International Journal of Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
Impact Factor (RJIF): 5.57
www.computersciencejournals.com/ijcai
IJCAI 2025; 6(2): 238-247
Received: 19-09-2025
Accepted: 28-10-2025

Sandeep Kumar Verma
Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India

Md Tarique Jamal Ansari
Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India

Suhel Ahmad Khan
Department of Computer Science, Indira Gandhi National Tribal University, Madhya Pradesh, India

Raees Ahmad Khan
Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India

Corresponding Author:
Sandeep Kumar Verma
Department of Information Technology, Babasaheb Bhimrao Ambedkar University, Lucknow, Uttar Pradesh, India

Enhancing Security and Energy Efficiency in Health Industry 5.0: Issues, Applications, and Research Opportunities

Sandeep Kumar Verma, Md Tarique Jamal Ansari, Suhel Ahmad Khan and Raees Ahmad Khan

DOI: https://doi.org/10.33545/27076571.2025.v6.i2c.203

Abstract
The Health Industry 5.0 expansion relies on advanced technologies such as AI, IoT, blockchain, and big data, transforming healthcare and healthcare service delivery by introducing hyper-automation of activities, the customisation and personalisation of care, and patient-centric management of care delivery. The integration of these advanced technologies introduces security challenges, including data privacy, cybersecurity, and regulatory compliance. This paper presents the evolution of the Health Industry 5.0, including the evolution of Health, and a security framework for the Health Industry 5.0 area that will address vulnerabilities and support security against threats. The framework will suggest introducing technologies such as encryption, AI-based threat activity detection, and blockchain to enhance data integrity and protect healthcare and health technology systems. Lastly, we will discuss the application to real-world practitioners and the implications of the security framework for future healthcare advances. Altogether, this paper will serve as a roadmap for adopting Health Industry 5.0 technologies, focusing on security, ethical and legal implications, emerging security trends, and compatibility with regulatory frameworks.

Keywords: Healthcare 5.0, Healthcare 4.0, Cyber Security, Industry 5.0, Privacy, Security

Introduction
Over the past years, the healthcare field has revolutionized using assistive devices and cutting-edge technologies like healthcare applications, telemedicine and telehealth, mobile health, patient monitoring, electronic health records (EHR), and health information notifications. Such technology is referred to as a transition of healthcare services in the digital era. In the medical field, there has recently been a shift from a hospital-centric to a patient-centric perspective, allowing the patient to control health-related personalized operations [1]. This patient-centric and IoT sensor-driven analytical view is referred to as Healthcare 5.0, and it enables patients to receive smart and personalized connected care. The term “Healthcare 5.0” uses the technology of Industry 5.0 to provide healthcare. To increase patient-centric outcomes, minimize healthcare service costs, and improve sustainability in healthcare delivery, Health Industry 5.0 offers proactive, individualized services. IoT, AI, ML, and cognitive computing are the main new technologies driving the technology transformation in the healthcare sector, and these technologies have been the subject of numerous studies [2]. These studies also draw attention to several privacy and ethical issues in the era of digital sphere.
The most recent development in the IT market, known as "industry 5.0," represents the next generation of businesses, societies, and governments to create models that use science and technology to address social, economic, and environmental impacts while also considering ecological well-being[2]. The fundamental principle of Industry 5.0 encourages prosperity for people, planet, society, equity, profit, and the environment." The industry 5.0 market is set for significant expansion, propelled by technology advances and changing industrial requirements. Projections indicate that the market will increase from USD 131.13 billion in 2022 to a notable USD 658.4 billion by 2032, with a compound annual growth rate (CAGR) of 18.0% from 2023 to 2032, as seen in Figure 1. This rapid acceleration is supported by the rising adoption of artificial intelligence (AI), automation, and human-machine collaboration that facilitate industrial processes.

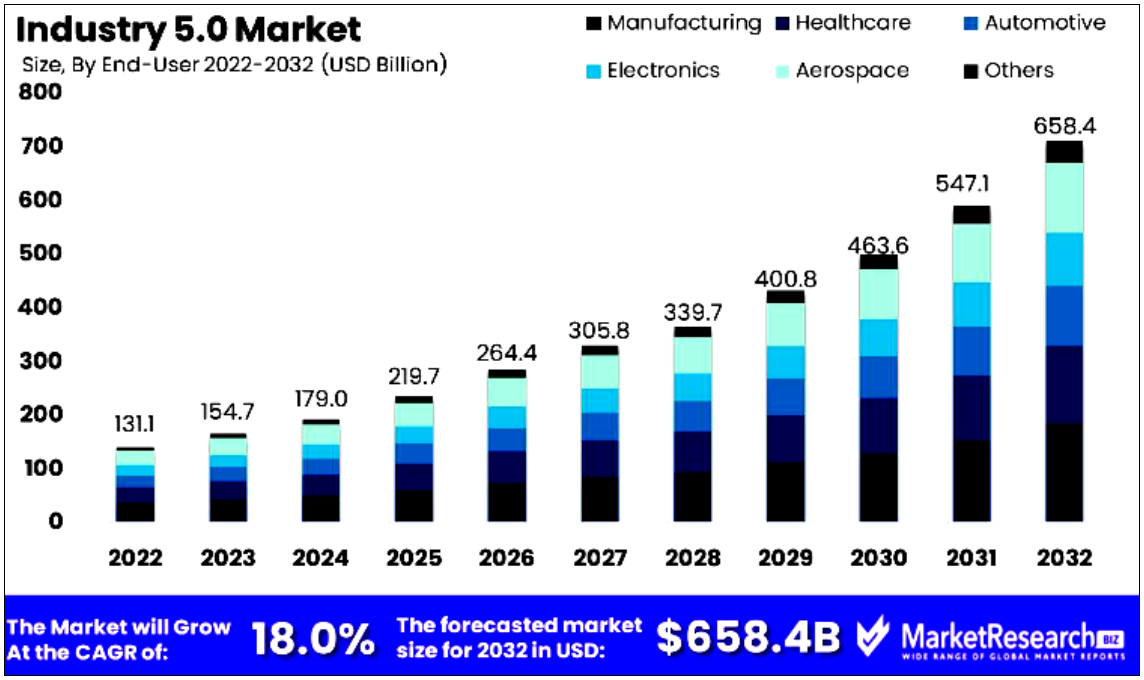

Fig 1: Market size for digital transformation (USD billion) by region, 2018-2030 (Source: Polaris Market Research).

While Industry 4.0 is mainly centred on advanced automation and efficiency, Industry 5.0 is focused on human-centric manufacturing, where smart machines work with people to improve productivity and customisation. The increased need for custom manufacturing, efficiency, and sustainable solutions across industries is also driving the adoption of Industry 5.0 technology. Companies are aware of the advantages of merging advanced robotics, cognitive computing, and IoT-backed solutions into more innovative, responsive, and adaptive manufacturing settings. The Industry 5.0 market is expected to revolutionise manufacturing and industrial operations, as industries adopt these new technologies.

The relationship between digital transformation and Industry 5.0 is illustrated in Figure 2, where Industry 5.0 refers to the many new technological platforms that enhance quality processes. In order to address patient needs successfully, a considerable degree of flexibility and the ability to create real, innovative solutions is important to healthcare. Industry 5.0 will amplify healthcare services through the higher level of design processes that will help manage risks and decision-making and facilitate clarity across organisational objectives. A compelling example is during the COVID-19 pandemic when businesses began generating customised PPE kits. Advancing on the existing construction technologies allowed these businesses to quickly adapt to the levels of demand experienced. These examples contribute to a case study on efficient and timely personalisation in healthcare.

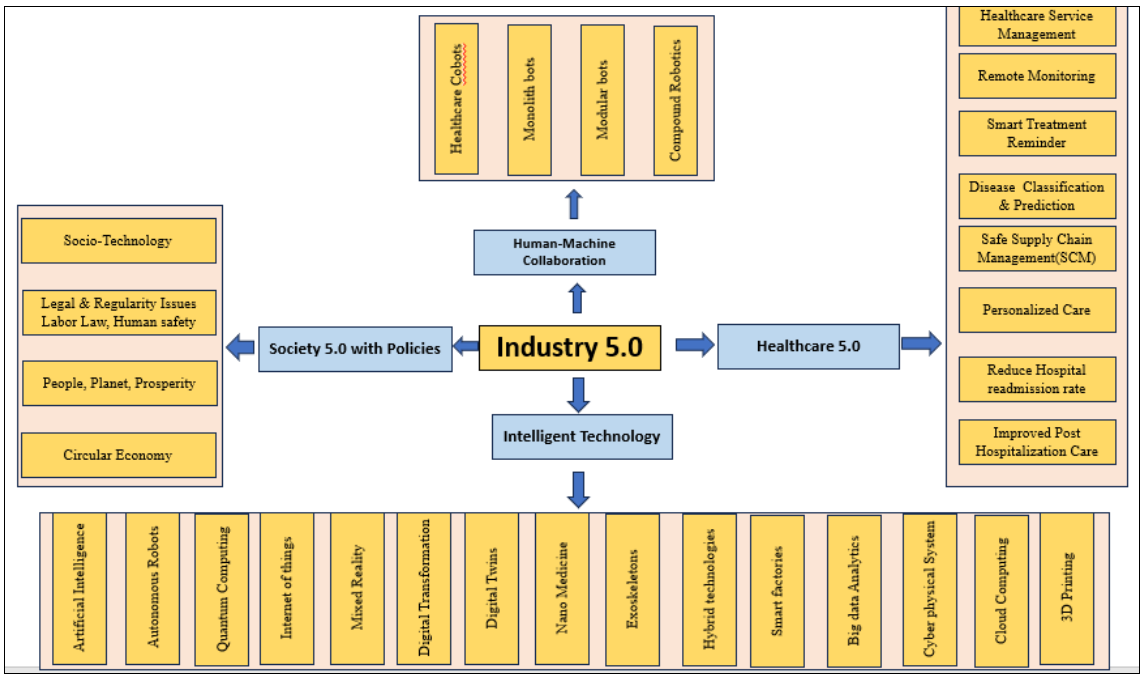

Fig 2: Digital Infrastructure for Industry 5.0

Industry 5.0 takes innovation to the next level by blending highly advanced machinery with human creativity, allowing for more precise and effective solutions. This approach becomes particularly valuable in healthcare, where personalisation and risk assessment play a crucial role, especially during pandemics. This article explores how Industry 5.0 enhances healthcare security services by emphasising tailored solutions and proactive precaution systems to improve patient outcomes in critical situations.

One of the primary drivers of market share growth is the healthcare sector. Age-related disorders and lifestyle diseases have become more common due to the sedentary lifestyle and the aging population. Table 2 presents a comparison of both Industry 4.0 and Industry 5.0 based on security factor analysis from the perspective of healthcare. Table 3 presents a comparative analysis between Health Industry 4.0 and Health Industry 5.0.

Security Challenges in the Healthcare System

Healthcare 5.0 experiences several challenges, including handling huge amounts of data, inadequate infrastructure and lack of standards, threats to data privacy and security, regulatory compliance, data availability, quality, interoperability, etc [7]. Various types of security attacks, ransomware attacks, data breaches, insider threats, phishing, regulatory compliances, physical security, and data encryption are possible security attacks in Healthcare 5.0[8]. Due to these attacks, we proposed an ECC-based secure model in Health Industry 5.0.

Research Contributions

This paper highlights the main research contributions as given below-

- This paper reflects the movement from Industry 1.0 to Industry 5.0 along with the healthcare domain in line with the increasing demand for personalization.
- In this paper, the author has discussed various types of applications, security challenges, and future directions in the current scenario.
- The author has proposed a secure generalized framework of the Health Industry 5.0 and the ECC model to preserve data integrity.

Related Work

Mohamed Abdel-Basset *et al.* [11] proposed a hybrid multi-criteria decision-making(MCDM) technique in a neutrophilic environment to assess the benefits of industry 5.0 technologies in the healthcare sector. This system is designed within an uncertain neutrosophic climate to ensure accuracy in the evaluation process and shows the most influential technology in the healthcare sector. These findings demonstrate that cloud computing and artificial intelligence are the two most important technologies in healthcare. Bhaivin *et al.* [12]. Investigated various security architectures to protect electronic health records (EHR) and introduced a blockchain-based architecture for Healthcare 5.0. This enabled users to access database data according to their assigned roles. They used blind signatures to create blocks on the Hyperledger Fabric blockchain, protecting the encryption scheme from potential future attacks. Key results included transaction throughput, resource utilization, and network traffic.

Shamshad *et al.* [13] discussed a previously published case study of an ecosystem built around Artificial Intelligence (AI), Cloud Computing, Big Data Technology, and Industrial Cyber-Physical Systems (I-CPS) that is applicable to Healthcare 5.0. Their work described the physical and cyber security challenges in such a system, and they proposed an efficient key establishment scheme to do a secure system-wide key establishment that considers physical and cyber security. This scheme was constructed using useful cryptographic building blocks such as fuzzy extractors, hash function, and XOR operators to implement a trustworthy scheme with physical security. By incorporating a Physically Unclonable Function (PUF) into the scheme, it successfully achieved resilience against physical and cyber-attacks.

Additionally, both formal and informal security assessments were performed describing the adequacy of the scheme to contain some of the possible physical and cyber threats. The authors also utilized the NS3 simulator tool (a well-known simulation framework) to evaluate the scheme in practical conditions in a real world network application. The evaluations indicated that their scheme exhibited lower computational and communication overhead than schemes analogous to their implementation and maintained its ability to function securely.

Gupta *et al.* [14] discussed some of the security, privacy, and communications challenges surrounding Healthcare 5.0 enabled telesurgery systems and proposed a Blockchain-enabled Intelligent Scheme for Telesurgery Systems (or BITS) that improves security and efficiency in telesurgery procedures. They also described how BITS effectively mitigated the aforementioned problems in the system. Nastaran Farhadighalati *et al.* [15] indicated that the healthcare industry is becoming quickly reliant on a computing-based model, despite the fact cloud computing does not satisfy the requirements for real-time data processing. Edge computing is an important technology of Industry 5.0 that resolves these issues of real-time processing, but it comes with an increase in security and privacy risk. Due to the complexities of managing these risks in a healthcare environment, it is essential to classify the threats. In this respect, the SAFE-HEALTH framework is established to provide multi-layer security for edge-computing-enabled healthcare systems, emphasizing the security measures required to detect attacking at different levels of the system, including how to resolve identified vulnerabilities.

Pawani Porambage *et al.* [15] suggested that Industry 5.0 is an evolving concept that integrates the physical and digital spheres to establish a more connected and efficient industry. This study investigates the security and privacy challenges emerging from Industry 5.0 and examines the network-level elements necessary for supportive collaborative robotics, digital twins, and Industry 5.0. Although this study considers digital twin studies and 5G options, the paper also seeks to explore the considerations of 6G networks in relation to industrial automation and their potential impact on the development of Industry 5.0. This knowledge helps readers to make clearly informed deliberations about the security and privacy aspects of Industry 5.0 and whether it is achievable in their industry.

Aryan Dahiya and colleagues [16] explained that the transition from Industry 4.0 to Industry 5.0 changes manufacturing and healthcare by incorporating new and emerging technologies including artificial intelligence, IoT, and blockchain. Industry 5.0 develops patient-centric

healthcare with efficacious, innovative, and relevant business models to address security vulnerabilities. This paper consider the industrial transition, the healthcare landscape, as well as the hurdles of implementation. Moreover, this paper suggests a threat model and offers proposed future research directions to achieve Healthcare 5.0.

Ch. Rupa *et al* [17] design the Ensuring the security of sensitive data in an Industry 5.0-based blockchain application to manage medical certificates using the Remix Ethereum blockchain. This application also uses a distributed application (DApp) that uses a test RPC-based Ethereum blockchain and a user expert system as a knowledge agent. The main strength of this work is the maintenance of existing certificates on the blockchain with the creation of new certificates using the Logistic Map Encryption Cipher on existing medical certificates while uploading them to the blockchain. This application helps in quickly analyzing birth, death, and sick rates according to certain attributes like location and year.

Abdulwahab Alazeb *et al*. [18] suggested that this research presents two new models for hijacking fog computing for healthcare: one for private fog computing distribution and another for public fog computing distribution. These models also provide a specialized framework for assessing the influence of malicious attacks as a mechanism to accurately identify compromised transactions and recover data if needed. Specifically, we will utilize a transaction-dependency graph approach to enable ongoing monitoring and examination of transactions in the system. A simulation-based assessment was conducted to evaluate the usability and effectiveness of the proposed models. The results indicated that the proposed models are a viable and credible means of improving security and resilience for fog computing in healthcare contexts.

Abdur Rehman *et al*. [2] indicate that security and privacy are essential challenges of the Internet of Medical Things (IoMT) affecting its deployment at scale. However, the upcoming healthcare 5.0 in IoMT via machine learning, and coupled with blockchain has innovated secure and intelligent health monitoring. Federated learning (FL) enables decentralised data processing, while privacy-preserving security is ensured. In our study, we investigate the incorporation of blockchain and FL to secure, detect intrusions and enable accurate disease prediction in real-time. The proposed system achieved 93.22% in disease prediction and 96.18% in intrusion detection, demonstrating its use.

Bruno Santos *et al* [19] state that while the full promise of Industry 5.0 can only be realised through the establishment of robust cybersecurity. Industry 5.0 ushers in an industrial era that reinstates human-centred values while addressing key global issues, including resource sustainability, climate change, and social sustainability. The added vulnerabilities to cyber threats posed by advanced enabling technologies warrant discussion of potential threats and plausible mitigating approaches. This is also related to the evaluation of contemporary industrial regimes along with their respective limitations in regard to facilitating the safe transition from Industry 4.0 to Industry 5.0. In this way, this theory encourages creating a cybersecurity framework focused on enabling safe and continuous practices of Industry 5.0 across organizations.

Proposed Model for Secure ECC Architecture of Health Industry 5.0

In Figure 3, the utilization of sensor-based collection of healthcare data comprises many advanced sensing devices that can monitor, capture, and transmit physiological data and environmental data in real-time. This model utilizes biomedical engineering principles, the Internet of Things (IoT), and data science. The sensors, which can be wearable devices, implantable devices, and environmental monitors, measure key health parameters such as heart rate, blood pressure, glucose level, oxygen saturation, and overall physical activity. These sensors depend on their embedded microelectronic processing of data to enable bi-directional communication based on wireless sensor networks using needed communication technologies provided by Bluetooth, Wi-Fi, or other wireless communication. In order to enhance the security features of sensor-based medical healthcare system devices, we evaluated an energy-efficient, elliptic-curve cryptography-based routing protocol (ECCEERP) for secure and encrypted transmission for secured routing to healthcare cloud compute environments. The common element among the connected devices is the patient who is monitored using electrochemical sensors, pressure, temperature, and optical sensors, along with electronic devices and systems in healthcare institutions. The data being generated by the electronic sensing from the patient, or patient data, is crucial in understanding the health status by processing raw health data parameters into many areas of diagnostics. For a secure connection, the patient data from the patients' activity is observed and generated by home IoT sensors, outdoor IoT sensors, and hospital and clinic implementation are then used to generate secure real time monitoring that allows for ongoing evaluation and assessment of the condition of the patient. The sensors described above refer to the cocoons that will prepare diagnostic data, which we described above.

After the data has been collected, it is encrypted using ECC (Elliptic Curve Cryptography) and sent through a firewall, which appears to be secure over the internet security protocols - protecting against the risk of cyber threats and unauthorized access. After being decrypted, the data is stored on a cloud storage system for further analysis. The network deployment facilitates communication between the different parts of the system. The collected data then proceeds to retrieval and security management before being stored on a local server/database. The data, after processing the information, is published to the application interface for each of the healthcare professionals - doctors, healthcare administrators, emergency care units, the medical laboratory, nurses. This gives healthcare professionals, including each one of the medical team, the ability to visualize and respond to real-time patient health regarding further medical action if warranted.

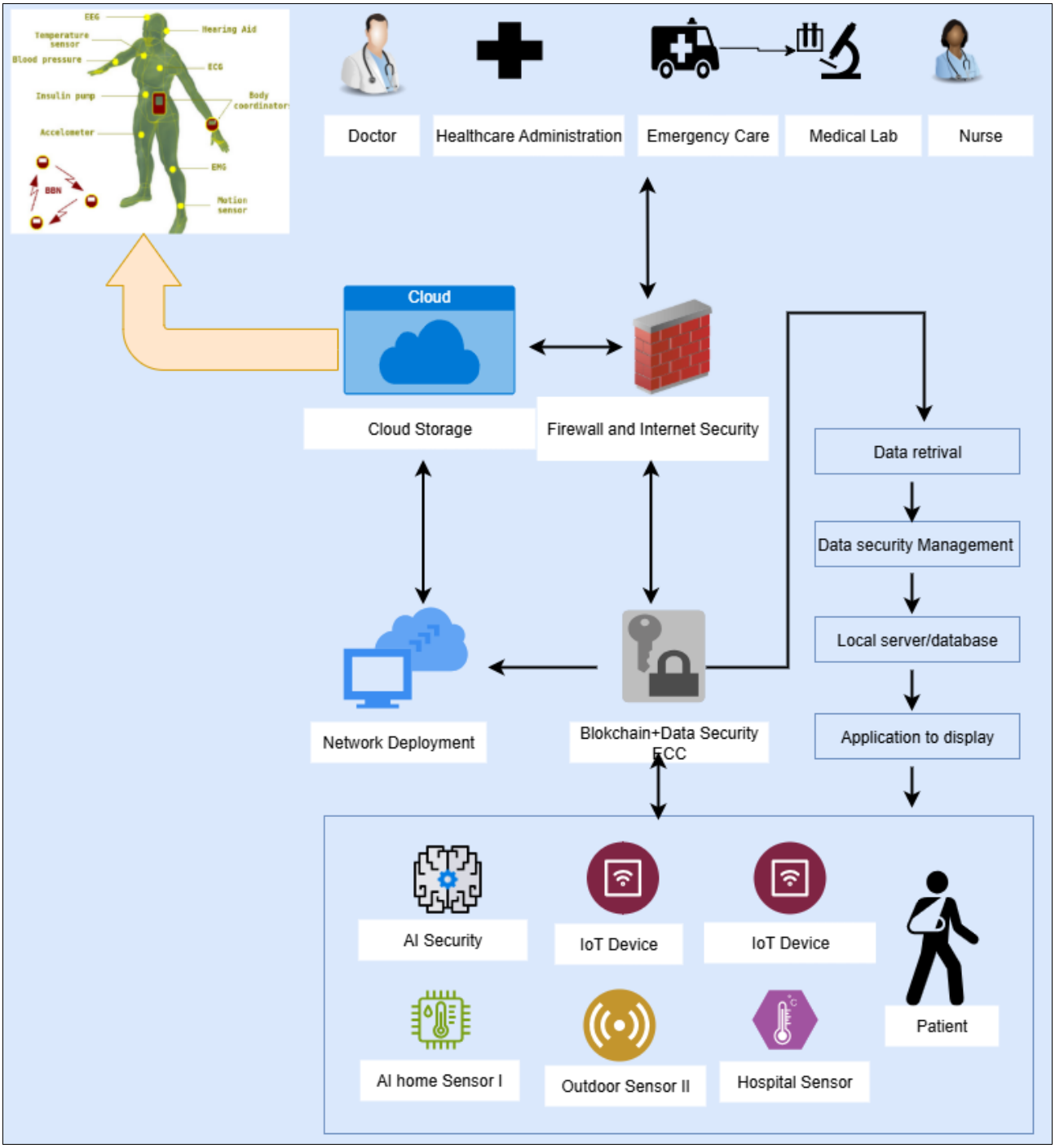

Fig 3: Architecture model of the proposed AI-based Healthcare Industry 5.0 Security Scheme

Figure 3 shows a new healthcare monitoring system that enhances quality of patient care with secure data transfer, real-time alerts and cloud-based data management. This system utilizes AI, IoT, and cloud computing to provide a safe and efficient healthcare solution and to protect patient data.

Data Integrity, Access control, and data sharing in Healthcare informatics

One of the primary challenges in the digital transition to Health Industry 5.0 is ensuring data integrity in healthcare systems. The literature covers several strategies that handle healthcare data exchange, access control, and integrity verification at different levels. These strategies range from blockchain-based frameworks to cryptographic techniques and secure cloud infrastructures. A thorough review of research [20]_[21] shows the advantages and disadvantages of current approaches.

The suggested Elliptic Curve Cryptography (ECC) method provides the best security of medical information in healthcare systems, with also low-power and lightweight factors, solving issues from previous methods. Unlike blockchain systems that are computationally intensive, ECC has comparable security, smaller key sizes, has less overhead, and more timely integrity checks. Therefore, ECC is ideal for resource-constrained environments and environments that are both real-time and energy-sensitive, such as in portable medical devices and IoT-enabled healthcare systems.

Working of Elliptic Curve Cryptography (ECC) Algorithm with Blockchain

In the Health Industry 5.0, we can establish a strong system that protects data confidentiality using blockchain technology and elliptic curve cryptography (ECC). Because of the structure provided by blockchain technology, data can never be changed or deleted without the permission of the owner. This allows the information to be stored in a shared record and complicated mathematics is implemented to link each block in succession. Additionally, ECC conserves computational power required for data encryption and generating digital signatures. Not only is this data is protected, but it is also authenticated. Therefore, the chain of these two provides a secure environment where any activity can be tracked, no activities can be tampered with and that health-related data is protected.

Elliptic Curve Cryptography (ECC) is a form of public-key encryption that provides a level of security equivalent to RSA but requires considerably fewer keys. This renders it more efficient. Here is a detailed description of the process of ECC encryption:

In Key Generation, each user generates a public-private key pair and chooses a private key: A random integer **d** from the range [1, n-1], where n is the order of the elliptic curve. Compute public key from P=d*G, where G is a predefined generator point on the elliptic curve.

In the Encryption process, the sender sends a message to the receiver. Convert the plaintext message M into point M_P on the elliptic curve and also generate a random Integer k (ephemeral key) compute the two points these are C_1 = k*G(this is the shared ephemeral key) and $C_2 = M_p + k.P_B$, where P_B is the receiver's Public key and sends the ciphertext (C1, C2) to the receiver.

In the Decryption Process, the receiver receives (C_1, C_2) and decrypts it as follows Compute $k*P_B$ using C_1, from the following equation $k*P_B = d_B*C_1$ where d_B is the receiver's private key. Retrieve the original message from $M_P = C_2 - d_B*C_1$, since $d_B*C_1 = k*P_B$ subtracting this from C_2 gives M_P and Convert M_P back to the plaintext message.

Performance Analysis and Security of Proposed Model-

Security of Proposed Existing Models- Healthcare equipment frequently struggles to provide adequate security standards with constrained resources. By successfully encrypting the data, the recommended technique in Figure 4 improves security. Table 1 displays the security of both the suggested and current solutions, demonstrating that the recommended strategy offers higher security than earlier strategies in WSNs.

Table 1: Displays the security of both the suggested and current solutions, demonstrating that the recommended strategy offers higher security than earlier strategies in WSNs

Method	Security (%)
OptiGea[37]	42
RBE-EKM[38]	62
RPL-RPMA[39]	85
ACI-GSO[40]	53
PSL-RH[41]	71
ECC-EERP(Proposed)	98

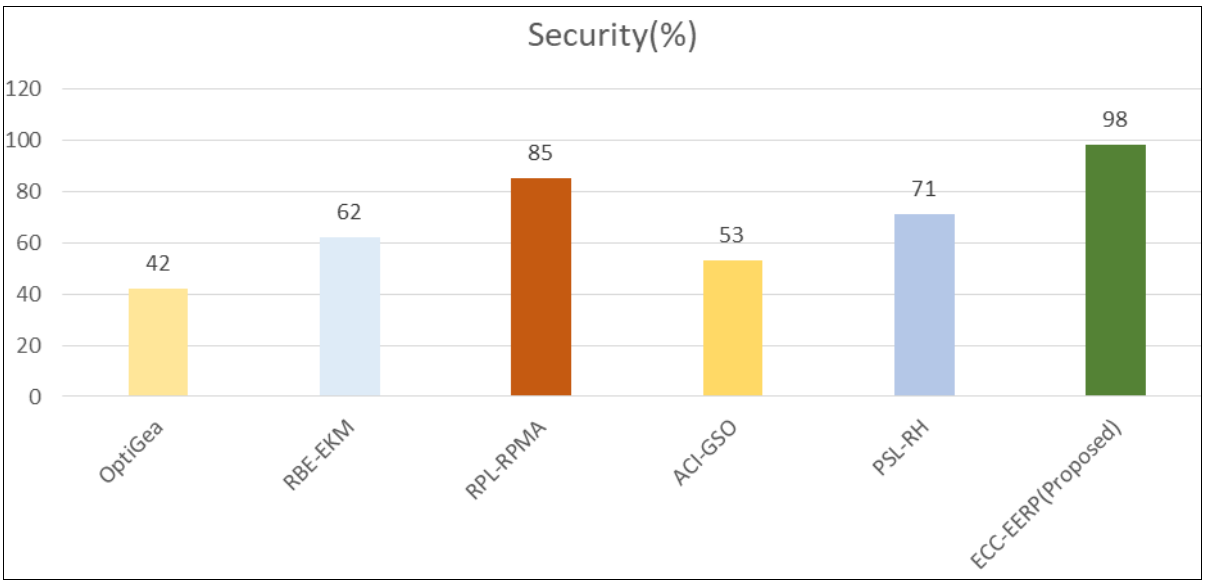

Fig 4: Security Percentage

Encryption Throughput

Encryption throughput is the total amount of plaintext data that is encrypted correctly and quickly. The average amount of plaintext in q bits divided by the average encryption time gives the throughput for an encryption algorithm. The recommended method encrypted the data successfully and securely. The encryption throughput provided by the proposed and current methods is displayed in Figure 5 Table 4, which shows that the recommended strategy provides a reliable and secure encryption throughput.

Number of Node	Encryption Throughput(Percentage)					
	OptiGe	RBE-EKM	RPL-RPMA	ACI-GSO	PSL-RH	ECC-EERP
10	5	54	30	49	51	97
20	7	60	31	89	63	95
30	9	62	38	70	74	95
40	12	72	39	74	78	99
50	15	81	43	79	82	99

Fig 5: Encryption throughput

Energy Efficiency - The total number of bits delivered to the terminal network (or, in the case of storage technologies, the core network) divided by the total energy used by the network to send these bits is known as energy efficiency. The energy efficiency of the suggested and existing approaches is illustrated in Figure 6 and Table 5, demonstrating that the proposed methodology requires less energy for transmission.

Method	Energy Efficiency%
OptiGeA	54
RBE-EKM	38
RPL-RPMA	62
ACI-GSO	84
PSL-RH	73
ECC-EERP(Proposed)	97

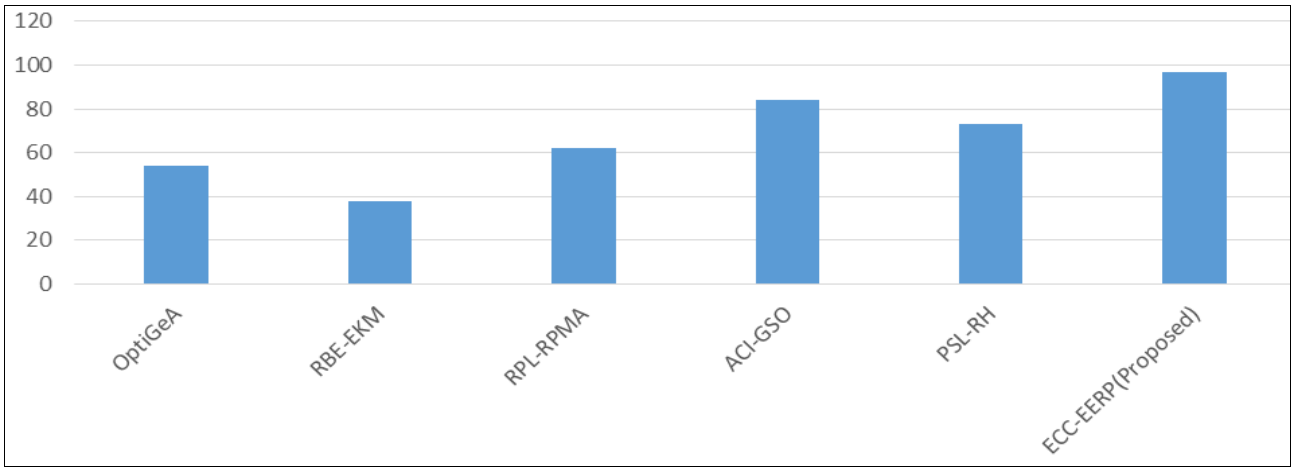

Fig 6: Energy efficient Comparision

Network Lifetime

In WSNs, energy saving is the most dominant issue that relegates the network lifetime. A critical performance metric in WSNs is the network life, which is measured in terms of the length of time that the power of the first sensor runs out. Managing the message overhead among sensor nodes is essential for prolonging the lifetime of networks. The lifetimes of the network offered by the proposed and state-of-the-art techniques are depicted in Figure 7 and listed in Table 6. The proposed approach implies a longer network lifetime for WSNs.

Number of Node	Network lifetime (%)					
	OptiGe	RBE-EKM	RPL-RPMA	ACI-GSO	PSL-RH	ECC-EERP
10	42	72	53	84	72	93
20	47	74	60	81	80	99
30	44	79	52	82	84	92
40	50	76	60	88	88	99
50	41	71	60	86	88	97

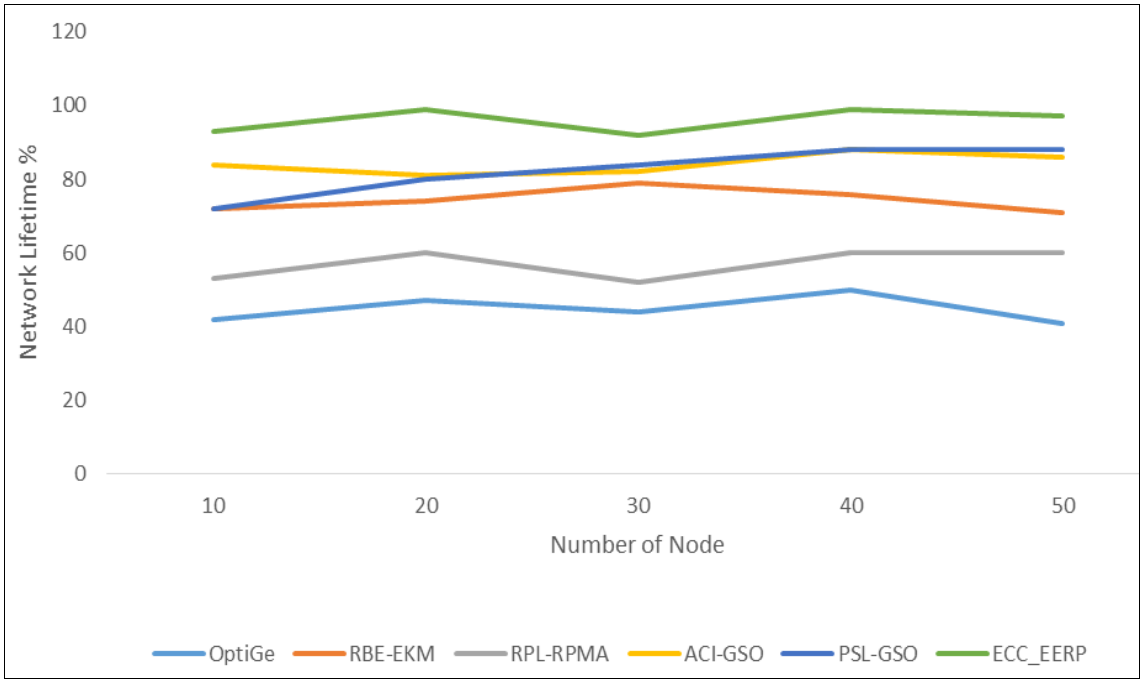

Fig 7: Network lifetime Comparison

Communication Overload

Number of Node	Communication Overload					
	OptiGe	**RBE-EKM**	**RPL-RPMA**	**ACI-GSO**	**PSL-RH**	**ECC-EERP**
10	97	51	74	86	62	10
20	94	58	76	89	73	13
30	99	56	72	81	90	22
40	92	52	78	84	92	31
50	92	63	84	87	90	42

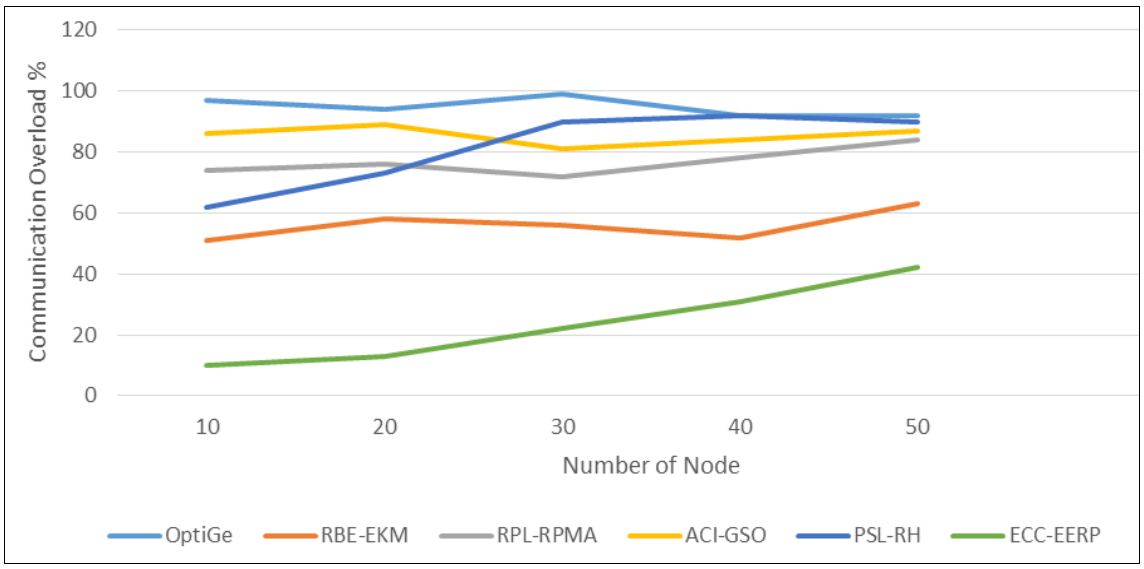

Fig 8: Communication overload Comparison

Computation Time

Method	**Computational Time%**
OptiGeA	94
RBE-EKM	72
RPL-RPMA	61
ACI-GSO	58
PSL-RH	82
ECC_EERP(Proposed)	44

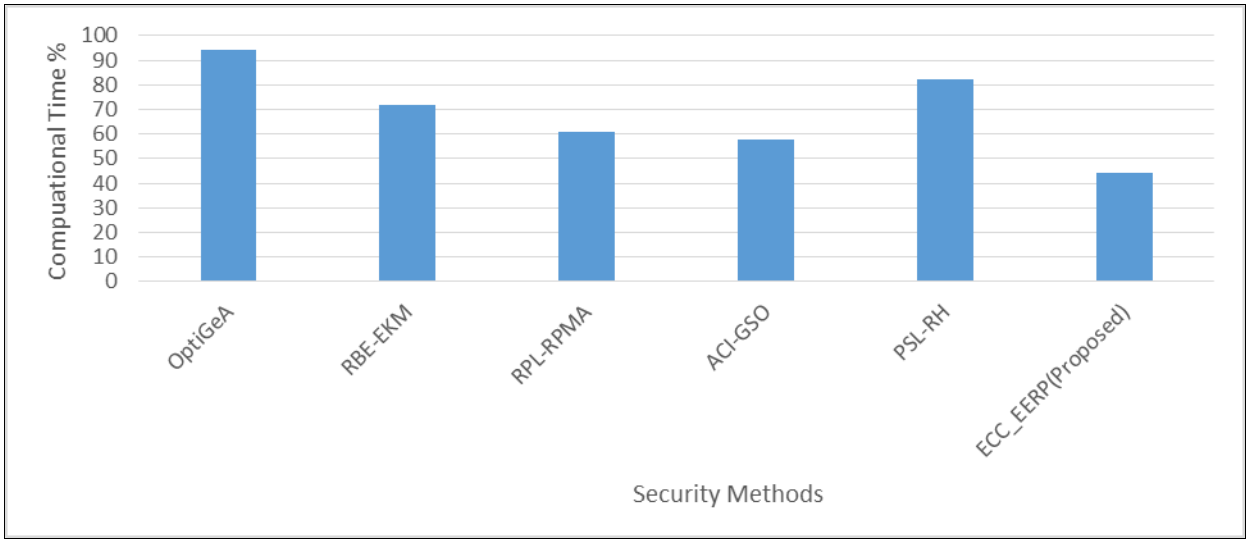

Fig 9: Computation Time Comparison

Implement Cost

Method	Implementaion Cost(%)
OptiGeA	94
RBE-EKM	82
RPL-RPMA	72
ACI-GSO	64
PSL-RH	54
ECC_EERP(Proposed)	40

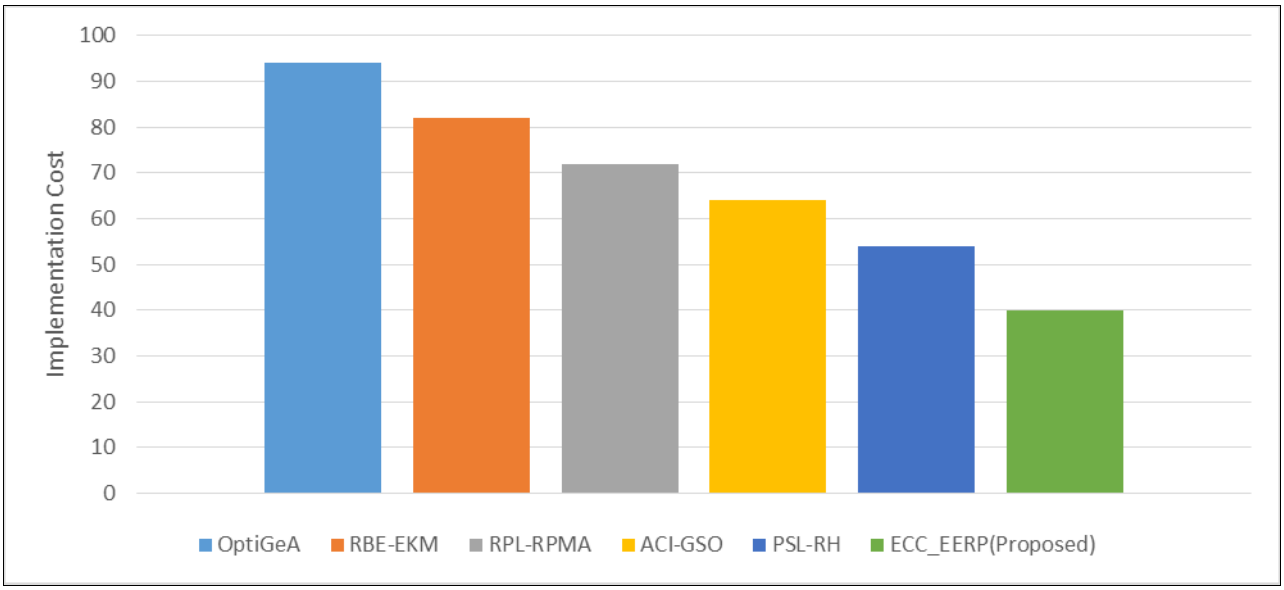

Fig 10: Implement Cost Comparison

Conclusion

The transition in the healthcare industry from traditional systems to Health Industry 5.0 represents a significant shift towards personalized, intelligent, and data-driven healthcare. The uptake of such technologies as artificial intelligence, the Internet of Things, blockchain, and big data would only support increased automation and patient-centered care, but the significant security implications of their integration must be addressed in order to safeguard trust, assurance, reliability, and compliance. Alongside offering an extensive discussion of a holistic security framework, designed specifically for Healthcare 5.0, which incorporates advanced encryption, AI-enabled threat detection, and blockchain technologies for data integrity, this paper hopes to focus on the very need to address common threats to security, which may include data breaches, cyber attacks or threats, interoperability issues, and compliance. The security model proposed is geared towards protecting the healthcare data while also achieving efficiency, scalability, and privacy. Future work should aim to provide even more secure configurations, ensure compatibility on a digital platform, and consider how to address existing scalability issues to account for increased complexity in the healthcare system. Overall, Healthcare 5.0 can achieve its full potential of providing personalized and efficient provision of medical services with its

accompanying protection of data security and ethical standards if a secure and resilient infrastructure is in place. Collaboration among researchers, healthcare professionals, and policymakers will be important to resolve current issues and realize the future of digital healthcare.

References

1. Gomathi L, Mishra AK, Tyagi AK. Industry 5.0 for healthcare 5.0: opportunities, challenges and future research possibilities. In: 2023 7th International Conference on Trends in Electronics and Informatics (ICOEI). IEEE; 2023.
2. Wazid M, *et al*. An ensemble-based machine learning-envisioned intrusion detection in industry 5.0-driven healthcare applications. IEEE Trans Consum Electron. 2023;70(1):1903-1912.
3. Iyengar KP, *et al*. Industry 5.0 technology capabilities in trauma and orthopaedics. J Orthop. 2022;32:125-132.
4. Basulo-Ribeiro J, Teixeira L. The future of healthcare with industry 5.0: preliminary interview-based qualitative analysis. Future Internet. 2024;16(3):68.
5. Abbas T, *et al*. Multidisciplinary cancer disease classification using adaptive FL in healthcare industry 5.0. Sci Rep. 2024;14(1):18643.
6. Yadav H, *et al*. Smart healthcare: paradigm shift in industry 5.0 using AI. In: Recent Trends in Artificial Intelligence Towards a Smart World: Applications in Industries and Sectors. Singapore: Springer Nature Singapore; 2024. p. 67-97.
7. Barata J, Kayser I. Industry 5.0 - past, present, and near future. Procedia Comput Sci. 2023;219:778-788.
8. Baz A, *et al*. Security risk assessment framework for the healthcare industry 5.0. Sustainability. 2023;15(23):16519.
9. Abdel-Basset M, Mohamed R, Chang V. A multi-criteria decision-making framework to evaluate the impact of industry 5.0 technologies: case study, lessons learned, challenges and future directions. Inf Syst Front. 2025;27(2):791-821.
10. Ahmed F, *et al*. Enhancing healthcare data integrity and access control using blockchain and industry 5.0. IEEE Internet Things J. 2025.
11. Abdel-Basset M, Mohamed R, Chang V. A multi-criteria decision-making framework to evaluate the impact of industry 5.0 technologies: case study, lessons learned, challenges and future directions. Inf Syst Front. 2024;1-31. DOI: 10.1007/S10796-024-10472-3.
12. Bhavin M, Tanwar S, Sharma N, Tyagi S, Kumar N. Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications. J Inf Secur Appl. 2021;56:102673. DOI: 10.1016/J.JISA.2020.102673.
13. Shamshad S, *et al*. An efficient privacy-preserving authenticated key establishment protocol for health monitoring in industrial cyber-physical systems. IEEE Internet Things J. 2022;9(7):5142-5149. DOI: 10.1109/JIOT.2021.3108668.
14. Gupta R, Tanwar S, Tyagi S, Kumar N, Obaidat MS, Sadoun B. HaBiTs: blockchain-based telesurgery framework for healthcare 4.0. In: International Conference on Computer, Information and Telecommunication Systems. 2019. DOI: 10.1109/CITS.2019.8862127.
15. Baz A, *et al*. Security risk assessment framework for the healthcare industry 5.0. Sustainability. 2023;15(23):16519. DOI: 10.3390/SU152316519.
16. Dahiya A, Dhull A, Singh A. Advancing healthcare security: exploring applications, challenges, and future research paths in healthcare 5.0. In: 2024. p. 93-120. DOI: 10.1007/978-3-031-65434-3_5.
17. Rupa C, *et al*. Industry 5.0: Ethereum blockchain technology-based DApp smart contract. Math Biosci Eng. 2021;18(5):7010-7027. DOI: 10.3934/MBE.2021349.
18. Alazeb A, Panda B, Almakdi S, Alshehri M. Data integrity preservation schemes in smart healthcare systems that use fog computing distribution. Electronics. 2021;10(11):1314. DOI: 10.3390/ELECTRONICS10111314.
19. Santos B, Luís R, Costa C, Santos L. Cybersecurity in industry 5.0: open challenges and future directions. 2024. Available from: http://arxiv.org/abs/2410.09538
20. Özdemir V, Hekim N. Birth of industry 5.0: making sense of big data with artificial intelligence, the internet of things and next-generation technology policy. Omics. 2018;22(1):65-76.
21. Jambli MN, *et al*. 5G-enabled IoT applications in healthcare: transforming the industry 5.0 healthcare landscape. In: The Future of Human-Computer Integration. CRC Press; 2024. p. 110-120.