Secure Data Delivery in a Software-Defined Wireless Body Area Network

Zahraa M. Yahya and Mohammed F. Al-Gailani

Al-Nahrain University, Baghdad, Iraq

https://doi.org/10.26636/jtit.2024.2.1491

Abstract — High security solutions are highly important in wireless medical environments, since patient data is confidential, sensitive and must be transmitted over a secure connection. Accordingly, a hybrid encryption method is proposed to ensure data confidentiality (RSA-2048 for key exchange using ACL in SDN with the addition of AES-256-CTR and a hashed secret key for data encryption), and the encrypted data is stored in a private blockchain with the DBFT consensus algorithm to ensure the integrity of data before it being accessed by a doctor's application which decrypts and displays the relevant information. The system was programmed using Python, in an NS3.37 simulator installed on Ubuntu with a MySQL database created using the Apache XAMPP. The product turned out to be a highly secure system for transmitting data from a medical sensor to the doctor's application, offering a throughput of approximately 9 Gbps for both encryption and decryption tasks, while the processing time equaled 0.014 µs per a 128-bit block size for both encryption and decryption, with latency amounting to 0.14 s per 1 KB of data, and the blockchain agreement time equaling 4 ms per 1 KB.

Keywords — blockchain, SDN, SD-WBAN, WBAN

1. Introduction

A wireless body area network (WBAN) is a form of wireless sensor network composed of small biomedical nodes located around, within, or over the surface of the body [1]. Standards applicable to WBAN networks are specified in IEEE 802.15.6 and the solutions of this type are used to meet a variety of applications over a wide range of data rates and with stable short range communication capabilities [2]. In the case of such networks, it is crucial to analyze the data quickly, so that services supporting real-time decision making may be provided. In the majority of actual WBAN use cases, low latency levels must be ensured to monitor the patient's condition [3]. The most recent WBAN developments may be relied upon to improve patient care, optimize monitoring processes, quickly take actionable decisions and lower the overall cost of healthcare systems.

The primary challenges faced in a typical implementation of WBANs focus on security and privacy issues, as sensitive data is transmitted by sensor nodes [4]. Any data breaches could harm the patients' privacy rights and even pose a threat to their lives [5].

Software defined networks (SDN) have become of interest for industrial, academic, and government sectors due to the rapid advances in new technologies and the application of networking techniques. By innovatively separating the control and data planes, this new technology allows to control and manage the network in a programmable manner [6].

SDN architectures are defined by four factors [7]:

- Network devices act as packet forwarding elements without any control-related features, thus separating the control plane from the data plane;
- The choice of the forwarding element is flow-based, meaning that it matches a certain condition in a sequence of instructions carried out by a set of values in the packet field. The Open Flow protocol is utilized with various APIs for communication between different planes in SDN;
- For overall network management, the SDN controller functions as a centralized logical host with an abstract view of the entire network;
- Through programmability, applications running on top of an SDN controller collaborate with the essential data plane components.

SDNs have become highly effective as an alternative to traditional networks due to their flexible and dynamic network management characteristics [8]. The addition of SDN, in particular to WBAN applications, shows promise in terms of overcoming difficulties related to such issues as traffic management, energy efficiency, security, etc., simultaneously improving supervisory control [9]. As medical data has to be transmitted through a secure channel, the need for strong security solutions in the wireless environment rises [10]. WBANs are used in medical applications to monitor and collect data from wearable medical sensors placed on the human body. Therefore, they must deliver healthcare-related data in a highly secure manner.

This paper describes the process of creating a highly secure system meeting the applicable confidentiality, integrity, and availability (CIA) criteria, while simultaneously offering adequate authentication and authorization protections. The proposed model is characterized by all those features as it needs to ensure secure delivery of data from medical sensors to doctor applications, ensuring information security, high throughput rates and short processing times required for on-time data delivery. The key contributions in the field of information security include the following:

1) The public key is generated in the doctor's application, with the use of the RSA-2048 algorithm, to exchange the keys in order to perform mutual authentication. A random

secret key, with the block size of 256, is generated in the patient's device, using SHA-3;

2) An access control list (ACL) protocol-based device MAC address in the SDN controller is applied to control traffic flow and to announce the RSA-2048 public key;
3) Healthcare data encryption is ensured by a symmetric AES-256-CTR algorithm (allowing for efficient parallel processing) with a hashed secret key for data confidentiality;
4) A private blockchain that uses SHA-3 with a block size 256 hash function is used to generate a hash of the collected data, with the blockchain utilizing DBFT consensus algorithms. The private blockchain used to store the encrypted healthcare data ensures data integrity and availability, with a patient ID, the data proper and a time stamp;
5) Blockchain blocks hashed values are encrypted by using AES-128 with master key, and are stored in the database;
6) The encrypted healthcare data, along with the date and time stamp, are stored in the database;
7) Healthcare data is decrypted, using AES-256-CTR with the hashed secret key, in the doctor's application for authorization.

This paper is organized into six sections, with the introduction being the first of them. Section 2 describes the related work, while the information security algorithms used are explained in Section 3. Section 4 introduces the proposed network model and the algorithm combination. Section 5 presents and discusses the results achieved. Finally, conclusions are drawn in Section 6.

2. Related Work

Integration of blockchain with software-defined wireless body area networks (SDWBAN) is a relatively new concept. However, to create an effective architecture for the design and its security features have been taken seriously in the SDN-based WBAN-enabled healthcare system. To achieve this objective, an in-depth study of the field has been conducted, focusing on basic concepts of healthcare data encryption and the integration of SDWBAN systems with a private blockchain.

To safeguard healthcare data in IoT-enabled healthcare infrastructures, an encryption method that employs elliptic curve cryptography with AES was chosen in [11]. The drawback of this approach is small key size, which makes the key space limited.

In paper [12], a WBAN framework asymmetric encryption algorithm is used. Such a method is known as elliptic curve cryptography-based ciphertext-policy attribute-based encryption (CPABE) without bilinear pairing operations. Unfortunately, such a solution requires long processing times while transmitting data. Another WBAN framework relying on a pseudo-randomly generated secure key and stream cipher was proposed in [13] to encrypt the exchanged data, while in [14] a symmetric encryption algorithm AES with blockchain was implemented. The drawback of such methods is the key exchange process. The process of integrating blockchain with a WSN network was also presented in [15].

In article [3], the AES-128 standard is used to encrypt data using blockchain. The proposed methodology creates a hash of the collected data using the SHA-256 bit algorithm and relying on the proof of work (PoW) consensus algorithm. Key exchange vulnerability is one of the main drawbacks of this approach. The proposed blockchain consensus algorithm is characterized by long processing times.

The AES standard is proposed to encrypt the data sensed from an SDN controller in [16]. The data encrypted by the SDN controller is collected by a directly connected sink node, and not by the collecting node, which creates vulnerability-related issues.

3. Security Algorithms Used

The encryption and key distribution techniques employed in wireless networks are crucial for maintaining the confidentiality and integrity of data transfers. Wireless networks use a variety of security techniques [17]:

- RSA (Rivest-Shamir-Adleman) – a public-key encryption method utilized to protect the initial key exchange in wireless network security protocols for secure communication and data exchange through insecure channels (Fig. 1).
- AES (Advanced Encryption Standard) – is widely used in wireless networks for encryption, particularly when combined with RSA. It is a symmetric encryption algorithm that ensures data confidentiality. It consists of four basic functions used in the encryption and decryption processes. The combination of these functions, which are performed multiple times over a specific number of rounds, ensures a high level of security (Fig. 2).

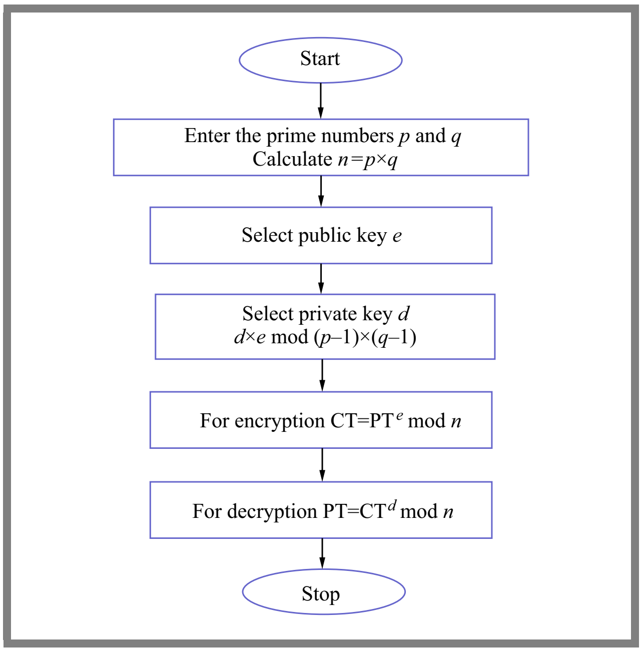

Start
Enter the prime numbers p and q
Calculate $n=p\times q$
Select public key e
Select private key d
$d\times e$ mod $(p-1)\times(q-1)$
For encryption CT=PT^{e} mod n
For decryption PT=CT^{d} mod n
Stop

Fig. 1. RSA algorithm for hashed secret key encryption.

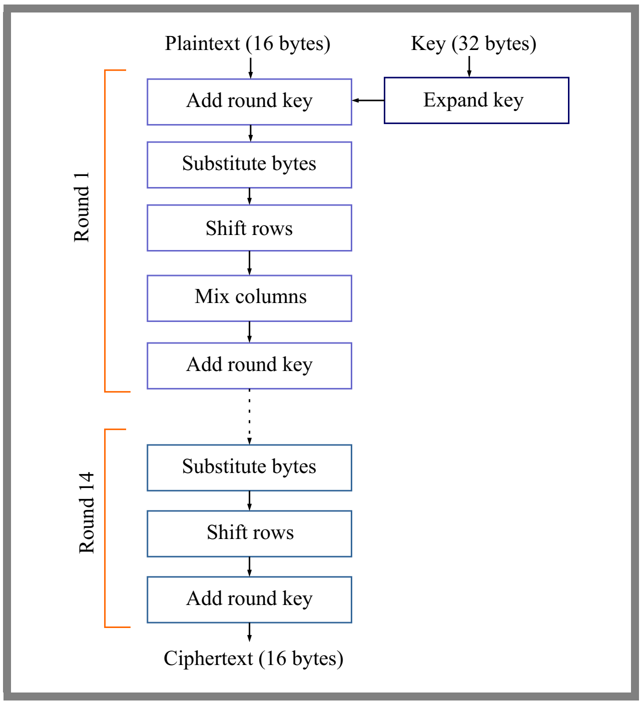


Fig. 2. AES encryption algorithm.

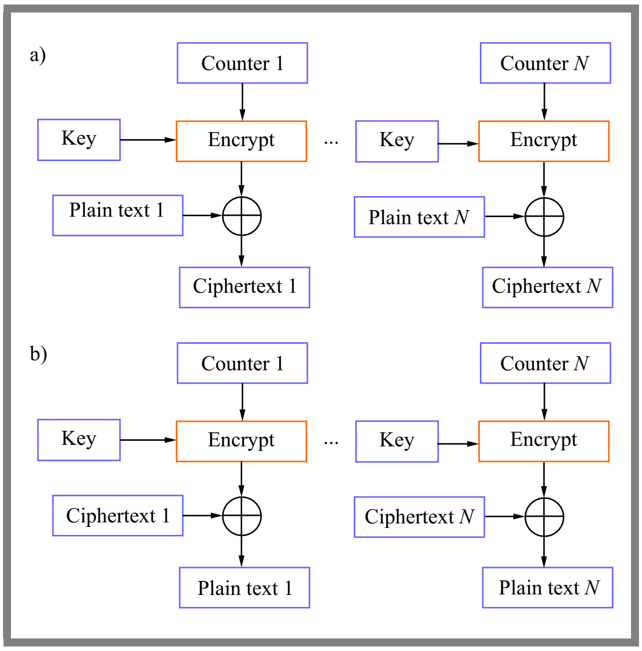


Fig. 3. CTR mode: a) encryption and b) decryption.

- Counter operation mode with AES. The AES is combined with the counter mode in the AES-CTR mode. It considers every data block to be a separate entity, enabling parallelization, effective random access, and ensuring low latency. Each block starts with an increment of the counter value, which is then combined with the nonce to create a special nonce, and is then encrypted using the AES method to create a keystream. The ciphertext is created by XORing this keystream with the plaintext, as shown in Fig. 3.
- SHA-3 (Secure Hash Algorithm 3) – is a cryptographic hash function that is designed to take an input (message) and produce a fixed-size output, which is typically a digest or hash value. The primary purpose of the SHA-3 algorithm is to ensure data integrity and authentication. SHA-3 is known for its strong cryptographic properties, including immunity to collision attacks. It is widely used in security applications, including digital signatures, data integrity verification, and password storage.

4. Proposed Model

The proposed architecture is shown in Fig. 4. It consists of three sensors (temperature, oxygen, and blood pressure). These sensors are connected to a switch network device to collect and transmit the sensing data to the network. Thus, each patient has a switch and multiple sensors located around the surface of the body.

The OpenFlow switch that is connected directly to the SDN controller is used to organize the traffic from the switch to the access point. The controller manages the forwarding of data to the connected network devices. Such an approach allows to scale the network, as the SDN controller is programmable and flexible. It is capable of controlling and managing the network due to the separation of data and control planes, meaning that the controller has a full overview of the network and the devices that are directly connected thereto. An access point is a network device used to integrate the network with the private blockchain. Because the controller is centralized and the blockchain is decentralized, the blockchain can be integrated with a distributed device, such as an access point.

The network was built by using modules in the NS3.37 software, and the security algorithm was added to the network using Python, in NS3.37, on the Ubuntu operating system. NS-3 is a discrete event network simulator and a tool commonly used in researching and developing network communication protocols, examining traffic behaviors and analyzing network systems.

The process we propose is divided into five phases:

1) public key generation, random secret key generation, secret key hashing, and key exchange,
2) healthcare data encryption using a symmetric AES-256-CTR,
3) encrypted healthcare data storage using private blockchain,
4) storage, in a database, of the encrypted healthcare data, patient ID, date and time of collecting data, and the encrypted block hash value,
5) decryption of healthcare data using AES-256-CTR with the hashed secret key, in the doctor's application.

In phase 1, the RSA key pair – as shown in Fig. 1 – with a key size of 2048 bits is generated in the doctor's application. Then, the RSA public key is delivered to the patient switch device (it is sent to the SDN's application plane). In the SDN application, the ACL protocol-based device MAC address is used in the directly connected switch. If the assigned rule matches, then the SDN controller announces the public key

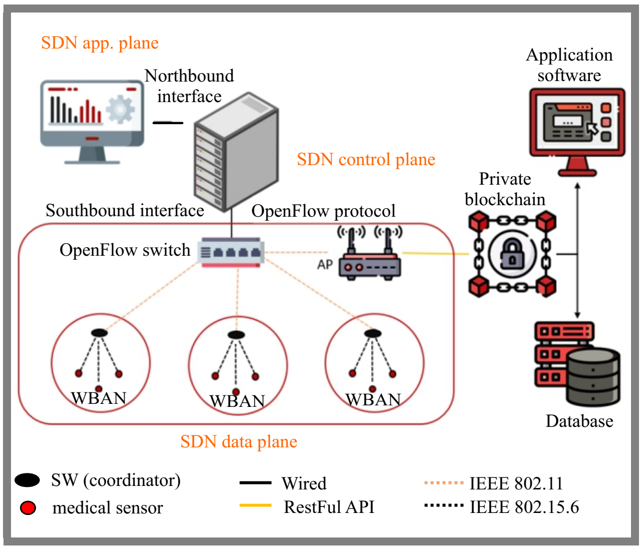


Fig. 4. Healthcare SD WBAN system.

to the device to allow is to access network. Next, a 32-byte random key is generated in each patient switch device and hashes the AES secret key using the SHA-3 algorithm with a hash size of 256 bits. The hashed secret key is sent to the destination using RSA.

These operations ensure mutual authentication between the two parties (the sender's switch and the doctor's application). This shared key can be then used to encrypt and decrypt actual data exchanged between the parties.

Phase two ensures symmetric encryption of the data collected from the patient's sensors using AES-256, as shown in Fig. 2, and CTR mode of operation (Fig. 3a), with a randomly generated nonce and a shared hashed secret key. The resulting encrypted data is stored as a string of integers to facilitate transmission between the parties.

Confidentiality of this operation is ensured by relying on a secure cryptosystem. It needs to be noted that the use of AES with the CTR mode ensures faster execution and reduces complexity, as the same algorithm is used at both ends.

In phase three, the encrypted sensed data, concatenated with the encrypted hashed secret key, is stored in the blockchain with all relevant information, plus the date and time. Private blockchain uses distributed ledger databases that rely on trusted nodes to maintain network integrity. Each block contains a set of transactions or data that are validated by the participating nodes. The blocks are linked together to form a chain, using a cryptographic hash function which creates a unique digital fingerprint of the contents of the previous block. The hash of the previous block serves as a tool to ensure the integrity of the blockchain, thus creating a tamper-evident system. This provides a high level of trust and security.

Additionally, each participant on the network owns a copy of the entire blockchain and can access it at any time. In specific blockchain systems, a consensus mechanism, called delegated byzantine fault tolerance (DBFT), is employed to spread nodes in a distributed network for agreement. It is an adaptation of the byzantine fault tolerance (BFT) consensus method designed for ensuring network efficiency while offering excellent security and scalability.

DBFT provides low latency and quick transaction confirmation times. Because of its efficient and speed-enhancing architecture, it is suitable for applications that need to execute transactions rapidly. With DBFT, a block cannot be reversed or broken after it has been verified and added to the blockchain. This feature is highly important for applications that demand a high level of security and assurance.

In phase 4, a MySQL database (named Patients) was created using Apache XAMPP. Then, a table (named Record) was created. Next, the database table (Record) was connected to the Python code to insert the sensing encrypted data into the table (patient ID, sensing data, time, and date).

The block hash number and the encrypted hashed secret key are linked to the data table. After that, healthcare data is collected as a unified database, with data integrity verified by matching it with the original data documented in the blockchain.

5. Results and Discussion

The model used in the simulation is illustrated in Fig. 5. First, an analysis of the hybrid encryption and decryption approaches is presented. The results are related to a single patient, with the observation period lasting 24 hours. The amount of data transferred depends on how critical the patient's status is. The same results are obtained for each patient, because each patient has a separate switch device.

5.1. Encryption and Decryption Process Parameters

In cryptography, processing time analysis assesses the lead time required for encryption and decryption processes, taking into account a number of variables, such as key size, algorithm, mode of operation and data size. Effective cryptographic designs require that performance restrictions be balanced with security-related needs. The results obtained for the proposed solution are shown in Fig. 6, where encryption and decryption process lead times are presented for AES-CTR with a 128-bit block size. Unlike in other algorithms, in which delays are experienced in the decryption process, in the proposed solution the encryption and decryption process lead times are the same. This stems from the fact that both sides using the encryption algorithm rely on the CTR mode. Due the properties of AES-CTR, the size of the encrypted file is similar to the original, meaning that no overhead data is added during the transmission.

In the field of cryptography, the term throughput describes the rate at which cryptographic operations can be performed or the amount of data that can be processed within a specific time period.

$$Throughput = \frac{Block_{size}}{Total_{time}}\ [\text{bps}]\,. \tag{1}$$

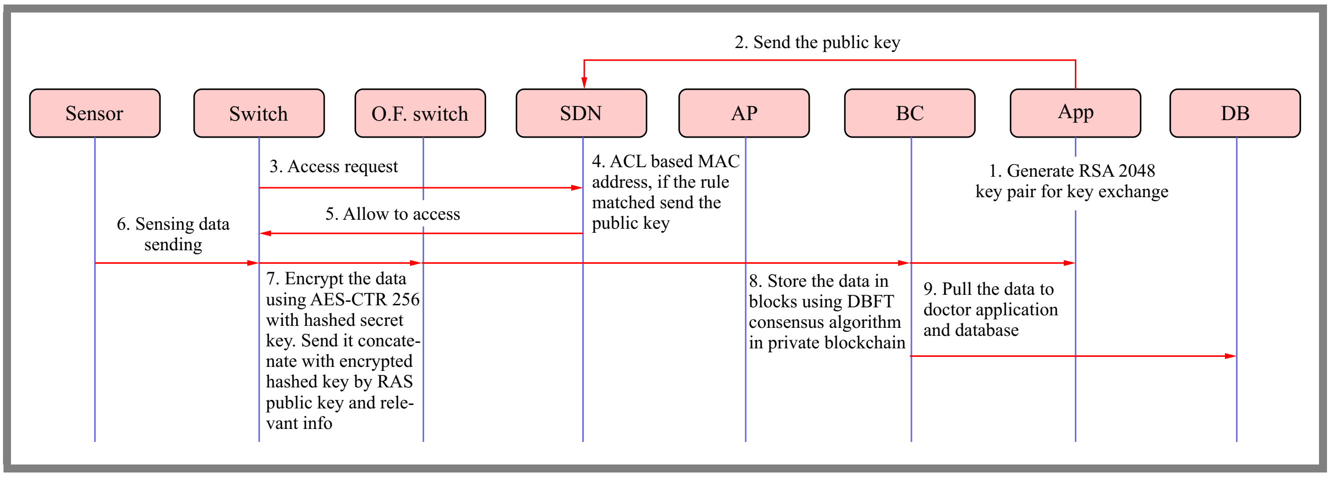

Sensor
Switch
O.F. switch
SDN
AP
BC
App
DB
2. Send the public key
1. Generate RSA 2048 key pair for key exchange
3. Access request
4. ACL based MAC address, if the rule matched send the public key
5. Allow to access
6. Sensing data sending
7. Encrypt the data using AES-CTR 256 with hashed secret key. Send it concatenate with encrypted hashed key by RAS public key and relevant info
8. Store the data in blocks using DBFT consensus algorithm in private blockchain
9. Pull the data to doctor application and database

Fig. 5. Simulation model.

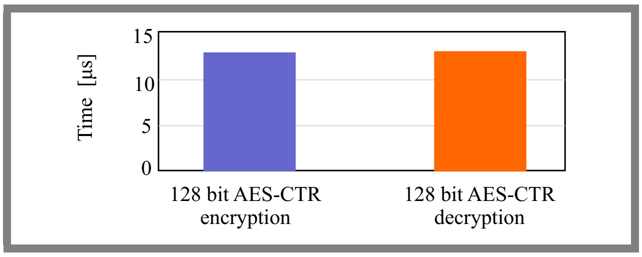


Fig. 6. Comparison of encryption and decryption process lead times.

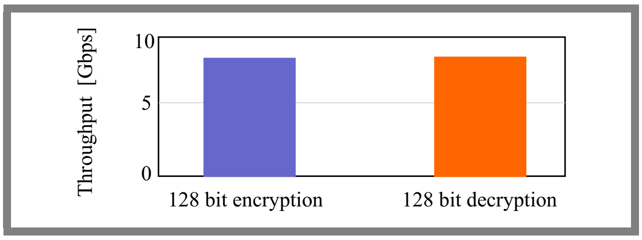


Fig. 7. Encryption and decryption throughput of the proposed system.

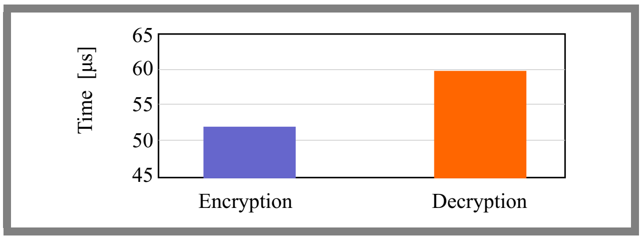


Fig. 8. Key exchange processing times (RSA).

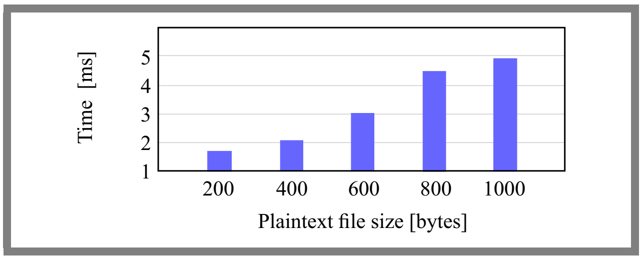


Fig. 9. Blockchain agreement time versus file size.

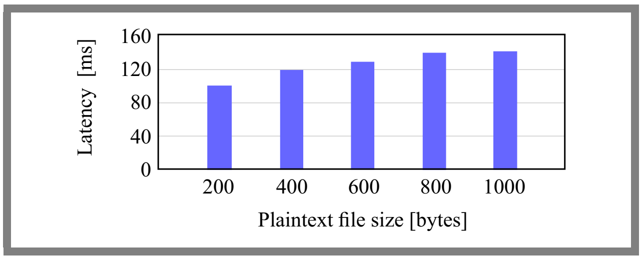


Fig. 10. Latency for different plaintext block sizes.

Encryption throughput is equal to decryption throughput as shown in Fig. 7 because the CTR mode on both sides of the link.

5.2. Key Exchange Processing and Blockchain Agreement Times

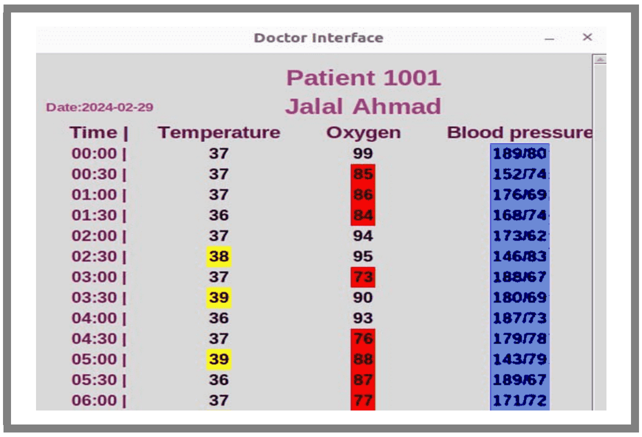
The encryption process lead time is shorter than that required for the decryption phase, as shown in Fig. 8, because the encryption of an original data file of any length (224, 256, 384, 512 bits) of SHA3 algorithm sizes may be performed in one block, without the need to repeat the process to accommodate a higher number of blocks. Meanwhile, the decryption lead time is longer because the size of the ciphertext file is expanded due to the modulus.

As the DBFT process depends on a defined group of delegates rather than on the entire network taking part in the consensus process, the blockchain agreement time is shorter than in other consensus algorithms, including proof of work (PoW).

It needs to be stressed that although DBFT offers quick agreement times shown in Fig. 9, it does so under the premise that the majority of nodes are trusted and that a system exists to deal with malicious nodes.

5.3. Latency

The time passing between the start of an operation and its end is referred to as latency. Latency is crucial for evaluating the effectiveness and quality of communication systems used in cryptography, especially in the case of solutions operating in real-time. The system's total latency L may be considered as a sum of:



Patient 1001
Jalal Ahmad
Date:2024-02-29

Time |	Temperature	Oxygen	Blood pressure
00:00 |	37	99	189/80
00:30 |	37	85	152/74
01:00 |	37	86	176/69
01:30 |	36	84	168/74
02:00 |	37	94	173/62
02:30 |	38	95	146/83
03:00 |	37	73	188/67
03:30 |	39	90	180/69
04:00 |	36	93	187/73
04:30 |	37	76	179/78
05:00 |	39	88	143/79
05:30 |	36	87	189/67
06:00 |	37	77	171/72

Fig. 11. Patient-decrypted data in the application.

Tab. 1. Security characteristics of the proposed solution – comparison with recent works from the literature.

Security aspect	Paper [3]	Paper [16]	Proposed
Confidentiality	●	●	●
Integrity	●	●	●
Availability	×	×	●
Authentication	●	×	●
Authorization	●	×	●

$$L = K + E + BC + D\,. \tag{2}$$

where K is the key generation and exchange lead time, E is the encryption process lead time, i.e. the time it takes to encrypt the data, BC is the blockchain agreements process lead time, and D is the decryption process lead time, i.e. the time it takes to decrypt encrypted data.

The proposed algorithm shows an acceptable latency of approx. 0.1 s in delivering different amounts of data to the application, as shown in Fig. 10.

5.4. Doctor's Application

As a part of this work, an application was developed to view the patient's healthcare data. The software decrypts the data and then displays the log in an easy-to-read form (Fig. 11).

5.5. Security Measurement

To ensure that the system is highly secure, a comprehensive approach needs to be adopted that covers various aspects of security. Although achievement of absolute security is a serious challenge, the best practices described below may significantly enhance the level of security:

- authentication and authorization processes verify user identity and allow to grant the necessary access rights only,
- data encryption protects sensitive data during storage and transmission,

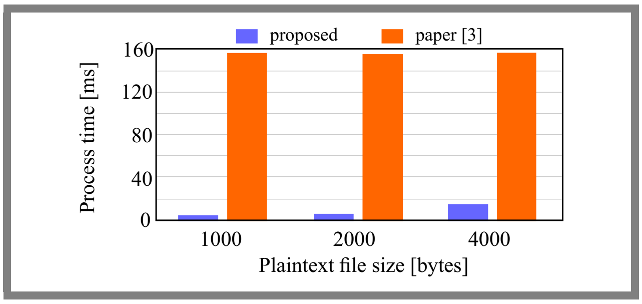


Fig. 12. Time required to generate blocks in blockchain.

- proper patch management practices keep the software and operating systems updated with security patches, thus mitigating the degree of their vulnerability,
- physical security measures prevent physical access to hardware,
- regulatory compliance ensures that the system complies with relevant industry regulations and data protection standards.

In such a context, the proposed SDWBAN system is compared with several systems verified in previous studies, as shown in Tab. 1, to evaluate CIA characteristics of the individual solutions.

In such applications, time is a very important metric, as patient data must be transmitted without any delays. In Fig. 12, a comparison of the time required to generate blocks in blockchain is compared for the proposed solution and the approaches described in other papers. Block generation is a time-consuming process, and the figure below shows that our proposal offers a significant advantage in this respect.

6. Conclusions

WBAN is a new technology and much research is still required to address related challenges inherent to this approach. In this paper, issues related to data delivery have been discussed and some security solutions for WBAN applications have been proposed. The security methods used should be of a comprehensive nature. Therefore, a hybrid encryption method with specific key protection measures is proposed and the entire system is integrated with private blockchain to enable its use in healthcare applications. The approach described in the paper meets the CIA characteristics to ensure information security.

References

[1] B. Abidi, A. Jilbab, and E.H. Mohamed, "Wireless Body Area Networks: A Comprehensive Survey", *Journal of Medical Engineering & Technology*, vol. 44, no. 3, pp. 97–107, 2020 (https://doi.org/10.1080/03091902.2020.1729882).

[2] T. Benmansour, T. Ahmad, S. Moussaoui, and Z. Doukha, "Performance Analyses of the IEEE 802.15.6 Wireless Body Area Network with Heterogeneous Traffic", *Journal of Network and Computer Applications*, vol. 163, 2020 (https://doi.org/10.1016/j.jnca.2020.102651).

[3] K. Hasan, *et al.*, "A Blockchain-based Secure Data-sharing Framework for Software Defined Wireless Body Area Networks", *Computer*

Networks, vol. 211, art. no. 109004, 2022 (https://doi.org/10.1016/j.comnet.2022.109004).

[4] T. Jabeen, H. Ashraf, and A. Ullah, "A Survey on Healthcare Data Security in Wireless Body Area Networks", *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 9841–9854, 2021 (https://doi.org/10.1007/s12652-020-02728-y).

[5] M.S. Hajar, M.O. Al-Kadri, and H.K. Kalutarage, "A Survey on Wireless Body Area Networks: Architecture, Security Challenges and Research Opportunities", *Computers & Security*, vol. 104, art. no. 102211, 2021 (https://doi.org/10.1016/j.cose.2021.102211).

[6] J.C.C. Chica., J.C. Imbachi, and J.F.B. Vega, "Security in SDN: A Comprehensive Survey", *Journal of Network and Computer Applications*, vol. 159, art. no. 102595, 2020 (https://doi.org/10.1016/j.jnca.2020.102595).

[7] D. Kreutz *et al.*, "Software-defined Networking: A Comprehensive Survey", *Proceedings of the IEEE*, vol. 103, pp. 14–76, 2015 (https://doi.org/10.1109/JPROC.2014.2371999).

[8] Y. Meng et al., "SDN-based Security Enforcement Framework for Data Sharing Systems of Smart Healthcare", *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 308–318, 2019 (https://doi.org/10.1109/TNSM.2019.2941214).

[9] K. Hasan *et al.*, "A Novel Framework for Software Defined Wireless Body Area Network", *2018 8th International Conference on Intelligent Systems, Modelling and Simulation (ISMS)*, Kuala Lumpur, Malaysia, 2018 (https://doi.org/10.1109/ISMS.2018.00031).

[10] B. Narwal and A.K. Mohapatra, "A Survey on Security and Authentication in Wireless Body Area Networks", *Journal of Systems Architecture*, vol. 113, art. no. 101883, 2021 (https://doi.org/10.1016/j.sysarc.2020.101883).

[11] S. Das and S. Namasudra, "A Novel Hybrid Encryption Method to Secure Healthcare Data in IoT-enabled Healthcare Infrastructure", *Computers and Electrical Engineering*, vol. 101, art. no. 107991, 2022 (https://doi.org/10.1016/j.compeleceng.2022.10799).

[12] K. Sowjanya and M. Dasgupta, "A Ciphertext-policy Attribute Based Encryption Scheme for Wireless Body Area Networks Based on ECC", *Journal of Information Security and Applications*, vol. 54, art. no. 102559, 2020 (https://doi.org/10.1016/j.jisa.2020.102559).

[13] S. Singh *et al.*, "A GA-based Sustainable and Secure Green Data Communication Method Using IoT-enabled WSN in Healthcare", *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7481–7490, 2022 (https://doi.org/10.1109/JIOT.2021.3108875).

[14] A.E. Guerrero-Sanchez *et al.*, "Blockchain Mechanism and Symmetric Encryption in a Wireless Sensor Network", *Sensors*, vol. 20, no. 10, art. no. 2798, 2020 (https://doi.org/10.3390/s20102798).

[15] H. Benaddi *et al.*, "A Framework to Secure Cluster-header Decision in Wireless Sensor Network Using Blockchain", *Second International Conference, ACOSIS 2019*, Marrakesh, Morocco, 2020 (https://doi.org/10.1007/978-3-030-61143-9_17).

[16] T. Manjunath and A.S. Shobha, "Design & Development of Transmitted & Encrypted Datas Using SDN and Energy Self-healing Concepts Used in RF Energy Harvesting Wireless Sensor Nets", *2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT)*, Kannur, India, 2022 (https://doi.org/10.1109/ICICICT54557.2022.9917923).

[17] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson, 7th ed., 768 p., 2016 (ISBN: 9780134444284).

Zahraa M. Yahya, M.Tech.
College of Information Engineering
https://orcid.org/0009-0006-8218-1619
E-mail: zahraa.mohammad.yk@gmail.com
Al-Nahrain University, Baghdad, Iraq
https://nahrainuniv.edu.iq

Mohammed F. Al-Gailani, Ph.D.
College of Information Engineering
https://orcid.org/0000-0003-4307-941X
E-mail: mf.algailani@nahrainuniv.edu.iq
Al-Nahrain University, Baghdad, Iraq
https://nahrainuniv.edu.iq