10.48047/jocaaa.2024.32.02.66

# Study and Implementation of Enhancing Security for Sensitive Medical Data in IoT-Based Healthcare Applications

**Mukesh Kumar Bhardwaj[1], Manish Saraswat[2]**
Faculty of Science & Technology, The ICFAI University, Himachal Pradesh

*Corresponding Author: mukeshbhardwaj85@gmail.com

## Abstract

The Internet of Things (IoT) is great for healthcare because it lets doctors keep a closer eye on patients and analyse data. The Internet of Things (IoT) can collect vital signs by connecting medical devices like blood pressure cuffs and glucose meters. However, protecting healthcare data in IoT-cloud environments is a major job because of weaknesses and attacks. In the age of artificial intelligence (AI), it is becoming more common to use AI to improve information security in these kinds of situations. However, AI has problems like high sensor costs and computational complexity. This study proposes Probabilistic Super Learning (PSL) Arbitrary Hashing (RH), an AI-based method designed to enhance both security and cost-effectiveness in IoT healthcare records management.

**Keywords**: Artificial Intelligence, Security System, IoT, Healthcare Applications, Probabilistic Super Learning

## 1. Introduction

The internet of things (IoT) is the connection of physical objects with built-in intelligence and connectivity. It has changed many industries, including healthcare. IoT devices that have software, sensors, and internet access can easily collect and share data. This seamless integration into existing laptop-based systems enhances operational accuracy and efficiency, yielding economic benefits [1]. IoT technologies are used in digital physical structures in healthcare. They use sensors and actuators for things like smart grids, smart homes, and remote monitoring of medical devices [2]. The increasing prevalence of IoT in healthcare is illustrated by the forecast that by 2020, the IoT will comprise nearly 50 billion interconnected devices, a substantial proportion of which will be dedicated to scientific applications [2]. There are many different types of these devices, from implantable medical devices like pacemakers to wearable devices like health trackers. All of these devices are part of a huge network of connected healthcare devices.

Because the facts are so sensitive, it is very important to keep healthcare facts safe in IoT settings. Cybercriminals really want patient information, like medical records and treatment histories, and it needs to be protected to keep patient privacy and trust [3]. Following the rules and regulations along with the health insurance for medical care The Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) are very important because breaking

10.48047/jocaaa.2024.32.02.66

them can have serious financial and reputational consequences for healthcare companies [3]. Also, making sure that records are safe is important for keeping patient safety and care high quality, because bad data can directly affect treatment plans and patient health. [3].

There are some unique problems with protecting the Internet of Things in the healthcare zone. Because there are so many different kinds of IoT devices used in healthcare settings, it is hard to standardise security measures. This makes the attack surface bigger and the control more difficult [4]. In healthcare, real-time data processing and access are very important. Any security measures that make it harder to get to this data can be bad for patient care [4]. Combining old systems with new IoT devices can be hard because older systems may not have all the safety features they need [4]. In addition, IoT devices used in healthcare often have limited resources, such as low processing power and memory, which makes it hard to add strong security features [4]. In the end, flaws in medical devices are very dangerous because they can be used to put patient safety and care at risk [4]. In conclusion, although the Internet of Things (IoT) has huge potential to change healthcare, it is important to deal with the security issues that come with it in order to protect the integrity, privacy, and availability of healthcare information and services.

Integrating artificial intelligence (AI) into security strategies for Internet of Things (IoT) frameworks is a crucial area of investigation. This article analyses traditional security methods and assesses their benefits and drawbacks in relation to their functional elements and attributes. The IoT architecture [4] included an AI device to make healthcare apps safer. It did this by using a Deep Neural Network (DNN)-based malware detection system that cut down on response time, sped up packet delivery, and cut down on latency while also limiting unauthorised access to cloud data and improving key authentication with specific weight and bias values. The smart and safe IoT framework [5] was made to make healthcare safer by using AI-related rules and guidelines like accountability, transparency, data privacy, safety, interoperability, and sustainability. It focused on finding different types of attacks based on host attributes, data disturbances, and network characteristics, but it didn't have specific ways to find network threats, which hurt the overall performance of the system.

To make smart healthcare systems, we looked at the latest trends in IoT-AI framework design [6]. We combined Wireless Body Sensor Networks (WBSN), field sensor networks, and cloud services into a three-tier architecture to make Web of Medical Things (IoMT) systems. A thorough examination [7] was performed on diverse AI methodologies employed in IoT (Healthcare IoT) systems, highlighting the necessity of compliance with standards such as interoperability, integrity, low latency, privacy, and security to create efficient and secure IoT networks. This study encompassed various similarity matching techniques, including dimensionality reduction methods, discriminant analysis, K-means, logistic regression, and linear regression, alongside their practical applications.

## 2. Objective of Study

10.48047/jocaaa.2024.32.02.66

As more and more IoT devices are used in healthcare, people are worried about how to safely store and get information from IoT-cloud frameworks. Current records safety answers face challenges in figuring out and shielding in opposition to each ordinary and antagonistic records access, posing an enormous chance to affected person data and healthcare machine integrity. There are limits to traditional encryption methods when it comes to key generation, encryption times, complexity, and computational costs [8-12]. The objective of this study is to address these challenges by creating an artificial intelligence-driven Probabilistic Soft Learning (PSL) model for real-time data security. It also suggests using Elliptic Curve Cryptography (ECC) to make Random Hashing (RH) better for encrypting and decrypting data. The goal is to make it easier to store and access healthcare data in IoT-cloud environments while also effectively finding and dealing with security threats [13-15].

## 3. Proposed Method

In this part, section three, there is a full description of the proposed method, including algorithm and flow drawings. The primary contribution of this study is the identification of the characteristics and attributes of data obtained from IoT devices, alongside the implementation of our proposed framework utilising an AI-based Probabilistic Super Learning (PSL) model to facilitate secure data transactions [8]. On the other hand, the w adjustment). In ECC (Elliptic Curve Cryptography), the Random Hashing method is used for encryption and decryption steps. This makes sure that the stored and retrieved data is safe [9]. We used the ECC Random Hash Technique for Data Security and the Probabilistic Super Learning (PSL) Algorithm to reach our goals [16-20].

### 3.1 ECC Random Hash Technique for Data Security

The ECC Random Hash Technique for Data Security encodes the source data before RH stores it in the IoT cloud. In many application systems with rich data feature arrangement, making sure that data is safe is a tough and difficult job [10]. Data security has always included the usual things like storing data safely in an unencrypted form before encrypting it and then accessing it in a way that is safe and verified after decrypting it. AES, DES, and RS4 are just a few of the different standards that classical works talk about. But they take longer to generate keys and encrypt data, are hard to set up, and cost money to run. This paper therefore integrated the intelligent RH key generation method with an encryption mechanism founded on ECC. Hashing plays an important role in ECC-based cryptosystems, particularly for:

- Generating unique and secure keys.
- Ensuring data integrity.
- Preventing replay attacks.

### 3.2 Probabilistic Super Learning

The PSL Algorithm also uses feature learning on a large scale to find attacks and trains the model by using the system's features. The PSL method from section 3 is used to get the features from the IoT device. This changes the training data model to include both normal and adversarial feature

10.48047/jocaaa.2024.32.02.66

classes. The PSL is a feature learning model that helps match the dataset's important features to the model and find attacks when certain alerts go off.

This training model compares the features of IoT devices to see if any devices that could be hacked would try to get to the data stored in the cloud during the process of storing and retrieving it. If the access was allowed, automatic actions like storing and retrieving data were taken [11]. If someone is determined, the firewall or routing device that first blocks access can get an automatic report. Figure 1 shows how the proposed security framework will work as a whole.

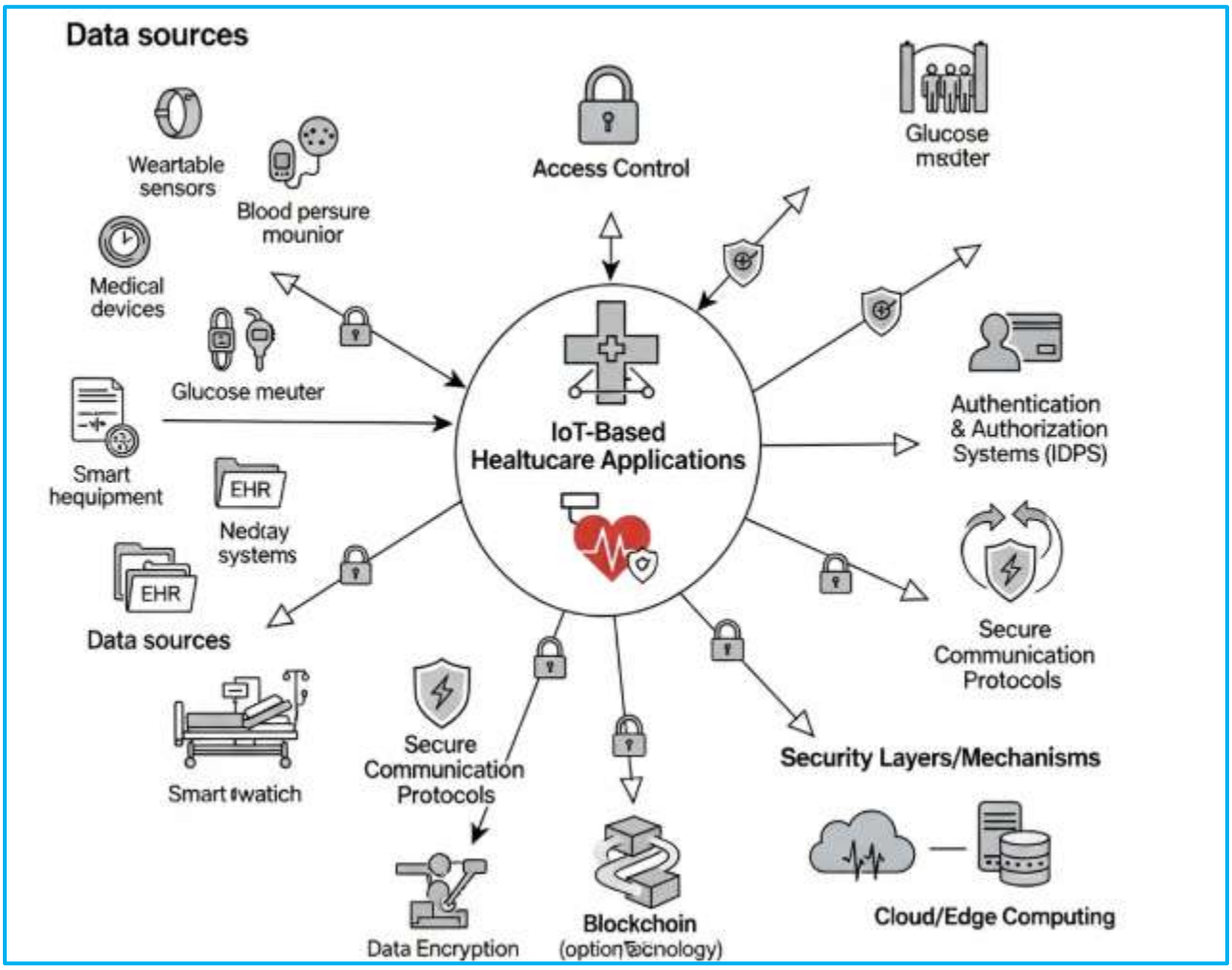



Fig 1 (a)**:** The proposed System

To put the proposed method into action, a few important steps need to be taken. To start, you need to use the Probabilistic Super Learning (PSL) model to deal with data security and threat detection. This means choosing the right machine learning or artificial intelligence framework and training the model with labelled data so that it can tell the difference between normal data access and possible threats. Real-time monitoring is very important, and the PSL model is very important for finding and dealing with security threats as they happen. It is also important to keep updating and improving the

10.48047/jocaaa.2024.32.02.66

model based on new threats and changes in data patterns. Next, it is important to combine Elliptic Curve Cryptography (ECC) with Random Hashing (RH) to protect facts. ECC and RH must be implemented in the records storage and retrieval systems, with records encrypted using ECC and decrypted using RH. It is important to manage keys and parameters correctly to keep the encryption process private and safe.

## 4. Research Methodology

The section looks at how well current and proposed safety techniques work by looking at metrics like F1-rating, Matthews Correlation Coefficient (MCC), throughput, packet transport fee, and computational time. The study looks at how well different encryption methods work, such as high-level Encryption Standard (AES), Ciphertext Policy-Attribute Based Encryption (CP-ABE), modified CP-ABE (MCP-ABE), and the suggested ECC-RH approach, with different key sizes. Results show that bigger key sizes usually need more computing power. AES always has lower computing costs, while ECC-RH has the highest computing needs but offers better security. In Fig. 1 (a) and Fig. 1(b) shows the basic concept and complete methodology.

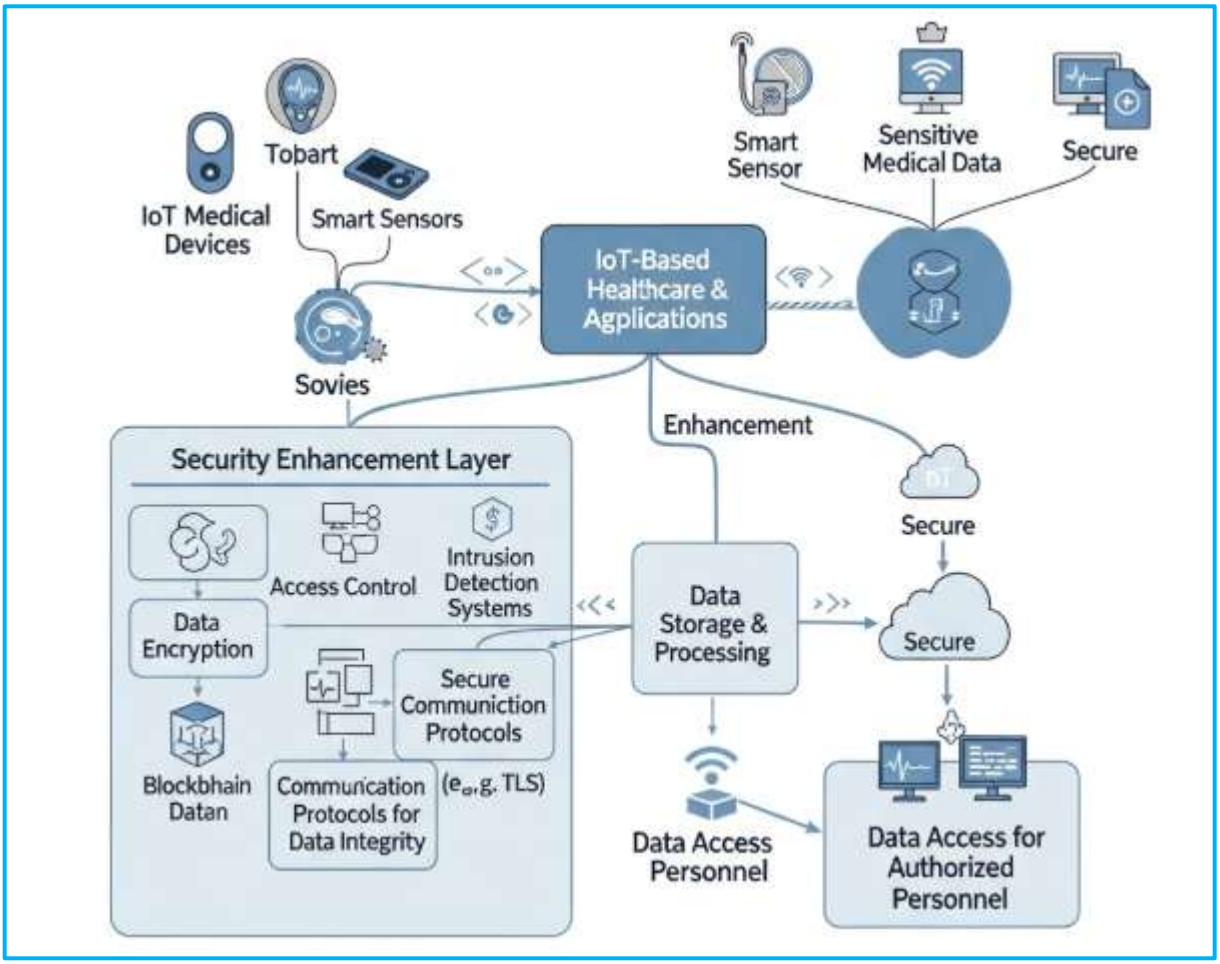



Fig. 1(b) Concept of applied methodology

### 4.1 Data Collection

10.48047/jocaaa.2024.32.02.66

One can use many real-world datasets to simulate:

**Medical datasets:** Add policies based on attributes, such as Role: Doctor and Department: Cardiology. MIMIC-III dataset is an example.

**Financial datasets:** Policies can be based on things like access level, branch, etc.
IoT datasets: Access control is important for many IoT applications, such as smart homes and smart cities. For example, Kaggle has IoT datasets.

### 4.2 Data Analysis

The conversation stresses how important it is to find a balance between safety needs and computational performance when choosing cryptographic methods for specific uses. The studies also suggest a two-layered approach that combines characteristic-based totally Encryption (ABE) and position-based totally get entry to manipulate (RBAC) to make IoT-Cloud frameworks safer, especially in healthcare apps. This method aims to give you full control over who can access your data while also making sure that strong security measures are in place.

At this point, machine learning is often used to find attacks by making a model based on the parts of the system. The proposed PSL method takes features from IoT devices (Fig. 2). The data model is improved by adding both normal and adversarial features to the model. The PSL is a machine learning model that looks for attacks by linking device attributes with datasets. This model checks the features of IoT devices to see if any malicious devices are trying to access or change data stored in the cloud while it is being stored and retrieved. After getting the go-ahead, automated tasks like storing or recovering data are carried out. Also, the firewall or controlling device that first limits access can get a modified report that shows how secure the system is.

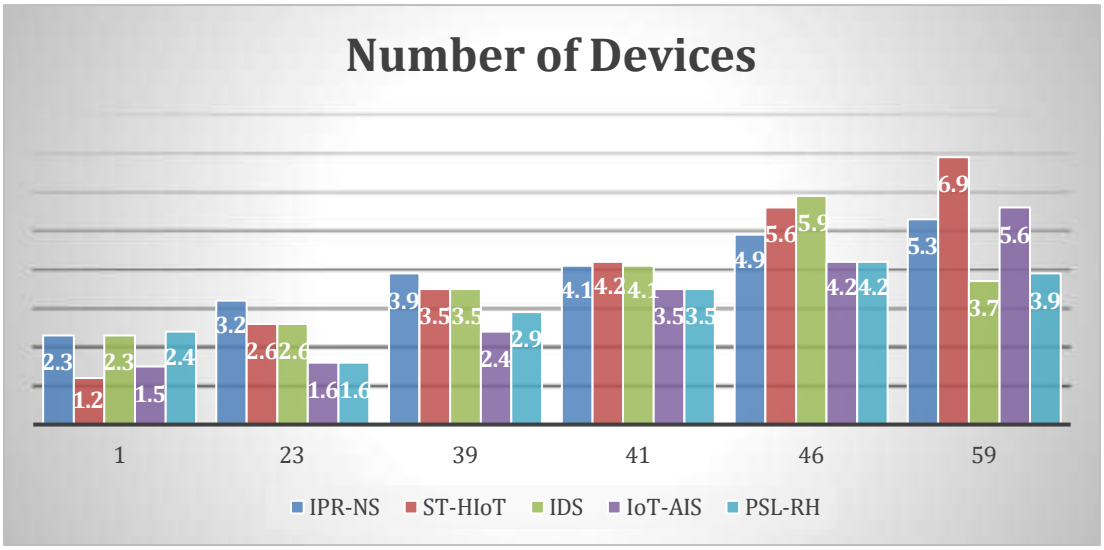
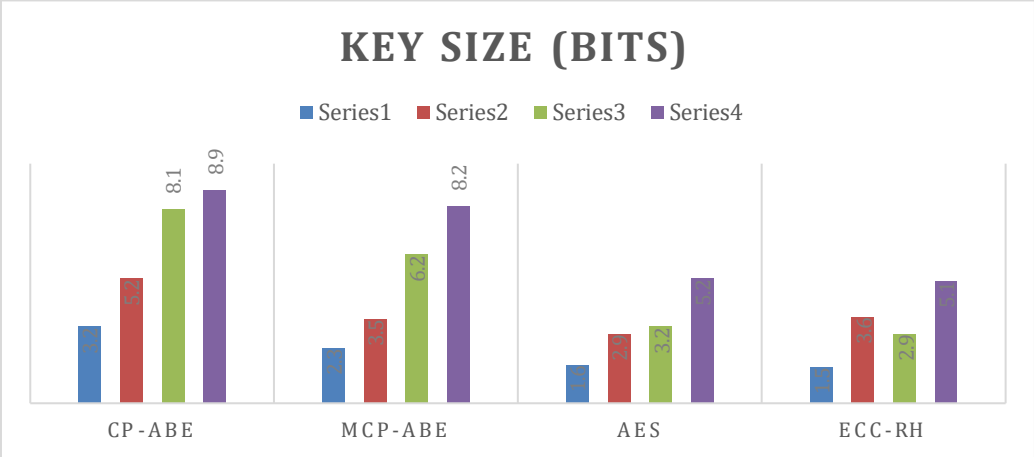



**Figure 2:** Investigation of current and recommended approaches' throughput

10.48047/jocaaa.2024.32.02.66

Figure 3 compares the encryption and decryption instances of existing encryption strategies that use variable key size (bits). These strategies include superior Encryption fashionable (AES), Ciphertext coverage-characteristic based Encryption (CP-ABE), modified CP-ABE (MPC-ABE), and the proposed ECC-RH technique.

.




.

**Figure 3:** Encryption times for current and impending information security techniques.

| Encryption Times | Series1 | Series2 | Series3 | Series4 |
|---|---|---|---|---|
| **CP-ABE** | 3.2 | 5.2 | 8.1 | 8.9 |
| **MCP-ABE** | 2.3 | 3.5 | 6.2 | 8.2 |
| **AES** | 1.6 | 2.9 | 3.2 | 5.2 |
| **ECC-RH** | 1.5 | 3.6 | 2.9 | 5.1 |

**Table 1:** Encryption times for current and impending information security techniques

The data presented in Fig.4 demonstrates the analysis of different cryptographic algorithms concerning their bit key sizes. A consistent pattern is observed across all four encryption techniques (CP-ABE, MCP-ABE, AES, and ECC-RH) as the key size increases. Specifically,

10.48047/jocaaa.2024.32.02.66

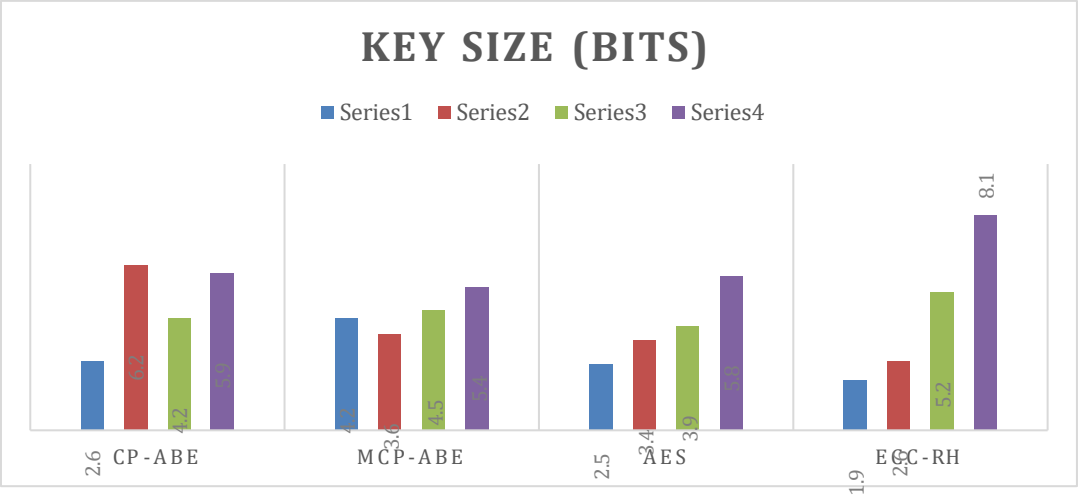



**Figure 4:** Unscrambling times for current and impending information security strategies.

| Unscrambling times | Series1 | Series2 | Series3 | Series4 |
|---|---|---|---|---|
| **CP-ABE** | 2.6 | 6.2 | 4.2 | 5.9 |
| **MCP-ABE** | 4.2 | 3.6 | 4.5 | 5.4 |
| **AES** | 2.5 | 3.4 | 3.9 | 5.8 |
| **ECC-RH** | 1.9 | 2.6 | 5.2 | 8.1 |

**Table 2:** Unscrambling times for current and impending information security techniques

Larger key sizes mean more processing power is needed, which means more processing resources are needed. AES always needs the least amount of computing power, regardless of key size, while ECC-RH always needs the most. This trend shows how important it is to find a balance between security needs and computational efficiency when choosing a cryptographic algorithm for a certain security application. ECC-RH is better for applications that need a lot of security but also need a lot of processing power. AES is better for applications that don't need as much security and don't need as much processing power. [13].

The data above looks at how well different cryptographic algorithms work with keys of different sizes. The results show a number of trends. For example, CP-ABE needs a lot less computing power than other methods when the key sizes are small (132 and 186 bits). But as the key size gets bigger,

10.48047/jocaaa.2024.32.02.66

the computing power needed for CP-ABE also gets bigger, until it is the same as other methods, especially AES and MCP-ABE. [14] The symmetric encryption method AES consistently has low computational costs across all key sizes. ECC-RH, on the other hand, is based on elliptic curve cryptography and has higher computational costs, even for smaller key sizes. However, it is more secure because it decrypts faster than AES and MCP-ABE for the largest key size (1039 bits). These results show how security and computational performance are at odds with each other. They also show how important it is to choose the right cryptographic method for a given application based on its security needs and key sizes.

## Conclusion and Discussion

In nut-shell, this study gives a progressive synthetic intelligence-based totally safety answer geared toward safeguarding the privacy and confidentiality trendy healthcare programs inside an IoT-cloud environment. The primary objective ultra-modern this take a look at is to leverage artificial intelligence techniques to make certain at ease data storage and retrieval processes. The proposed Probabilistic fantastic brand new (PSL) technique, designed to count on assaults proactively, is intended to decorate the safety contemporary the healthcare application framework through schooling the version with a numerous set contemporary learned capability. moreover, to make certain the at ease garage and retrieval latest facts, the research has advanced and integrated a Random Hashing (RH)-based key generation method with the Elliptic Curve Cryptography (ECC) mechanism. This precise synthetic intelligence technique includes maintaining a trained facts version with a variety of everyday and attack attributes, allowing early detection latest capability threats. additionally, it carries an alert machine that notifies the firewall and updates the skilled model with the information ultra-modern any detected assaults. furthermore, the data safety device is reinforced by means of producing a random key based at the hash price and signature pattern present day the information grid.

The research also highlights the challenges posed by the entry of devices into a healthcare provider's temporary workplace, such as the complexities of determining the device's operating system and life cycle management, especially in cases like Bring Your Own Device (BYOD). Devices that connect to the network through unconventional channels may present connectivity issues and exploit vulnerabilities due to their unorthodox entry into the network, requiring heightened awareness and security measures. Overall, this research contributes to the field of data security in IoT-cloud environments by proposing an advanced artificial intelligence-based security solution that addresses the specific challenges of healthcare applications. By integrating cutting-edge techniques and methodologies, the proposed solution aims to establish a robust and proactive security framework for protecting sensitive healthcare data.

## References

1. Kelly, J. T., Campbell, K. L., Gong, E., & Scuffham, P. (2020). *The Internet of Things: Impact and Implications for Health Care Delivery.* Journal of Medical Internet Research,

10.48047/jocaaa.2024.32.02.66

22(11): e20135. doi: **10.2196/20135**.

2. M. Masoud, Y. Jaradat, A. Manasrah, and I. Jannoud, "Sensors of smart devices in the internet of everything (IoE) era: Big opportunities and massive doubts," Journal of Sensors, vol (2019), 26 pages, https://doi.org/10.1155/2019/6514520.
3. Z. Ahmed, K. Mohamed, S. Zeeshan, and X. Dong, "Artificial intelligence with multi-functional machine learning platform development for better healthcare and precision medicine," Database. vol. (2020) DOI: 10.1093/database/baaa010
4. K. Saleem, I. S. Bajwa, N. Sarwar, W. Anwar, and A. Ashraf, "IoT healthcare: design of smart and cost-effective sleep quality monitoring system," Journal of Sensors, vol. (2020), 17 pages, https://doi.org/10.1155/2020/8882378
5. T. M. Ghazal, "Internet of things with artificial intelligence for health care security," Arabian Journal for Science and Engineering, vol.2, (2021), pp. 1–12. https://doi.org/10.1007/s13369-021-06083-8
6. M. R. Valanarasu, "Smart and secure IoT and AI integration framework for hospital environment," Journal of ISMAC, vol.1, (2019), pp. 172–179. DOI:10.36548/jismac.2019.3.004
7. L. Greco, G. Percannella, P. Ritrovato, F. Tortorella, and M. Vento, "Trends in IoT based solutions for health care: moving AI to the edge," Pattern Recognition Letters, vol. 135, (2020) pp. 346–353. DOI: 10.1016/j.patrec.2020.05.016
8. H. K. Bharadwaj, A. Agarwal, V. Chamola et al., "A review on the role of machine learning in enabling IoT based healthcare applications," IEEE Access, vol. 9, (2021) pp. 38859–38890, DOI:10.1109/ACCESS.2021.3059858
9. M. Anuradha, T. Jayasankar, N. Prakash et al., "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing," Microprocessors and Microsystems, vol. 80, (2021) article 103301. DOI:10.1016/j.micpro.2020.103301
10. J.-X. Hu, C.-L. Chen, C.-L. Fan, K. H. Wang, and K.-H. Wang, "An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing," Journal of Sensors, vol. (2017), pages 11. https://doi.org/10.1155/2017/3734764
11. G. B. Mohammada, S. Shitharthb, and P. R. Kumarc, "Integrated machine learning model for an URL phishing detection," International Journal of Grid and Distributed Computing, vol. 14, (2020) no. 1, pp. 513–529. DOI: https://doi.org/10.4108/eai.20-4-2022.173950
12. S. S. Gill, S. Tuli, M. Xu et al., "Transformative effects of IoT, blockchain and artificial intelligence on cloud computing: evolution, vision, trends and open challenges," Internet of Things, vol. 8, (2020),article 100118. https://doi.org/10.1016/j.iot.2019.100118
13. S.Shakya, "An efficient security framework for data migration in a cloud computing
14. environment," Journal of Artificial Intelligence, vol. 1, (2019) no. 1, pp. 45–53. DOI 10.36548/jaicn.2019.1.006
15. M. Hao, H. Li, X. Luo, G. Xu, H. Yang, and S. Liu, "Efficient and privacy-enhanced federated learning for industrial artificial intelligence," IEEE Transactions on Industrial Informatics,,vol. 16, (2019) no. 10, pp. 6532–6542, DOI:10.1109/TII.2019.2945367

10.48047/jocaaa.2024.32.02.66

16. T. Hidayat and R. Mahardiko, "A systematic literature review method on aes algorithm for data sharing encryption on cloud computing," International Journal of Artificial Intelligence Research, ,vol. 4,( 2020) no. 1, pp. 49–57. DOI:10.29099/ijair.v4i1.154
17. S. Shitharth, N. Satheesh, B. P. Kumar, and K. Sangeetha, "IDS detection based on optimization based on WI-CS and GNN algorithm in SCADA network," in Architectural Wireless Networks Solutions and Security Issues, Springer, Singapore 2021. https://doi.org/10.1155/2022/8457116
18. Habibzadeh, H., Sharma, G., et al. (2020). *A Survey of Healthcare Internet-of-Things (HIoT): A Clinical Perspective.* IEEE Internet of Things Journal, 7(1), 53–71. doi: **10.1109/JIOT.2019.2946359**.
19. Rejeb, A., Rejeb, K., Treiblmaier, H., Appolloni, A., et al. (2023). *The Internet of Things (IoT) in healthcare: Taking stock and moving forward.* Internet of Things (Elsevier), Article 100721. doi: **10.1016/j.iot.2023.100721**.
20. Al-rawashdeh, M., Keikhosrokiani, P., Belaton, B., Alawida, M., & Zwiri, A. (2022). *IoT Adoption and Application for Smart Healthcare: A Systematic Review.* Sensors, 22, 5377. doi: **10.3390/s22145377**.