A Secure Anonymous Authentication Protocol for IoT Based Health-care System using Wireless Body Area Network

Shanthapriya R (shanthaarona@gmail.com)  
Sri Sivasubramaniya Nadar College of Engineering  https://orcid.org/0000-0002-8700-6418

Vaithianathan V  
Sri Sivasubramaniya Nadar College of Engineering

Research Article

Keywords: IoT, security, health-care system, hash-key authentication, WBAN, SAAPAES algorithm

DOI: https://doi.org/10.21203/rs.3.rs-730538/v1

License: ☑️ This work is licensed under a Creative Commons Attribution 4.0 International License.  
Read Full License
A Secure Anonymous Authentication Protocol for IoT Based Health-care System using Wireless Body Area Network

Shanthapriya.R¹
shanthaarona@gmail.com
ECE Department
Sri Sivasubramaniya Nadar College of Engineering
Kalavakkam-603110
Tamilnadu, India.

V. Vaithianathan²
vaithianathany@ssn.edu.in
ECE Department,
Sri Sivasubramaniya Nadar College of Engineering
Kalavakkam-603110
Tamilnadu, India.

Corresponding author:
Name: Shanthapriya.R
Mail id: shanthaarona@gmail.com
Mobile no: 9080216600
Abstract:
The current technology in healthcare and its information are enhanced with IoT system. In most of IoT system, there exists a gateway between a wireless body area network (WBAN) and the internet to upload and retrieve the health information. These IoT gateways normally transmit data to a cloud. Therefore, the importance of IoT devices and health care data could be critical. Hence security constraints are required to retain the data. This paper introduces a novel concept called a secure anonymous authentication protocol with advanced encryption standard (SAAPAES) a cryptographic scheme to guarantee the security services and to protect confidential client data in the healthcare system.

Our SAAPAES protocol offer the following aspects
1. Anonymous authentication, this is one of the easy and efficient way to protect patient/doctor identities from the server on cloud storage by using hash key authentication algorithm by disclosing the security aspects like password and username.
2. Patient’s health information is encrypted with SAAPAES and then uploading these data in cloud. Finally, downloading the health information from personal data assistant (PDA) in decrypted form using SAAPAES. The proposed authentication approach provides an efficient authentication mechanism with high security in the health-care system.

Keywords: IoT, security, health-care system, hash-key authentication, WBAN, SAAPAES algorithm.

1. Introduction

In recent past, the field of telemedicine has gained high thrust due to the requirement in various medical experts worldwide, which demanded interaction between the experts through virtual meet like video conferencing. But, when it comes for an expert to know the medical background of a patient who is less informed on the technical background of his physical disorders, it has become a prominent feature to maintain a database of the patient that could be accessed by such appropriate physician to know the patient’s problem (Anzanpour et al. 2008)

In such event, cloud-based healthcare system helps in storing the confidential data of patients and their health condition. But unfortunately, security and privacy of such data stored has become the main concern (Challa et al. 2007; Li et al. 2014). To maintain the security of healthcare data, both cloud service providers and healthcare organizations should take unavoidable measures to secure safe handling of patient’s data mainly from the target of unethical attackers. Therefore, high-security measure and assurance must be required in cloud-based healthcare systems (Zanjal et al. 2016). (Farahani et al. 2014) has pictured that the organizations must make sure that the sensitive health report is stored on cloud in a more secure and encrypted way, such that, they do not have the control over the security of the data access devices, being used to transmit the data or else it may create a substantial risk with growth of network size with new network devices.

Governments’ policies should be in place to ensure that the cloud service providers should comply with all necessary means to secure patients’ data privacy. If such requirements are met by the cloud service providers, there is an opportunity for efficient
management of data with proper security. The first in row to mainly fear over the data is the patient, whose information is stored in the cloud, must have control over his health records. The patient should be privileged for granting access to persons only who possess the corresponding key.

(Yang et al. (2017); Alzahrani et al. (2020)) depicted the mode of encryption and decryption for secured transmission of data in IoT ecosystem. The importance of such encryption and decryption of data must be accompanied with key to access the information in cloud in order to avoid the unauthorized users from getting access (Abdmeziem et al. 2015). Based on the encryption type (symmetric or asymmetric) a provider chooses the key (public and private) for the encryption process which must authenticate himself or herself (Mohammad et al. (2018); Ashish et al. (2019)). The authorization method normally involves in giving the user login credential; based on the information provided to the cloud server during the authorization, the patient is linked or tracked using their access history or preferences (Tang et al. 2018; Sun et al 2017).

In current times, various IoT based privacy-preserving authentication techniques have been proposed for secure data transmission which was elaborated in (Abdmeziem et al. 2018; Song et al. 2013). The work demonstrated the benefits of symmetric cryptography which has fast processing time than asymmetric cryptography. A precise work (Gong et al. 2015) has specifically noted that the system is scalable and secure sharing of personal healthcare data of patients using symmetric encryption (Xu et al. 2017; Li et al. 2016; Lounis et al. 2013; Lounis et al. 2016) have explained cloud-based healthcare encryption protocol, where a homomorphic encryption algorithm was used to secure the data stored in the cloud from an unauthorized access. Following the progressive idea of encryption in cloud-based system has found application for various domains. (Li et al. 2012; Bezawada et al. 2015; Miao et al. 2016; Li et al. 2011; Huang et al. 2018; Chhajed et al. 2015; Shi et al. 2019; Hussain et al. 2021; Chatterjee et al. 2020) has exposed the encryption of health information collected from the patients through wireless body area network (WBAN) before transmission.

But, on considering the works demonstrated by researchers pointed above, irrespective of type of cryptography employed which may be symmetric (AES) or asymmetric (Elliptic Curve Cryptography, ECC) (Sowjanya et al. 2020), Rivest–Shamir–Adleman (RSA) none of these schemes provide ‘complete anonymity’. But our research aims to allow patients to use healthcare services without revealing their identities which helps to avoid tracking by an eavesdropper.

In this regard, on considering the privacy of the patient data, a secure anonymous authentication protocol with advanced encryption standard (SAAPAES), is proposed. The SAAPAES based healthcare system not only provides its patients with the highest security compare to the other encryption/decryption algorithms do but also minimize the encryption and decryption time on its terminal devices. The SAAPAES also provides high potency so that the doctors can easily access the past or current medical records for emergent patients everywhere through networks. We are also clear that, the symmetric cryptography proposed in our work would help in fast rate of encryption and decryption.

2. Proposed methodology

This section provides the information on the architecture of proposed model, flow of healthcare
information accounting the authentication and registration are discussed.

The proposed system provides a platform where the patient’s personal health information is stored in a cloud which can be accessed by any authenticated doctor to know the medical background of patient who appears before him. This handles the medical history of each individual and provide access to all registered hospitals to read or update the data for future use by any other registered doctor. The hospital which accesses the database must be registered and might have got a license which is noted as a ‘unique database accessing code’. The patients’ details are stored in the database, and an identification number will be generated during this process. Whenever they go for any treatment, their medical data will be stored into the database using their identification number without the requirement of any personal proof or exposing the personal details of them.

It must also be noted that, for security reasons, any person who wants to view their data will be allowed only to read the data by giving access over their stored personal data. This will help the patient to overlook or check their personal information are not exaggerated or misinterpreted. But, on the same line any updates (write data) can be done only by the doctor who has proper technical knowledge over health care preventing layman to change the technical meaning of any data.

The Figure 1a and Figure 1b shows the proposed architecture and the flow diagram of SAAPAES which contains the following blocks namely,

1. Anonymous authentication
2. Data encryption using SAAPAES
3. Data decryption using SAAPAES

Initially, when the patient’s details are collected from the WBAN sensor nodes, they are stored in a Personal Data Assistant (PDA). Prior to this, the doctors and patients will get registered by hash key algorithm. The patients’ general information profile can be seen only by doctors who are having the Patient Identification number or shortly ID. The
patients may consult many doctors by sharing the uploaded cloud data to them. In general, the patient data contains details of various diseases. In our proposed work, two authentication key plays a major role for securing the healthcare data.

From fig.1b, first block explains medical data collection of patients, data management, which includes data pre-processing and analysis, which are later stored in PDA. Second and third block is where the encryption of the healthcare data from PDA is cipher texted by applying the proposed novel SAAPAES algorithm for secured storage in the IoT ecosystem. The authentication block is associated with the key generation process. When PDA make a data request on databases, it forwards a request to the authentication page. The key generation process starts with LOGIN page when AS (Authentication Server) receives a username and password. This process will check the details in IP (Identification provider) and send the acceptance message. The fourth block, which is almost same as the second module, but decryption is done here. Data sources decrypted by authenticated persons using SAAPAES approach are send to PDA. Finally, medical information and reports about the patients will be sent to clients or patients thereby completing the process of request and read/write data.

For better understanding of the generalized function of various blocks in the proposed architecture, they are briefed as follows with typical applications of them.

2.1 Data collection

In Wireless Body Area Network (WBAN) particularly when employed in health care system, patient’s data are collected using sensor nodes and send it to the administrator/PDA. WBAN involves tiny wireless sensors that are embedded inside or surface-mounted on the body of a patient in which sensors continuously monitor the vital physiological parameters from the patients. Collected personal health data are aggregated and transmitted to PDA via a wireless interface, such as Bluetooth or WLAN. Information gathered from patients is highly confidential and should be shielded from the hacker, or any third party may abuse the patient’s information and use for illicit purposes.

2.2 Data in PDA (Personal data assistant)

PDA in the framework oversees patient details digitally and allocates access mechanism to different authorities. These PDA data can be updated and processed after cloud storage whenever and wherever necessary and become promptly available to the specified specialists and clients.

2.3 Anonymous authentication

As data should be kept secret and confidential from adversaries, it is necessary that every user in the health care system must be authenticated. This helps the administrator confirm the identity and access of the patient’s records to the doctor instantly. Here the users can register with personal details for authentication so that the users can upload or view the medical records. The main idea of user authentication is to find matching information between user and server. Among these factors’ password authentication is the simple and best approach in network applications due to its low costs and easy implementation.

Hash-based message authentication code (HMAC) is employed to aggregate the key from cryptography with hash function. The HMAC offer the private key for both the client and server distinctively. This can be used to verify the integrity and authenticity of a
message. It is more secure than existing MAC, because the message and key are hashed in distinct steps

\[
HMAC(key, msg) = H(mod1(key) \parallel H(mod2(key) \parallel msg))
\] (1)

2.4 Patient/doctor Registration

Patient/doctors has a completely unique account. Hence, every member like patient and doctors must sign in to begin the registration process before getting access to cloud system. An account is created by the doctor/patient with unique username and password during registration process. Then she/he can get admission to the cloud from anywhere via login credentials and additionally upload/download documents through document upload and a download module.

The following steps must be followed by the user to register in the hospital registration center:

Table 1: Notations and description:

| Notations | Description |
|-----------|-------------|
| U         | User        |
| S         | Service provider |
| ID        | Unique ID  |
| PW        | Password    |
| b         | Random number |
| Ts        | Timestamp   |
| \(\oplus\) | Bitwise XOR operation |
| \(\parallel\) | Concatenation |
| \(h(.)\)  | Hash function |

1. The user U approach the service provider S during registration process with unique user ID and password PW.

2. Then U picks a random number \(b\) and submit the registration message \((ID, h(PW), b)\) to the S through a secure channel.

3. Once registration message received by S from U, S generates timestamp \(T_s\) and uses \(ID \& h(PW)\) to compute 3 secret values \(P, Q\) and \(V\).

\[
P = h(y) \oplus (ID \parallel T_s)
\] (2)

\[
Q = h(y \parallel T_s) \oplus h(h(PW) \oplus b)
\] (3)

\[
V = h(ID \parallel h(y \parallel T_s) \oplus b)
\] (4)

S issues access card (AC) with \(P, Q, V\) & \(h(.)\) parameters to U through a secure channel.

4. Then U incorporates \(b\) into it

\[
\{P, Q, V, h(.), b\}
\]

2.4a Login

If user U wants to login. The user must enter unique user \(ID\) and \(PW\). Then the system performs the following steps:

1. By using random number \(b, PW\) & \(Q\) to compute a value \(h(y \parallel T_s)'\) and calculate \(V'\).

\[
h(y \parallel T_s)' = Q \oplus h(h(PW) \oplus b)
\] (5)

\[
V' = h(ID \parallel h(y \parallel T_s)' \oplus b)
\] (6)

Check \(V' = V\)

If equation (7) satisfies, the system generates a \(T_u\) and computes messages \((C_1, SK, C_2)\) or else the login request gets discarded.

\[
C_1 = Q \oplus h(h(PW) \oplus b) \oplus T_u
\] (8)

\[
SK = h(h(y \parallel T_s) \parallel T_u)
\] (9)

\[
C_2 = h(h(ID) \parallel T_u \parallel SK)
\] (10)
2. System sends login request messages \((P, C_1, C_2)\) to S

### 2.4b Authentication

After receiving the login request \((C_1, SK, C_2)\), S performs the following steps to authenticate U:

1. S uses the received value \(P\) and its secret key \(y\) to obtain \(ID'\) and \(T_S'\).
   
   \[
P \oplus h(y) = (ID' \parallel T_S')
   \]
   
   To check the authentication message \(C_2\) is valid or not, S computes \(T_u'\) and \(SK'\).
   
   \[
   T_u' = C_1 \oplus h(y \parallel T_S')
   \]
   
   \[
   SK' = h(h(y \parallel T_S') \parallel T_u')
   \]
   
   \[
h(h(ID' \parallel T_u' \parallel SK')) \equiv C_2
   \]

   If equation (14) satisfies, S confirms that U is a legal user and responds with a message \(C_3\) to U:
   
   \[
   C_3 = h(ID' \parallel T_u' \parallel SK')
   \]

   If the equation (16) verifies, U confirms S is valid then U and S can use the same session key (SK) to securely communicate to each other.

### 2.4c Password change

1. The user log in to the system using user ID and password.

2. The access card validates and examines the ID&PW and verifies \(V' \equiv V\). If it holds, user U is allowed to create a new password and calculates \(Q'\).

\[
Q' = Q \oplus h(PW) \oplus h(PW_{nw}) = h(y \parallel T_v) \oplus h(PW_{nw})
\]

### 2.5 Cloud storage

Cloud users should register their details to get permission to access the cloud data. Data owner accepts the request from users, then shares the data private key. Data users get key from the owner to access the cloud data. Then, the users can log in using their credentials and upload a file after encryption. And later she/he can download the file using the identical key. When uploading the file, the content will be encrypted using SAAPAES encryption before saved into the database. 128-bit SAAPAES encryption is used to provide security to the user uploaded data. SAAPAES is a fast-symmetric encryption algorithm.

### 3. Experimental results

The above analytically demonstrated work was implemented in Cooja toolkit, and security is implemented using homomorphic encryption as shown in figure 2. The data was imported from the SQL database, and the security was implemented over that data.

![Image](image.png)

**Figure 2**: IoT simulation result

#### 3.1 Patient/Doctor login page
The initial authentication is performed through the user credentials that are verified over the stored database provided the user has already registered to create username and password. The login page has the following three attributes as username, password, and user type for login. If not registered the page will be redirected to registration page.

### 3.2 Patient or Doctor Registration Form

Patient or doctors are given with unique credential for logging in. After completing the registration process, either patient or doctor can access the system to upload/view medical data.

### 3.3 Encrypting the data using SAAPAES

Authorization is the process of confirming a user's privilege to access a given platform. A unique file ID is generated to upload a file in the cloud environment. Authorized user can use this ID for downloading and editing their uploaded data. After uploading a medical file, these details are encrypted by using SAAPAES encryption algorithm. The key size employed for encrypting the plain text is 128 bits. Figure 3 shows that, the encryption of the patient data in user end and stored encrypted data in IoT Server.

### 3.4 Decrypting the data using SAAPAES

The cipher texts will be retrieved from the cloud and decrypted to get the original plaintext. The decryption is done with the help of a private key which is made available to the doctors and other users who need the healthcare data. The key is generated from the SAAPAES algorithm which is also used for decrypting the text files. Figure 4 shows that decrypted user data stored in IoT server with hash authentication key for security.

| Hash Key | Encrypted Data |
|----------|----------------|
| 79175468470975123845 | Encrypted Patient Details |
| Patient Name: John Doe |
| Patient ID: 1234 |
| Sex: Male |
| Date of Birth: 01/01/1980 |
| Blood Pressure: 120/80 |
| Glucose: 100 |

**Figure 3: Encrypted data**

| Hash Key | Decrypted Data |
|----------|----------------|
| 79175468470975123845 | Decrypted Patient Details |
| Patient Name: John Doe |
| Patient ID: 1234 |
| Sex: Male |
| Date of Birth: 01/01/1980 |
| Blood Pressure: 120/80 |
| Glucose: 100 |

**Figure 4: Decrypted data**

### 4. Security Analysis

#### 4.1 Replay attack

In our scheme, a timestamp mechanism is employed to avoid the replay attack. If an intruder try to replay the preceding messages \((P, C_1, C_2)\) to obtain authentication, the intruder fails to do the task because timestamp \(T_u\) is different for each session. As result the attacker will be unable to authenticate using earlier messages.

#### 4.2 User impersonation attack

During registration process, server S generates a timestamp \(T_s\) to calculate parameter P using user’s ID and secret key y, where \(T_s\) is unique for each user. As...
a result, the attacker attempting to guess $y$ with an unknown $T_s$ is not possible. Hence user impersonation attack is not possible in our proposed scheme.

4.3 Eavesdropping attack

An attacker mostly target the unsecure connection in eavesdropping attack. In our proposed system all the patients information are encrypted by AES. AES is one of the best encryption protocol thereby eavesdropping attack can be prevented in our proposed approach.

4.4 Man-in-middle attack

The attacker establishes an independent connection between a valid sender and receiver without the knowledge of true sender and receiver is known as a man-in-the-middle attack. In our proposed system the use of HMAC provides authentication to validate the genuine user and AES is used for encryption thereby the system is secure from attackers.

4.5 Password guessing attack

An attacker A obtains the U’s access card and intercepts prior messages in this scenario. A must have the secret key $x$ and the Timestamp $T_s$ to compute identical parameters for comparison with parameter $Q$ in order to infer $U$’s $PW$ from the access card stored parameter $Q$. A, on the other hand, can utilise $Q$ and the captured $P$ to compute identical messages $(P, C_1', C_2')$ and send them to S in order to predict $U$’s $PW$. It's tough to perform this password guessing assault since A has two unknown variables, $ID$ and $PW$.

5. Performance evaluation

SAAPAES is a suitable method, as it consumes less energy when compared to other existing algorithm which is realized through the simulations done using Cooja toolkit. Here the data is encrypted and decrypted using SAAPAES with 128bits key.

The simulation results helped us to compare SAAPAES with DES, BLOWFISH and AES algorithm in terms of computation time, network lifetime, scalability, latency, security and encryption & decryption time. The computation time is the time taken for computing and verifying the keys in the cloud environment. The proposed SAAPAES algorithm attains the computation time of 117ms. The time attained by the proposed technique is found to be lesser than the existing DES, BLOWFISH and AES with time of 135ms, 128ms and 121.6ms. The comparison between the proposed SAAPAES and existing algorithm is given in figure 5(a). The network lifetime (NL) is another important measure of performance in the proposed security model. The NL is the aggregated active time that the node can sustain during the effective data transmission. In the proposed SAAPAES technique, the network lifetime is about 195.71s and it is better than the existing algorithms with the network lifetime of 150s, 155s and 168.75s. The comparison on existing algorithm and SAAPAES over network lifetime is given in figure 5(b). Latency is the measure of delay that occurs during the data transmission in the cloud. The existing approaches has the latency of about 0.622ms, 0.56ms and 0.5ms, however the proposed SAAPAES approach attained the latency of 0.494ms. The comparison over the latency performance for both SAAPAES and existing algorithms is given in figure 5(c). Scalability is the measure of ability of the cloud to handle the resources that are stored in it. The proposed SAAPAES has the scalability of 0.896 which is higher than that of the existing approaches with the scalability of 0.59ms, 0.89ms and 0.731ms. The comparison over the
scalability for the proposed SAAPAES and existing algorithm is given in figure 5(d). The security, encryption and decryption time are the most important aspect of any security algorithm. Encryption time and decryption time of SAAPAES is 38ms and 77ms is less than the existing algorithms encryption and decryption time of 52ms & 85ms, 43ms & 82ms, and 39ms & 78ms is given in figure 5(e). The proposed SAAPAES algorithm provides the security of about 97% and is higher than the existing algorithms with security of 87%, 82% and 95% is given in figure 5(f). The table 1 given below gives the comparative performance analysis between SAAPAES and other existing techniques.

Figure 5a: Computation time  
Figure 5b: Network lifetime

Figure 5c: Latency  
Figure 5d: Scalability
### Table 2: Performance validation of SAAPAES and with existing algorithm

| Sl. | Parameters            | DES  | BLOWFISH | AES    | SAAPAES |
|-----|-----------------------|------|----------|--------|---------|
| 1.  | Computation time      | 135ms| 128ms    | 121.6ms| 117ms   |
| 2.  | Network lifetime      | 150s | 155s     | 168.75s| 195.71s |
| 3.  | Latency               | 0.622ms| 0.56ms | 0.5ms  | 0.463ms |
| 4.  | Scalability           | 0.59ms| 0.89ms  | 0.731ms| 0.92ms  |
| 5.  | Security              | 87%  | 82%      | 95%    | 97%     |
| 6.  | Encryption time       | 52ms | 43ms     | 39.0ms | 38.0ms  |
| 7.  | Decryption time       | 85ms | 82ms     | 78.0ms | 77.0ms  |

### 5. Conclusion

Healthcare industries want revolutionary and cost-effective technique to help healthcare companies in locating extra effective strategies to deal with the numbers of patient’s data. Apart from urban area, this IoT based health care solution would surely benefit the rural population with cost effective approach avoiding them to travel miles to meet a physician. But such platform must gain the trust of people where such trust is directly proportional to the security or privacy provided to their data. This has always motivated researchers to go for different cryptographic techniques which can delight the user’s (Jian et al. 2018; Fushan 2018). In such run, this paper has demonstrated the encryption of message and authentication with a unique identification number to individual user/person without exposing any other identity of them. Thereby we successfully developed an anonymous authentication encryption technique and increased its performance by various measures.

On the performance side, the 128-bit SAAPAES encryption approach has advanced and strengthened the security of records to its highest-degree secrecy with minimum energy consumption comparatively which was justified using simulations.
Conflict of Interest

The authors declare that there is no conflict of interest.

References

1. Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. “Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach” in Future Generation Computer Systems, pp. 641-658, 2018.

2. Challa, S. Das, A. K., Odelu, V., Kumar, N., Kumari, S., Khan, M. K., & Vasilakos, A. V. “An efficient ECC-based provably secure three-factor user authentication and key agreement protocol for wireless healthcare sensor networks” in Computers & Electrical Engineering journal, 2017.

3. M. Li, W. Lou and K. Ren, "Data security and privacy in wireless body area networks," in IEEE Wireless Communications, vol. 17, no. 1, pp. 51-58, February 2010.

4. Zanjal, S. V., & Talmale, G. R. “Medicine reminder and monitoring system for secure health using IoT”. Proc in Computer Science journal, pp. 471- 476, 2016.

5. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., & Mankodiya, K. “Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare” in Future Generation Computer Systems, pp.659-676, 2018.

6. Yang, Y., Zheng, X., & Tang, C. “Lightweight distributed secure data management system for health Internet of Things” in Journal of Network and Computer Applications, pp.26-37, 2017.

7. Alzahrani, B.A., Irshad, A., Albeshri, A. et al. A Provably Secure and Lightweight Patient-Healthcare Authentication Protocol in Wireless Body Area Networks. Wireless Pers Commun (2020).

8. Abdmeziem, M. R., & Tandjaoui, D. “An end-to-end secure key management protocol for eHealth applications” in Computers & Electrical Engineering journal, pp.184-197, 2015.

9. Mohammad Ubaidullah Bokhari, Qahtan Makki Shallal and Yahya Kord Tamandani, “Reducing the Required Time and Power for Data Encryption and Decryption Using K-NN Machine Learning” in IETE Journal of Research, Jan 2018.

10. Ashish Joshi & Amar Kumar Mohapatra, Authentication protocols for wireless body area network with key management approach, Journal of Discrete Mathematical Sciences and Cryptography, 22:2, 219-240, 2019.

11. J. Tang, A. Liu, M. Zhao, and T. Wang, "An aggregate signature-based trust routing for data gathering in sensor networks," in Security and Communication Networks, vol. Article ID 6328504, pp 1-30, 2018.

12. W. Sun, Z. Cai, F. Liu et al., “A survey of data mining technology on electronic medical records,” in Proceedings of the International Conference on E-Health Networking Application and Services, pp. 1–6, 2017.

13. M. R. Abdmeziem and D. Tandjaoui, “A cooperative end to end key management scheme for e-health applications in the context of internet of things,” in Ad-hoc Networks and Wireless, Springer, Berlin Heidelberg, pp. 35–46,2014.

14. Song, X. Lin, X. Shen et al., “Kernel regression based encrypted images compression for e-healthcare systems,” in Proceedings of the International Conference on Wireless Communications and Signal Processing, pp. 1–6, 2013.
15. T. Gong, H. Huang, P. Li, K. Zhang, and H. Jiang, “A Medical Healthcare System for Privacy Protection Based on IoT,” in Proceedings of the 7th International Symposium on Parallel Architectures, Algorithms, and Programming, PAAP ’15, pp. 217–222, Dec 2015.
16. J.-X. Hu, C.-L. Chen, C.-L. Fan and K.-H. Wang, "An intelligent and secure health monitoring scheme using IoT sensor based on cloud computing," in Journal of Sensors, vol. 2017, Article ID 3734764, pp. 1-11, 2017.
17. C.-T. Li, C.-C. Lee, and C.-Y. Weng, "A secure cloud-assisted wireless body area network in the mobile emergency medical care system," in Journal of Medical Systems, vol. 40, no. 5, pp. 1–15, 2016.
18. Lounis, A. Hadjidji, A. Bouabdallah, and Y. Challal, “Secure medical architecture on the cloud using wireless sensor networks for emergency management,” in Proceedings of the 2013 IEEE 8th International Conference on Broadband, Wireless Computing, Communication and Applications, BWCCA 2013, pp. 248–252, Oct 2013.
19. Lounis, A. Hadjidji, A. Bouabdallah, and Y. Challal, “Healing on the cloud: secure cloud architecture for medical wireless sensor networks,” in Future Generation Computer Systems, vol. 55, pp. 266–277, 2016.
20. M. Li, S. Yu, and Y. Zheng, “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, 2012.
21. Bezawada, A. X. Liu, B. Jayaraman, A. L. Wang, and R. Li, “Privacy Preserving String Matching for Cloud Computing,” in Proceedings of the 35th IEEE International Conference on Distributed Computing Systems, ICDCS ’15, pp. 609–618, Jul 2015.
22. Y. Miao, J. Ma, X. Liu, F. Wei, Z. Liu, and X. A. Wang, “m2- ABKS: attribute-based multi-keyword search over encrypted personal health records in multi-owner setting,” in Journal of Medical Systems, vol. 40, no. 11, pp 239-246, 2016.
23. M. Li, S. Yu, N. Cao, and W. Lou, “Authorized private keyword search over encrypted data in cloud computing,” in Proceedings of the 31st International Conference on Distributed Computing Systems (ICDCS ’11), IEEE, USA, pp. 383–392, Jul 2011.
24. M. Huang, A. Liu, T. Wang, and C. Huang, "Green data gathering under delay differentiated services constraint for the internet of things," in Wireless Communications and Mobile Computing, vol. 2018, Article ID 9715428, 2018.
25. P. Chhajed, D. Baviskar, R. Ahire, A. Bumb and M. V. Korade, "Certificateless remote anonymous authentication technique for Wireless Body Area Networks," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 1035-1041, 2015.
26. K. Shim, "Universal Forgery Attacks on Remote Authentication Schemes for Wireless Body Area Networks Based on Internet of Things," in IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9211-9212, Oct. 2019
27. Hussain, S.J., Irfan, M., Jhanjhi, N.Z. et al. Performance Enhancement in Wireless Body Area Networks with Secure Communication. Wireless Pers Commun 116, 1–22 (2021).
28. Chatterjee, K. An Improved Authentication Protocol for Wireless Body Sensor Networks
Applied in Healthcare Applications. *Wireless Pers Commun* **111**, 2605–2623 (2020).

29. Sowjanya, K., Disrupt, M. & Ray, S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. *Int. J. Inf. Secure.* **19**, 129–146 (2020).

30. Jain Shen, Ziyuan Gui, Sai Ji, Jun Shen, Haowen Tan, Yi Tang. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks, *Computers & Electrical Engineering*, **Vol 65**, Pages 322-331, 2018.

31. Fushan Wei, P. Vijayakumar, Jian Shen, Ruijie Zhang, Li Li. A provably secure password-based anonymous authentication scheme for wireless body area networks, *Journal of Network and Computer Applications*, Vol 106, Pages 117-123, 2018.