineering, Pune, Maharashtra, India

Received Date: March 27, 2025
Accepted Date: May 2, 2025
Published Date: December 22, 2025

Citation: Eshwar Gopad, Rohan Bihari Jangid, Riya Sandeep Salvi, Mahesh Sunil Belhekar. A Review of Real-Time Human Detection. International Journal of Image Processing and Pattern Recognition. 2025; 11(2): 29–39p.

Challenges in Traditional People Counting Methods

Despite its importance, traditional people-counting methods face several limitations. Conventional approaches, such as infrared sensors, turnstiles, and manual counting, are labor-intensive and often inaccurate. While computer vision-based solutions have improved accuracy, they still suffer from significant constraints. One of the major challenges is dependency on movement. Many systems require individuals to be in motion to detect and count them, making it difficult to track stationary people in waiting areas, queues, or densely packed crowds. Additionally, traditional methods struggle with complex backgrounds, as they work best in controlled environments with minimal distractions. Another critical limitation is the reliance on high-resolution images. Many surveillance systems operate with low-resolution cameras, reducing the effectiveness of conventional people counting algorithms. These challenges highlight the need for an advanced, real-time system that can function accurately in diverse and complex environments.

The Role of Deep Learning and Computer Vision in People Counting

The advancement of deep learning and computer vision has significantly enhanced people counting capabilities. Modern object detection models, such as YOLO (You Only Look Once) and Faster R-CNN, have shown remarkable accuracy in detecting individuals in real time. Additionally, object tracking algorithms, like Deep SORT (Simple Online and Realtime Tracker), enable systems to maintain consistent tracking of individuals, even in densely crowded areas. By leveraging deep learning techniques, people counting systems can overcome traditional limitations. They can detect and count individuals in both moving and stationary states, adapt to complex backgrounds, and process low-resolution video feeds with optimized computational efficiency. Furthermore, these advanced techniques provide additional insights, such as gender classification and age estimation, making them valuable for security, retail analytics, and smart city applications. The combination of deep learning and computer vision offers a scalable and efficient solution for real-time people counting in dynamic environments.

THE IMPACT OF COVID-19 ON CROWD MANAGEMENT

The COVID-19 pandemic caused widespread disruptions across industries that rely on large gatherings such as events, retail, and hospitality. To prevent virus transmission, governments imposed strict crowd control measures, increasing the demand for automated people counting solutions. Real-time monitoring of crowd density became essential to ensure compliance with social distancing guidelines and minimize health risks. For instance, in Kuala Lumpur, Malaysia, the government identified 150 COVID-19 hotspot locations in malls, hypermarkets, and grocery stores using big data analytics and artificial intelligence. This highlights the critical role of people counting systems in managing crowd density and enhancing public safety. The pandemic underscored the necessity of efficient crowd monitoring solutions, further driving the adoption of AI-powered people counting technologies.

Object Detection as a Solution for Crowd Management

Object detection has emerged as a highly effective solution for automated crowd management. Unlike traditional manual crowd control methods, which require extensive planning, risk assessment, and human supervision, object detection enables real-time monitoring with minimal operational overhead. By integrating deep learning-based people counting systems with existing surveillance infrastructure, authorities and businesses can efficiently monitor foot traffic patterns, predict peak crowding times, and enforce social distancing measures. Additionally, these systems optimize public space utilization, enhance security, and prevent overcrowding in high-risk areas. The automation provided by object detection makes crowd management more efficient, accurate, and scalable, ensuring safety in public spaces like malls, transportation hubs, and entertainment venues.

Objectives of the Real-Time Human Detection and Counting System

The objective of this project is to develop an advanced people counting system that utilizes deep learning and computer vision for real-time human detection, classification, and analysis. The system is designed to detect individuals in real time using YOLO V8, ensuring high accuracy and efficiency. By integrating Deep SORT tracking, the system maintains precise and non-redundant counting, even in dynamic environments. Beyond counting, the system provides demographic insights by classifying gender and estimating age. Advanced image processing techniques, such as frame differencing and histogram of oriented gradients (HOG), enhance detection accuracy in challenging conditions.

Additionally, a flask-based web framework is implemented to enable secure user authentication, real-time monitoring, and easy data management. The detection results, including male, female, and total counts, are stored in a structured JSON format for seamless retrieval and analysis. These objectives ensure that the system is not only accurate but also adaptable to real-world applications.

SIGNIFICANCE OF THE PROJECT

The real-time human detection and counting system holds significant value across multiple domains. In public safety and surveillance, real-time crowd monitoring enhances security in areas such as shopping malls, airports, and transportation hubs. By providing accurate people counting, the system helps authorities manage large gatherings, detect anomalies, and improve emergency response times. In the retail sector, businesses can use people counting data to optimize store layouts, enhance customer experience, and develop targeted marketing strategies. Understanding visitor footfall patterns allows retailers to make data-driven decisions that improve operational efficiency. Additionally, smart cities can benefit from people counting technologies by analyzing pedestrian movement patterns, improving infrastructure planning, and optimizing public transportation systems. Healthcare and pandemic control are also key areas where this system can be impactful. By monitoring social distancing compliance and identifying overcrowded areas, the system helps mitigate health risks in high-traffic locations. These applications demonstrate the broad significance of real-time people counting in modern urban environments.

CHALLENGES AND FUTURE DIRECTIONS

While deep learning-based people counting systems have made significant progress, several challenges remain. One of the main challenges is handling occlusions in crowded environments. In densely populated areas, individuals may be partially or completely obscured, making detection difficult. Future research can explore advanced occlusion-handling techniques to improve accuracy. Another challenge is improving detection in low-light conditions. Many public spaces operate in environments with poor lighting, reducing the effectiveness of traditional computer vision models. The integration of thermal imaging and infrared cameras could enhance night-time detection capabilities. Additionally, optimizing the computational complexity of people counting models is crucial for deployment on edge devices and low-power hardware. Efficient deep learning models that can run on embedded systems will enable broader accessibility and scalability. Future developments could also include AI-powered anomaly detection, predictive analytics, and cloud-based monitoring solutions. These enhancements would further strengthen the effectiveness and usability of real-time people counting systems, making them more adaptable to different environments and use cases.

In summary, the real-time human detection and counting system represents a major advancement in automated crowd monitoring and analysis. By leveraging deep learning and computer vision techniques, the system ensures accurate human detection, gender classification, and age estimation in real-world scenarios. The integration of YOLO V8, Deep SORT tracking, and advanced image processing techniques make the system highly efficient and adaptable to various applications. The growing need for intelligent crowd management solutions highlights the importance of this project in enhancing security, retail analytics, smart city initiatives, and public health. With future improvements in occlusion handling, low-light detection, and computational efficiency, the system has the potential to become a robust and scalable tool for real-time people counting and analytics. By addressing real-world challenges, this project contributes to the development of next-generation crowd monitoring solutions, ensuring safety, efficiency, and data-driven decision-making in dynamic environments.

LITERATURE SURVEY

Cho and Kang [1] introduced a real-time people counting system aimed at estimating foot traffic in retail stores. The system consists of three key components: foreground extraction, motion search, and flow analysis. Foreground extraction is performed using the average picture level (APL) method, which differentiates moving individuals from static background objects. The maximum a posteriori probability (MAP)-based motion search enhances tracking accuracy, particularly in complex environments with overlapping individuals. Lastly, multiple touching sections (MTS) flow analysis helps resolve occlusion-related issues, ensuring an accurate count of individuals. This approach is beneficial for businesses looking to optimize customer service, staffing, and store layout based on real-time foot traffic data. The proposed system demonstrates high reliability and efficiency, making it a valuable tool for modern retail analytics, smart surveillance, and urban planning applications. Its scalability suggests potential for broader use in crowd management and public space monitoring.

Hou and Pang [2] explored the challenges associated with human detection and people counting in complex environments. Their study highlights the limitations of traditional methods, which often require high-resolution images, simple backgrounds, or continuous human movement to function effectively. However, in real-world scenarios, people may be stationary, partially occluded, or present in low-resolution surveillance footage. To overcome these challenges, the researchers proposed an advanced computer vision-based detection system that combines motion analysis, shape recognition, and adaptive background modeling to improve counting accuracy. The study also addresses the effects of environmental conditions, such as light variations and complex backgrounds, which often hinder people-counting systems. Their research demonstrates that machine learning and adaptive algorithms can significantly enhance the precision of human detection, particularly in applications like crowd control, retail analytics, and public safety monitoring. The findings lay a foundation for more robust, AI-driven people-counting technologies.

Senthilkumar et al. [3] proposed a secure cloud-based system for managing healthcare data using smart card-based healthcare (SCB-HC) technology. The study introduces a privacy safeguard protocol that utilizes elliptic curve cryptography (ECC) to enhance data security and ensure confidentiality in cloud storage environments. Given the sensitivity of medical records, protecting patient information from unauthorized access and cyber threats is crucial. The proposed system employs advanced encryption techniques to safeguard data while maintaining efficient storage and retrieval capabilities. This security model is particularly relevant for remote healthcare services, where patient records must be accessible yet securely protected. By integrating blockchain-inspired authentication methods, the study ensures tamper-proof data storage and secure communication channels between healthcare providers and patients. The research significantly contributes to the development of secure e-health solutions, improving the reliability of telemedicine, smart hospital systems, and IoT-based healthcare services.

Al-Rawashdeh et al. [4] conducted a comprehensive review of Internet of Things (IoT) applications in smart healthcare. Their study highlights how IoT-enabled devices facilitate remote patient monitoring, real-time health data analysis, and automated diagnostics. The review identifies key challenges, such as data privacy concerns, cybersecurity risks, and interoperability issues, among different healthcare platforms. The research also discusses AI-driven predictive analytics, which allow early detection of diseases and improved medical decision-making. By integrating IoT with cloud computing and AI, healthcare providers can enhance efficiency, reduce costs, and improve patient outcomes. The paper emphasizes the growing need for robust security frameworks to ensure the integrity of patient data, given the increasing reliance on connected medical devices. Ultimately, the review underscores IoT's transformative role in modern healthcare, particularly in personalized medicine, emergency response systems, and smart hospital infrastructures.

Abdulmalek et al. [5] reviewed the latest IoT-based healthcare monitoring systems, highlighting their role in improving patient care, disease management, and overall quality of life. Their research outlines the integration of wearable sensors, real-time health monitoring devices, and cloud-based analytics to provide continuous patient tracking. The study also discusses the role of AI and machine learning in processing vast amounts of patient data to detect abnormalities and predict health conditions early. However, despite its advantages, IoT-based healthcare faces challenges such as data security risks, high implementation costs, and system scalability. The authors propose blockchain-based authentication protocols as a potential solution for enhancing data privacy and security. The review concludes that IoT-driven healthcare systems have the potential to revolutionize personalized medicine, reduce hospital visits, and provide proactive care solutions, ultimately enhancing patient well-being in both clinical and home settings.

Abdulbaqi et al. [6] explored the Internet of Medical Things (IoMT) and its potential to revolutionize telehealth and remote patient care. Their research introduces a smart system that leverages IoMT devices, AI algorithms, and cloud computing to support healthcare professionals in providing real-time patient monitoring. The system enables remote caregiving by utilizing wearable devices and biosensors that continuously collect patient vitals such as heart rate, oxygen levels, and temperature. The study also highlights the importance of security and data privacy, proposing an authentication model to prevent unauthorized access. By integrating machine learning, the system can predict health conditions and alert caregivers to potential medical emergencies. The findings suggest that IoMT has significant potential to enhance elderly care, chronic disease management, and emergency response systems, ultimately reducing healthcare costs and improving patient outcomes in smart healthcare ecosystems.

Yuanbing et al. [7] proposed a secure authentication protocol for wireless medical sensor networks (WMSN) used in smart healthcare systems. The research addresses data security vulnerabilities in wireless sensor networks, particularly in medical applications where patient privacy is a critical concern. The proposed protocol enhances authentication mechanisms by integrating password-based encryption with cryptographic techniques, ensuring that patient data remain secure and tamper-proof. Additionally, the study emphasizes the need for low-latency communication in healthcare environments, as delays in data transmission could lead to life-threatening situations. The results indicate that this protocol provides robust security, efficient authentication, and reduced computational overhead, making it ideal for real-time patient monitoring systems. The study concludes that advanced security frameworks are essential for the successful implementation of IoT-driven healthcare solutions, ensuring data integrity, reliability, and accessibility for both patients and medical professionals.

Abdulbaqi et al. [6] introduce a smart system designed for healthcare caregivers, leveraging the IoMT to enhance tele-health caregiving. The study emphasizes how IoMT enables real-time patient monitoring, ensuring that caregivers can respond promptly and efficiently to emergencies. The authors discuss the architecture of the proposed system, which includes sensor-based health monitoring, cloud integration, and AI-driven analytics. The findings suggest that IoMT significantly improves communication between caregivers and patients, allowing for remote diagnosis and timely medical interventions. The study also explores security and data privacy challenges in IoMT-based healthcare, proposing encryption mechanisms to safeguard patient data. Their research highlights the potential of IoT-driven telemedicine in addressing healthcare accessibility issues, particularly for elderly patients and individuals with chronic illnesses. The system's effectiveness is validated through real-world case studies, demonstrating its applicability in modern healthcare infrastructure.

Tsu-Yang et al. [8] propose a secure authentication and key agreement protocol specifically designed for cloud-based smart healthcare environments. Given the sensitive nature of medical records, the authors highlight the critical need for robust security in cloud storage systems. Their proposed protocol ensures secure communication between patients, healthcare providers, and cloud servers, preventing unauthorized access, data breaches, and cyber threats. The research integrates cryptographic algorithms, session key management, and multi-factor authentication (MFA) to enhance data integrity and confidentiality. The study includes formal security proofs to validate the protocol's effectiveness against potential cyberattacks such as replay attacks, impersonation attempts, and insider threats. Their findings suggest that this authentication framework significantly enhances privacy, security, and efficiency in cloud-driven telemedicine, electronic health records (EHR), and AI-assisted diagnostics. By implementing their model, healthcare organizations can safeguard patient data while maintaining system performance.

Amintoosi et al. [9] introduce a lightweight authentication scheme tailored for smart healthcare services, addressing security concerns in resource-constrained healthcare environments. Traditional cryptographic solutions often overload IoT-based medical devices, making them inefficient for real-time applications. The proposed scheme balances security and performance, ensuring secure data transmission with minimal computational overhead. The authors highlight the importance of optimized encryption mechanisms that allow fast authentication while preventing unauthorized access to patient data. Their experimental evaluations demonstrate that this scheme provides efficient authentication, making it suitable for wearable biosensors, remote patient monitoring, and smart hospitals. Additionally, the study outlines potential use cases in emergency healthcare response systems, where rapid authentication is critical for timely medical interventions. By integrating AI-driven security enhancements, this framework enhances privacy, security, and accessibility in modern telemedicine and IoMT-based healthcare ecosystems.

Abdullah et al. [10] propose PRISED Tangle, a privacy-aware framework designed for secure, decentralized healthcare data sharing using IOTA Tangle. Unlike blockchain-based systems, IOTA Tangle eliminates miners, ensuring tamper-proof, cost-effective, and scalable data transactions. The research highlights data privacy concerns in smart healthcare, where centralized systems often expose patient records to cyber threats and unauthorized access. PRISED Tangle enhances security through decentralized encryption protocols, ensuring that healthcare data remains private and immutable. The authors evaluate the framework's effectiveness in interoperable EHR, AI-driven diagnostics, and IoT-based patient monitoring. Their findings suggest that IOTA-based decentralized solutions significantly improve trust, security, and efficiency in cross-institutional healthcare collaborations. This study paves the way for future advancements in privacy-focused smart healthcare infrastructure, allowing real-time, secure medical data exchange while ensuring regulatory compliance (HIPAA, GDPR, etc.).

Lin et al. [11] propose a smart card-based Single Sign-On (SSO) system tailored for 5G-IoT telemedicine applications. The study emphasizes how 5G networks enable high-speed, low-latency medical data processing, which is crucial for remote healthcare services. Traditional authentication methods often fail to provide seamless, secure access across multiple telemedicine platforms. To address this, the proposed SSO system integrates smart cards with cryptographic authentication, allowing healthcare providers to securely access cloud-based patient records without repeated logins. The study evaluates the security and efficiency of the proposed model, demonstrating its resilience against unauthorized access, phishing attacks, and identity theft. The findings highlight that smart card-based authentication significantly enhances usability and security in 5G-enabled healthcare ecosystems, supporting real-time diagnostics, wearable medical devices, and AI-assisted telehealth consultations. This research contributes to the development of scalable and privacy-centric authentication frameworks for next-generation healthcare networks.

Peralta-Ochoa et al. [12] provide a comprehensive review of smart healthcare applications powered by 5G networks. Their research explores how 5G enhances telemedicine, AI-driven diagnostics, and real-time patient monitoring by offering ultra-low latency and high-speed data transmission. The study categorizes 5G applications into key areas, including robotic surgery, remote diagnostics, smart wearables, and cloud-based healthcare platforms. The authors identify cybersecurity challenges, such as data privacy risks, unauthorized access, and network vulnerabilities, which need to be addressed for 5G healthcare adoption. Additionally, they discuss policy and regulatory issues that influence global 5G healthcare integration. The findings suggest that while 5G can revolutionize healthcare by improving efficiency and accessibility, further security advancements and infrastructure investments are required.

Their review serves as a valuable resource for researchers and policymakers, highlighting emerging trends and future directions in 5G-powered smart healthcare systems.

Al Omar et al. [13] introduced a privacy-preserving healthcare platform using blockchain-based smart contracts, aimed at enhancing security and transparency in smart city healthcare ecosystems. Traditional centralized healthcare databases often face security breaches and inefficiencies, making patient data vulnerable to cyber threats. The proposed blockchain solution enables decentralized, immutable record-keeping, ensuring secure medical transactions while reducing fraudulent activities in health insurance claims and prescriptions. The study demonstrates how smart contracts automate healthcare payments, insurance processing, and patient authentication, eliminating the need for manual verification processes. By integrating decentralized identity management, this system ensures that only authorized healthcare providers can access patient data, significantly improving privacy protection. The findings highlight that blockchain-powered smart contracts can optimize urban healthcare infrastructures, making medical data transactions more efficient, transparent, and secure in smart city environments.

Wu et al. [14] address security vulnerabilities in cloud-based smart healthcare environments by proposing a provably secure authentication and key agreement protocol designed to enhance patient data security and privacy. The study critiques existing authentication mechanisms, highlighting their susceptibility to impersonation attacks, desynchronization risks, and data breaches. To address these concerns, the authors develop a cryptographic authentication framework integrating ECC and session key management, ensuring secure data exchange between patients, healthcare providers, and cloud servers. The proposed protocol undergoes formal security analysis and performance evaluations, demonstrating resistance against replay attacks, man-in-the-middle (MITM) attacks, and key compromise impersonation (KCI) attacks. Comparative results indicate that the new protocol outperforms previous models by offering improved anonymity, lower computational costs, and enhanced resistance to cyber threats. The authors conclude that their protocol is highly efficient for smart hospitals and telemedicine applications, suggesting future enhancements through biometric authentication and blockchain integration.

SUMMARY OF THE LITERATURE REVIEW

The summary of the literature survey is depicted in Table 1.

Table 1. Summary of literature review.

Author(s) and Year	Title/Focus Area	Key Contributions	Methodology/Approach	Findings/Implications
Cho & Kang [1]	Real-time people counting system for retail analytics	Developed a system using foreground extraction, motion search, and flow analysis to improve foot traffic estimation	Used APL for background removal, MAP for motion search, and MTS for occlusion handling	Enhanced counting accuracy for retail analytics, smart surveillance, and urban planning.
Hou & Pang [2]	Challenges in human detection and people counting	Addressed limitations of traditional people counting methods in complex environments	Combined motion analysis, shape recognition, and adaptive background modeling	Improved detection accuracy for crowd control, retail analytics, and public safety monitoring.
Senthilkumar et al. [3]	Secure cloud-based SCB-HC system	Introduced a privacy safeguard protocol using ECC for cloud security	Implemented blockchain-inspired authentication and encryption techniques	Improved confidentiality, tamper-proof storage, and secure access in telemedicine and IoT healthcare.
Al-Rawashdeh et al. [4]	IoT applications in smart healthcare	Reviewed IoT-enabled patient monitoring, AI-driven analytics, and interoperability challenges	Analyzed IoT-cloud-AI integration for real-time diagnostics	IoT enhances efficiency but requires stronger security and interoperability frameworks.

Abdulmalek et al. [5]	IoT-based healthcare monitoring systems	Examined wearable sensors, real-time monitoring, and cloud-based analytics for patient care	Evaluated AI and ML techniques for abnormality detection	IoT improves disease management but faces security and scalability issues.
Abdulbaqi et al. [6]	IoMT in telehealth	Developed a smart system integrating IoMT, AI, and cloud computing for real-time healthcare monitoring	Used wearable sensors and cloud-based AI for patient data analysis	IoMT enhances elderly care, chronic disease management, and emergency response.
Yuanbing et al. [7]	Secure authentication protocol for WMSN	Proposed a protocol to secure patient data in wireless medical networks	Used password-based encryption with cryptographic techniques	Improved security and efficiency in real-time patient monitoring systems.
Abdulbaqi et al. [6]	Smart system for healthcare caregivers using IoMT	Designed a remote monitoring system with AI-driven analytics	Sensor-based health tracking, cloud integration, and encryption mechanisms	IoMT improves caregiver–patient communication and emergency response.
Tsu-Yang et al. [8]	Secure authentication protocol for cloud-based smart healthcare	Developed a MFA protocol for healthcare security	Used cryptographic algorithms and session key management	Enhanced privacy, security, and efficiency in cloud-driven healthcare.
Amintoosi et al. [9]	Lightweight authentication scheme for smart healthcare	Proposed an optimized encryption mechanism for low-power healthcare environments	Used AI-driven security enhancements and low-overhead cryptographic methods	Efficient authentication for wearable biosensors, remote monitoring, and smart hospitals.
Abdullah et al. [10]	PRISED Tangle: Privacy-aware framework for secure healthcare data sharing	Utilized IOTA Tangle for decentralized tamper-proof transactions	Eliminated miners for cost-effective and scalable data exchange	Improved security and interoperability of EHR and IoT-based healthcare monitoring.
Lin et al. [11]	Smart Card-based SSO for 5G-IoT telemedicine	Developed an authentication system for secure multi-platform access	Integrated smart cards with cryptographic authentication	Enhanced security and usability in 5G-enabled real-time diagnostics.
Peralta-Ochoa et al. [12]	5G applications in smart healthcare	Reviewed AI-driven diagnostics, robotic surgery, and real-time monitoring over 5G networks	Categorized 5G use cases and cybersecurity challenges	5G enhances healthcare efficiency but needs stronger security.
Al Omar et al. [13]	Blockchain-based healthcare platform for smart cities	Developed a privacy-preserving healthcare platform using smart contracts	Used decentralized identity management and secure transactions	Optimized urban healthcare with transparent, secure data handling.
Wu et al. [14]	Secure authentication and key agreement protocol for cloud-based healthcare	Developed an ECC-based authentication protocol for secure data exchange	Used formal security analysis and performance evaluations	Improved security, efficiency, and privacy for telemedicine and smart hospitals.

RESEARCH GAP

Despite significant advancements in people counting systems, IoT-driven healthcare, and authentication protocols, several challenges remain unaddressed. Existing people counting solutions, such as those by Cho & Kang [1] and Hou & Pang [2], have improved tracking accuracy using motion analysis and adaptive background modeling. However, they still struggle with occlusions, low-resolution imagery, and real-world environmental variations, limiting their applicability in highly dynamic or crowded environments. Additionally, most current IoT-based healthcare solutions [4–5] focus on remote patient monitoring and AI-driven diagnostics but face challenges such as data security risks, interoperability issues, and high infrastructure costs. While authentication protocols [3–8] have introduced encryption-based security models, many still have computational overheads that make them inefficient for resource-constrained IoT medical devices and real-time healthcare applications. Furthermore, while blockchain and IOTA-based frameworks [10–13] provide tamper-proof security for healthcare data, issues, such as scalability, transaction speed, and energy consumption, remain a challenge. 5G-enabled smart healthcare solutions promise low-latency, high-speed medical data transmission, but concerns about cybersecurity, regulatory compliance, and integration with existing healthcare infrastructures persist.

RESEARCH CONTRIBUTIONS

This research makes significant contributions in the areas of people counting, IoT-based healthcare security, and authentication protocols. By analyzing existing people detection models, this study highlights the need for enhanced real-time tracking algorithms that can function efficiently in occluded, low-light, and high-density environments. The research also emphasizes the integration of AI-driven analytics and deep learning techniques to improve the accuracy and adaptability of people counting systems in smart surveillance and urban planning. Additionally, it contributes to the growing body of IoT-enabled healthcare solutions by identifying key security vulnerabilities in existing frameworks [4–5]. By addressing data privacy concerns, interoperability issues, and real-time monitoring challenges, this study advocates for hybrid cloud-edge computing models that enhance the efficiency and security of remote patient monitoring and telemedicine applications. Furthermore, this research advances the field of authentication and data protection in smart healthcare by critically evaluating cryptographic security models [3, 8]. It proposes the adoption of lightweight encryption techniques for low-power IoT medical devices, ensuring secure and efficient authentication without excessive computational overhead. Additionally, by examining blockchain-based frameworks [10, 13], this research suggests decentralized identity management solutions to improve healthcare data integrity and secure transactions in smart cities. The study also explores the role of 5G networks in enhancing real-time healthcare communication, proposing strategies to mitigate cybersecurity risks while optimizing ultra-low latency healthcare applications.

Existing System Analysis

The process begins with the hospital staff inputting a Hospital's Unique Code, which verifies the request and ensures that the data is being accessed by an authorized medical facility.

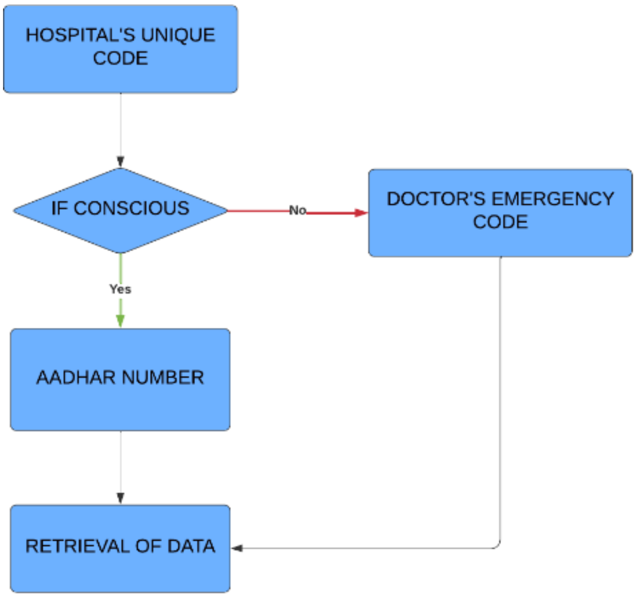

Figure 1. Existing system.

The Figure 1 represents a medical data retrieval system that ensures secure access to a patient's information based on their conscious state. The process starts with a hospital's unique code, which likely serves as an authentication step for authorized medical institutions. The next step involves checking if the patient is conscious or unconscious. If the patient is conscious, they provide their Aadhar number, a unique identification number used in India, which allows the system to retrieve their medical data. This ensures that the patient consents to access their health records, maintaining privacy and security. If the patient is unconscious, the process follows an alternative route where a doctor's emergency code is used instead. This suggests that authorized medical professionals have a special access mechanism to retrieve critical health data when the patient is unable to provide consent. The retrieval of data occurs after authentication through either the Aadhar number (if conscious) or the doctor's emergency code (if unconscious). This system ensures efficient access to medical records, particularly in emergencies, while balancing security and patient privacy.

CONCLUSIONS

Smart health cards are a revolutionary approach to patient data management and care quality in healthcare systems, particularly in developing countries. They centralize and digitize patient information, improving accessibility and accuracy of medical records. Cloud computing and advanced security measures protect sensitive health data, addressing privacy and data security concerns.

The cards also support preventive healthcare initiatives by providing timely reminders for vaccinations and routine checkups, promoting proactive health management. In emergencies, the immediate availability of comprehensive patient information can significantly improve outcomes. As healthcare evolves, the smart healthcare system is a scalable solution for improving healthcare delivery, patient experiences, and coordination among providers. However, challenges, such as implementation costs, interoperability, and patient accessibility, must be addressed to fully realize its benefits.

REFERENCES

1. Cho SI, Kang SJ. Real-time people counting system for customer movement analysis. IEEE Access. 2018;6:55264–72.
2. Hou YL, Pang GK. People counting and human detection in a challenging situation. IEEE Trans Syst Man Cybern A Syst Hum. Sep 20;41(1):24–33.
3. Senthilkumar S, Brindha K, Kryvinska N, Bhattacharya S, Reddy Bojja G. SCB-HC-ECC–based privacy safeguard protocol for secure cloud storage of smart card–based health care system. Front Public Health. 2021;9:688399.
4. Al-Rawashdeh M, Keikhosrokiani P, Belaton B, Alawida M, Zwiri A. IoT adoption and application for smart healthcare: A systematic review. Sensors (Basel). 2022;22(14):5377.
5. Abdulmalek S, Nasir A, Jabbar WA, Almuhaya MA, Bairagi AK, Khan MA, Kee SH. IoT-based healthcare-monitoring system towards improving quality of life: A review. Healthcare (Basel). 2022;10(10):1993.
6. Abdulbaqi AS, Obaid AJ, Alazawi SA. A smart system for health caregiver based on IoMT: Toward tele-health caregiving. Int J Online Biomed Eng. 2021;17(7).
7. Yuanbing W, Wanrong L, Bin L. An improved authentication protocol for smart healthcare system using wireless medical sensor network. IEEE Access. 2021;9:105101–17.
8. Wu TY, Yang L, Luo JN, Wu JM. A provably secure authentication and key agreement protocol in cloud-based smart healthcare environments. Secur Commun Netw. 2021;2021:2299632.
9. Amintoosi H, Nikooghadam M, Shojafar M, Kumari S, Alazab M. Slight: A lightweight authentication scheme for smart healthcare services. Comput Electr Eng. 2022;99:107803.
10. Abdullah S, Arshad J, Khan MM, Alazab M, Salah K. PRISED tangle: A privacy-aware framework for smart healthcare data sharing using IOTA tangle. Complex Intell Syst. 2023;9(3):3023–41.
11. Lin TW, Hsu CL, Le TV, Lu CF, Huang BY. A smartcard-based user-controlled single sign-on for privacy preservation in 5G-IoT telemedicine systems. Sensors (Basel). 2021;21(8):2880.

12. Peralta-Ochoa AM, Chaca-Asmal PA, Guerrero-Vásquez LF, Ordoñez-Ordoñez JO, Coronel-González EJ. Smart healthcare applications over 5G networks: A systematic review. Appl Sci (Basel). 2023;13(3):1469.
13. Al Omar A, Jamil AK, Khandakar A, Uzzal AR, Bosri R, Mansoor N, et al. A transparent and privacy-preserving healthcare platform with novel smart contract for smart cities. IEEE Access. 2021;9:90738–49.
14. Wu TY, Yang L, Luo JN, Wu JM. A provably secure authentication and key agreement protocol in cloud-based smart healthcare environments. Secur Commun Netw. 2021;2021:2299632.

