A Secure Two Factor Authentication Protocol for Cloud-Assisted Wireless Body Area Network Using Blockchain

[1]Boniface Anjoh Anak George, [2]Chelsea Celestie Anak Bubi John, [3]Elrynna Edora Anak Romeion, [4]Jacellyn Justin, [5]Jacqualine Cristhy Anak Ujil and [6]Jestiny Elnie Anak Edmund Nayong

Faculty of Computer Science and Information Technology, University of Malaysia Sarawak, 94300 Kota Samarahan, Sarawak, Malaysia

email: [1]bonifaceanjoh@gmail.com, [2]chelseacelestie56@gmail.com, [3]elrynna.edora@gmail.com, [4]jacellynjustinjuis@gmail.com, [5]jacqualinecristhy@gmail.com, [6]jestinyelnie@gmail.com

Date received: 24 August 2021
Date accepted: 22 October 2021
Date published: 8 November 2021

Abstract - *The recent advancements in technologies have allowed us to come so far and resulted in many breakthroughs. One of the various examples is internet of things, wireless communication, and cloud computing which can be useful if utilize in many fields. In the field of medical, these advancements allowed any medical centres to improve patient's health remotely simply by using wearable devices on patients that then will amalgamate with the wireless body area network (WBAN). However, WBAN has limited resources which limits its services. To solve this problem, cloud computing is used to provide storage and computation. Unfortunately, these methods allow the system to be vulnerable to various malicious attacks. Attackers can easily gain access to the medical records of patients hence the integrity of security and privacy of confidential data have been compromised. In this paper, we presented a secure protocol for cloud-assisted database using multi-factor authentication and blockchain as an added measure to ensure security. Accordingly, we prove that the presented scheme offers more security and privacy. Therefore, it is the most practical method to be applied in the medical field.*

Keywords: Security, blockchain, multifactor authentication, wireless body area network (WBAN), attack mitigation

1 Introduction

Mutual authentication and specifically multifactor authentication mechanism is not a new research paradigm. Several researchers have proposed several methods to ensure secure authentication mechanisms in any communication protocols (Khan et al., 2021), (Khan et al., 2019), (Maikol et al., 2020), (Khan et al.,2015), (Balan et al., 2018). With its ever-present technologies such as wearable devices, cloud computing, smart sensors, and wireless communication, wireless body area network (WBAN) has been making its name in various fields, including the medical fields. In the field of medicine, the internet of things (IoT) such as wearable devices have allowed doctors to monitor their patients remotely. The wearable devices are used to capture the data of patient's health that, via a public channel, is then forwarded to the medical centre server.

Nonetheless, there is a flaw where adversary attacks such as replay, and impersonation attacks might occur via the general channel. To avoid the integrity of the data from being destroyed, it is best if the patient and server authenticate each other securely. Moreover, the nature of WBAN has limited storage power hence it makes it hard to store a continuous amount of patients' health data in real-time. This is where cloud computing comes in. Its technology comes in handy to amplify the capability of WBAN by offering adequate storage service for

WBAN nodes. This enables the patients to transfer their health information to the cloud server where medical professionals then access the cloud server to make their diagnosis of their patients. This results in an effective and efficient task in using cloud computing with WBAN. Hence, the quality of services provided has seen an improvement by using cloud assisted WBAN.

Despite the fact that the cloud assisted WBAN helps in storing patients' health data in real-time, there is a downside to it caused by the character of wireless communication where the privacy of patients' data and data legitimacy are the prime issues. The security threats are abundant where the data of patients can be easily obtained by an attacker. If the cloud server has been invaded by malicious attackers, they can easily alter, falsify, and eradicate patient's information. This can cause significant difficulty for the patients.

In order to avoid such issues, two-factor authentication can be used to protect patients' health data. Two-factor authentication could be "something you know" (such as passwords), "something you have" (such as cell phone), or "something you are" (such as fingerprints). Furthermore, the integrity of the cloud server can be compromised by attacks from adversaries. In order to curb these security threats caused by the environment of wireless communication, blockchain technology can be used. Blockchain technology is a distributed ledger or database that can be a solution to avoid the privacy and integrity of data from being diminished. Through blockchain, every data is stored in blocks that are then chained together. The blockchain is formed with every activity that is recorded in the ledger, chained with hash values. In the blockchain, every user retains control hence attackers cannot change the data on the blockchain.

Therefore, using two factor authentication and blockchain can mitigate the attacks on the security and privacy of patient's health data. The comparison of security and performance proves that the proposed protocol has a lower computational and authentication overhead. The contributions in this proposed scheme are such as below:

- We present a more secure authentication protocol for a cloud assisted WBAN using blockchain and two factor authentication. The cloud server stores the patients' health information while the blockchain stores the relevant data such as address, hash, and access tree of patients' health information.
- Blockchain is applied to guarantee data security as well as its integrity. Patients create the access structure so that only doctors who meet the criteria can access the patients' health data. In our case, in the presented scheme, consortium blockchain is realised. A consortium blockchain is somehow decentralised since it is governed by several groups of consortium nodes that approve blockchain transactions (Gu et al., 2018). Only authorised nodes in a consortium blockchain can view ledgers as well as submit transactions to the blockchain. The proposed work can be extended to enhance end to end security mechanism in network intrusion detection system or malware detection system (Ahmad et al., 2021), (Dildar et al., 2017), (Khan et al., 2021), (Khan et al., 2017).

2 Related works

Recently, there have been discussed several secure authentication schemes using blockchain and two factor authentication. Son et al., (2020) proposed a secure authentication protocol for a cloud assisted TMIS with access control based on blockchain to address the problem of hostile assaults attempting to carry out different attacks, including as replay and impersonation attacks, through a public channel.

Dwivedi et al., (2019) advocated the use of a blockchain to offer safe healthcare big data administration and analysis. This is to address issues of medical data security and privacy that may arise as a result of a treatment delay.

For smart mobile devices in WBANs, Wang et al., (2018) developed an identity-based rapid authentication system. In an emergency, the method can reduce the time it takes to authenticate a device.

An outline of blockchain architecture is provided by Zheng et al., (2017). They spoke about the most common blockchain consensus algorithms. They demonstrated that blockchain's fundamental properties of decentralisation, persistency, anonymity, and audibility have the potential to revolutionise established industries.

Rawat et al., (2020) gave a comprehensive assessment of Blockchain technology applications and use cases for securing and trusting smart systems. They demonstrated a variety of blockchain types as well as the layout of a typical blockchain chain of blocks.

Azaria et al., (2016) have created working prototypes that use blockchain to manage EMRs (Electronic Medical Record). Patients have full control over their data. Healthcare professionals behave like enticed minors in two ways. Due to the nature of the sensitive nature of these records, they are vulnerable to exploitation by hackers (Azaria et al., 2016).

A study conducted by Al Omar et al., (2017) proposed a model that gives patients complete control over their medical data, and it uses blockchain technology to secure and protect their data.

3 Proposed solution

We present a secure authentication protocol that enables cloud-based WBANs to be authenticated using blockchain. This proposed protocol includes initialization, registration, and authentication. Figure 1 depicts the suggested cloud-assisted blockchain system concept.

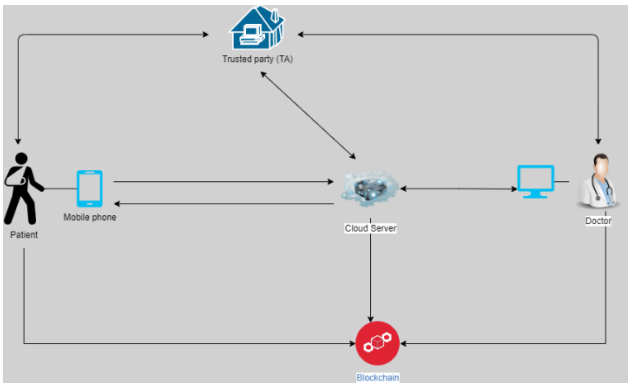

Figure 1. Cloud-assisted system model with blockchain

Detailed descriptions for the entities in **Figure 1** are as below:

- **Trustworthy party (TA)**: TA is a trusted entity that enables patients, doctors, and hospitals to register and gain access to various services and facilities (Wang et al., 2018).
- **Cloud Server**: The capacity of the cloud server is enough to store all the data needed by patients and doctors. However, it can be vulnerable to an attack due to its centralized nature. To prevent the exploitation of the system, patients and doctors should implement a secure cloud storage strategy such as blockchain.
- **Patient**: The patient uses a public channel to send their health data to the cloud. To prevent unauthorized access, the data must be authenticated to the cloud.
- **Doctor**: Doctors should be able to request their patients' health data from the cloud server, and they should be able to obtain data that is relevant to their expertise. TA also assigns attribute keys to each doctor based on their field, location, affiliation, and *etc.* The doctor's identity and attributes are stored on the blockchain after acquiring attribute keys from TA. The doctor can obtain a hash access tree of health information stored on the cloud server by reading the blockchain. The doctor can use the hash of the data to assess if it corrupted after getting the data from the cloud server. The doctor may then decrypt the data and submit the diagnostic results to the cloud server with the use of attribute keys.
- **Blockchain**: The consortium blockchain is made up of health centres and local hospitals. The public key, address, hash, and access tree of the data uploader are all connected to data saved on a cloud server in a blockchain transaction. The Proof-of-Authority (PoA) technique is used by consortium nodes to agree to these transactions. Doctors and patients may access ledgers on the blockchain, and transactions can be sent to the cloud server. Furthermore, the blockchain is used to handle the doctor's identification and attributes. As a result, when a doctor asks data from a cloud server, the blockchain verifies if the doctor's attribute matches the data's access trees. The data is delivered to the doctor by the cloud server if the criteria is satisfied (Wang et al., 2018).

Steps

Below are the steps of the protocol:

i. Initialization

In this phase, the **TA** conducted the system initialization. The **TA** generates an addictive cyclic group and a multiplicative cyclic group with the same order as a bilinear map and generates a secret key of **TA,** a generator, and a hash function. Next, a public key is generated by **TA** and does the computation to generate attribute keys and a bilinear map for decryption. The **TA** then publishes the details and computations results and keeps the secret key of **TA.**

ii. Registration

In order to participate in the network **Patient** and the **cloud server** register to **TA**.

- **Patient registration: The patient** generates the first random number and computes Hash Identity and then transmits the Hash Identity to **TA** securely. Then, in the secure memory **TA** stores the Hash Identity. Then, **TA** sends a smart card with a secret identity to the **Patient** securely. **The patient** generates the second random number and computes Hash Password, A which is the hash of Identity concatenation operation with Password, and XOR operation with the first random number. Other than that, the Hash Password XOR operation with the second random number and Secret Identity of **Patient** XOR operation with the second random number multiply with **Patient**. Next, registration is computed by hashing the concatenation operation between the first random number, second random number, Hash Password, and Secret Identity. The results from all the calculations replace the Secret Identity of the **Patient** in the Smart Card.
- **Cloud server registration: Cloud Server** generates a random number and computes the **Patient** Identity of Cloud Server and sends it with the random number to the **TA** securely. Then, **TA** computes the Identity and Secret key of the **Cloud Server**. After that, **TA** stores the **Patient** Identity of the Cloud Server and the random number, and in the secure memory the Hash Identity is retrieved. Next, **TA** securely sends the Secret Key of **Cloud Server** and Hash Identity to **Cloud Server**. Afterward, the **Cloud Server** computes the Public Key of **Cloud Server**, computes the Verification table, and stores the verification table in the database.

iii. Authentication

In this phase, the authentication between the **Patient** and **Cloud Server** and the establishment of the session key took place.

Step 1: **Patient** inputs their Identity and Password into the Smart Card. Then the Smart Card does computation. Next, the Smart Card checks whether Registration is equal to the value stored in the memory. If it's equal, the **Patient** is successfully logged in to Smart Card.

Step 2: A random secret and current timestamp generated by Smart Card and the public key are calculated. Then it continues to do computation. Thereafter, through a public channel, the message is sent to the **Cloud Server** by the **Patient**.

Step 3: After the **Cloud Server** receives the message from the Smart Card, it validates the received timestamp. If it is valid, the **Cloud Server** computes and compares the result to the value stored in the database. If they are both equal, the **Patient** is registered.

Step 4: Next, **Cloud Server do** computations and check whether the value is equal or not. If it is equal, the authentication of the **Patient** is successful. Next, a random secret and current timestamp is generated by **Cloud Server** and does computation. Thereafter, **Cloud Server** sends the message to the **Patient** via an open channel.

Step 5: The **Patient** first validates the received timestamp after receiving the message. If the timestamp is correct, the **Patient** performs computation. Following that, the **Patient** determines whether the value is equal to the value stored in the database. If they are the same, the session key is established between the **Patient** and the **Cloud Server**.

Blockchain

The blockchain architecture is depicted in depth in **Figure 2**.

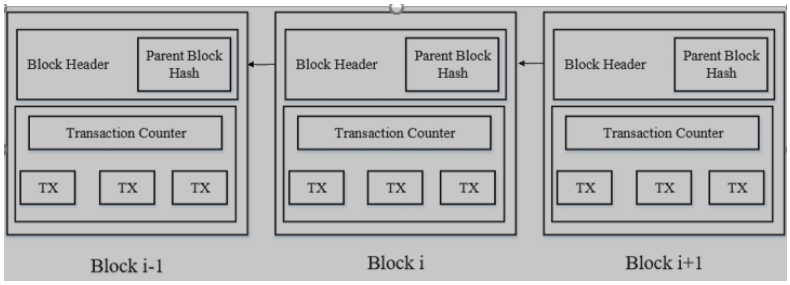

Figure 2. Blockchain with continuous sequence of block

Blockchain is a sequence of blocks that record a full list of transaction data, similar to a typical public ledger (Zheng et al., 2017). **Figure 2** depicts a blockchain as an example. If the block header contains a previous block hash, the block has just one parent block. The hashes of uncle blocks (children of the block's forefathers) would also be saved on the Ethereum network. In a blockchain with no parent blocks, the genesis block is the first block. The internals of blockchain are then thoroughly discussed.

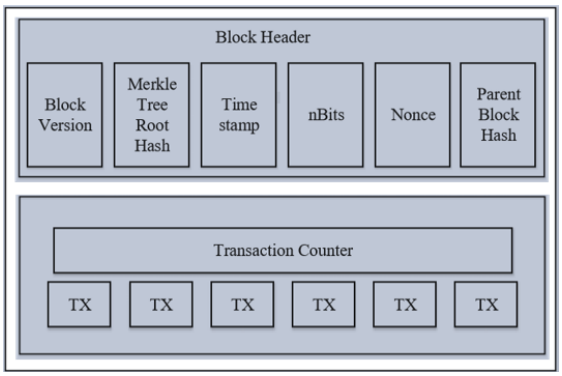

Figure 3. Block structure

As illustrated in **Figure 3**, a block comprises of a block header and a block body. The block header contains the block version, Merkle tree root hash, Timestamp, nBits, Nonce, and Parent block hash. To begin, the block version provides the set of block validation criteria that will be applied. Second, the Merkle tree root hash is the sum of all the transactions in the block's hash values. Since January 1, 1970, the timestamp has been the current time in seconds in universal time. A valid block hash's objective threshold is nBits. Once upon a time, there was a four-byte field that started at 0 and grew with each hash computation. The hash of the parent block is a 256-bit integer that refers to the block preceding it.

4 Security Analysis

We show how the suggested secure authentication protocol resists different threats in this section. Below are the following attacks:

1) **User anonymity**: Except for the Cloud Server and Doctor, user anonymity assures that the user's true identity stays concealed. The attacker must create the Cloud Server's private ket in order to expose the patient's true identity. As a result, the opponent was unable to determine the patient's true identity.

2) **Session key security**: In the proposed secure authentication protocol's authentication phase, the patient and cloud server agree on a shared session key. The session key security is assured to be difficult to crack.

3) **Patient untrace-ability**: To ensure patient untraceability, an attacker must not be able to follow a patient through transmitted communications. The authentication request message in the proposed protocol is based on a random integer. As a consequence, each session's authentication request messages will be unique, preventing the attacker from tracing patients through previous sessions' communications.

4) **Perfect forward secrecy**: An attacker cannot compute the session key since he cannot calculate the Cloud Server's Validation without secret random numbers.

5) **Stolen verifier attack**: For mutual authentication, the cloud server has no information about any patient. As a result, no information can be taken.

6) **Impersonation attack**: An attacker can send an authentication message pretending to be a real patient. To carry off this attack, an attacker must be able to produce a legitimate authentication message. However, because the patient's identity is computed using a secret identification, the attacker cannot construct a lawful patient's identity.

7) **Replay and Man in the Middle (MITM) attacks**: The attacker can receive transmitted messages over a public channel using the assumed model of the proposed protocol, but because every sent message carries a timestamp, the attacker cannot replay or MITM attacks with these messages.

8) **Smart Card stolen attack**: If an attacker acquires or takes a real patient's smart card, the attacker can perform the power analysis attack to extract the smart card's stored value. The attacker, on the other hand, is unable to get any information about the patient, such as the patient's identification (PID) or password (PPW) and is unable to compute the patient's identity in order to create a valid authentication message.

9) **Off-line guessing attack**: An opponent may guess a patient's identity and password at the same time using the stated adversary model. In addition, the attacker can steal the patient's credentials from the smart card and listen in on transmitted communications through a public channel. The adversary, on the other hand, cannot compute the secret key without simultaneously knowing both the right identity and password guesses. As a result, using the recovered hash password, the adversary is unable to validate either the identity or the password.

10) **Privileged-insider attack**: During the Cloud Server registration phase, if the attacker is a privileged insider, the attacker can obtain the patient's hash identity and the Cloud Server's secret key. The cloud server, on the other hand, creates a random number in the session, and the attacker is unable to compute the session key since the attacker is unable to calculate the cloud server's validation without a random number generated by the cloud server.

5 Complexity Analysis

I. Authentication overhead

We compare the authentication overhead with related schemes (Ahmed et al., 2020), (Gope et al., 2019), (Park et al., 2020) during the authentication process. In (Ahmed et al., 2020), the proposed scheme as depicted in **Figure 4** by forcing bilinear pairing and restricting partial blind signatures, a secure connection can be established and the privacy in V2G networks is being protected. As a result, the bilinear pairing process necessitates high computational costs, increasing the load on the V2G network. These protocols, on the other hand, provide an informal approach to security analysis, with the protocol focusing on conceptual issues related to the physical and structural layers of V2G systems. Therefore, a heuristic system is needed for V2G, which cannot only provide powerful capabilities and protect privacy but also resist various attacks.

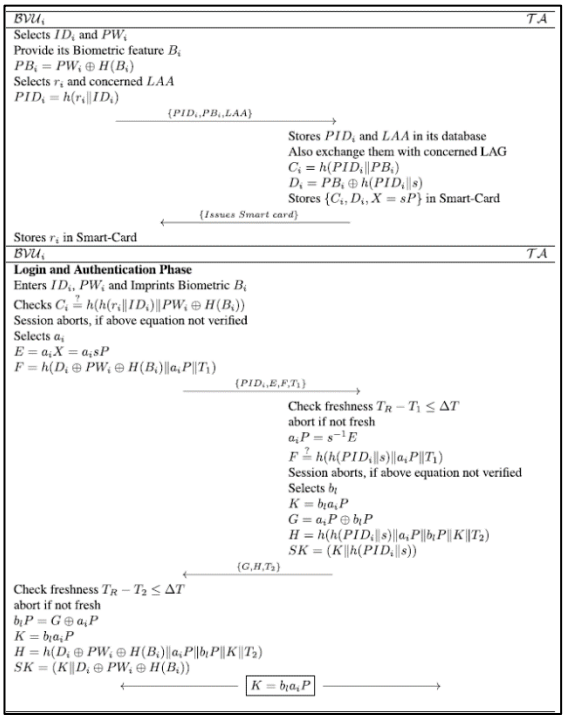

Figure 4. Authentication of Proposed Scheme

In (Gope et al., 2019) the proposed scheme is based on lightweight cryptographic primitives, such as one-way cryptographic hash functions, physical unclonable functions (PUF) (Gope and Quek., 2018), and bitwise exclusive-or operations, and its computational overhead is limited. As a result, it is appropriate for sensing devices with limited resources in IWSN. For example, there is a user U who

wishes to receive real-time data access directly from a specific sensor; in this case, mutual authentication must be performed by the user with both the gateway and the selected sensor node. The mutual authentication and key agreement procedure are elaborated in the following.

According to Vasudev et al (Park et al., 2020), their system guarantees safe message authentication between each entity. However, an MA can get the VS's secret key KVS as well as the symmetric key between each entity. The MA may then create authentication request messages {Ba,Ia,Ga,Ya,Ra} and response messages {EMrply,EMrp,EMrep,EMrpy,EMreply} and effectively achieve message authentication with other entities. As a result, Vasudev et al approach's does not provide secure message authentication. **Figure 5** shows V2V authentication process of IoV-SMAP. A safe message authentication mechanism for IoV communication that addresses the present scheme's security flaws. The IoV-SMAP procedure is divided into three steps:
a) initialization, b) registration, and c) authentication.

Vehicle (V_A)	**Vehicle** (V_E)
Inputs ID_{A_i} and PW_{A_i}	
Computes	
$RID_i = h(ID_{A_i}\|\|PW_{A_i})$	
$RN_i = E_i \oplus h(PW_{A_i}\|\|RID_i)$	
$RPW_i = h(PW_{A_i}\|\|RN_i)$	
$K_{VS} = Q_i \oplus h(RID_i\|\|RPW_i)$	
$W_i = h(RPW_i\|\|K_{VS})$	
Checks $W_i^* \stackrel{?}{=} W_i$	
Generates a random nonce R_1	
and timestamp T_1	
Computes	Checks $\|T_1^* - T_1\| \leq \Delta T$
$M_1 = R_1 \oplus h(K_{VS}\|\|T_1)$	Inputs ID_{E_i} and PW_{E_i}
$M_2 = M_{request1} \oplus h(R_1\|\|K_{VS})$	Computes
$M_{AE} = h(M_{request1}\|\|R_1\|\|K_{VS}\|\|T_1)$	$RN_e = E_e \oplus h(ID_{E_i}\|\|PW_{E_i})$
	$RID_e = h(ID_{E_i}\|\|RN_e)$
$Msg_{V2V1} = \{M_1, M_2, M_{AE}, T_1\}$	$RPW_e = h(PW_{E_i}\|\|RN_e)$
(via public channel)	$K_{VS} = Q_e \oplus h(RID_e\|\|RPW_e)$
	$W_e = h(RPW_e\|\|K_{VS})$
	Checks $W_e^* \stackrel{?}{=} W_e$
	Computes $R_1 = M_1 \oplus h(K_{VS}\|\|T_1)$
	$M_{request1} = M_2 \oplus h(R_1\|\|K_{VS})$
	$M_{AE}^* = h(M_{request1}\|\|R_1\|\|K_{VS}\|\|T_1)$
	Checks $M_{AE}^* \stackrel{?}{=} M_{AE}$
	Generates a random nonce R_2
	and timestamp T_2
	$M_3 = (M_{response1}\|\|R_2) \oplus h(K_{VS}\|\|R_1\|\|T_2)$
	$SK = h(R_1\|\|R_2\|\|K_{VS})$
Checks $\|T_2^* - T_2\| \leq \Delta T$	$M_{EA} = h(M_{response1}\|\|SK\|\|T_2)$
$(M_{response1}\|\|R_2) = M_3 \oplus h(K_{VS}\|\|R_1\|\|T_2)$	$Msg_{V2V2} = \{M_3, M_{EA}, T_2\}$
$SK = h(R_1\|\|R_2\|\|K_{VS})$	(via public channel)
$M_{EA} = h(M_{response1}\|\|SK\|\|T_2)$	
Checks $M_{EA}^* \stackrel{?}{=} M_{EA}$	
Both V_A and V_E store the shared common session key SK	

Figure 5. V2V authentication process of IoV-SMAP

II. Computational overhead

We consider the evaluation of operations on super singular curve y2 + y = x3 + x having embedding degree 4 and use the eta pairing ΔT: E(F2271) × E(F2271) → E(F24.271). In order to analyse the performance of the proposed scheme, we take the following (Kumar and Chand, 2021) cryptographic operations: scalar multiplication on elliptic curve, point addition on elliptic curve, pairing operation on two points on elliptic curve, pairing exponentiation, map-to-point hash function, modular inversion and modular-multiplication operations, which we represented by TSM, TA, TP, TE, TH, TI, and TM, which execution time (ms) 0.304, 0.001, 2.373, 0.297, 0.319, 0.008, and 0.027 respectively.

For evaluating communication overhead, we consider the size of timestamp and identity as 2 B, i.e., $|T|$ = |ID| = 16 b. The proposed protocol has a slightly higher computational overhead than the other scheme. However, when compared to other schemes, the proposed protocol has lower communication costs and higher security.

6 Conclusion

In conclusion, using Blockchain and Two Factor Authentication, we presented a secure protocol for cloud assisted WBAN. The designed protocol made use of blockchain technology to ensure data integrity on the cloud server, as well as a consortium blockchain for scalability and low computing costs. The designed protocol is clearly more secure against different threats such as user anonymity, sensor key security, patient untrace-ability, perfect forward secrecy and many more as shown in Security Analysis. Lastly, this designed approach is more computationally efficient, according to the complexity study.

Acknowledgement

The authors would like to thank Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak to support this research work. This work is carried out as a short-term research-based class project.

References

Khan, A.S., Javed, Y. & Abdullah, J. (2021). "Trust-based lightweight security protocol for device-to-device multihop cellular communication (TLwS)," Journal of Ambient Intelligence and Humanized Computing, 10.1007/s12652-021-02968-6.

Khan, A.S., Balan, K., Javed, Y., Abdullah, J. and Tarmizi, S. (2019). Secure trust-based blockchain architecture to prevent attacks in VANET. Sensors (Switzerland), 19(22), 1.

Maikol, S. O., Khan, A. S., Javed, Y., Bunsu, A. L. A. & Petrus, C. (2020). "A novel authentication and key agreement scheme for countering MITM and impersonation attack in medical facilities," International Journal of Integrated Engineering, vol. 13, no. 2, pp. 127-135, 2020.

Khan, A. S.; Lenando, H.; Abdullah, J.; Fisal, N. (2015). Secure authentication and key management protocols for mobile multihop WiMAX networks. Jurnal Teknologi, 73(1), 75–81.

Balan, K., Khan, A. S., Julaihi, A. A., Tarmizi, S. & Pillay, K. S. (2018). RSSI and Public Key Infrastructure based Secure Communication in Autonomous Vehicular Networks, International Journal of Advanced Computer Science and Applications (IJACSA) Volume 9 No 12 December 2018; pp. 298-304

Ahmad, Z., A. S. Khan, Shiang, C. W., Abdullah, J. & Ahmad, F. (2021). "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging Telecommunications Technologies, vol. 32 no.1, pp. e4150, 2021, 10.1002/ett.4150.

Dildar, M. S., Khan, J. B., Abdullah, J. & Khan, A. S. (2017). "Effective way to defend the hypervisor attacks in cloud computing," 2nd International Conference on Anti-Cyber Crimes (ICACC), pp. 154-159, 2017, 10.1109/Anti-Cybercrime.2017.7905282.

Khan, A.S.; Ahmad, Z.; Abdullah, J. & Ahmad, F. A. (2021). Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network, IEEE Access, 2021, 9, 87079–87093.

Khan, N., Abdullah, J. & Khan, A.S. (2017). Defending malicious script attacks using machine learning classifiers, Wireless Communications and Mobile Computing, vol. 2017; doi:10.1155/2017/5360472

Son, S., Lee, J., Kim, M., Yu, S., Das, A. K., & Park, Y. (2020). Design of Secure Authentication Protocol for Cloud-Assisted Telecare Medical Information System Using Blockchain. IEEE Access, 8, 192177–192191. https://doi.org/10.1109/access.2020.3032680

Dwivedi, A., Srivastava, G., Dhar, S., & Singh, R. (2019). A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. Sensors, 19(2), 326. https://doi.org/10.3390/s19020326

Wang, C., Zheng, W., Ji, S., Liu, Q., & Wang, A. (2018). Identity-Based Fast Authentication Scheme for Smart Mobile Devices in Body Area Networks. Wireless Communications and Mobile Computing, 2018, 1–7. https://doi.org/10.1155/2018/4028196

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 IEEE International Congress on Big Data (BigData Congress). https://doi.org/10.1109/bigdatacongress.2017.85

B. Rawat, D., Chaudhary, V., & Doku, R. (2020). Blockchain Technology: Emerging Applications and Use Cases for Secure and Trustworthy Smart Systems. Journal of Cybersecurity and Privacy, 1(1), 4–18. https://doi.org/10.3390/jcp1010002

Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management. 2016 2nd International Conference on Open and Big Data (OBD). https://doi.org/10.1109/obd.2016.11

Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). MediBchain: A Blockchain Based Privacy Preserving Platform for Healthcare Data. Security, Privacy, and Anonymity in Computation, Communication, and Storage, 534–543. https://doi.org/10.1007/978-3-319-72395-2_49

Gu, J., Sun, B., Du, X., Wang, J., Zhuang, Y., & Wang, Z. (2018). Consortium Blockchain-Based Malware Detection in Mobile Devices. IEEE Access, 6, 12118–12128. https://doi.org/10.1109/access.2018.2805783

Ahmed, S., Kumari, S., Saleem, M. A., Agarwal, K., Mahmood, K., & Yang, M. H. (2020). Anonymous Key-Agreement Protocol for V2G Environment Within Social Internet of Vehicles. IEEE Access, 8, 119829–119839. https://doi.org/10.1109/access.2020.3003298

Gope, P., Das, A. K., Kumar, N., & Cheng, Y. (2019). Lightweight and Physically Secure Anonymous Mutual Authentication Protocol for Real-Time Data Access in Industrial Wireless Sensor Networks. IEEE Transactions on Industrial Informatics, 15(9), 4957–4968. https://doi.org/10.1109/tii.2019.2895030

Yu, S., Lee, J., Park, K., Das, A. K., & Park, Y. (2020). IoV-SMAP: Secure and Efficient Message Authentication Protocol for IoV in Smart City Environment. IEEE Access, 8, 167875–167886. https://doi.org/10.1109/access.2020.3022778

Kim, M., Yu, S., Lee, J., Park, Y., & Park, Y. (2020). Design of Secure Protocol for Cloud-Assisted Electronic Health Record System Using Blockchain. Sensors (Basel, Switzerland), 20(10), 2913. https://doi.org/10.3390/s20102913

Jabeen, T., Ashraf, H., & Ullah, A. (2021). A survey on healthcare data security in wireless body area networks. Journal of ambient intelligence and humanized computing, 1–14. Advance online publication. https://doi.org/10.1007/s12652-020-02728-y

Singh, S. & Singh, N. (2016). "Blockchain: Future of financial and cyber security," 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), 2016, pp. 463-467, doi: 10.1109/IC3I.2016.7918009.

Konan, M., & Wang, W. (2019). A Secure Mutual Batch Authentication Scheme for Patient Data Privacy Preserving in WBAN. Sensors (Basel, Switzerland), 19(7), 1608. https://doi.org/10.3390/s19071608

Wang, D., Zhao, J. & Wang, Y. (2020). A Survey on Privacy Protection of Blockchain: The Technology and Application. IEEE Access, 99, 1-1. https://doi.org/10.1109/access.2020.2994294

Gope, J. Lee & Quek, T. Q. S. (2018). Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions, IEEE Trans. Inf. Forensics Security, vol. 13, no. 11, pp. 2831-2843. https://hull-repository.worktribe.com/OutputFile/893520

Kumar, M., & Chand, S. (2021). A lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network. IEEE Systems Journal, 15(2), 2779–2786. https://doi.org/10.1109/jsyst.2020.2990749