E.O. Okpu et al., Vol 2(1), pp 18-24
https://doi.org/10.55306/CJDTES.2025.020102
e-ISSN: 3048-8389
Ci-STEM Journal of Digital Technologies and Expert Systems

Analysing the Integration of AES-256 Encryption and HMAC Hashing in IoT Smart Healthcare Systems

Eterigho Okpomo Okpu[1] and Onate Egerton Taylor[2]
[1]Department of Cyber Security, Delta State University of Science & Technology, Ozoro, Delta State, Nigeria.
[2]Department of Computer Science, Rivers State University, Port-Harcourt, Rivers State, Nigeria.
[1]email: okpuoe@dsust.edu.ng, [2]email: taylor.onate@ust.edu.ng.

Open Access
Review Article
Received : 10/01/2025
Accepted : 02/03/2025
Published : 11/03/2025
Corresponding author email:
okpuoe@dsust.edu.ng
Citation:
E.O. Okpu and O. E. Taylor., "Analysing the Integration of AES-256 Encryption and HMAC Hashing in IoT Smart Healthcare Systems," Ci-STEM Journal of Digital Technologies and Expert Systems, Vol. 2(1), pp.18-24, 2025, doi: 10.55306/CJDTES.2025.020102

Published By:
Ci-STEM Global Services Foundation, India.

Abstract:
The exponential growth of Internet of Things (IoT) technology has been a driving force in the development of smart healthcare systems, facilitating patient monitoring and clinical decision support. It uses IoT-enabled medical devices and wearable sensors under the umbrella of Internet of Medical Things (IoMT) to continuously monitor health from afar. Yet, the fundamental security weaknesses of IoT structure and the high sensitivity of medical data reveal serious security and privacy problems. Therefore, this research suggests a comprehensive security framework to provide the confidentiality, integrity, and authenticity of data transmission in IoMT ecosystems. At the physical layer, the framework utilizes AES-256 encryption and HMAC (Hash-based Message Authentication Code) hashing to minimize cyber threats and prevent unauthorized access. The only additional computation cost at any performance evaluation is negligible, but we gain a lot more in terms of security on the data. The findings confirm the seeing of implementation and demonstration of a feasible security model to protect the multifarious healthcare architecture from ever- existing threats created by the number of cyber-attacks.
Keywords:
AES-256 Encryption, Cyber Threats, Data Security, HMAC Hashing, Internet of Things (IoT), Internet of Medical Things (IoMT), Patient Monitoring, Privacy Protection, Smart Healthcare Systems, Wearable Sensors.

1. INTRODUCTION

Cryptography, the study and application of techniques that protect data and communication from adversaries, guarantees, among other things, information nonrepudiation, confidentiality, integrity, and authenticity. To secure sensitive data, modern cryptographic techniques (such as hashing algorithms like HMAC; symmetric encryption like AES [1]). Advanced Encryption Standard (AES) is the most adopted standard for data protection and secure communication in many digital platforms. AES replaced the older Data Encryption Standard (DES) which was vulnerable to brute force attacks [2]. AES employs a symmetric-key method [3], in which one key is used for both encryption and decryption. HMAC generates a unique fixed-size hash value called a tag by hashing the message to be authenticated with a secret key using hashing functions like MD5 or SHA-256. HMAC ensures the data integrity by computing a tag that will depend on the content of the message and the secret key. According to [4], HMAC is strongly resistant to various attacks such as manipulation and impersonation. SHA-256 is a cryptographic hash function from the secure hash algorithm (SHA) family. It aims to return a 256-bit fixed-size output irrespective of the input length [5]. The course was the Diffie-Hellman key exchange, which allowed two parties to derive a shared secret key over an unsecured channel, significantly changing without reason to communicate securely. In the Diffie-Hellman key exchange, two parties called Jackie and Ahmed share public values generated by their

individual secret keys. This study comes forth to tackle the privacy and security problems in IoMT surroundings, especially in the context of remote patient monitoring systems. This provides an efficient framework to secure data about IoT-enabled medical device equipment and also enhances security in smart healthcare systems. We do this with AES-256 encryption and HMAC hashing at the physical layer.

2. LITERATURE REVIEW

Researchers oncerns regarding how some encryption algorithms can help protect the protected health information (PHI) [6]. This also covered the connection of patient data, metering data and diagnosis and methods of information security and data integrity. The viability of this strategy in the protection of healthcare data, along with its benefits over other methodologies and the state of its integration in the system, are discussed in the conclusion of this study. [7] analyzes existing works in the domain of E-Health but in a methodical and comprehensive manner. They discuss at length ABE frameworks oriented towards healthcare and evaluate them based on a set of descriptive criteria. The authors then organize them across ten different domains and sub-domains, offering observations and potential recommendations

A brand-new Lionized Remora Optimization-Based Serpent (LRO-S) encryption technique is proposed by [8] in 2023 to secure sensitive data and lessen privacy violations and cyberattacks from hackers and unauthorized users. Combining an enhanced security algorithm with hybrid metaheuristic optimization is the LRO-S technique. Researchers are always looking for appropriate lightweight ciphers for certain applications, which have led to a constant evolution in the field of cryptography techniques for IoT device security [9]. [9] Emphasized that in order to overcome security vulnerabilities in cloud computing, new cryptographic algorithms must be developed. The scalability and security of the LORENA approach for symmetric-key generation in IoHT settings were demonstrated by [10]. A range of MAC-based techniques have been investigated in other studies, including those by [4] and [11], to guarantee data authenticity and integrity. Furthermore, [12] strengthened security against MITM attacks by combining RSA cryptography with DH key exchange. Together, these efforts highlight how crucial it is to incorporate reliable cryptography methods into Internet of Things systems in order to reduce security threats.

An overview of cryptography, or the practice of secure communication in the presence of other parties, is given in [13]. It attempts to hinder eavesdroppers from comprehending the conversation. [14] States that the author addresses the use of the matrix decomposition method and Laplace transform to hyperbolic functions in cryptography. The latch-type voltage sensitive amplifier used in [15] AES secret key generation structure uses the Strong-ARM latch-type sensitive amplifier difference structure as PUF. Galois field multiplier system is used for encryption transformations in the AES engine with real-time S-box production [16]. AES is employed in the suggested secure system to encrypt medical data, according to [17]. AES guarantees the safe conversion of readable data into unreadable forms. AES is a component of hybrid encryption that was suggested for use with medical data by [18]. The suggested AES-based approach enhances data integrity and security. For data security, hybrid encryption employs ECC, Serpent, and AES. The security and data integrity of IoT healthcare data are enhanced by this solution.

A combination of 3DES and LSB was suggested in [19] for the security of medical data. The integration of 3DES and LSB for enhanced security was achieved through the creation of a Java simulation application. A suggested method secures medical data by using mutual authentication. In [20], the researchers presented a hybrid architecture that combined the OpenStack private cloud platform with Cryptography as a Service (CaaS). With the help of this architecture, cloud clients can operate cryptographic operations and deploy keys in the cloud without interference from cloud providers. Two cryptographic approaches are compared and examined by [21]. The first cryptographic approach combines the AES-256 encryption algorithm to preserve data confidentiality with the HMAC-SHA-256 hashing approach to ensure data integrity. The AES-GCM (Galois/Counter Mode) technology, which provides assurance of integrity and confidentiality in a single, integrated process, is used in the second strategy. In the context of healthcare applications, searchable encryption (SE) is described in [22] research, which also categorizes SE use cases into four situations. Then, in

accordance with various EHR retrieving scenarios and requirements, the writers gave a thorough overview of the four representative SE techniques: searchable symmetric encryption (SSE), public key encryption with keyword search (PEKS), attribute-based encryption with keyword search (ABKS), and proxy re-encryption with keyword search (PRES).

The system places a strong emphasis on the confidentiality and integrity of healthcare communication. For safe transfer, it additionally offers a mutual authentication and session key exchange mechanism [23]. [24] State that the Diffie Hellman key exchange was suggested as a means of protecting the transfer of medical data. To authenticate the shortest path for data transfer, a probabilistic neural network was employed. The Diffie Hellman key exchange was employed in the encryption and decryption procedures. MACs guarantee message authentication and data integrity in telemedicine applications, according to [25]. The data integrity and message authentication in telemedicine applications were highlighted by the SHA2 algorithm optimized for MAC construction in Java for security. A Secured framework using the SHA-512 algorithm for integrity assurance was carried out in [26]. System security is improved by the Improved ECC with secret key. The correlation coefficient of the proposed IECC is around 0.045, and the encryption and decryption times are 1.032 μs and 1.004 μs, respectively.

3. METHODOLOGY

In order to guarantee the integrity and confidentiality of private information gathered by wearable health monitoring devices, the integration of HMAC hashing and AES-256 encryption must be done as follows:

1. Data Identification: Identify the health information that wearables are collecting that has to be encrypted. We utilize "TCD_data," a dataset from physionet.org that includes measurements of blood flow velocity in the main arteries of the brain, for this investigation.
2. AES Configuration: AES-256 is selected due to its great security. A 256-bit key is used in this symmetric-key approach for both encryption and decryption.
3. Key Generation: Create strong encryption keys that are safely kept on wearable technology and unavailable by unauthorized individuals.
4. Data Encryption: Before sending sensitive health data over communication channels, encrypt it with AES-256.
5. MAC Computation: To ensure data integrity and authenticity, use HMAC-SHA256 to create a MAC over the encrypted data. This procedure is facilitated by the PyCryptodome framework.
6. Secure Transmission: Provide other systems, including cloud servers or healthcare platforms, with encrypted health data in a secure manner.
7. Data Decryption: After gaining access to the encrypted health data, re-compute the MAC by implementing decryption capabilities in the recipient systems with the appropriate AES-256 keys. If both the computed and acquired MACs match, it indicates that the data was not changed during communication.
8. Key Management: To avoid unwanted access or disclosure of encryption keys, implement key creation, distribution, rotation, and revocation protocols.
9. Testing and Validation: To guarantee the security framework's efficacy and resilience, thoroughly test and validate it.

To further strengthen the security of the suggested system, the practical implementation uses the [27] Diffie-Hellman key exchange method to securely create shared secret keys via dubious communication channels. An example of the SUBJ001 dataset in usage is shown in Table 1. These datasets on blood pressure were gathered from physionet.org.

Table 1. SUBJ001 Dataset

Sample Rate: 200				
Relative Time	Date	Time Stamp UTC	Left MCA	Right MCA
0	7/12/2018	3:21:43 PM	0.84564209	0.738830566
0.01	7/12/2018	3:21:43 PM	0.834960938	0.739135742
0.02	7/12/2018	3:21:43 PM	0.828552246	0.739440918

Sample Rate: 200				
Relative Time	Date	Time Stamp UTC	Left MCA	Right MCA
0.03	7/12/2018	3:21:43 PM	0.826416016	0.739440918
0.04	7/12/2018	3:21:43 PM	0.826416016	0.739440918
0.05	7/12/2018	3:21:43 PM	0.826416016	0.738830566
0.06	7/12/2018	3:21:43 PM	0.825195313	0.736083984
0.07	7/12/2018	3:21:43 PM	0.821228027	0.72845459

4. RESULT AND DISCUSSION

Table 2 showed the encrypted results with the alphabet serving as the secret key. This displays the secret key, the HMAC key, the encryption key, and the encrypted file. The whole encryption and decoding result were shown in Table 3. TRD stands for Time to Read Data from CSV, TDK for Time to Derive Keys, TEDH for Time to Encrypt Data and Compute HMAC, TREH for Time to Read Encrypted Data and HMAC Values from Files, and TDDH for Time to Decrypt Data and Verify HMAC are all displayed in these tables. TRD, TDK, TEDH, TREH, and TDDH scores in SUBJ001 data are, in order, 0.26 seconds, 0.20 seconds, 36.58 seconds, 0.92 seconds, and 38.96 seconds. The complete encryption and decoding results were displayed graphically in Figure 1. The results of hashing, decrypting, and encrypting data using the AES 256 and HMAC techniques are shown in Figure 1.

Table 2. Encrypted result using alphabet as secret key

#	Encrypted file	Encryption Key	HMAC Key	Secret Key
1	SUBJ001_encrypted.csv	*337cef0c2d8717300dd7242dffae6b47b86704102ff74e93132fdfd89145e213*	*4b04e2829ba3535d85cdac4722e05c7b678f283f3d58acb75029aac8d4a32bf4*	*6fef284c8312604732142f9aa67238ef6f3bbcba621d806c3fbdb474bf84dc3e3d4c08cb14b7ffe95206877fc2217a67d00ba58491747082080f00b8236d14f5d8e9aed755af133b7d7bca834ed973fe183dbb28a04170ccc1c848687ea82516d089c1b1c917ef4cd5ed841278663e094694b2bf5ed30779c5b3eedc894231e9a27f672ff8c225d79e01ad4f63afa2ffc5ca460ad4662d14846fc63f91bf82e3477b5680fe8167983504c8bfc7be1edbb633bde8aa423a064d487e9240b7472b05469323d40721afe3e5f15714575140e0eb3c1b42898a17502ebb3dfe624a67da6aaa5f7dbc1cd1cb8cb597aedf080c1c1c4b9504455c45ad96785d7bd81e07*
2	SUBJ002_encrypted.csv	*34896e629c8aa52a7dcd554aa1d930bb0fe5e7fcc739167bc525053d76c850b0*	*a2a2b95bd5924f1c0c4a74b0d16486f97815539848eb3198fff6ec3a6ca5ccd0*	*945e4c76e55c083b4929a5475489625dd0f69f2d3b351396653f086dd7948cdab4ba1f1540dcc51c2c6aa6a8fe27c86129d8a7ccf8c993b08ff84ca236c58ba6e3e9a1a2e25fdf246e3f273c391320af7acf216dea81bedb76433cff37fe8665688d4285a5e4bfdb16721486e76740a17e040aad4b141d43b1e10c67c9d350307647e83fecf6558a44309db7597b481c87d01c77f25296bd87199838330e2dd11753f2aed87eafea2b0c9b5522a06a00528336ed21b8b3d476d19fc77e1212833e5fb2bf79305b1c8283c062a7d7788c56f9f2e3f4f9802da56e3ca1b4000ea13e0e62c0aaf09741b78983e21d9853058d1e778209235263d44dd8171ce220d4*
3	SUBJ003_encrypted.csv	*460ff791cfce214449f10ca0f152f9ef9d047c927a5fae6df6aebb04e8b34812*	*5faaa1375eeac4e36976403659c72cfd7387639e4216a803532a2abaab9e29f7*	*0316abf204af99bb734be75647c141797635a55741b0504fea73df53bc101fe192c773f6038eaad724baaa54f418a8e15dae018078a8497d00f798b217ee2c696cfebb46c99f6511b6588a25462172ba55af0693cfa37917260637f138e6ed1b810d0330f266ff456d95e91ce17b4468547701cd06fe94d9b9ee04397423cb546293eaa9c3e18ef7e4494e50aa18dba13a6e2678a103ec0c688bfc48563614157ce9174170 16b45f849fd570b3f9d11855ed76deaf7d857245b428f77033fbd9ded69b611b10e4ebbbeef45b59695303dce20d831a8454d6c8afbfeab3232d303faa7268d108bc90e24de5f463b1ee68d1a91dacdadd85b16ecb9116b8bc6755*
4	SUBJ004_encrypted.csv	*af48652bb80e143ca8fb25266574d88b2f9fb9934de7d59c4257c989f498750c*	*1d5bf82b2d79f6b2a8da57ad765a6098280afe661a05975e0a4be1c0f9b7658c*	*a9453724a4ffcc43f19d63367edeba7d83f4471635e69e231e9a944473bfa3961bb262c03fd10055e7233322ef04aa25c9b2406e0bfd8bc606a6ef6f68d4372848b573bb0210a2085bf08084c9d90aeb83ef90365143b6a8812b3e87b0ae8fc0a634cdbeaeb0f4723563925088a7d0eb369ae8fbf23002cc83c433c7bf357ae6b3819cbff1c98790bfb340742e486cbdfee9ac52b90223a973a47959cb12beb3f992f8e568ee37f18a07428944dc0385927852a5d7d3222e9f98e015c9a419ab57cc5ee1582954419417c4957a355718e5be6f47ecc65495468082c2ca7f1dcc427c79f6734a9559630f41935aa5cf47f1d3d1fc0cec1ba465988cfcd5f278c6*

#	Encrypted file	Encryption Key	HMAC Key	Secret Key
5	SUBJ005_encrypted.csv	*6ae6bb25ce12d40cd17e1b3d2a9368ba24660a14b8396257bec57f82b796926e*	*e31657c2958d8e817d8a5885e53bc904939a1a0a3cd660cb381091a293a36e90*	*52993b81daf5ceafc7110735537786cc4671aec284246f80ee4a8d74695dca9b4228d5e052291995e31c9fe473defdef9c9b8c1207b2a1d6279acbdd48b6289c6d5ef79bcc36af903f838d08ccadf75a33e2a6c076e6cc8fcf803beaca0eecd45fbbd9acea73eb0585c9a0bc57bf9274a7262f702de20c9b98a18c3be90470ddabeea0f3dfbe3c39efb3118598e1252174fdcbacc5c12e9f8a7bcc485f1cf0618599313b231f39c254dad0940aebec454f015dcbc33a3c3221d35c2ec50760f17b319143ff597d485eb857c0bed30b999d44741dc64d438f7c2a09c0f0caddcf46c06aaff883d93385e091fbe3c5910b8f8e81f624b3af52fb3f3cba7631e3f5*

Table 3 Full Result of encryption and decryption

S/N	Data	TRD	TDK	TEDH	TREH	TDDH
1	SUBJ001	0.26	0.2	36.58	0.92	38.96
2	SUBJ002	0.18	0.24	7.69	0.7	10.26
3	SUBJ003	0.33	0.23	28.26	0.64	30.38
4	SUBJ004	0.19	0.2	30.99	0.74	34.55
5	SUBJ005	0.24	0.22	26.29	0.63	22.67

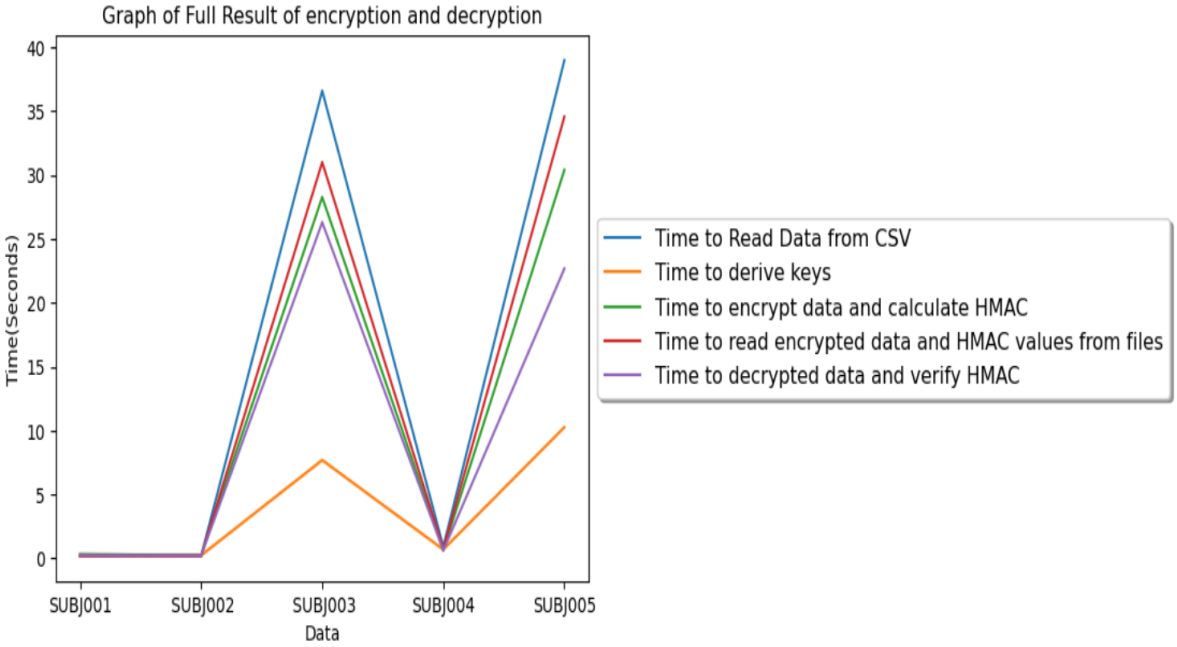

Figure 1: Results of Encryption, Hashing and decryption using the AES 256 and HMAC Techniques

5. CONCLUSION

This study applies the HMAC hashing approach to verify data integrity at the physical layer of IoMT and integrates the AES-256 encryption technique to assure data secrecy there as well. Python was used as the programming language to create the system. TRD, TDK, TEDH, TREH, and TDDH scores for file SUBJ001 are 0.26 seconds, 0.20 seconds, 36.58 seconds, 0.92 seconds, and 38.96 seconds, in that order. The results of this study will improve safe IoT smart healthcare systems and offer insightful information to practitioners and researchers alike.

DECLARATIONS:

Acknowledgments : Not applicable.

Conflict of Interest : The authors declares that there is no actual or potential conflict of interest about this article.

Consent to Publish : The authors agree to publish the paper in the Global Research Journal of Social Sciences and Management.

Ethical Approval : Not applicable.

Funding : Author claims no funding was received.

Author Contribution : Both the authors confirms their responsibility for the study, conception, design, data collection, and manuscript preparation.

Data Availability Statement : The data presented in this study are available upon request from the corresponding author.

REFERENCES

[1] Arunkumar, J. R., Velmurugan, S., Chinnaiah, B., Charulatha, G., Prabhu, M. R., & Chakkaravarthy, A. P. (2023). Logistic Regression with Elliptical Curve Cryptography to Establish Secure IoT, *Computer Systems Science & Engineering*, 46(1).

[2] Wang, J., Han, J., Li S., Zhou, F., & Wang, N., (2024). A Lightweight Combined Physical Layer Encryption and Authentication Scheme for Industrial Internet of Things, *IEEE Access*.

[3] Kumar, C., Prajapati, S. S., & Verma, R. K. (2022). A Survey of Various Lightweight Cryptography Block ciphers for IoT devices, *In 2022 IEEE International Conference on Current Development in Engineering and Technology (CCET)*, 1-6, IEEE.

[4] Devi, S., Kuruba, C., Nam, Y., & Abouhawwash, M. (2023). Paillier Cryptography Based Message Authentication Code for IoMT Security, *Computer Systems Science & Engineering*, 44(3), DOI: 10.32604/csse.2023.025514.

[5] Katulić, F., Sumina, D., Groš, S., & Erceg, I. (2023). Protecting Modbus/TCP-Based Industrial Automation and Control Systems Using Message Authentication Codes*, IEEE access*.

[6] Abhishek, Tripathy, H. K., & Mishra, S. (2022). A succinct analytical study of the usability of encryption methods in healthcare data security*, In Next Generation Healthcare Informatics* (pp. 105-120). Singapore: Springer Nature Singapore.

[7] Imam, R., Kumar, K., Raza, S. M., Sadaf, R., Anwer, F., Fatima, N., & Rahman, O. (2022). A systematic literature review of attribute based encryption in health services, *Journal of King Saud University-Computer and Information Sciences*, 34(9), 6743-6774.

[8] Almalawi, A., Khan, A. I., Alsolami, F., Abushark, Y. B., & Alfakeeh, A. S. (2023). Managing security of healthcare data for a modern healthcare system, *Sensors*, 23(7), 3612.

[9] Sasikumar, K., & Nagarajan, S. (2024). Comprehensive Review and Analysis of Cryptography Techniques in Cloud Computing, *IEEE Access*.

[10] Coelho, K. K., Nogueira, M., Marim, M. C., Silva, E. F., Vieira, A. B., & Nacif, J. A. M. (2022). Lorena: Low memory symmetric-key generation method for based on group cryptography protocol applied to the internet of healthcare things, *IEEE Access*, 10, 12564-12579.

[11] Mohammed, M. A., Abood, L. K., & Maliki, M. (2016). MMAC: Fast and Secure Message Authentication, *International Journal of Science and Research (IJSR)*, 6(12), 576-579.

[12] Gupta, C., & Reddy, N. S. (2022). Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography, *In Journal of Physics: Conference Series*, 2161(1), IOP Publishing.

[13] Archana, B., U., & Niranjana, V. (2023). Overview of Cryptography, 2, doi: 10.46632/daai/3/2/15

[14] Zaryab, A. (2022). Cryptology Based on Laplace Transform of Hyperbolic Function and Matrix Decomposition Method, *Meeting abstracts,* doi: 10.1149/ma2022-02642364mtgabs.

[15] Zhao, Y., He, J., Shu, Q., & Yang, S. (2015). Advanced encryption standard (AES) secret key generation structure based on physical unclonable function (PUF) of latch-type voltage sensitive amplifier.

[16] Stein, Y., & Kablotsky, J. A. (2008). U.S. Patent No. 7,421,076. Washington, DC: U.S. Patent and Trademark Office.

[17] Modi, T., Patel, J., Paliwal, M., Shah, K., & Shastri, A. (2023, March). Enhancing Medical Domain Data Security using Inbuilt Data Encryption and Steganography, *In 2023 10th*

International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 181-187). IEEE.

[18] Fatima, S., Hussain, S., Shahzadi, N., ul Din, B., Sajjad, W., Saleem, Y., & Aun, M. (2022, December). A Secure Framework for IoT Healthcare Data Using Hybrid Encryption, *In 2022 International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)* (pp. 1-7). IEEE.

[19] Babatunde, A. O., Taiwo, A. J., & Dada, E. G. (2018). Information security in health care centre using cryptography and steganography. arXiv preprint arXiv:1803.05593.

[20] El Bouchti, A., Bahsani, S., & Nahhal, T. (2016, August). Encryption as a service for data healthcare cloud security, *In 2016 fifth international conference on future generation communication technologies (FGCT)* (pp. 48-54). IEEE.

[21] Okpu, E. O., Taylor, O. E., Nwiabu, N. D., & Matthias, D. (2024).Comparative Performance Analysis of Cryptographic Techniques for Securing the Physical Layer in Internet of Medical Things (IoMT) Systems, *International Journal of Computer Science and Mathematical Theory (IJCSMT)* E-ISSN 2545-5699, 10(2), 157-170.

[22] Zhang, R., Xue, R., & Liu, L. (2017). Searchable encryption for healthcare clouds: A survey, *IEEE Transactions on Services Computing*, 11(6), 978-996.

[23] Sowmiya, L., Rajasekaran, A. S., Suganyadevi, S., Sureshkumar, S., Subramaniam, G., & Jaazieliah, R. (2023, February). A Secure Authenticated Message Transfer in Healthcare Application, *In 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1-6). IEEE.

[24] Prabhu, A. J., & Rajesh, D. H. (2023). Authentication of WSN for Secured Medical Data Transmission Using Diffie Hellman Algorithm, *Computer Systems Science & Engineering*, 46(1).

[25] Lim, C. K., Iipinge, V. J., Tan, K. L., & Hambira, N. (2018, November). Design and development of message authentication process for telemedicine application, *In 2018 IEEE Conference on Wireless Sensors (ICWiSe)* (pp. 23-28). IEEE.

[26] Khan, M. A., Quasim, M. T., Alghamdi, N. S., & Khan, M. Y. (2020). A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data, *IEEE Access*, 8, 52018-52027.

[27] Patgiri, R. (2021). Privatedh: An enhanced diffie-hellman key-exchange protocol using RSA and AES algorithm, *Cryptology ePrint Archive.*

Authors' Profiles

Eterigho Okpomo Okpu: Pursued B.Sc. degree in Computer Science at Delta State University, Abraka, MSc and PhD at Rivers State University. He is currently a Lecturer in the Department of Cyber Security, Delta State University of Science & Technology, Ozoro. He is a member of the Computer Professionals of Nigeria (CPN). His research works focuses on Machine Intelligence Systems, Cyber Security, & IoT. (ORCID iD: https://orcid.org/0009-0004-0116-4506).

Onate Egerton Taylor Pursued B.Sc. degree in Computer Science at Rivers State University, MSc at the University of Ibadan, & PhD at the University of Port Harcourt. He is currently an Associate Professor & a Lecturer in the Department of Computer Science, Rivers State University, Port-Harcourt. He is a member of the Computer Professionals of Nigeria (CPN). He has published over 50 research papers in reputed international journals. His research works focuses on Machine Intelligence Systems, Cyber Security, & IoT. (ORCID iD: https://orcid.org/0000-0003-4477-9987).