SECURITY ANALYSIS OF DATA TRANSMISSION IN AN IoT BASED PLATFORM FOR TELEMEDICINE

[1] Rashidah Funke Olanrewaju, [2] Amuda Idowu Rahaman, [3] Aisha Hassan Abdallah Hashim

[1,2,3]Dept of Electrical and Computer Engineering,
International Islamic University, Gombak campus, Malaysia

Abstract: The Internet of Things offers an effective and increased job satisfaction when used for better services on the Internet. Decreased charges for materials and facilities on the network and breakthrough technology for modern society. Cryptography plays a major role in the defense of knowledge that has gained popularity as a result of digitization. The sharing of confidential personal data such as medical data continues to take place regularly across the globe; it is therefore crucial to protect data from unauthorized access by adversaries. One of the algorithms that is commonly used due to its exemplary security and use in extensive applications is the advanced encryption standard (AES) algorithm. This study proposes a modified folded pipeline architecture for resource restriction applications with an AES algorithm. Through time-multiplexing operations to a single functional unit, the folding transformation manages the circuit functions and decreases the time use for encryption and decryption by 30 percent and 20 percent, respectively. Using less power, the proposed architecture is implemented based on python programming language, thereby improving time and power requirements compared to the traditional algorithm. The work discussed in this thesis is important to the encryption and encryption of personalized electrocardiograph (ECG) signals for safe transmission are decrypted. This thesis work improved the throughput by 92.39% and 93.73% for encryption and decryption respectively and power by 96.93%, allowing its hardware to be implemented more efficiently than the traditional AES.

Index Terms **- Data on the Internet, Telemedicine, Protection, Privacy, Cryptography, ECG.**

I. INTRODUCTION

In internet of things-based telemedicine, data sharing is the method of gathering, processing, and tracking data for the key benefits of health and other medical services[1]. This mechanism is the brain behind the digitalized type of the health system in which all medical services are linked together to produce a healthier and more effective outcome. Numerous devices are used to track health problems, including temperature sensors, heart rate sensors, blood pressure sensors, hearing aid sensors, wristband sensors, and devices that can calculate a specialized implant[2]. As a result of the use of these devices, Smart Health has been developed to help patient health care by capturing, processing, transmitting, and storing health information. The telemedicine system gives a reasonable cost reduction for disabilities and aged peoples. The latest m-health services are based on a special application that depends on different architecture with interoperability issues, which doesn't give room for the customers to switch providers due to minimum flexibility and cost. The hospitalized patients that need medical attention will get it under the implementation of the internet of things technology[3][4].

With the telemedicine system, physiological data is collected from the primary source which is the patients and it will be sent to the cloud in other to store the information and it will be analysed while the output result will be transferred wirelessly to the health providers for a cross-examination which will provide efficient, reliable, timely and cost-effective health services. At the same time, the output data /information can be monitored at a remote distance to know the conditions of the health of the patients[5][6][7].

II. LITERATURE REVIEW

Telemedicine is the use of electronic information and communication systems in order to provide and facilitate health care where the system has been part of the U.S. health system for many decades, where distance divides[8]. Applications have been expanded to include education and administration, diagnosis and patient assessment, originally intended to address access to care problems, especially in rural areas. Improved technology and the current emphasis on healthcare cost management have placed telemedicine at the forefront of healthcare delivery[9][10]. Usually, telemedicine has expanded the influence of doctors and the clinical medical community into non-traditional environments such as home healthcare and prison health. Security and privacy of end-user data needs to be discussed as part of strategic planning and implementation of a telemedicine project. It is important to assess the consistency of the data transmission protection strategy in terms of a complete solution. To send a packet successfully over a public and/or private network infrastructure, there are several components necessary and all of these components must be secured against threats. The private infrastructure is not necessarily any better than public infrastructure[11][12].

III. RELATED WORK

Emergency response sensor networks: problems and possibilities released by Lorincz K., Malan D. J., Fulford-Jones T. R., Nawoj A., Clavel A., Shnayder V. & Moulton S. (2004) is focused on Code Blue as a wireless infrastructure for emergency medical care deployment, ensuring smooth data transfer between caregivers and enabling the successful allocation of hospital resources. The protection elements of Code Blue, however, are still left as a potential mission.

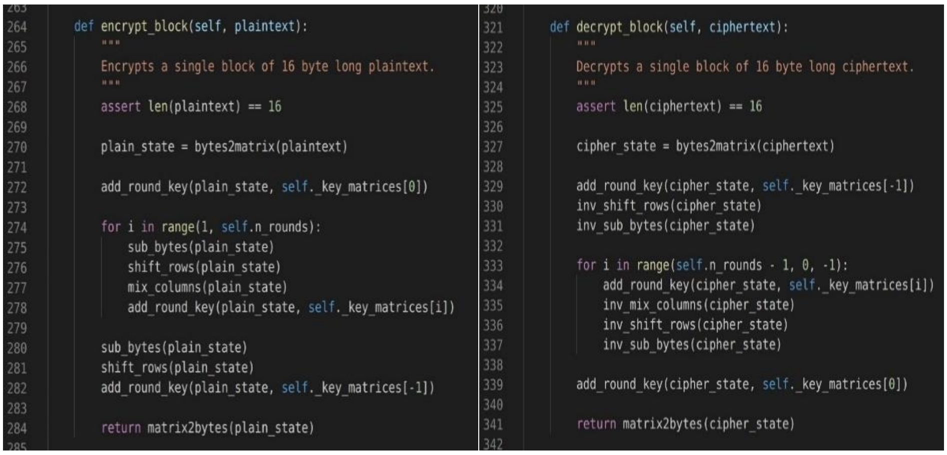
A Secure Information System Telecare Medicine Authentication Scheme. Computer Science Method. 98, by Abdellaoui A., Khamlichi Y. I. & Chaoui H. H. & H.(2016) based on an image-based authentication system, their contribution to improving authentication in the telemedicine information system overcomes various security problems, however, it has not been applied in an IoT environment.

RFID-based Concept of Wireless Health Monitoring System, 7th Asian-Pacific Aerospace Technology and Science Conference by J.M.Lina, C.H.Linb (2013), the authors implemented a device capable of monitoring health remotely using RFID tags. Their contribution, however, doesn't take data protection into account.

A privacy security scheme for source location based on Hao Wang Guangjie Han’s ring-loop routing for IoT, (2018). In this paper, a security of privacy for the location of which was investigated by the Ring-loop Routing method for Internet of things. Three ways of routing, ring routing, the proposed confused time domain and backbone routing were included in the paper. However, a single point of failure is the shortcoming for the method involved.

IV. RESEARCH METHODOLOGY

The Advanced Encryption Standard is based on a design principle known as a substitution-permutation network in both software and hardware and is easy. Using cryptographic keys of 128, 192, and 256 bits, the AES algorithm is able to encrypt and decrypt data in blocks of 128 bits.



```
def encrypt_block(self, plaintext):
    """
    Encrypts a single block of 16 byte long plaintext.
    """
    assert len(plaintext) == 16

    plain_state = bytes2matrix(plaintext)

    add_round_key(plain_state, self._key_matrices[0])

    for i in range(1, self.n_rounds):
        sub_bytes(plain_state)
        shift_rows(plain_state)
        mix_columns(plain_state)
        add_round_key(plain_state, self._key_matrices[i])

    sub_bytes(plain_state)
    shift_rows(plain_state)
    add_round_key(plain_state, self._key_matrices[-1])

    return matrix2bytes(plain_state)
```

```
def decrypt_block(self, ciphertext):
    """
    Decrypts a single block of 16 byte long ciphertext.
    """
    assert len(ciphertext) == 16

    cipher_state = bytes2matrix(ciphertext)

    add_round_key(cipher_state, self._key_matrices[-1])
    inv_shift_rows(cipher_state)
    inv_sub_bytes(cipher_state)

    for i in range(self.n_rounds - 1, 0, -1):
        add_round_key(cipher_state, self._key_matrices[i])
        inv_mix_columns(cipher_state)
        inv_shift_rows(cipher_state)
        inv_sub_bytes(cipher_state)

    add_round_key(cipher_state, self._key_matrices[0])

    return matrix2bytes(cipher_state)
```

Figure 1: Convectional AES encryption and decryption block fragment

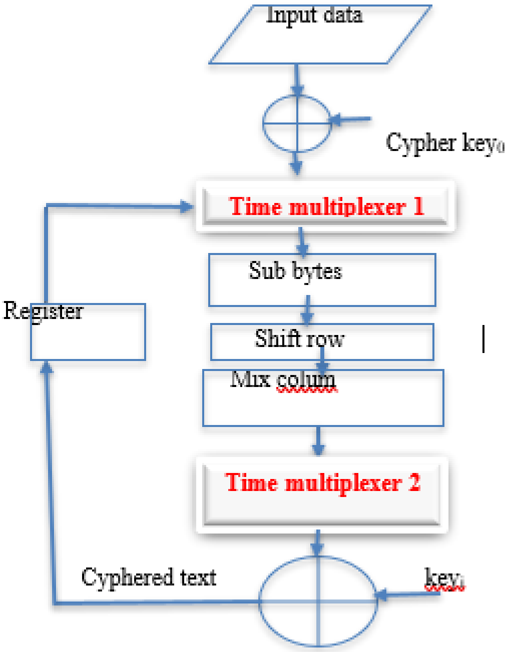
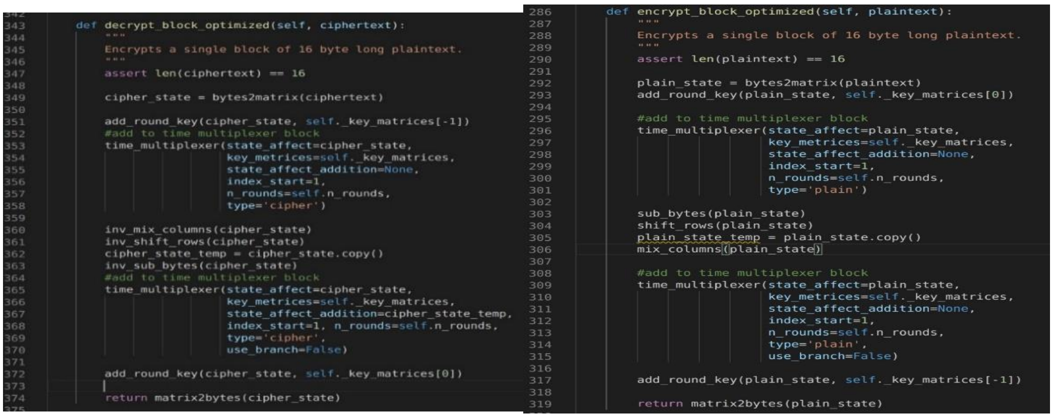


Figure 2: showing the modified AES flow chart

This research work was based on a modified AES algorithm with a low power consumption and with reduced functional units that can be used in an IoT based telemedicine. This modified AES algorithm is robust and reliable as compared to the convectional AES which can be used for data encryption.

It is well known that the AES algorithm involves the encryption of data and the expansion of the key, the modified AES implore a folding transformation technique and involves a minimized register there by reduced the number of functional unit based as shown in figure 2.The encryption of the data requires 10 rounds on the basis of the convectional AES and each round implements a sub-byte, shift-row and mix-column on the output data of the previous round. The 9th rounds are measured and the 10th round production is encrypted, this refers to the AES variants of 128bits. With the support of a multiplexer, all 9 rounds can be folded to form one block, (folding factor of nine) the input will be time multiplexed (Added or XORed) with the primary key that serves as an input to the counter units, the counter unit serves as a counter control from 1st to 9th rounds, then the output of the previous round is now multiplexed and acts as an input to the next round implemented by the counter unit and the encrypted data is collected when the 10th round is reached. The description process can also be modified in other to reduce the utilized resources. The source for the dataset for the ECG will be from MIT-BIH database with 100 data (mitdb/100) in which each pixel data comprises of 8bits, since we are using 128bits AES version, 16pixels will be needed (8 X 16pixels) which serves as the input data for the encryption process at a particular time. This encrypted data is fed in to the description module to get the encrypted image



```
    def decrypt_block_optimized(self, ciphertext):
        """
        Encrypts a single block of 16 byte long plaintext.
        """
        assert len(ciphertext) == 16

        cipher_state = bytes2matrix(ciphertext)

        add_round_key(cipher_state, self._key_matrices[-1])
        #add to time multiplexer block
        time_multiplexer(state_affect=cipher_state,
                         key_metrices=self._key_matrices,
                         state_affect_addition=None,
                         index_start=1,
                         n_rounds=self.n_rounds,
                         type='cipher')

        inv_mix_columns(cipher_state)
        inv_shift_rows(cipher_state)
        cipher_state_temp = cipher_state.copy()
        inv_sub_bytes(cipher_state)
        #add to time multiplexer block
        time_multiplexer(state_affect=cipher_state,
                         key_metrices=self._key_matrices,
                         state_affect_addition=cipher_state_temp,
                         index_start=1, n_rounds=self.n_rounds,
                         type='cipher',
                         use_branch=False)

        add_round_key(cipher_state, self._key_matrices[0])

        return matrix2bytes(cipher_state)
```

```
    def encrypt_block_optimized(self, plaintext):
        """
        Encrypts a single block of 16 byte long plaintext.
        """
        assert len(plaintext) == 16

        plain_state = bytes2matrix(plaintext)
        add_round_key(plain_state, self._key_matrices[0])

        #add to time multiplexer block
        time_multiplexer(state_affect=plain_state,
                         key_metrices=self._key_matrices,
                         state_affect_addition=None,
                         index_start=1,
                         n_rounds=self.n_rounds,
                         type='plain')

        sub_bytes(plain_state)
        shift_rows(plain_state)
        plain_state_temp = plain_state.copy()
        mix_columns(plain_state)

        #add to time multiplexer block
        time_multiplexer(state_affect=plain_state,
                         key_metrices=self._key_matrices,
                         state_affect_addition=None,
                         index_start=1,
                         n_rounds=self.n_rounds,
                         type='plain',
                         use_branch=False)

        add_round_key(plain_state, self._key_matrices[-1])

        return matrix2bytes(plain_state)
```

Figure 3: Modified AES encryption and decryption block fragment

V. Result and discussion

As it is indicated in the figure 4 below, the frequency for the encryption and description is 300MHz and the modified AES has 92.39% less resources usage for the encryption process while the power consumption is been optimized at 93.47% despite operating at higher frequency compared to the convectional AES. Likewise, the decryption process for the modified AES has 93.71% less resources usage while the power consumption is been optimized at 96.93% despite operating at higher frequency compared to the convectional AES. The throughput also increased by 92.39% and 93.73% for the encryption and the decryption respectively. Throughput = Operating Frequency X Total no.of bits been processed

Figure 4 depicted that as the frequency is reduced downwardly, so also the power consumption which shows how efficient the modified AES can be for an IoT applications. Also as indicated in figure 5, the time usage for the convectional and the modified AES was analyzed in which the modified AES has lesser time to implement in both the encryption and the decryption processes.

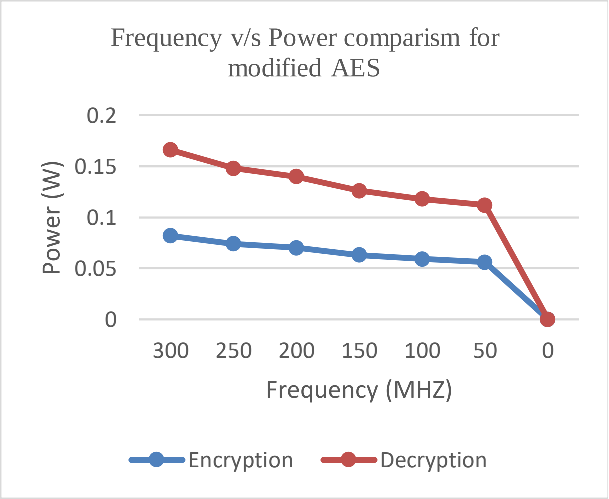


Figure 4: frequency versus power comparison for the modified AES

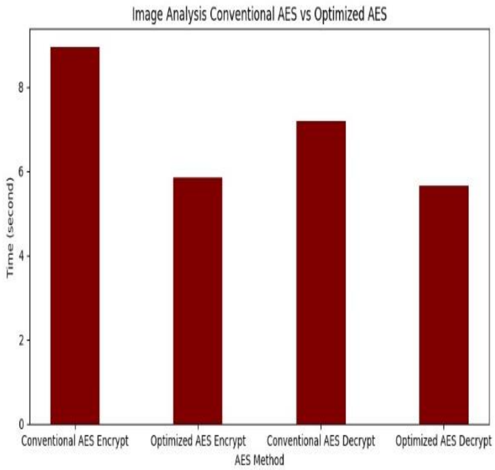
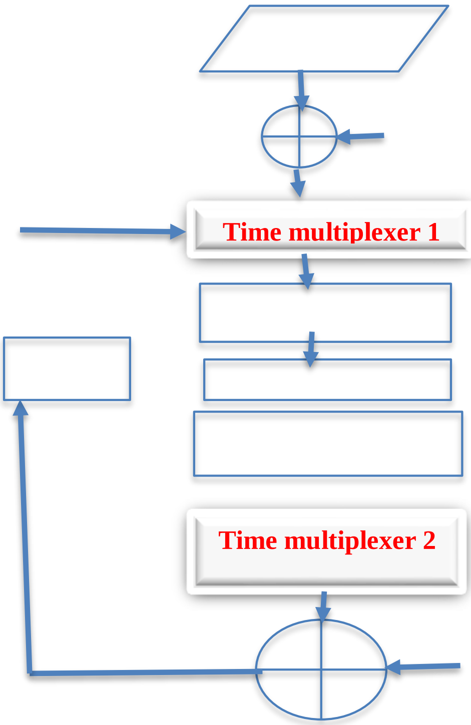


Figure 5: Time usage for convectional and Modified AES using 100files image data

VI. Conclusion

This research work showed how a python programming language with MIT-BIH dataset/100 can be used to achieve encryption and decryption of an electrocardiogram (ECG) signal in an IoT based telemedicine using a modified Advanced Encryption Standard (AES) compared to the convectional AES which was implemented by python programming language. Based on the analysis carried out, it can be concluded that using the modified AES, encryption has a lesser time usage of 30% for the encryption and 20% for the encryption. It can also be achieved with a 38.4Gbps of throughput with a lesser power of 0.18w at 300MHz frequency and likewise the decryption can be achieved with a 23.04Gbps throughput with a lesser power of 0.17w at 180MHz frequency for the data transmission in an IoT based telemedicine. The modified AES has an advantages over the convectional AES in terms of time usage with the aid of a time-multiplexer that serves as a folding factor of nine to reduce the numbers of round involves and also with lesser power. Finally, it is recommended that future work should include using another platform like Field Programmable Gate Array (FPGA) on Zedboard and Virtex (FPGA) to confirm the workability of the modified AES.



VII. Acknowledgment

This work was partially supported by the Ministry of Higher Education Malaysia (Kementerian Pengajian Tinggi Malaysia) under KNOWLEDGE TRANSFER PROGRAMME – RESEARCH INITIATIVE GRANTSCEME (KTP-RIGSSDG) 2019 number IRF19-005-0005.

References

[1] E. Bertino and E. Ferrari, "Big data security and privacy," in A Comprehensive Guide Through the Italian Database Research Over the Last 25 Years, Springer, 2018, pp. 425–439.

[2] R. Boussada, B. Hamdane, M. E. Elhdhili, and L. A. Saidane, "Privacy-preserving aware data transmission for IoT-based e-health," Computer Networks, 162, p.106866.

[3] J. Cao, P. Yu, X. Xiang, M. Ma, and H. Li, "Anti-Quantum Fast Authentication and Data Transmission Scheme for Massive Devices in 5G NB-IoT System," IEEE Internet of Things Journal, 6(6), pp.9794-9805.

[4] L. Ding, Z. Wang, X. Wang, and D. Wu, "Security information transmission algorithms for IoT based on cloud computing," Computer Communications 155 (2020): 32-39.

[5] Dubey, Harishchandra, Admir Monteiro, Nicholas Constant, Mohammadreza Abtahi, Debanjan Borthakur, Leslie Mahler, Yan Sun, Qing Yang, Umer Akbar, and Kunal Mankodiya. "Fog computing in medical internet-of-things: architecture, implementation, and applications." In Handbook of Large-Scale Distributed Computing in Smart Healthcare, pp. 281-321. Springer, Cham, 2017.

[6] A. Gawanmeh and A. Alomari, "Taxonomy analysis of security aspects in cyber physical systems applications," In 2018 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1-6. IEEE, 2018.

[7] A. Gondalia, D. Dixit, S. Parashar, V. Raghava, A. Sengupta, and V. R. Sarobin, "IoT-based Healthcare Monitoring System for War Soldiers using Machine Learning," Procedia computer science 133 (2018): 1005-1013.

[8] F. T. Jaigirdar, C. Rudolph, and C. Bain, "'can i Trust the Data i See?' A Physician's Concern on Medical Data in IoT Health Architectures," In Proceedings of the Australasian computer science week multiconference, pp. 1-10. 2019.

[9] M. Janveja et al., "Design of Efficient AES Architecture for Secure ECG Signal Transmission for Low-power IoT Applications," Proc. 2020 30th Int. Conf. Radioelektronika, RADIOELEKTRONIKA 2020, pp. 2–7, 2020.

[10] A. J. Jara, M. A. Zamora, and A. F. Skarmeta, "Knowledge acquisition and management architecture for mobile and personal health environments based on the Internet of things," in Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012, 2012.

[11] A. Karati, S. K. Hafizul Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments," IEEE Internet of Things Journal 5, no. 4 (2017): 2904-2914.

[12] R. Lavanya, M. Nivetha, K. Revasree, and K. Sandhiya, "Smart Chair-A Telemedicine Based Health Monitoring System," In 2018 second international conference on electronics, communication and aerospace technology (ICECA), pp. 459-463. IEEE, 2018., 2018.