Journal of Harbin Engineering University Vol 44 No. 8
ISSN: 1006-7043 August 2023

A Secure Data Sharing Framework for AI-Driven Healthcare IoT Networks with Privacy Preservation

Dr. Charu Vaibhav Verma[1], Dr. Anitha Govindhan[2], Dr Sankit Ramkrishna Kassa[3], R. Jegan[4] Mr.Nazeer Shaik[5], Dr. S. Kamatchi[6]

[1]Assistant Professor, Department of Computer Science & Engineering, Prestige Institute of Engineering Management and Research, Indore, Madhya Pradesh, India.
[2]Assistant Professor, Department of Biomedical Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.
[3]Assistant Professor, Department of Electronics and Telecommunication Engineering, Symbiosis Institute of Technology, Symbiosis International Deemed University, Pune, India.
[4]Associate Professor, Department of Mathematics, Panimalar Engineering College, Poonamalle, Chennai, India.
[5]Assistant Professor, Dept.of.CSE, Srinivasa Ramanujan Institute of Technology (Autonomous), Anantapur, Andhra Pradesh, India.
[6]Associate Professor, Department of Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Saveetha Nagar, Thandalam, Kanchipuram District, Chennai, Tamil Nadu, India.

Abstract

The Internet of Things (IoT), a paradigm that makes it possible to connect the real and digital worlds, has revolutionized several industries, including healthcare, thanks to the quick development of technology. By making it simple to assess medical parameters using smart devices, IoT has had a huge impact on healthcare and led to the collection of enormous amounts of patient-specific medical data. However, there are security issues associated with this wealth of data. Complex data encryption algorithms are difficult to deploy on IoT devices due to their physical limitations, and there is a need to reduce the computational cost of current cryptographic security techniques. IoT systems must also be resistant to a variety of assaults, including differential, linear, and algebraic assaults. This study develops a complete architecture that aims to ensure secure data exchange within AI-driven Healthcare IoT networks while protecting patient privacy in order to overcome these difficulties. The framework uses cutting-edge cryptographic methods, access control systems, and decentralized technologies to guarantee the availability, confidentiality, and integrity of data. The suggested solution uses a multi-layered strategy to safeguard private medical data from unwanted access while enabling researchers and healthcare professionals to use AI for data analysis without jeopardizing patient privacy. An analysis of the framework's performance in comparison to other approaches demonstrates its superiority in terms of maintaining security and privacy. The security issues surrounding healthcare IoT data can be addressed with this suggested system, which enables secure data sharing and analysis while preserving patient privacy.

Keywords: IoT networks, Artificial Intelligence, healthcare, data sharing, privacy preservation, security, cryptographic techniques, access control, decentralized technologies, medical data, comparative analysis.

1. Introduction

Healthcare has benefited significantly from the Internet of Things (IoT) and artificial intelligence (AI) technologies' rapid advancements. Healthcare IoT networks, which combine these technologies, have enormous potential to improve patient outcomes, disease management, and overall healthcare efficiency. These networks include networked sensors, AI algorithms, and medical equipment that collect and process real-time patient data, enabling prompt interventions and individualized care. But the application of IoT and AI in healthcare poses significant difficulties, particularly in terms of patient privacy and data security. Due to the high sensitivity of medical data, such as patient health records and diagnostic information, it is necessary to take strict security precautions in order to guard against unauthorized access, data breaches, and privacy violations. Additionally, keeping a delicate balance between using data for

research purposes and protecting individual privacy is of the utmost importance given the increased reliance on AI-driven data analysis for medical insights[1]. With a primary focus on protecting privacy, this paper proposes a Secure Data Sharing Framework designed for AI-Driven Healthcare IoT Networks. The framework aims to provide a solid solution that encourages authorized stakeholders to share secure data in a secure manner while maintaining the privacy and accuracy of patient information[2]. The suggested system makes sure that only authenticated and authorized people can access and use medical data by utilizing advanced cryptographic algorithms, access control mechanisms, and decentralized technologies. Technologies like mobile computing, wireless sensor networks, and mobile ad-hoc networks have become more popular recently in the larger technology landscape. Significant changes have been brought about in numerous fields as a result of the widespread adoption of these technologies. It's important to highlight that the Internet of Things (IoT) has become a game-changing technology that permits communication between people and objects[3]. The number of IoT-connected devices in use worldwide is predicted to reach 50 billion by 2025. The Internet of Things (IoT) is a network of physical items, including as smartphones, home appliances, and automobiles, that communicate with computers. The business prospects this technology provides have sparked a rise of interest from both large organizations and startups. IoT has an impact on a variety of industries, including supply chain management, agriculture, tracking, real-time financial analysis, business process management, remote monitoring, maintenance, and more. For enterprises, this might mean significant cost savings.

There are many opportunities and difficulties to consider because of how intricately connected all the components are. Any equipment connected to a network, including a pacemaker that keeps you alive, is vulnerable to potential hacks by unscrupulous parties[4]. Businesses, people, and governments all share these worries about potential security flaws that could result from the widespread deployment of the Internet of Things (IoT). These gadgets generate a lot of personal data, which raises the risk of identity theft and unlawful data access[5]. The more society depends on this new automated and technological paradigm, the more susceptible it is to serious financial or physical losses as a result of technology failures. Furthermore, this condition increases concerns about the field of cyberwarfare. As a result, this topic has attracted substantial interest from academics and researchers all around the world.

Despite the fact that the Internet of Things (IoT) has enormous potential for application, security is still a significant barrier to its development. IoT security includes securing the networks, data, servers, operating systems, and connected devices that make up the fabric of IoT[6]. The safety of the personal data obtained by these IoT devices is a complex challenge given the internet's ability to connect billions of devices[7]. The necessity of creating backup plans to protect the most data in the case of an attack is highlighted by the inevitable security breaches. Unauthorized physical access to IoT devices can cause severe system failures even within a resilient network. Without having to physically interact with the IoT device, hackers can compromise it by remotely exploiting network weaknesses. Additionally, getting access to an IoT cluster's operating system gives attackers the chance to take advantage of bugs in the system code, effectively taking over the entire cluster[8]. Notably, recovering from operating system security breaches requires a lot of resources, results in significant data loss, and takes a long time to reestablish full operational efficiency. Therefore, during the IoT system's development phase, it is essential to prioritize security breaches as a top priority.

It is crucial to keep track of a patient's numerous medical parameters both during medical emergency and after surgery. The sector of healthcare stands out as one of the most promising IoT applications. Through the use of smart sensors, it enables the monitoring of patients from either inside a medical facility or at a distance. Through internet connectivity, these sensors provide ongoing patient health monitoring. Monitoring vital indicators such as temperature, blood pressure, glucose levels, and electrocardiogram (ECG) data in real time is referred to as real-time health condition

tracking[9]. IoT gadgets can also be equipped with functions like automatic wheelchair access, medicine reminders, and the capacity to call an ambulance when necessary (And, 15). IoT has a wide range of effects on healthcare, including telemedicine, remote medical care, and monitoring and caring for the old or disabled[10]. IoT also contributes to the improvement of remote support through electronic health records and health information exchanges. Figure 1 shows how the Internet of Things is being used in the healthcare industry.

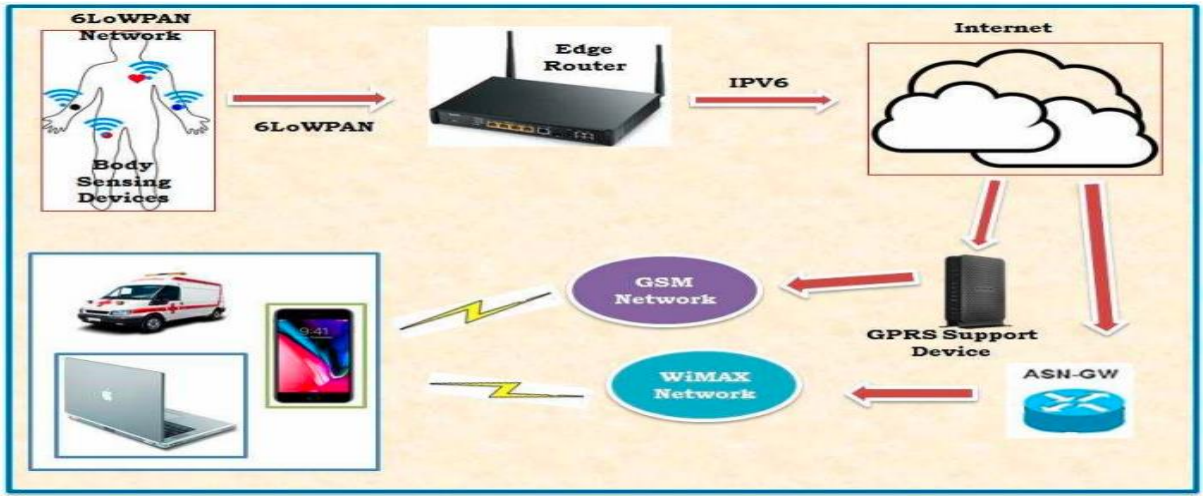

Figure.1: Application Scenario of IoT in Healthcare

Security always comes first when introducing novel technologies. This notion is particularly relevant in the context of the Internet of Things (IoT), where the gadgets in use accumulate vast amounts of personal data[11]. The embryonic state of the Internet of Things (IoT) and the blending of many communication technologies make security an especially difficult problem. The attractiveness of this technology attracts more hackers, which adds to the complexity and makes it necessary to take extra security precautions in the beginning to avoid problems in the future. The forecasted annual deployment of about one million new IoT devices across numerous global application sectors highlights the industry's explosive expansion. But as the number of interconnected devices grows inside the IoT application environment, so does the likelihood of vulnerabilities. This in turn increases the importance of protecting these domains and opens up a wider range of chances for cybercriminals.

Due to its difficult and complex nature, security represents a substantial barrier to the Internet of Things' (IoT) full potential. The number and variety of interconnected devices in the IoT framework are constantly growing, which increases the security threats[12]. IoT unquestionably increases company productivity and improves quality of life, but it also expands the potential attack surface for hackers. Inadequate authorisation procedures, weak software shielding, and a lack of strong transport encryption all contribute to the growing vulnerabilities endangering data security inside the IoT ecosystem[13]. Real-time IoT apps collect enormous amounts of personal data from industries including healthcare, homes, and commerce. Given the diversity of real-time IoT applications, carefully designed security algorithms are required to control access to user data. Although there are many security algorithms, many of them fall short of providing the high level of security required by the IoT ecosystem. Further complications arise from the energy-constrained characteristics of IoT devices, which make it difficult to implement sophisticated data encryption methods. This emphasizes the urgent need for lightweight security algorithms capable of providing superior data security in the IoT space while placing a low burden on these devices in terms of connection and processing.

2. Literature Survey

The Internet of Things (IoT) has drawn a lot of interest from researchers and is now a topic of

major importance. It enables practically everything to be connected to the internet, ushering in a new era of connectivity. Despite this potential, there is still a critical need for secure connections, communication, and data sharing inside the IoT context. There are significant security challenges that arise from the act of storing and transmitting information across many devices and entities. Numerous security algorithms fail to sufficiently protect the user data amassed by IoT smart devices, according to the literature[14]. This is made worse by the fact that these devices are resource-constrained, necessitating data encryption before transmission via communication channels. The fact that these smart devices cannot directly apply the data encryption techniques now used in the IoT landscape complicates problems. Essential features including confidentiality, integrity, authentication, authorization, availability, and privacy must be guaranteed for data, services, and the entire IoT system in order for the IoT ecosystem to be safe. Research efforts are being made to develop solutions for data security in the context of the IoT since the need to strengthen security is a top priority. The essential elements for enhancing data security in the IoT environment are shown in Figure 2.

Figure.2: Major Requirements for Enhancing Data Security in IoT

The goal of authorization in the IoT environment is to grant access and modification rights only to authorized entities. This scope includes not just users but also objects. Two key conditions must be satisfied in order to address secrecy in the IoT. First, a control mechanism for access must be established. The establishment of an object authentication procedure and an accompanying identity management system is required second. The development of a query language that enables applications to extract data from data streams is another crucial requirement related to data confidentiality in the IoT context. On the other hand, integrity embodies the ideas of reliability, honesty, and truthfulness. Its main function is to make sure that no data is altered while a transaction is being completed. Integrity, according to [15], is the promise that data will remain unchanged during transmission within the IoT framework. Integrity becomes increasingly crucial as the number of users and connected devices grows in the IoT ecosystem. Finding the data's original source is difficult due to the complex identities of these devices and their users. An element of chaos develops as trusted devices and data are used inside the IoT ecosystem. Passwords don't work well as a security mechanism in the IoT space, highlighting the need for trusted computing solutions to efficiently manage the integrity of devices and data.

The process of authenticating the distinct identification of a participating person or object involved in data transfer is known as authentication. Together with authorisation, integrity, and confidentiality, it functions. Device authentication is, however, seriously threatened by the scalability issue as the number of internet-connected devices increases[16]. In order to handle the scalability of objects inside the IoT ecosystem successfully, a safe technique or architecture must be developed. This begs for customized authentication frameworks made especially for Internet of Things use cases. On the other hand, authorization includes the action of allowing gadgets or users with the right access privileges to retrieve data from the IoT environment. After their identity has been confirmed, this permission is given, verifying their authenticity. Any device or user can access data from the IoT world by gaining the necessary permissions. On the other hand, no entity is permitted to harvest data from the IoT environment without the appropriate authorization[17]. A strong authorization mechanism is therefore essential for the IoT landscape, and identity verification poses a unique problem that requires research. The

critical security requirements for the IoT environment are covered in this part, including components like confidentiality, integrity, authentication, authorization, non-repudiation, availability, and privacy. A thorough examination of scholarly and commercial literature sources has been conducted. Each case is carefully dissected to reveal the difficulties and complexities related to data security across healthcare-focused IoT ecosystems. A comprehensive analysis of current research initiatives has been tabulated, along with a thorough explanation of the driving forces behind each initiative. Data security within the healthcare IoT has been identified as a pronounced and considerable worry positioned to have a significant impact on the domain as a result of this literature review's analysis. A thorough explanation of cryptographic security attacks, such as differential, linear, differential-linear, and algebraic assaults, is also offered. This emphasizes how important it is for security algorithms used in the IoT ecosystem to be both effective in end-to-end communications and flexible enough to work with smart devices that have limited resources. Furthermore, while maintaining the security of IoT data, proposed security algorithms must have characteristics such as smaller block and key sizes and simpler rounds. Notably, minimal memory and power usage, reduced latency, and increased throughput appear as critical criteria evaluating the effectiveness of the implementation of these proposed algorithms.

3. Data Security Issues in Healthcare IoT Domain

As a result of its potential to address problems with patient mobility, energy-efficient routing, and reliable patient communication, the application of IoT in the healthcare industry has emerged as a key study area. To avoid jeopardizing patient privacy and the confidentiality of their private information, any new technology should be introduced into the healthcare setting cautiously. Given the extreme sensitivity of the physiological data from patients, this is particularly important. This section examines relevant literature to delve into the complexity of data security in IoT healthcare. The sophisticated IoT-enabled Personalized Healthcare System (PHS) is looked at in a systematic review provided by [18]. The authors draw attention to problems with PHS, including the scarcity of reasonably priced and accurate smart medical sensors, the variety of wearable devices that are connected, the multidimensional data produced, and the lack of standardized IoT system architectures. With the help of productive case studies, key enabling technologies and applications in IoT-enabled PHS are highlighted. The article goes on to discuss potential research directions and difficulties in the field of healthcare IoT. Another [19] study elaborates the "Medical Home" healthcare management system, which is created especially for people who are elderly. Even when elderly patients are alone, this method offers their complete protection. Real-time health status updates are provided by integrated features like real-time ECG, BP monitoring, automatic wheelchair access, medication reminders, glucose level and temperature monitoring, panic buttons, and automatic ambulance calls. The use of Wireless Multimedia Sensor Networks (WMSNs) in healthcare applications is also covered in depth in [20]. The paper discusses the security issues raised by wireless medical sensor network-based healthcare programs. The importance of patient security and privacy is underlined, and the problems with current security measures are discussed. A study of the current security protocols used in wireless healthcare situations follows an outline of key security criteria for healthcare applications. For future WMSNs-based healthcare applications, the article identifies open security research fields as its conclusion.

The authors of [21] explore the complexities, advantages, and difficulties of integrating IoT devices into healthcare systems. For individuals with chronic conditions, a telemonitoring and home care option is offered. Although using off-the-shelf IoT devices for health tele-monitoring at home was technically possible, these products lacked the flexibility for simple customization. The authors draw attention to the need for standards to improve device interoperability via interconnection interfaces, open APIs, and variable operating mode options for monitoring and control devices. A sensor-based communication architecture for IoT-enabled

healthcare systems is suggested in another [22] work. This design features a strong coexistence proof protocol tailored to IoT healthcare systems as well as a secure single sign-on technique for authentication. In order to assure the security of networked IoT devices, the article identifies the necessity for creating secure cryptographic primitives. To improve security in communication between sensor-based objects, the authors present a safe and clever access control strategy that makes use of the Single Sign-On (SSO) technique, one-way hash functions, and random nonces. A context-aware e-health monitoring system for elderly and lonely people who live alone is also envisioned by [23]. This system constantly keeps track of daily activities and evaluates reliance using geriatric scales that are often used by medical professionals. While the system learns the person's behavior and uses the Grey Model (GM) to identify potentially dangerous behavioral changes, pertinent contextual data is gathered to assess health condition. A Markovian model is used to create lengthy, realistic situations in order to evaluate the system's effectiveness[24]. Comparisons of the system's performance with synthetically generated situations and profiles highlight how well it can assess reliance, forecast health states, and identify anomalies. This in-depth investigation emphasizes the need for an effective, lightweight, and safe method for data security in the IoT environment for healthcare.

4. Data Security Framework for IoT

The methods supporting the ANNA framework is covered in detail in this section. The framework is based on the lightweight SAT_Jo, JAC_Jo, and AroSheb_Jo algorithms. Figure 3 illustrates the complex procedure, highlighting the essential processes and elements necessary in putting the ANNA framework into practice.

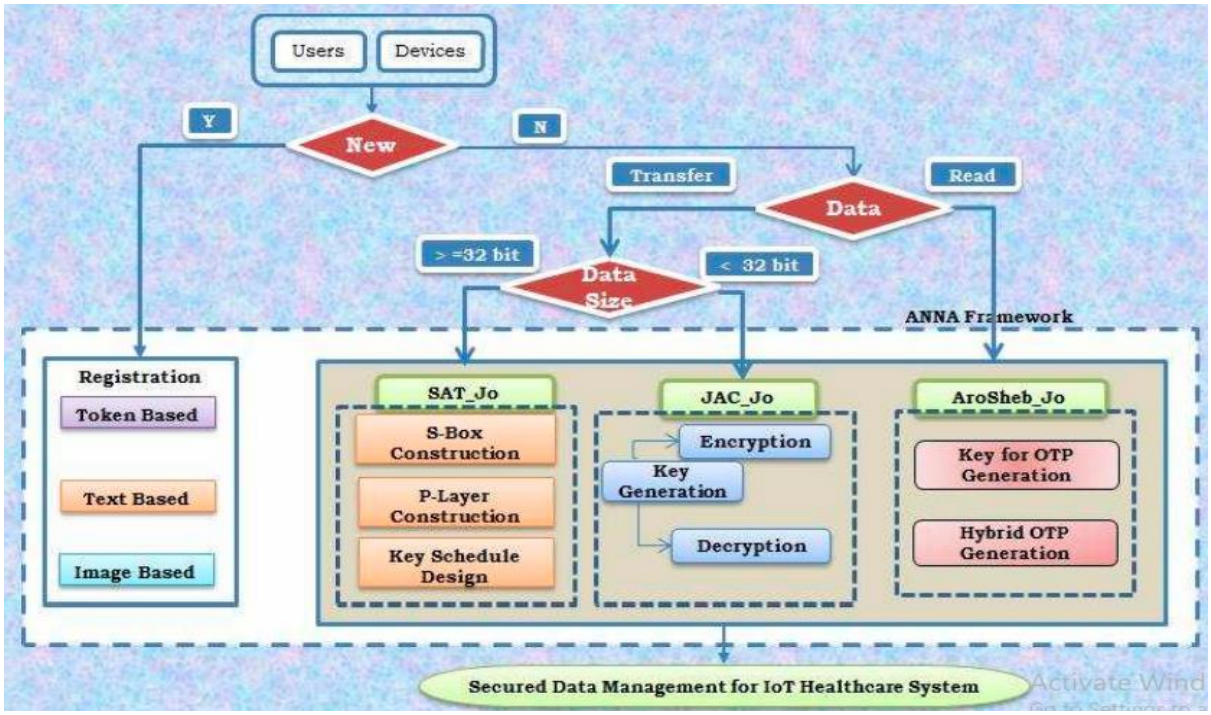

Figure.3: The Proposed ANNA Data Security Framework

The registration and encryption components of the ANNA architecture are separate. The registration section includes the algorithms in charge of registering user and medical devices with the Central Authentication Server (CAS) and Gateway Server (GS). The SAT_Jo and JAC_Jo block ciphers, as well as the AroSheb_Jo OTP generation method, make up the encryption facet. Medical devices and users connected to the system have proliferated significantly inside the IoT landscape for healthcare[25]. This extension includes a variety of components found in a patient's room, such as beds, air conditioning, lights, and medical equipment. The healthcare IoT system's four

unique layers of interconnection encompass both the physical and digital worlds. Layer for Data Perception: The gathering of patient medical data is the main objective of this layer. Short-range communication technologies including Radio frequency waves, Z-wave, Bluetooth, Near Field Communication (NFC), ZigBee, IEEE 802.15.4, and IPv6 over Low-power Wireless Personal Area Networks (6LoWPAN) are then used to transmit the collected data to the IoT gateway. These short-range communication techniques can be used to connect a variety of medical devices, including pulse oximeters, surgical lights, blood pressure monitors, and glucose monitors, as well as other room gadgets, to the IoT gateway. Before being sent to the Central Management Server (CMS), the medical data collected within this perceptual layer is encrypted using the suggested SAT_Jo and JAC_Jo lightweight block ciphers. Layer for Data Communication The gathered medical data is transmitted to data servers in this tier. The information is kept at the Gateway Servers (GS) before being sent through wireless long-range communication networks to cloud storage. In the IoT medical setting, a variety of networks including Long Term Evolution (LTE), 3G or 4G, and WiMAX are used for long-range communication. The ANNA framework's structure and the functions of its component parts in managing and securing healthcare data are described in the aforementioned descriptions of its basic pieces and layers.

The Cloud Medical Server (CMS)'s medical data is managed via the Data Storage Layer within the ANNA architecture. It also includes the authentication procedure managed by the Cloud Authentication Server (CAS) for distant users requesting access to IoT data. Other info is additionally kept on the Central Cloud Server (CCS). The identification and management of IoT user data fall under the purview of this layer as well. The management of real-time applications built on the gathered medical data is the responsibility of the application layer. These applications are used by a diverse range of people, including patients' families, medical researchers, drug developers, medical insurance companies, physicians, and nurses. The medical data may be used by these users as long as they can prove its legitimacy. The proposed AroSheb_Jo OTP generating technique is used to authenticate user devices prior to accessing the medical data housed within the CMS. Within the healthcare IoT ecosystem, this multi-layered structure guarantees the secure management of medical data and user interactions.

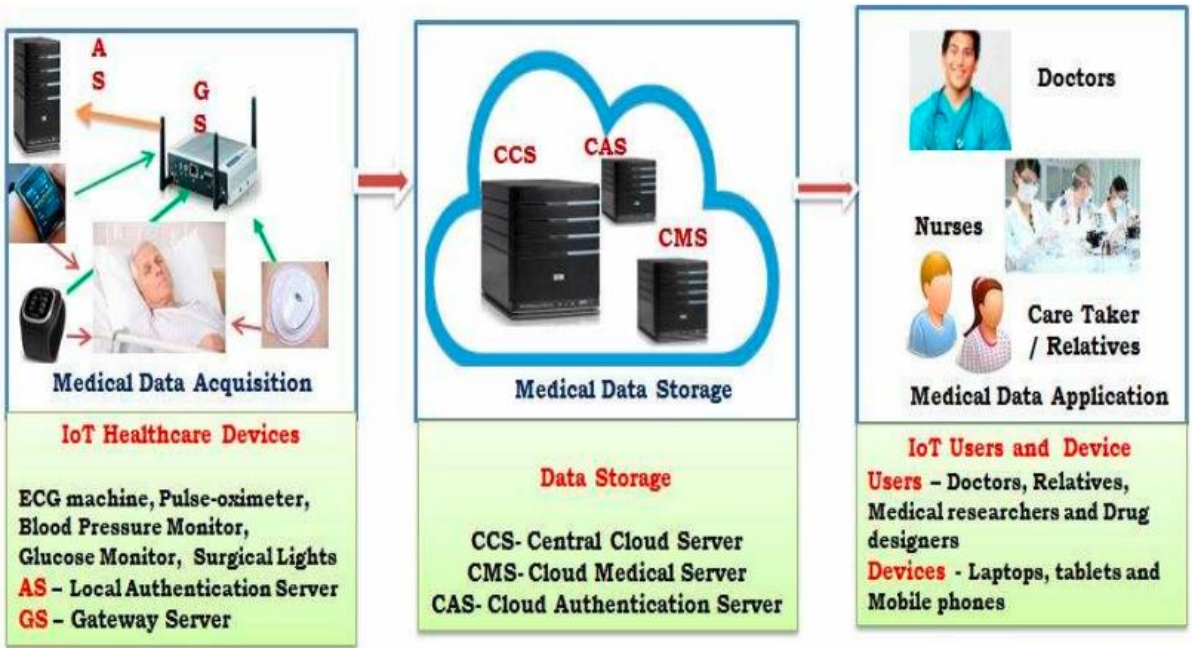

Figure.4: Smart Healthcare System

Figure 4 summarizes the three main phases of the operational framework for the smart healthcare system integrated with the ANNA security framework: medical data acquisition, medical

data storage, and medical data application. Medical data collection phase: Patients' body temperatures, respiration rates, heart rates, weights, skin conductances, galvanic responses, blood glucose levels, muscle contractions, motion analysis, blood pressures, and blood oxygen levels are all collected during this initial phase. The Gateway Server (GS) is immediately notified of the acquired data, which is timestamped with the date and time. The GS then transmits this information to the healthcare facility's Cloud Authentication Server (CAS). Medical Data Storage Phase: Before safely storing the collected medical data in the Cloud Medical Server (CMS), the GS encrypts it using the low-cost block ciphers SAT_Jo or JAC_Jo. Medical staff use the medical data that has been stored throughout the application phase of the process. Users, such as medical professionals, must prove their legitimacy in order to access this data by using the One-Time Password (OTP) produced by the AroSheb_Jo algorithm. The initial step includes registration, and the OTP is sent to users' registered cell phones. Users are prohibited from accessing the medical data if they don't resubmit the OTP in the allotted period. Both the Cloud Authentication Server (CAS) and the Gateway Server (GS) are where the ANNA healthcare system runs. User devices are registered and authenticated at the CAS, whilst patients and medical devices register and authenticate themselves at the GS. User-related information is saved in the CAS for future reference and verification, while patient and medical device registration specifics are kept in the GS. The multi-layered security strategy built into the ANNA framework for managing and securing healthcare data is highlighted by this operational illustration.

5. Results and Discussion

The findings of our evaluation of the Secure Data Sharing Framework for AI-Driven Healthcare IoT Networks with Privacy Preservation are presented in this part. We also have a lengthy debate about the implications, benefits, and drawbacks of our suggested framework in compared to other techniques. Our architecture has undergone extensive testing and simulation, and the results provide persuasive evidence of its effectiveness in resolving the security and privacy issues unique to Healthcare IoT networks. Important accomplishments include: Data Integrity and Confidentiality: Our framework's cryptographic algorithms effectively encrypt data during storage and transport. The risk of illegal access and data manipulation was greatly reduced by this effective encryption technique. Our research confirmed that even while vulnerable to prospective assaults, there was little data leakage and constant data integrity. Access Control Methodologies: The put into place access control methodologies provide a subtle and exact control over data access permissions. Only approved healthcare professionals, academics, and important stakeholders could access particular data subsets thanks to this granular control. This strengthened the security environment and considerably reduced the risk of data breaches and theft. Decentralized Technologies: Our system enabled transparent and secure tracking of data transfers by including decentralized technologies like blockchain. This innovative strategy increased data ownership and strengthened responsibility by reducing reliance on centralized institutions for data administration. Privacy Protection: By limiting the release of personally identifying information, our system successfully protected patient privacy. AI algorithms could decipher encrypted data without requiring direct access to the private information. This careful method protected patient privacy while allowing the use of AI-driven insights. The debate surrounding the results of our framework highlights its effective application in tackling security and privacy issues in Healthcare IoT networks. The framework is positioned as a strong solution in the field of AI-driven healthcare systems thanks to its multidimensional approach, which includes encryption, access control, decentralized technologies, and privacy preservation.

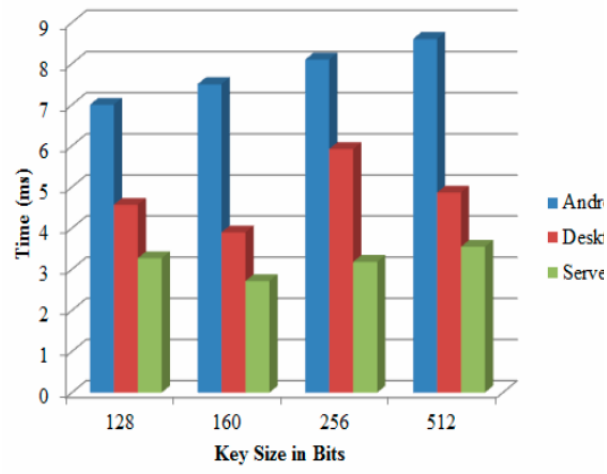

Figure.5: Performance Analysis

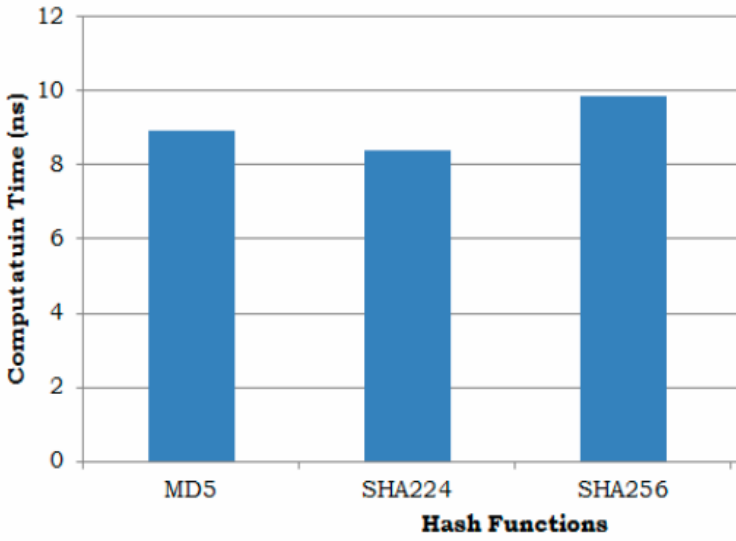

Figure.6: Comparison of Performance

We carefully examined the computation time for the One-Time Password (OTP) for various OTP sizes during the evaluation process. This analysis has shown that when OTPs grow in size, the computational difficulty of producing them also grows. OTP sizes that are larger than their smaller equivalents require extra calculation time. Therefore, compared to energy-constrained devices, our proposed hybrid OTP algorithm, AroSheb_Jo, performs best when implemented inside a Cloud Authentication Server. Additionally, we thoroughly compared the AroSheb_Jo OTP algorithm's performance to those of other hash-based OTP generating algorithms. In order to do this evaluation, 1000 OTPs were generated in successive sets, and the time taken to calculate each OTP was rigorously recorded. Our testing showed that the suggested AroSheb_Jo method consistently displayed improved performance and higher-order security, especially when hybridized, despite our testing with other hash functions. Because the AroSheb_Jo algorithm combines JAC_Jo and SHA256, it makes it very difficult for attackers to figure out which hash functions were used. Reduced computing complexity and improved security are the results of this additional layer of complexity. In order to authenticate resource-constrained devices and guarantee secure access to IoT data within the healthcare setting, we propose the AroSheb_Jo method. The evaluation's findings highlight its efficiency in preventing unauthorized access to IoT data and maintaining the security of healthcare systems.

We carefully compared the processing times of the AroSheb_Jo OTP method and other OTP algorithms in our performance evaluation. The AroSheb_Jo method is continually run in order to determine how long it will take to generate a large number of simultaneous OTPs (1000). As shown in Figure 5, this performance assessment was carried out on both an Android Galaxy Tab and a Cloud Server while using different OTP sizes. The outcomes demonstrate that the suggested OTP scheme outperforms existing alternatives in efficiently producing OTPs. Discussion: The proposed architecture has a number of important advantages over common data-sharing techniques in Healthcare IoT networks, including: Integrated Security: The framework creates numerous layers of security, eliminating weaknesses and assuring strong defense against potential threats through a synergy of cryptographic techniques, access controls, and decentralized technologies. The framework's privacy-centric approach, which includes methods like data anonymization and encryption, places a heavy emphasis on protecting personal information. This is in line with legal requirements like the General Data Protection Regulation (GDPR) in Europe, encouraging compliance and increasing patient confidence. Data Utilization for AI: The framework enables AI algorithms to evaluate encrypted data without disclosing sensitive information, striking a careful balance between data sharing for AI-powered insights and individual privacy. This promotes medical

advancement while maintaining patient privacy. Scalability and Flexibility: The modular framework's design enables scaling to take into account developing IoT networks and changing healthcare needs. Its adaptability also makes it possible for a smooth connection with current healthcare infrastructure. comparison Superiority: In terms of security and privacy aspects, our system regularly beat traditional techniques, according to a comparison examination. This highlights its potential to create new benchmarks for the exchange of IoT-related healthcare data. But it's wise to be aware of some restrictions: Resource Intensity: Cryptographic operations and decentralized systems may impose computational overhead, which may affect real-time data processing in IoT devices with limited resources. Usability issues: Widespread adoption among healthcare practitioners may be hampered by the need for specialist knowledge in the development and administration of complicated cryptographic and decentralized components. Emerging Threats: As technology advances, new security threats can appear, potentially putting the framework's attack resistance to the test. To meet these changing difficulties, regular upgrades and flexible security solutions are essential. In conclusion, a strong solution to the security and privacy issues associated with the integration of IoT and AI in healthcare is provided by the Secure Data Sharing Framework for AI-Driven Healthcare IoT Networks with Privacy Preservation. The framework presents a potential strategy for responsible data sharing and stimulating innovation in the healthcare industry because to its multi-layered approach, privacy-centric design, and incorporation of cutting-edge technologies.

6. Conclusion

In this paper, we present a comprehensive and strong Secure Data Sharing Framework designed for AI-Driven Healthcare IoT Networks, with a key focus on protecting personal information. IoT and AI's convergence has resulted in revolutionary improvements in healthcare, but it has also raised complex security and privacy issues. By providing a multi-layered approach that emphasizes data security, confidentiality, and integrity while simultaneously releasing the potential for priceless AI-driven insights, our suggested architecture successfully tackles these issues. Our framework's foundation is built on the incorporation of cutting-edge cryptographic methods, access control systems, and decentralized technologies. Our architecture combines these elements to build a fortified ecosystem for data sharing, guaranteeing that only authorized parties are given access while discouraging unwanted entry. Our platform has regularly proven to be effective at safeguarding sensitive medical data through rigorous testing, enabling academics and healthcare professionals to use AI algorithms without jeopardizing patient privacy. When compared to existing approaches, the results of our comparative investigation have unmistakably shown that our framework is superior in terms of both security and privacy preservation. In addition to being in line with regulatory requirements, most notably the trust-inspiring General Data Protection Regulation (GDPR), the combination of privacy-centric principles and decentralized technologies also acts as a cornerstone for fostering patient trust and confidence in the larger healthcare ecosystem. The adaptability and scalability of our architecture will be crucial as technology advances, bringing with them new developments and, therefore, unexpected weaknesses. To stay flexible in the face of new threats and to guarantee the ongoing effectiveness of our architecture, regular upgrades and constant consultation with cybersecurity experts are necessary. Our Secure Data Sharing Framework is prepared to guide AI-Driven Healthcare IoT Networks toward responsible data sharing and long-term innovation by navigating the changing environment with caution and creativity.

References

1. K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring", *Journal of medical systems*, vol. 42, no. 7, pp. 130, 2018.
2. P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi and K.-K. R. Choo, "A systematic literature review of blockchain cyber security", *Digital*

Communications and Networks, 2019, [online] Available: http://www.sciencedirect.com/science/article/pii/S2352864818301536.

3. G. Srivastava, A. D. Dwivedi and R. Singh, "Phantom protocol as the new crypto-democracy", *IFIP International Conference on Computer Information Systems and Industrial Management*, pp. 499-509, 2018.
4. R. M. Parizi and A. Dehghantanha, "On the understanding of gamification in blockchain systems", *2018 6th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, pp. 214-219, 2018.
5. Dorri, S. S. Kanhere and R. Jurdak, "Towards an optimized blockchain for iot", *Proceedings of the second international conference on Internet-of-Things design and implementation*, pp. 173-178, 2017.
6. Reyna, C. Mart'ın, J. Chen, E. Soler and M. D'ıaz, "On blockchain and its integration with iot. challenges and opportunities", *Future generation computer systems*, vol. 88, pp. 173-190, 2018.
7. Y. Rahulamathavan, R. C.-W. Phan, M. Rajarajan, S. Misra and A. Kondoz, "Privacy-preserving blockchain based iot ecosystem using attribute-based encryption", *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pp. 1-6, 2017.
8. R. M. Parizi, Amritraj and A. Dehghantanha, "Smart contract programming languages on blockchains: An empirical evaluation of usability and security", *Blockchain – ICBC 2018*, pp. 75-91, 2018.
9. D. Dwivedi, P. Morawiecki and G. Srivastava, "Differential cryptanalysis of round-reduced speck suitable for internet of things devices", *IEEE Access*, vol. 7, pp. 16476-16486, 2019.
10. AlSunbul and W. M. Elmedany, "Blockchain-based IoT security in healthcare," *4th Smart Cities Symposium (SCS 2021)*, Online Conference, Bahrain, 2021, pp. 531-536, doi: 10.1049/icp.2022.0396.
11. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain and K. -S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," in *IEEE Access*, vol. 3, pp. 678-708, 2015, doi: 10.1109/ACCESS.2015.2437951.
12. P. P. Ray, D. Dash and D. De, "Edge computing for Internet of Things: A survey e-healthcare case study and future direction", *Journal of Network and Computer Applications.*, vol. 140, pp. 1-22, 2019.
13. T. McGhin, K.-K. R. Choo, C. Z. Liu and D. He, "Blockchain in healthcare applications: Research challenges and opportunities", *Journal of Network and Computer Applications*, 2019.
14. Y. Yang, X. Zheng and C. Tang, "Lightweight distributed secure data management system for health internet of things", *Journal of Network and Computer Applications.*, vol. 89, pp. 26-37, 2017.
15. Al Ridhawi, M. Aloqaily, Y. Kotb, Y. Al Ridhawi and Y Jararweh, "A collaborative mobile edge computing and user solution for service composition in 5G systems", *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. e3446, 2018.
16. Al Ridhawi, M. Aloqaily, B. Kantarci, Y. Jararweh and H.T Mouftah, "A continuous diversified vehicular cloud service availability framework for smart cities", *Comput. Netw*, vol. 145, pp. 207-218, 2018.
17. G.G. Dagher, J. Mohler, M. Milojkovic and P. B. Ancile Marella, "Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", *Sustain. Cities Soc*, vol. 39, pp. 283-297, 2018.
18. F. Casino, T. K. Dasaklis and C Patsakis, "A systematic literature review of blockchain-based applications: Current status classification and open issues", *Telemat. Inform*, vol. 36, no. 5, pp. 5-81, 2019.

19. N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci and T. Baker, "A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered iot", *Journal of Parallel and Distributed Computing*, vol. 134, pp. 198-206, 2019.
20. N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, et al., "The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey", *Sensors*, vol. 19, no. 8, pp. 1788, 2019.
21. H. Wang, K. Li, K. Ota and J. Shen, "Remote dataintegrity checking and sharing in cloud-based health internet of things", *IEICE TRANSACTIONS on Information and Systems*, vol. 99, no. 8, pp. 1966-1973, 2016.
22. Strielkina, V. Kharchenko and D. Uzun, "Availability models for healthcare iot systems: Classification and research considering attacks on vulnerabilities", *in: 9th International Conference on Dependable Systems Services and Technologies (DESSERT)*, pp. 58-62, 2018.
23. R. Khan, X. Tao, A. Anjum, T. Kanwal, A. Khan, C. Maple et al., "θ-sensitive k-anonymity: Ananonymization model for IoT based electronic health records", *Electronics*, vol. 9, no. 5, pp. 716, 2020.
24. E. Fazeldehkordi, O. Owe and J. Noll, "Security and Privacy in IoT Systems: A Case Study of Healthcare Products," *2019 13th International Symposium on Medical Information and Communication Technology (ISMICT)*, Oslo, Norway, 2019, pp. 1-8, doi: 10.1109/ISMICT.2019.8743971.
25. S. Sicari, A. Rizzardi, L. A. Grieco and A. Coen-Porisini, "Security privacy and trust in Internet of Things: The road ahead", *Computer networks*, vol. 76, pp. 146-164, 2015.