Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 2-A, pp. 513–524
DOI : 10.47974/JDMSC-1896

Privacy-preserving patient monitoring in healthcare IoT using attribute-based cryptography

Dhiraj Kumar Mane [†]
Krishna Institute of Medical Sciences
Krishna Vishwa Vidyapeeth (Deemed to be University)
Karad
Maharashtra
India

Shyam Deshmukh [*]
Department of Information Technology
Pune Institute of Computer Technology
Savitribai Phule Pune University
Pune
India

Prakash M. Durgawale [§]
Department of Community Medicine
Krishna Institute of Medical Sciences, (Deemed To Be University)
Karad
Maharashtra
India

Shrinivas T. Shirkande [‡]
Department of Computer Engineering
S. B. Patil College of Engineering Indapur
Pune
Maharashtra
India

[†] *E-mail:* dhirajmane123@gmail.com
[*] *E-mail:* dshyam100@yahoo.com (Corresponding Author)
[§] *E-mail:* drpdurgawale2007@gmail.com
[‡] *E-mail:* shri.shirkande8@gmail.com

Sarika T. Deokate [@]
Department of Computer Engineering
Pimpri Chinchwad College of Engineering Nigdi
Pune
Maharashtra
India

Nilesh P. Sable [#]
Department of Computer Science & Engineering (Artificial Intelligence)
Bansilal Ramnath Agarwal Charitable Trust's
Vishwakarma Institute of Information Technology
Pune
India

Abstract

Internet of Things (IoT) technology has revolutionized patient monitoring systems by providing real-time health data for better medical care. However, the rise of IoT devices raises privacy concerns about sensitive health data. This study uses Attribute-based Cryptography (ABC) in patient monitoring to address these concerns. The focus is on adapting attribute detail to IoT device features. Conventional encryption methods often struggle to adapt to IoT devices limited resources, which could compromise patient data privacy. This study suggests a tweak to ABC by adjusting the attribute granularity to better fit the limitations of IoT devices. These resource constraints present challenges, but the methodology proposes an innovative approach to handling and analyzing attributes while protecting patient confidentiality. A dynamic attribute granularity(DAG) model that adapts to IoT device capabilities ensures a data privacy-system performance trade-off in the study. The suggested approach optimizes attribute number and complexity to improve privacy-preserving patient monitoring system scalability and performance. The research thoroughly evaluates the modified ABC-DAG systems data privacy, scalability, and energy efficiency. The results show that the system can protect patient data in a healthcare IoT setting while reducing computational load on low-resource devices. The growing field of privacy-preserving healthcare Internet of Things benefits from this research. It addresses IoT attribute granularity challenges with a customized cryptographic method. The results improve ABC theory in healthcare and provide practical advice for secure and efficient IoT patient monitoring systems.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Attribute based cryptography, Internet of Things, Healthcare, Privacy-preserving, Patient monitoring.*

[@] *E-mail:* **sarikajaankar2017@gmail.com**
[#] *E-mail:* **drsablenilesh@gmail.com**

1. Introduction

In modern healthcare, cutting-edge technology and medical sciences have led to new methods. IoT technologies are a major advancement. Healthcare and IoT have created new opportunities for patient-focused, data-based care, especially in remote and ongoing patient monitoring. With the digital transformation of healthcare, IoT devices can collect real-time health data, analyze it, and implement personalized treatment plans. However, digital transformation faces challenges. Privacy and security concerns have arisen as patient monitoring increasingly uses IoT devices. Healthcare data is highly personal and sensitive, so strong mechanisms that enable data sharing and protect patient confidentiality are needed[1], [2].

Healthcare IoT includes wearables, sensors, and medical equipment that are seamlessly integrated into a network for remote patient monitoring. The idea is to use real-time data to enable proactive healthcare interventions, early disease detection, and personalized treatment plans. Wearable devices and sensors can help doctors monitor patients vital signs. This facilitates quick, informed medical decisions. The rise of IoT in healthcare shows a shift toward patient-centered care. Healthcare has traditionally been sporadic, with few opportunities for ongoing observation outside medical facilities. IoT allows real-time patient data collection in healthcare, transcending hospital boundaries. This evolution could improve patient outcomes, preventive care, and resource allocation[3], [4].

Patient monitoring systems are needed to provide healthcare professionals with timely, accurate, and contextually-aware health information. It is crucial for managing long-term illnesses, surgery recovery, and complex patients. Continuous monitoring allows for quick intervention in critical situations and empowers patients to actively participate in their care by providing immediate health feedback. Digitizing healthcare data presents a dilemma balancing the potential benefits with the need to protect privacy. IoT data on vital signs and medication adherence is sensitive. Unauthorized access, data breaches, and improper patient data handling threaten privacy. Privacy is a legal requirement in healthcare and essential to patient confidence and ethical data handling. Patient monitoring systems are needed to provide timely and accurate health data to help doctors make treatment decisions.[5], [6]

Advanced cryptographic solutions are needed to address privacy concerns. Access control and cryptography are combined in attribute-based cryptography (ABC). ABC uses attributes to create access policies

and generate cryptographic keys. ABC in healthcare data privacy links access policies to patient attributes to restrict access to specific health information to authorized entities. Expanding on ABC, we propose Attribute-based Cryptography - Dynamic Attribute Granularity (ABC-DAG) to address IoT device resource constraints. ABC-DAG balances privacy and efficiency by adapting to IoT device features with flexible attribute granularity.

Our contribution

This study introduces the Attribute-based Cryptography - Dynamic Attribute Granularity (ABC-DAG) functionality in healthcare IoT. The system dynamically adjusts attribute granularity to improve scalability, reduce computational overhead, and improve patient monitoring while protecting privacy.

Importance of Research

It addresses growing privacy concerns in healthcare Internet of Things, making this study crucial. The ABC-DAG model improves secure and efficient patient monitoring systems, boosting patient and healthcare professional trust. Successful ABC-DAG implementation can boost patient confidence in healthcare systems. This research aims to reduce privacy risks and secure data in healthcare IoT to set a new standard for privacy-preserving solutions.

2. Literature Review

The incorporation of IoT technologies in healthcare has led to extensive research focused on resolving privacy issues linked to the substantial volumes of sensitive health data produced. This literature review examines recent studies that specifically address privacy-preserving techniques in IoT-based healthcare. It highlights the methods used, their efficacy, and identifies any gaps in the current research that can be addressed by the proposed approach. Y. Yang et al.[7] discuss the issue of privacy in storing large amounts of healthcare data and propose a self-adaptive access control solution. The study highlights the significance of safeguarding patient confidentiality in the age of healthcare based on the IoT. R. Y. Patil [8] presents a novel access control scheme for ensuring the security and privacy of medical-IoT(MIoT) devices. The scheme utilizes attribute-based “signcryption” to facilitate secure data communication in

the context of medical-IoT. K. Seol et al.[9] suggests an attribute-based access control model for electronic health records, highlighting the importance of a detailed access control system to safeguard privacy in healthcare data. J. Sun et al.[10] specifically examines the implementation of detailed access control measures in the cloud-based Industrial-IoT healthcare setting. The main emphasis of the study is on maintaining privacy for both parties involved in order to ensure secure access to data.

J. A. Onesimu et al.[11] presents a novel approach to privacy preservation in IoT-based healthcare services by introducing clustering-based anonymization. E. Yang et al.[12] focuses on the perspective of edge computing and combines anomaly detection with dynamic attribute-based re-encryption to ensure privacy preservation in edge consumer electronics. K. Saranya et al.[13] centers on safeguarding privacy in healthcare transactional data through the utilization of multi-attribute case-based cryptography. The research emphasizes the significance of cryptographic techniques in ensuring the security of transactional information.

Y. Zhang et al.[14] focuses on efficient techniques for securing smart health systems by exploring policy-hiding attribute-based access control. Its main objective is to ensure privacy and security in the exchange of health data. J. A. Onesimu et al.[15] presents a method of anonymizing healthcare data that focuses on attributes, highlighting the significance of safeguarding privacy when sharing healthcare information. K. Azbeg et al.[16] presents a system for managing diseases that utilizes blockchain technology to ensure access control and protect privacy. It emphasizes the ability of blockchain to enhance the security of healthcare data.

The literature review uncovers a diverse array of studies that examine privacy issues in IoT-based healthcare. Every study provides valuable insights into various aspects of privacy preservation, ranging from access control to anonymization and the incorporation of emerging technologies such as blockchain. Nevertheless, the identified research gap emphasizes the necessity for a comprehensive solution that can flexibly adjust to the limitations of IoT devices. The proposed ABC-DAG method aims to address this gap by offering a comprehensive approach to safeguarding privacy in the ever-changing healthcare IoT environment.

3. Architecture for ABC-DAG for Privacy-preserving Patient Monitoring

The Figure-1 and 2 depicted architecture proposed secure approach to implementing ABC-DAG for safeguarding patient privacy in healthcare

IoT. The system employs various security measures to safeguard patient data, such as Attribute-Based Encryption (ABE), authentication, authorization, encryption, and key management. The system is additionally capable of being expanded and adapted to accommodate growth. The system allows for seamless integration of additional medical devices and authorized users, while maintaining robust security measures. The system comprises five primary components:

- Trusted Authority (TA): The TA is tasked with the generation and dissemination of both the master public key and master secret key. The TA is tasked with generating private keys for users, taking into account their specific attributes.
- Medical IoT Devices: Medical IoT devices are designed to gather patient data, including heart rate, blood pressure, and other vitals. Prior to transmission to the cloud server, the data undergoes encryption using ABC-DAG.
- Base Station: The base station functions as an intermediary between the medical IoT devices and the cloud server. The base station additionally carries out the process of encrypting and decrypting data.
- Access Control: The access control component is tasked with authenticating the credentials of users seeking access to patient data. The access control component additionally furnishes users with the corresponding private keys.

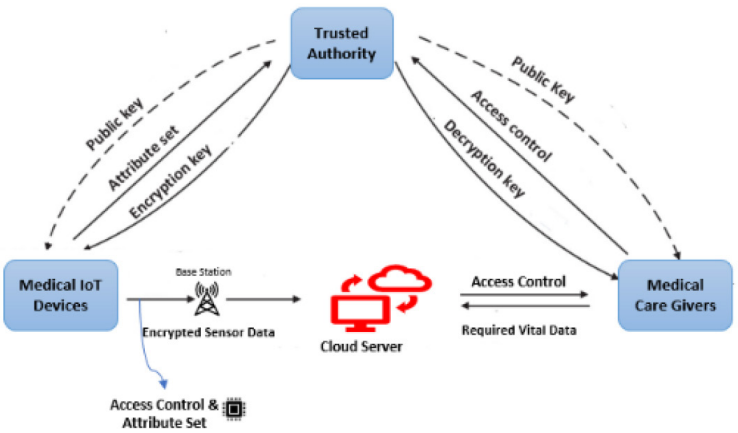

Figure 1

Proposed architecture

- Cloud Server: The cloud server is tasked with the storage and processing of encrypted patient data. The server additionally conducts data analysis to derive valuable insights regarding the patient's health.

The utilization of ABC-DAG in the system

Upon collection of patient data by a medical IoT device, the data undergoes encryption using ABC-DAG prior to transmission to the base station. Subsequently, the base station employs an alternative set of attributes to re-encrypt the data. This guarantees that the data is safeguarded from unauthorized access at all times.

Prior to gaining access to patient data, an authorized user, such as a doctor/ care giver, is required to authenticate themselves by presenting their credentials to the access control component. The access control component authenticates the user's credentials and subsequently grants them the necessary private keys for decrypting the data. The user can employ the private keys to decipher the data and gain entry to the patient's medical records. Advantages of Utilizing ABC-DAG

ABC-DAG offers numerous advantages for ensuring privacy in patient monitoring within the Healthcare IoT:

- Fine-grained access control: ABC-DAG enables precise control over access to encrypted data. Individuals with proper authorization are able to retrieve the necessary patient information.

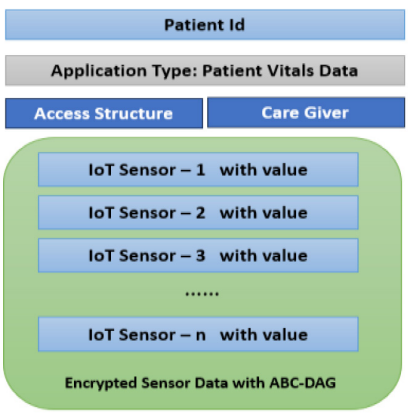

Figure 2

Structure of data transmission

- Dynamic attribute granularity: ABC-DAG enables the use of dynamic attribute granularity. This implies that the characteristics employed to encode and decode data can be modified in the course of time. In the healthcare IoT context, it is valuable to consider that the attributes utilized for granting access to patient data may vary based on the patient's condition and the authorized users.
- Privacy preservation: ABC-DAG safeguards patient privacy through data encryption prior to transmission to the cloud server. This guarantees that individuals without authorization are unable to access the data.

ABC-DAG is a highly promising technology for safeguarding patient data within the healthcare IoT framework. ABC-DAG offers precise access control over encrypted data, allowing for dynamic attribute granularity. ABC-DAG is a valuable tool for safeguarding patient data while still enabling authorized users to access the necessary information. Eq.1 and 2 represent the ABC-DAG

$$E(M,P) = M.H(A_1).H(A_2).....H(A_n) \tag{1}$$

$$D(E(M,P),K) = \frac{M}{H(S_1).H(S_2)...H(S_m)} \tag{2}$$

$E(M,P)$ and $D(E(M,P),K)$ = "encryption and decryption process resp.", M = "message (IoT device data) to be encrypted", P = "policy associated with encryption data", (A_1), (A_2) … (A_n) = "attributes defining the access control structure", $H(A)$ = "hash function applied to the attribute A", K= "private key derived from a subset of attributes S that satisfy the policy P", (S_1), (S_2) … (S_n)= "attributed associated with the private key K".

4. Experimental Setup

We created and tested a privacy-protecting patient monitoring system. The ABC-DAG method uses Attribute-based Cryptography and dynamic attribute granularity to build this system. The system had wearable devices, biosensors, and ambient environmental sensors in a simulated healthcare IoT environment. These IoT devices were strategically placed to monitor vital signs, activity levels, and environmental conditions that affect patient health. The system architecture used secure cloud servers for data storage and processing. Cryptographic operations were

computationally feasible on the servers. The privacy-preserving mechanism in our experiment relied on key generation. ABC linked access policies to patient attributes and dynamically adjusted attribute granularity to accommodate IoT devices. Key generation was secure, ensuring that cryptographic keys were based on user and IoT device attributes. This process strictly controlled access to sensitive healthcare data, allowing only authorized entities with the necessary credentials.

The experiment included patient identifiers, medical conditions, and device-specific characteristics to simulate real-life situations. Patient data was encrypted using generated keys between IoT devices and cloud servers to ensure confidentiality. Multiple attributes were used to measure the system'' performance, including communication time and cost. The proposed ABC-DAG model was tested for efficiency and larger scales. This experiment proved our privacy-protecting patient monitoring system works and showed how well it works with limited IoT device resources. The ABC-DAG model was tested in a simulated healthcare environment with real healthcare scenarios, proving its suitability for healthcare IoT infrastructures.

5. Experiment Evaluation

Here examined communication time and cost for different attributes when evaluating our privacy-protecting patient monitoring system. The system was tested against ABC and Homomorphic Encryption. The proposed system consistently outperformed Traditional ABC and Homomorphic Encryption in time as shown in Figure 3. The proposed system took 8 milliseconds with 10 attributes. Traditional ABC and Homomorphic Encryption took 14 and 8 milliseconds, respectively. Our computationally fast method became more efficient as attributes increased.

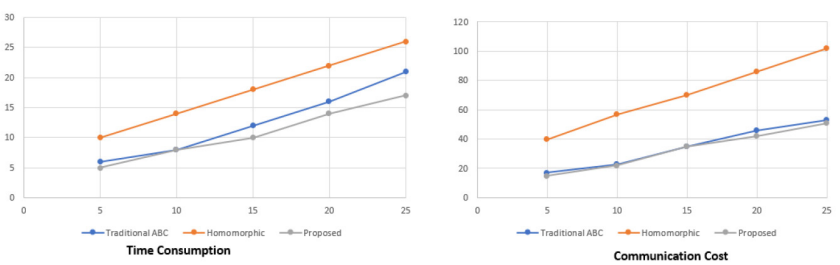

Figure 3

Time consumption and communication cost

Communication costs also showed similar patterns. The proposed system outperformed Traditional ABC and Homomorphic Encryption in communication cost. The 10-attribute system had a 22-communication cost. Traditional ABC cost 23 and Homomorphic Encryption 57. The trend continued as attributes increased, showing that the proposed system reduces data transmission resources. Proposed method optimizes time consumption and communication costs, which are crucial for the practical deployment of privacy-preserving patient monitoring systems in healthcare IoT environments.

6. Conclusion and Future Scope

Presented research has successfully tackled the issues of maintaining privacy in healthcare IoT by developing an innovative patient monitoring system that prioritizes privacy preservation. The ABC-DAG method, which incorporates Attribute-based Cryptography with dynamic attribute granularity, exhibits superior performance in terms of time consumption and communication costs compared to Traditional ABC and Homomorphic Encryption. It demonstrates adaptability to the specific constraints of IoT devices. The proposed system in our study achieves a balanced and effective approach by dynamically adjusting the level of detail in attributes. This ensures the privacy of patient data while also improving operational efficiency. As a result, our system provides a strong solution for protecting patient privacy in the changing field of healthcare IoT. As we consider the future, there are promising opportunities to further investigate and improve our proposed approach. Future research should focus on investigating the scalability of the ABC-DAG model, evaluating its performance with larger and more varied datasets. Furthermore, it is worth considering the incorporation of sophisticated machine learning methods for identifying abnormalities and dynamically adjusting the level of detail in attributes. Continuous innovation is required in the ever-changing field of healthcare technologies.

References

[1] S. M. Bhaskaran and R. Sridhar, "Hybrid solution for privacy-preserving access control for healthcare data," *Adv. Electr. Comput. Eng.*, vol. 17, no. 2, pp. 31–38 (2017), doi: 10.4316/AECE.2017.02005.

[2] C. Huang, K. Yan, S. Wei, and D. H. Lee, "A privacy-preserving data sharing solution for mobile healthcare," Proc. 2017 Int. Conf. Prog.

Informatics Comput. PIC 2017, pp. 260–265 (2017), doi: 10.1109/PIC.2017.8359554.

[3] M. Nasr Esfahani, B. Shahgholi Ghahfarokhi, and S. Etemadi Borujeni, "End-to-end privacy preserving scheme for IoT-based healthcare systems," *Wirel. Networks*, vol. 27, no. 6, pp. 4009–4037 (2021), doi: 10.1007/s11276-021-02652-9.

[4] M. Mandal, "Privacy-preserving fully anonymous ciphertext policy attribute-based broadcast encryption with constant-size secret keys and fast decryption," *J. Inf. Secur. Appl.*, vol. 55, p. 102666 (2020), doi: https://doi.org/10.1016/j.jisa.2020.102666.

[5] Y. Rahulamathavan, R. C. W. Phan, M. Rajarajan, S. Misra, and A. Kondoz, "Privacy-preserving blockchain based IoT ecosystem using attribute-based encryption," 11th IEEE Int. Conf. Adv. Networks Telecommun. Syst. ANTS 2017, pp. 1–6 (2018), doi: 10.1109/ANTS.2017.8384164.

[6] Sharma, Sandeep Kumar, Kumar, Anil, Ashtagi, Rashmi & Jain, Rekha. OCA: An intelligent model for improving security breach of biometric based authentication systems, *Journal of Discrete Mathematical Sciences and Cryptography,* 26:5, 1415–1425 (2023), DOI: 10.47974/JDMSC-1765.

[7] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Inf. Sci. (Ny).*, vol. 479, pp. 567–592 (2019), doi: 10.1016/j.ins.2018.02.005.

[8] R. Y. Patil, "A secure privacy preserving and access control scheme for medical internet of things (MIoT) using attribute-based signcryption," *Int. J. Inf. Technol.* (2023), doi: 10.1007/s41870-023-01569-0.

[9] S. K. Sharma, A. Chaurasia, V. S. Sharma, C. L. Chowdhary and S. Basheer, "GEMM, a Genetic Engineering-Based Mutual Model for Resource Allocation of Grid Computing," in *IEEE Access*, vol. 11, pp. 128537-128548 (2023), doi: 10.1109/ACCESS.2023.3333278.

[10] J. Sun, Y. Yuan, M. J. Tang, X. Cheng, X. Nie, and M. U. Aftab, "Privacy-Preserving Bilateral Fine-Grained Access Control for Cloud-Enabled Industrial IoT Healthcare," *IEEE Trans. Ind. Informatics*, vol. 18, no. 9, pp. 6483–6493 (2022), doi: 10.1109/TII.2021.3133345.

[11] J. A. Onesimu, J. Karthikeyan, and Y. Sei, "An efficient clustering-based anonymization scheme for privacy-preserving data collection

in IoT based healthcare services," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 3, pp. 1629–1649 (2021), doi: 10.1007/s12083-021-01077-7.

[12] E. Yang *et al.,* "Privacy preservation in edge consumer electronics by combining anomaly detection with dynamic attribute-based re-encryption," *Mathematics*, vol. 8, no. 11, pp. 1–13 (2020), doi: 10.3390/math8111871.

[13] K. Saranya and K. Premalatha, "Multi Attribute Case Based Privacy-preserving for Healthcare Transactional Data Using Cryptography," *Intell. Autom. Soft Comput.*, vol. 35, no. 2, pp. 2029–2042 (2023), doi: 10.32604/iasc.2023.027949.

[14] Y. Zhang, D. Zheng, and R. H. Deng, "Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2130–2145 (2018), doi: 10.1109/JIOT.2018.2825289.

[15] J. A. Onesimu, J. Karthikeyan, J. Eunice, M. Pomplun, and H. Dang, "Privacy Preserving Attribute-Focused Anonymization Scheme for Healthcare Data Publishing," *IEEE Access*, vol. 10, no. July, pp. 86979–86997 (2022), doi: 10.1109/ACCESS.2022.3199433.

[16] K. Azbeg, O. Ouchetto, and S. Jai Andaloussi, "Access Control and Privacy-Preserving Blockchain-Based System for Diseases Management," *IEEE Trans. Comput. Soc. Syst.*, vol. 10, no. 4, pp. 1515–1527 (2023), doi: 10.1109/TCSS.2022.3186945.