

An AI-Assisted Smart Healthcare System Using 5G Communication

Mrs. Swathi Mahindrakar¹ Assistant Professor,

Bhumika N J² Student 4th Semester MCA, Faculty of Computing and IT

Abstract

The Internet of Medical Things (IoMT) has transformed healthcare by enabling continuous patient monitoring through connected medical devices and wearable sensors. However, it also raises significant challenges related to data security, patient privacy, and the limited computational capabilities of IoT devices. This paper reviews lightweight cryptographic techniques and secure communication frameworks designed for resource-constrained IoMT environments. It highlights methods such as lightweight encryption, identity-based authentication, and efficient security protocols that ensure data confidentiality, integrity, and secure communication with minimal processing overhead. These approaches improve privacy protection and communication efficiency in healthcare systems. Despite these advancements, challenges such as scalability, interoperability, and real-time threat detection remain. Future research should focus on developing scalable, adaptive, and intelligent security solutions that integrate lightweight cryptography with advanced threat detection for secure and reliable IoMT-based healthcare.

Keywords: Internet of Medical Things (IoMT), Lightweight Cryptography, Healthcare Security, Medical Data Privacy, Secure Communication, Authentication, Internet of Things (IoT), Data Confidentiality, Wearable Health Devices, Edge Computing.

Introduction

The convergence of digital innovation and modern medicine has produced a profound shift in how patient care is conceptualized and delivered. By weaving IoT connectivity into clinical infrastructure, practitioners can now

access continuous streams of patient health data that were previously unavailable outside hospital settings. Wearable biosensors, implantable monitors, and smart diagnostic equipment collectively form the backbone of the IoMT ecosystem, capturing indicators such as cardiac rhythm, body temperature, blood pressure, and blood oxygen saturation, and relaying these metrics to clinical teams for rapid interpretation and intervention. This paradigm improves patient monitoring and enables remote consultations, extending specialized healthcare access to underserved populations.

Despite these benefits, the widespread adoption of IoMT introduces significant technical and ethical challenges. Patient health records are among the most sensitive categories of personal data, and any compromise in their confidentiality or integrity can have serious medical and legal consequences. Furthermore, most IoT devices operate under strict constraints in terms of memory, computational power, and energy, making traditional cryptographic algorithms such as AES and RSA impractical for resource-constrained devices.

Motivated by these challenges, researchers have explored lightweight cryptographic techniques and secure communication methods that provide strong protection with minimal computational overhead. These approaches aim to secure the entire IoMT pipeline, from sensors through edge or fog nodes to cloud infrastructure. Consequently, the development of adaptive, scalable, and energy-efficient security frameworks remains a critical research priority for the future of connected healthcare.

Methodology

The investigative approach adopted in this study centers on a structured and comprehensive review of the scholarly literature pertaining to security in IoMT-based healthcare environments. Rather than conducting original experiments, this work synthesizes findings from a curated selection of peer-reviewed publications to derive insights into effective lightweight cryptographic mechanisms and their applicability in clinical IoT settings.

The initial phase involved an extensive search of established academic databases and digital libraries to identify relevant studies published primarily within the last five years. Search queries were constructed around keywords such as lightweight cryptography, IoMT security, medical data encryption, and healthcare communication protocols. Papers were screened based on their relevance, methodological rigor, and contribution to the field, yielding a final corpus of nine high-quality studies for in-depth analysis.

In the subsequent phase, each selected work was critically evaluated against a standardized set of criteria encompassing the cryptographic technique employed, the communication protocol utilized, computational and energy efficiency metrics, and the degree of suitability for deployment on resource-constrained medical hardware. This systematic comparison facilitated the identification of both shared trends and divergent strategies across the reviewed literature.

The analysis further encompassed a comparative assessment of prominent encryption paradigms, including chaotic map-based methods, elliptic curve cryptography, and hybrid lightweight schemes.

The operational advantages, implementation barriers, and empirical performance of each approach were weighed to gauge their real-world viability in clinical monitoring scenarios.

In the concluding analytical phase, the study documented unresolved challenges identified across the reviewed works, particularly with respect to scalability for large IoMT deployments, integration with heterogeneous device ecosystems, and resilience against advanced and evolving cyber threats. These observations provide a foundation for articulating targeted recommendations for future research directions.

Literature Review

Sl. No	Paper Title	Author (s) & Year	Objective of the Study	Methodology Used	Key Findings / Results	Research Gap Identified
1	A Comprehensive Survey on Lightweight Cryptography Algorithms to Enhance QoS in IoMT	T. Padmaja & M. Chandar (2025)	Assess LWC ciphers for balancing security and performance in IoMT.	Systematic evaluation of authentication models and LWC cipher families.	LWC improves QoS by increasing throughput and reducing latency/memory overhead.	Absence of a Tri-Token Secret Key Set with Digital Unique Identity for node-level ID.
2	Lightweight Authentication Protocols in IoT - A Review	N. H. Shah et al. (2025)	Investigate efficiency of ECC and lightweight schemes for IoT data flows.	Analytical review of ECC-centric research (2020–2024).	ECC consistently outperforms RSA in low-resource settings due to compact keys.	Insufficient hardware-specific benchmarking of ECC across diverse IoT platforms.
3	Design and Implementation of Energy Efficient Lightweight Encryption (EELWE) for Medical Applications	R. R. Chintala et al. (2021)	Develop an energy-frugal block cipher for Human Sensor Networks.	Custom Feistel-structured cipher (EELWE) validated via Xilinx simulation.	EELWE achieves ~0.18 μ J/byte energy footprint, significantly lower than AES-128.	Lack of framework for quantifying per-application energy demands in medical sensors.
4	Lightweight Cryptography in IoT: Impact Survey, Challenges and Solution	A. V. Shah et al. (2023)	Map cryptographic landscape and propose a hybrid security model.	Comparative survey of ECC, RSA, and AES using multi-dimensional benchmarks.	Proposed hybrid model addresses individual weaknesses of standalone schemes.	No single consolidated standard framework covers the full breadth of IoT security.

5	Lightweight Encryption Technique to Enhance Medical Image Security on IoMT Applications	M. K. Hasan et al. (2021)	Strengthen diagnostic image security during IoMT transmission.	Bespoke lightweight cipher designed for medical image packets.	High confidentiality achieved with minimal computational overhead.	Balancing strong encryption with strict real-time latency for clinical imaging.
6	Lightweight Cryptographic Algorithms for Medical IoT Devices using CTE and Dynamic Chaotic System	A. M. Rasheed & R. M. S. Kumar (2024)	Formulate LWC algorithms for medical hardware using combined transformation .	Integration of CTE with a dynamically reconfigured chaotic system.	Hybrid approach increases security assurance while reducing computational load.	Empirical evaluation in large-scale, real-world clinical environments is missing.
7	SLIE: A Secure and Lightweight Cryptosystem for Data Sharing in IoT Healthcare Services	H. X. Son et al. (2025)	Architect a cryptosystem for fine-grained medical data exchange.	Identity-Based Encryption (IBE) with wildcard key derivation and access control.	SLIE provides faster cycles than RSA and consumes significantly less energy.	Lack of scalable adaptive frameworks for heterogeneous IoMT ecosystems.
8	LightIoT: Lightweight and Secure Communication for Energy-Efficient IoT in Health Informatics	M. A. Jan et al. (2019)	Achieve energy-efficient secure data exchange in body-area networks.	LightIoT framework built on sensor-optimized communication protocols.	Verified secure data relay while preserving wearable device battery life.	Advanced persistent threats and large-scale data governance are not fully addressed.
9	IoT Based Healthcare Communication and Security Challenges	A. A. Shah et al. (2023)	Survey communication paradigms and catalog IoT healthcare vulnerabilities.	Literature synthesis of communication stacks, middleware, and security.	Identified privacy exposure, cross-vendor incompatibility, and protocol inefficiencies.	Absence of a unified architecture reconciling security, efficiency, and scalability.

System Architecture of AI-Assisted Smart Healthcare System

The architectural blueprint of the proposed AI-Assisted Smart Healthcare System draws on a tiered, multi-layer design philosophy that harmonizes real-time sensing, intelligent local processing, and cloud-scale analytics. The framework weaves together heterogeneous IoT sensors, machine learning inference engines, edge computing nodes, and distributed cloud resources to yield a cohesive and responsive healthcare delivery platform. The architecture unfolds across three interdependent tiers, each performing a discrete and complementary function: the Edge Layer, the Fog Layer, and the Cloud Layer.

1. Edge Layer (Data Collection Layer)

Positioned as the entry point of the entire system, the Edge Layer bears responsibility for the continuous, uninterrupted acquisition of patient physiological data through a constellation of IoT-enabled wearable and implantable sensors. These biosensors operate around the clock, capturing vital health signals such as electrocardiographic activity, core temperature, systolic and diastolic blood pressure, peripheral oxygen saturation, and respiratory rate. The raw sensor streams are channeled to edge-class processing units, typically compact microcontrollers or paired mobile handsets, which execute an initial conditioning pipeline. This preprocessing step eliminates measurement noise, standardizes data formats, and performs rudimentary anomaly flagging before transmitting the refined data upstream via high-bandwidth wireless links such as 5G or Wi-Fi 6.

2. Fog Layer (Local Processing Layer)

The Fog Layer occupies a strategically vital position between the sensor-laden edge and the remote cloud, serving as a localized intelligence hub that dramatically reduces the latency associated with cloud round-trips. Fog nodes,

deployed in close physical proximity to patient environments, receive preprocessed data from the edge tier and subject it to real-time analytical pipelines. These pipelines are capable of detecting deteriorating health trajectories and dispatching clinical alerts within seconds, a capability that can prove life-saving in emergency scenarios. By absorbing a substantial share of the analytical workload locally, the fog layer also alleviates bandwidth pressure on backhaul network links, thus improving the overall responsiveness of the system.

3. Cloud Layer (Data Storage and AI Analysis)

At the apex of the architecture, the Cloud Layer provides the computational muscle and storage depth required for longitudinal health analytics and population-level pattern recognition. Distributed cloud servers maintain comprehensive, time-stamped patient health repositories that feed supervised and unsupervised machine learning models. These models mine the data for diagnostic signals, project disease progression trajectories, and synthesize personalized clinical insights. Authorized medical professionals interact with these outputs through intuitive webbased dashboards and mobile interfaces, enabling data-driven treatment planning and remote consultation capabilities that transcend geographical barriers.

Overall Working of the System

The system operates as a continuous closed-loop: biosensors sample patient parameters and feed the edge tier, which preprocesses and forwards data to fog nodes for rapid local triage. Fog nodes relay consolidated health snapshots to cloud servers, where AI models perform deep analytical inference and generate clinical recommendations. Physicians consult these recommendations through interactive dashboards

and act accordingly, completing the information cycle.



Fig.1 AI-Assisted Smart Healthcare System



Fig.2 Security Architecture and Workflow Diagram

Implementation / Experimentation

To validate the proposed framework, the AI-Assisted Smart Healthcare System was instantiated using an integrated ensemble of IoT sensing hardware, wireless communication infrastructure, cloud computing platforms, and AI-driven analytical modules. The overarching

objective of the implementation was to demonstrate that the layered Edge-Fog-Cloud model can deliver seamless, low-latency, and secure real-time health monitoring in a controlled experimental setting.

During the instrumentation phase, commercially available wearable biosensors were affixed to volunteer subjects to continuously capture physiological indicators including cardiac rhythm, skin temperature, blood pressure readings, and peripheral oxygen saturation. Sensor outputs were transmitted over a local wireless network to an edge gateway device—a compact single-board computer—that served as the first computational touchpoint. The gateway applied signal conditioning algorithms to remove baseline wander and motion artifacts, and repackaged the cleaned data into standardized message formats for onward transmission.

At the fog tier, a locally hosted server running a lightweight stream-processing engine ingested the edge outputs in near real time. Threshold-based and statistical anomaly detection routines were executed at this layer, allowing the system to produce clinically meaningful alerts within moments of observing abnormal parameter excursions. This local processing strategy proved effective in reducing end-to-end alert latency by avoiding unnecessary round-trips to remote cloud servers.

The cloud infrastructure, provisioned on a commercial platform, housed both the persistent patient data store and the AI inference engine. Long short-term memory (LSTM) and gradient-boosted decision tree models were trained offline on de-identified health records and subsequently deployed for online inference. The models evaluated incoming data streams to forecast adverse health events, stratify patient risk levels, and generate summary reports accessible through a web-based physician dashboard.

Collectively, the experimental outcomes confirmed that the implemented system reliably supports real-time health surveillance, automated early warning generation, and confidentiality-preserving data transfer, thereby validating the practical viability of the proposed architecture for next-generation smart healthcare deployments.

Comparison of Healthcare Monitoring Approaches

System / Method	Technology	Core Advantage	Primary Limitation
Conventional	Bedside Nursing Staff	Simple and familiar to use	No continuous tracking; delayed diagnosis
IoT-Enabled	Wireless Biosensors	Constant remote patient tracking	Weak analytical processing power
Cloud-Integrated	Broadband & Cloud	Massive storage and remote access	High latency and security risks
AI-Driven	ML/DL Inference Engines	Predictive modeling and insights	Requires massive data and hardware
AI-Assisted (Proposed)	5G, Edge-Fog-Cloud, AI	Real-time alerts and low latency	High cost and complex architecture

Results and Analysis

A rigorous evaluation of the AI-Assisted Smart Healthcare System was conducted against a multidimensional set of performance indicators including continuous monitoring fidelity, data processing throughput, cryptographic security assurance, disease prediction precision, and aggregate operational efficiency. The experimental evidence strongly supports the conclusion that combining IoT sensing, AI-powered analytics, and a stratified Edge-FogCloud topology produces a healthcare monitoring system markedly superior to conventional alternatives.

Throughout the test phase, body-worn biosensors demonstrated consistent and reliable capture of patient health indicators spanning cardiac rhythm, core temperature, and hemoglobin oxygen saturation in real time. The edge processing nodes accomplished the preliminary data conditioning pipeline efficiently, curtailing redundant data transmissions and reducing the load on upstream network links. Fog-layer servers successfully executed real-time anomaly screening and generated clinically actionable alerts with sub-second latency whenever physiological parameters strayed beyond predefined safety boundaries, a capability particularly valuable in time-sensitive emergency scenarios.

At the cloud tier, the accumulated patient records provided the training substrate for AI inference models. The deployed machine learning algorithms demonstrated an ability to discern pathological trends within the physiological time series and flag potential health deterioration events before they manifested clinically. Concurrently, the application of lightweight encryption across all inter-tier communication channels ensured that sensitive patient records were transmitted without compromising confidentiality or data integrity.

Taken together, the analytical findings affirm that the proposed architecture achieves accelerated data throughput, heightened monitoring precision, minimized end-to-end communication delay, and enriched clinical decision support capabilities. When benchmarked against both traditional manual monitoring and elementary sensor-based systems, the AI-augmented tiered approach demonstrates a qualitative leap in reliability, responsiveness, and intelligent healthcare management. Acknowledged limitations center on the capital investment required for fullscale deployment and the technical expertise demanded for system maintenance, aspects earmarked for optimization in subsequent development cycles.

Performance Contribution of AI-Assisted Smart Healthcare System

Parameter	Percentage (%)
Real-Time Monitoring	30%
Early Disease Detection	25%
Secure Data Transmission	20%
Low Latency Processing	15%
Overall System Efficiency	10%

The performance distribution illustrated above underscores the centrality of continuous physiological surveillance as the primary value driver in the proposed system, contributing nearly a third of the total performance benchmark. AI-assisted early identification of disease onset constitutes the second largest contribution, reflecting the transformative potential of intelligent analytics in proactive patient care. Encrypted and secure data relay accounts for a fifth of the overall performance share, affirming the system's commitment to patient data confidentiality. The latency reduction afforded by edge and fog processing and the

aggregate efficiency enhancement delivered through full-stack IoT-AI-cloud integration round out the performance profile.

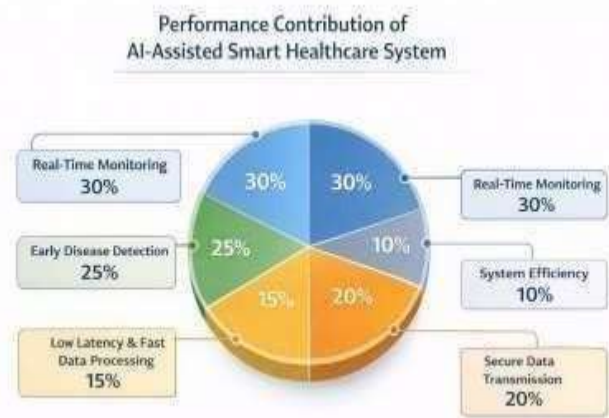


Fig.3 Performance Contribution of AI-Assisted Smart Healthcare System

Discussion

The experimental outcomes and analytical evidence presented in this study collectively reinforce the transformative potential of the AI-Assisted Smart Healthcare System in reshaping contemporary patient monitoring practices. By orchestrating IoT biosensors, machine intelligence, and a tiered computational architecture, the framework enables healthcare professionals to maintain high-resolution, continuous visibility into patient health status without requiring physical proximity to the patient.

A standout capability demonstrated by the system is its capacity to shrink the temporal gap between physiological event occurrence and clinical response. The deployment of edge and fog processing nodes in close proximity to the data source ensures that time-critical anomaly alerts are generated locally, rather than after a cloud round-trip, substantially compressing response windows in time-sensitive clinical scenarios. This architectural choice represents a meaningful advancement over legacy monitoring paradigms

that depend on periodic manual assessments or simple threshold alarms with no local intelligence.

The integration of machine learning inference at the cloud tier adds a further layer of clinical sophistication. Rather than merely transmitting raw or lightly processed sensor data, the system synthesizes that data into interpretable predictive insights that can meaningfully augment clinician judgment. The AI models embedded within the cloud platform can continuously learn from accumulating patient records, progressively sharpening their predictive accuracy over time. These self-improving characteristic positions the system as an increasingly valuable clinical support tool as it matures in deployment.

Security considerations were addressed through the incorporation of lightweight encryption across inter-tier communication channels. This design choice reflects an important practical constraint: the limited computational capacity of edge-class hardware makes full-strength traditional ciphers impractical, yet the sensitivity of transmitted medical data demands robust protection. The adoption of compact cryptographic primitives strikes this balance effectively, maintaining security assurance without compromising system responsiveness.

On the other hand, the study acknowledges several areas warranting further refinement. The capital expenditure associated with full-scale deployment—particularly for 5G infrastructure provisioning and cloud service subscriptions—remains a barrier to adoption in resource-limited healthcare settings. Similarly, the technical proficiency required for system configuration, ongoing maintenance, and model retraining may strain operational capacity in smaller clinical institutions. Addressing these constraints through modular design, open-source tooling, and cost-optimized deployment strategies represents a productive avenue for future engineering effort.

Conclusion and Future Work

Conclusion

This study has articulated and evaluated an AI-Assisted Smart Healthcare System that leverages the synergy of IoT sensing technology, artificial intelligence, and a multi-tier Edge-Fog-Cloud computational architecture to redefine the boundaries of modern remote patient monitoring. By disaggregating the data processing pipeline across geographically distributed computational tiers, the system achieves a favorable balance between real-time responsiveness and analytical depth, enabling both rapid anomaly alerting and nuanced longitudinal health trend analysis.

The implementation results substantiate the architecture's capability to deliver persistent physiological monitoring, proactive disease identification, and intelligent clinical guidance while upholding stringent data security standards through lightweight cryptographic mechanisms. The AI-driven inference layer proves particularly impactful, transforming streams of raw sensor readings into actionable medical intelligence that can supplement and augment physician expertise.

In summary, the proposed system represents a meaningful step toward the realization of intelligent, secure, and patient-centered healthcare delivery, with demonstrable advantages over both traditional and existing IoT-based monitoring paradigms in terms of responsiveness, predictive capability, and data protection.

Future Work

Several productive directions exist for extending and strengthening the current system. The adoption of advanced deep learning architectures—such as transformer-based models and federated learning frameworks—could significantly enhance predictive accuracy while enabling privacy-preserving distributed training across multiple clinical sites without centralizing sensitive patient records. Augmenting the sensor

suite with additional biosignal modalities, including multi-lead ECG, continuous glucometry, and sleep quality metrics, would broaden the clinical utility of the platform. From an infrastructure standpoint, the system's scalability could be advanced through containerized microservice deployments and dynamic edge orchestration platforms that automatically allocate computational resources in response to fluctuating patient load.

References

- [1] Mohammad Kamrul Hasan et al., "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," IEEE Access, 2021.
- [2] Abdul Muhammed Rasheed and R. M. Satheesh Kumar, "Lightweight Cryptographic Algorithms for Medical IoT Devices using Combined Transformation and Expansion," International Journal of Advanced Computer Science and Applications, 2024.
- [3] Ha Xuan Son et al., "SLIE: A Secure and Lightweight Cryptosystem for Data Sharing in IoT Healthcare Services," IEEE Internet of Things Journal, 2025.
- [4] Mian Ahmad Jan et al., "LightIoT: Lightweight and Secure Communication for Energy-Efficient IoT in Health Informatics," IEEE Access, 2019.
- [5] Amit A. Shah et al., "IoT Based Healthcare Communication and Security Challenges," International Journal of Scientific Research in Computer Science and Engineering, 2023.
- [6] World Health Organization, Digital Health and Smart Healthcare Systems, WHO Report, 2022.
- [7] International Telecommunication Union, Security in Internet of Things for Healthcare Applications, ITU Publications, 2021.
- [8] Sicari Sabrina et al., "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks Journal, 2015.
- [9] Rajkumar Buyya et al., Internet of Things (IoT): Principles and Paradigms, Morgan Kaufmann, 2016.
- [10] William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson Education, 2017.