IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

A Novel Linearly Complex Extended Signed Response-Based Node Authentication Scheme for Internet of Medical Things

MUHAMMAD SAUD KHAN[1], MUHAMMAD SARDARAZ [2], MUHAMMAD TAHIR[2], ABDULLAH ALOURANI[3]

[1]Department of Computer Science, Air University Aerospace and Aviation Campus, Kamra 43570, Pakistan;
[2]Department of Computer Science, COMSATS University Islamabad, Attock Campus 43600, Pakistan;
[3]Department of Management Information Systems, College of Business and Economics, Qassim University, Buraydah 51452, Saudi Arabia;

Corresponding author: Abdullah Alourani (e-mail: ab.alourani@qu.edu.sa)

ABSTRACT The Internet of Things (IoT) is considered the future of the Internet due to its immense potential. It has captured the interest of researchers who are exploring new possibilities in this field. Unlike the current internet structure, IoT involves the connection of billions of devices and entails a significant exchange of data, diverse traffic, and resource availability. The increasing use of IoT devices in vulnerable environments has presented two major challenges for researchers: authenticating sensor nodes and ensuring secure data routing. These challenges become more difficult by the presence of wireless sensors in communication devices, where all devices are not authenticated or have up-to-date software. Among the various IoT attacks, the Sybil attack poses a significant threat to the network. Consequently, the conventional solutions used for conventional wireless networks (CWN) do not apply to wireless sensor networks due to the differences in algorithms and associated costs in terms of processing and power consumption. To address these challenges, an extended signed response-based (ESRES) solution is proposed. The proposed framework utilizes a pre-distributed key embedded in a sensor node, while the authentication process employs a dual key-based algorithm with linear complexity. In this mechanism, the node uses pre-distributed keys to respond to a random challenge number sent by the server or sink, thus proving its legitimacy. Since there are different types of IoT networks, such as hierarchical and centralized structures, the proposed authentication scheme is designed to be flexible and implementable for both types. The performance of the proposed framework is analyzed and evaluated, considering the probability of attack detection with different authentication key pool sizes for the parameters i.e., processing overhead, probability, and power consumption.

INDEX TERMS IoT, Big Data, Wireless Network, Energy Efficiency, Algorithm

I. INTRODUCTION

THE world has witnessed a tremendous use of internet-based ubiquitous technology widely known as the Internet of Things (IoT). The role of IoT technology has become vital in the past two decades in daily life. It describes the physical objects with sensor nodes, processing, transmission abilities, software combinations, etc. to connect and exchange data with each other using the Internet or other communication platforms [1].

The IoT is a paradigm shift in the current era of cyberspace in which all the nodes that are concerned with any domain are connected and share their data for onward analysis. Rapid expansion in recent years has been observed in the worldwide market for IoT [2]. The revenue of IoT is anticipated to increase from 892 billion to more than 4 trillion USD by 2025 [3]. The application of IoT has enabled us not only to track resources but also to take care of and manage various domains like businesses, industries, diagnostic stations, hospitals, etc. IoT applications in healthcare known as the Internet of Medical Things (IoMT) can precisely monitor the

movement of people, equipment, specimens, and supplies as shown in Fig 1.

The IoMT is becoming a vital scientific development in health care that is focused on acquiring the respective patient's information through integrated devices that communicate with other resources for better treatment. They can effectively cater to a wide range of stakeholders, such as hospitals, diagnostic centers, nursing homes, and communities, enabling them to analyze the collected data [4]. The sensors are used to get accurate and quick information from targeted resources like patients or machines etc. in the hospital. Similarly, the devices in IoT can also be used to detect and prevent the prohibited activities of patients, monitoring various conditions like cardiac pattern, pulse, sugar level, oxygen, etc., and analyzing it under respective disease [5]. Nowadays smart healthcare systems are fully connected to technically advanced medical wearable devices. The respective patient data and other records can easily be transmitted over the Internet. Cloud and other large-scale storage facilities enabled the IoT to store this information over the servers by hospitals and other healthcare departments for quick access [6]–[8]. These records are also shared with other professionals and research communities to perform effective diagnoses and quick decisions ensuring the privacy and security of data [9]–[11]. Moreover, some of the IoMT vulnerabilities will lead to health disasters, while others will result in loss of data and a deficit of trust. For all these reasons, the research community has focused on designing authentication techniques for ensuring security in a resource-constrained heterogeneous IoMT environment [12]. Medical records are considered highly sensitive and intrusive. In many countries, patients do not like their medical or health-related records to be leaked or shared without consent. Thus, there comes a huge responsibility for data protection along with the ease in IoMT. The research and industry communities have developed cyber security standards to ensure the integrity and privacy of patient data, however, still there is a need for improvement [13], [17], [18].

The purpose of this research is to design a framework that prevents the nodes from attacks like Sybil, spoofing, etc. Initially, the target is focused on the Sybil attack. The reason we chose the Sybil attack is twofold. First, it is the most widely launched attack and remains a hot topic among research communities. Second, the selection of Sybil attack is to extend the simplicity and easy comprehension for the reader otherwise the proposed authentication protocol can be used to counter any authentication-based attack. From extensive simulations, we have proved that the proposed model is not only capable of defending against the Sybil attack but also poses less processing overhead resulting in a comparatively longer network life. The paper is organized as follows.

Section 2 presents the literature review followed by the proposed scheme in Section 3. Section 4 presents experimental setup, attack model, and defense strategy. Section 5 represents the results discussion and finally, the article is concluded with section 6.

II. RELATED WORK

There exists strong literature on security and authentication in IoT. Mostly, the security techniques are based on asymmetric and symmetric distributed keys to achieve the desired security goals. However, the maintenance and distribution of these public or private keys is a challenging task [12], [13]. The research community has introduced other key generation mechanisms such as elliptical cure, logistic curve permutation, etc. that can be coupled to generate cryptographic mechanisms [14].

Similarly, A blend of stenography and cryptography for secure transmission of patient information over the network is also used where the authors used bitwise XOR and Modified Jamal Encryption Algorithm (MJEA) to extend security and robustness [15]. Secure image-sharing technique that utilizes pixel adjustment by applying optimal pixel adjustment for image quality improvement under various payload capacities and authentication hits has also been used [16]. This section presents discussion of relevant methods including comparative analysis of different methods.

A cryptography-based solution is represented in [19]. The authors claim the integrity of data by symmetric and public key encryption along with the blowfish algorithm. In [20], the authors proposed a framework to achieve a secure, efficient, and fast transmission mechanism for data acquisition from ECG connected to Wireless Body Area Network (WBAN). The proposed scheme utilizes the combination of modified Set Partitioning in hierarchical trees encryption and the Quasigroup compression techniques which integrate error bits and the absolute zero tree concept in Quasigroup compression to achieve more security. The authors in [21] proposed a lightweight, anonymous user authentication protocol for IoT-based healthcare applications, using hash functions and XOR operations to ensure computational efficiency. The protocol secures real-time health monitoring by allowing only registered users to access IoT nodes, protecting against attacks like impersonation, replay, and denial of service (DoS). The strength of the protocol lies in its low computational and communication costs, robust security features, and preservation of user anonymity. In [22] the author proposed a solution known as Health Care Framework for Patient Privacy (HCPP) that addresses several security concerns like authentication, authorization, data access control, integrity, accountability, etc. The proposed scheme uses SSE and PEKS for data security. Moreover, the proposed scheme also utilizes Identified-cased cryptography to assign an identity to each targeted patient. The scheme also provides a solution for emergencies and response. The authors in [23] proposed a two-factor authentication scheme based on the elliptic curve cryptosystem, ensuring user anonymity, unlinkability, and forward secrecy. Although the proposed scheme has robust security and efficiency. The scheme relies on elliptic curve cryptography that leads to more computational resources compared to simpler schemes. Similarly, the authors in [24] proposed a scheme used to provide data security and authentication assurance. Region of Interest (ROI)-based watermarking se-

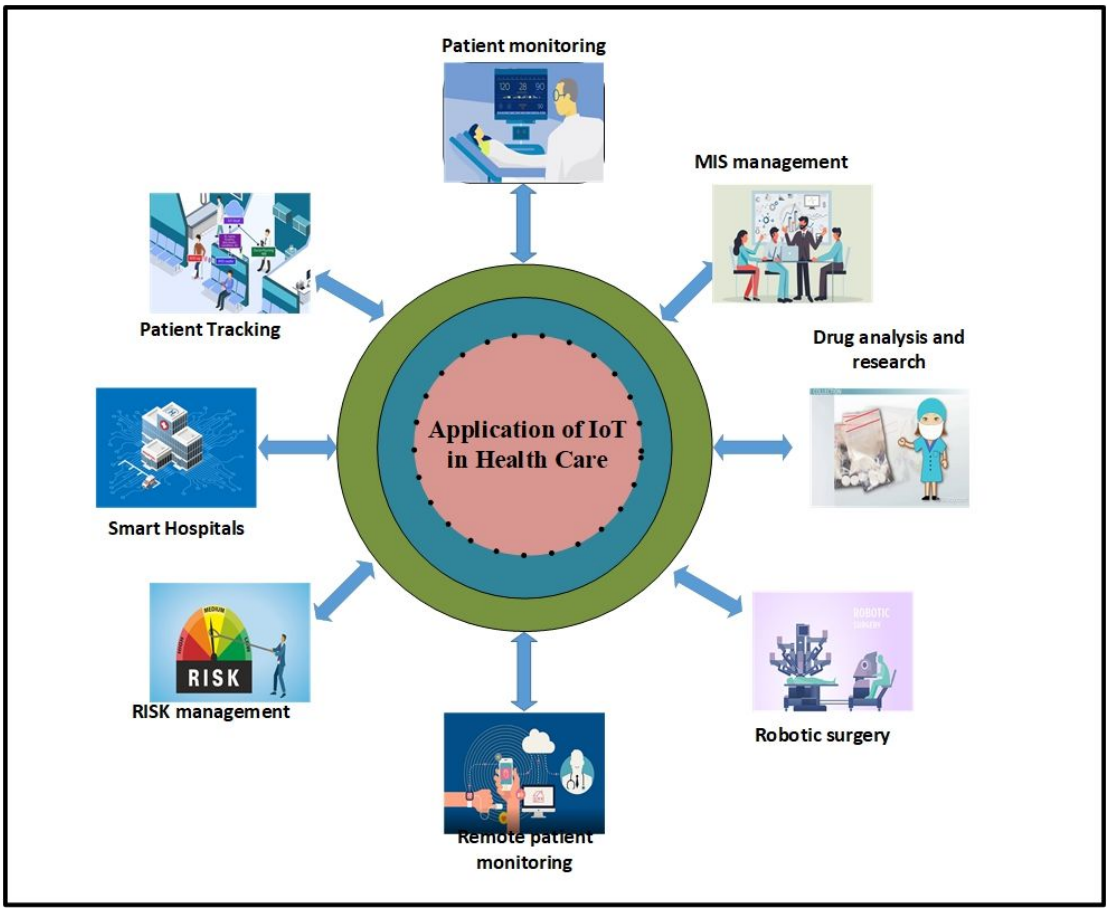

FIGURE 1. Some Applications of IoMT.

curity scheme is proposed in [25]. The proposed scheme also utilizes Discrete Wavelet Transform (DWT) to enhance data security. The authors in [27] proposed a cloud-based secure healthcare and prediction system. The proposed system acts like a line intelligent doctor which provides a solution to the user based on their symptoms. To achieve the confidentiality of transmitted data, the details are encrypted with a password-based encryption scheme. The proposed scheme also uses MD5 hashing algorithm to enhance the security of data. Similarly the authors in [28] proposed a secure framework for medical imaging. The scheme uses a 2D Zaslavski map and DNA cryptography which has two phases. In the initial phase, the pixels or the images are permuted whereas in the second phase, a combination of 2-D Zaslavski map and DNA encryption is applied.

The authors of [29] proposed a mutual authentication scheme for IoT systems. The scheme is based on the lightweight features of Constrained Application Protocol (CoAP) applied as application layer protocol for the communication following a client-server architecture. The secure communication channel is provided by the advantage of Advanced Encryption Standard (AES) cipher. Both the client and the server challenge each other for mutual authentication by encrypting a payload from the message of size 256 bits, and then exchanging payloads for verification. The authentication is done during the request-response interaction without the use of extra layers which increases the communication and computation cost.

Researchers in [30] proposed an authentication and key establishment protocol for Industrial IoT (IIoT) along with the integration with the 6TiSCH framework. The proposed protocol addresses the challenges of pre-shared keys by using certificates for node authentication and a consensus-based approach. The article proposes a robust environment against attacks, efficient performance in terms of communication, latency, and energy consumption, and suitability for constrained devices. However, the proposed mechanism incurs additional message exchanges, leading to increased latency and energy use. In [31], the authors proposed a biometric-based system to authenticate and preserve the confidentiality of medical and patient information. A heartbeat-based biometric system is proposed in [32] using local minutiae feature of the fingerprints matching algorithm for user authentication. The proposed scheme involves ECG signals and SVM which are passed through wavelet-based preprocessing model. Another heartbeat biometric-based au-

thentication system is presented in [33] which also uses Cascaded PCA Network (CPCAnet). The solution is evaluated on the PTB ECG pre-trained models to check its efficiency on various parameters. The scheme is compared with similar systems such as auto-encoder (AE), extreme learning machine (ELM), and ensemble extreme learning machine (EELM).

Moreover, the authors in [34] devised a technique based on Compressive Sensing (CS) and Fast Discrete Curvelet Transform (FDCT). The proposed technique uses fingerprint images and watermarks for data security and integrity. A healthcare system based on cryptographic algorithm and Fingerprint biometrics is proposed in [35]. The authors in [36] proposed an encryption-based solution for live monitoring of the health condition of a patient. The proposed system monitors the temperature, heart rate, pulse rate, and blood pressure through the sensor mounted on the body of the patient. The author [37] used biometrics and keystroke patterns for authentication to access medical data for onward processing. The authors proved that the use of two biometrics helps to prevent a large number of attacks despite the increase in complexity of an algorithm. The data is secured, transmitted, and tunneled through protocols such as Secure Socket Layer (SSL) and Ethernet over IP, etc. Blockchain is also considered the most recent technology which uses blocks like structure [38], [39]. It is responsible for maintaining the transactions and grouping them in blocks which are maintained in chronological order. With the introduction of blockchain, the need for a third party to handle financial and transactional matters is eliminated [40], [41]. After the success of Bitcoin and similar cryptocurrencies, the blockchain also attracted the research community of health sciences for keeping the data secure and maintaining its integrity [42]. A blockchain-based model for the storage of medical records over the cloud is presented in [43], [44]. Since cloud storage comes with the cost of trust over service providers, blockchain is used to overcome possible threats. The medical data is initially converted into fragments and then an encryption algorithm is applied before it is stored in the nodes.

The authors in [45] proposed a blockchain-based solution for the exchange of medical records over the Internet to prevent them from being tampered with or lost. The proposed scheme uses data masking and an interplanetary file system along with hash functions to enhance the security of data. Another blockchain and incentive mechanism-based model is presented in [46]. In [47], a blockchain-based solution is proposed for the protection of MRI images during its exchange between the hospitals. Similarly, the authors in [48] proposed a secure scheme known as tamper-resistant mHealth system using blockchain technology. The proposed scheme ensures audit of transactions in decentralized communication systems. In [49], the authors designed a smartphone application for the patients of Cognitive Behavioral Therapy for insomnia (CBTi). The gathered data and local analysis performed by the application are sent to a server for further decisions. The scheme uses Practical Byzantine Fault Tolerance (PBFT) to prevent the data from being tempered. Table 1 shows comparative analysis of the proposed framework with existing solutions.

Algorithm 1: Pseudo code for ESRES Generation and Verification

```
Generate 128-bit RAND, send to node.
ESRES Generation at Node
Function gen_signed_res(RAND, Ki):
    for i = 0 to 63 do
        key1[i] = RAND[i] XOR Ki[i+64]
    end for
    for i = 0 to 31 do
        key2[i] = key1[i] XOR key1[i+32]
    end for
    for i = 0 to 15 do
        key3[i] = key2[i] XOR key2[i+16]
    end for
return
Function expansion_box(key3):
    Expand key3 to 48-bit
return
Function compare_responses(server_response,
 node_response):
    server_response == node_response
return
Function main():
    RAND = generate_128_bit_random_number()
    send_to_node RAND
    Ki = get_pre_distributed_key()
    node_res = GEN_SIGNED_RES(RAND, Ki)
    server_res = GEN_SIGNED_RES(RAND, Ki)
    res=COMPARE_RESPONSES(server_res,
     received_res)
    if res==true then
        print("Authentication successful.")
    else
        print("This is a Sybil node.")
    end if
return
```

III. PROPOSED SCHEME

A multitude of attacks targeting healthcare systems through IoT exist, each with its own objective, such as system degradation or data acquisition. Among these attacks, Sybil is commonly employed in the context of Internet of Medical Things (IoMT). In a Sybil attack, a malicious node generates multiple identities within the network to deceive other nodes and gain network access. Once integrated into the network, the Sybil node can obtain all routing information and transmit data to the base station. Thus, there is a need for

TABLE 1. A comparative analysis of proposed scheme with current solutions.

Reference	Layer	Process Type	Strength, Weakness
Proposed Scheme	P	XOR,ESRES	(+) Implemented at MAC layer and target the registers directly.No application layer overhead. The perturbation at various levels adds exponential complexity for attacker. Feasible for low-cost sensor nodes with low memory and processing power.
14	A	elliptical and logistic curve	(+) Strong in cryptographic efficiency and security, (-) Complex to implement on small scaled IoT devices.
15	A	RIWT, DCT, SVD	(+) The method is robust and secure, leveraging RIWT, DCT, and SVD to enhance imperceptibility and resistance to attacks. (-) increase complexity and computational demands. (-) The method's effectiveness might be limited to the specific contexts tested, such as the UCID database
18	A	Steganography	(+) Genetic algorithms, while powerful, can be computationally intensive, especially for high-dimensional image data.. (-) The paper did not fully address the robustness of the steganographic scheme against various attacks, such as steganalysis or data corruption
21	A	Elliptic Curve	(+) Robust security and efficiency, though its reliance on elliptic curve cryptography.. (-) May require more computational resources compared to simpler schemes
27	A	AES, Diffie-Helman	(+) +Two separate servers for storing cryptography and authentication data. (+) Resistance to brute force, timing, and MITM -No performance analysis is done.
28	A	census-based authentication	(+) Robustness against attacks, efficient performance in terms of communication, latency, and energy consumption, and suitability for constrained devices. (-) (-) Incurs additional message exchanges, leading to increased latency and energy use.

a secure framework that can address the problem in a way that consumes less energy and keeps the complexity level low. It is a fact that the attack mechanisms and the devices used for this purpose are strong enough to break any weak secure mechanism in general, therefore a one-tier security framework (like authentication only) may not be sufficient to counter the attacks.

This research aims to devise a security framework to design an energy-efficient framework to ensure node authentication. The proposed solution is the extension of research work done in [50] which is inspired by the node authentication scheme used by GSM. The proposed scheme known as Extended Signed Response (ESRES) uses a linearly complex challenge-response procedure to ensure a secure node authentication process. The ESRES starts the process by using a random number sent as a challenge by the sink node or server and a pre-distributed key Ki to produce 32 and extended 48 bits signed after applying A3 and extension procedures respectively. Keeping in view the current processing capability of attacking nodes, we modified the originally signed response and expanded it to 48 bits to maximize the complexity for attacking nodes by keeping the energy consumption low. ESRES is evaluated to prove its strength and improved capabilities. The detailed working of A3 algorithm is discussed below:

- The 128-bits challenge RAND is passed to the node and is converted into LHS and RHS
- The pre-distributed key Kc is divided into LHS and RHS.
- The XoR operation is initiated. The bits from LHS of Kc is XoRed with the RHS of RAND and produce a 128 bit result.
- In next step, the 128 bits result is again divided into RHS and LHS. XOR Operation is again performed between the bits of LHS and RHS of same bit stream which produces a 64 bit result.
- This 64 bit result is again divided into RHS and LHS of 32 bit each and again XoR operation is performed resulting a 32 bit Signed Response.
- Apply Expansion process to extend the 32-bits stream to 48 bits as a last step of algorithm.

The ESRES can be used centralized and in ad-hoc situations. Fig 2 explains the overall Signed Response generation process. The node authentication procedure is summarized as below:

- The node receives a random number broadcast from the source (a cluster head, sink or neighbor node). Since every node is equipped with a MAC address and pre-distributed key ki therefore any of the MAC or the Ki can be used depending upon the implementation..
- The node executes the ESRES algorithm to produce the response as explained in Figure 2.
- The source node also executes the same procedure to produce a response for correlation.
- Upon the reception of a 48-bit response from the node, the source node compares both values.
- If both values are correlated, the node is authenticated and allowed to become part of a network otherwise, the

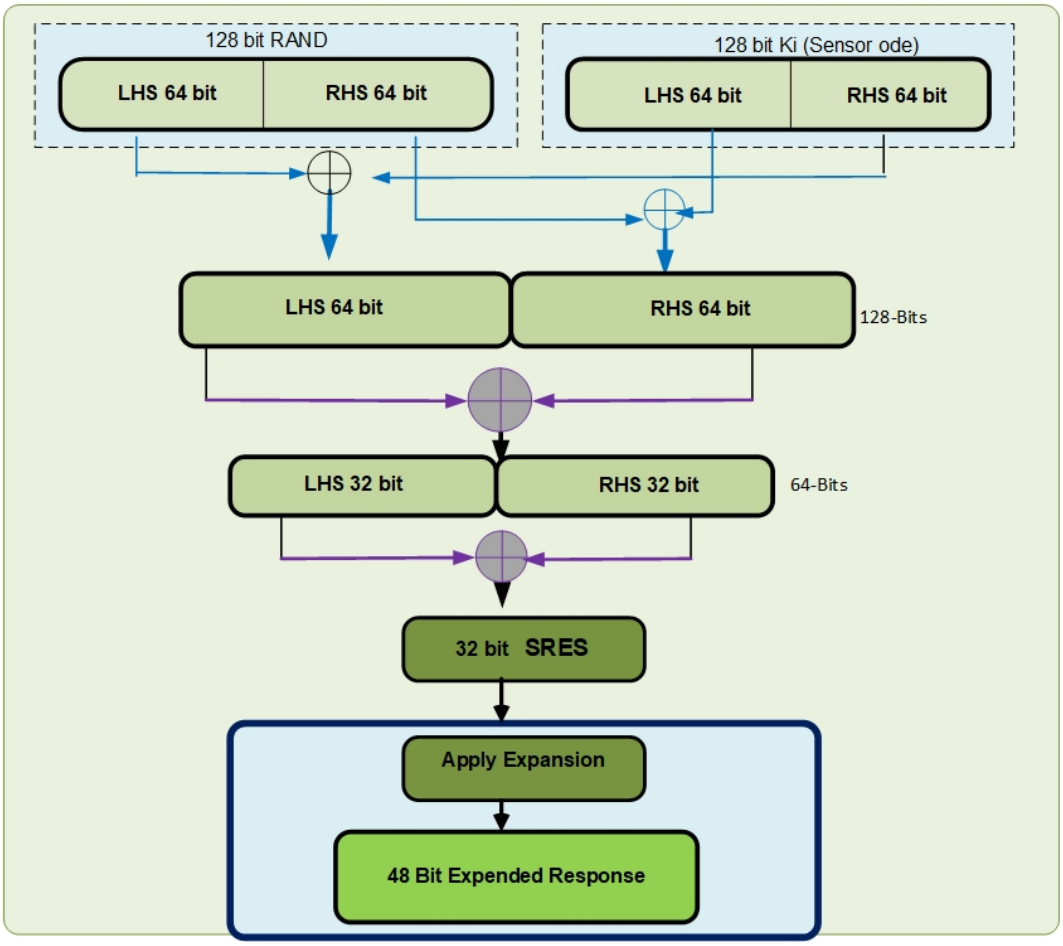

FIGURE 2. Block diagram of proposed ESRES.

node is declared as a Sybil attacking node.

The block diagram of entire node authentication along with key expansion and substitution processes are shown in Figure 3.

A. PROBABILISTIC MODEL

Let the key is represented by δ with size 32 or 48 bits and the pool of keys is represented by γ. The pre-distributed key is represented by K_{ei} where $(1 \leq i \leq n)$ from a space of keys $K_1, K_2, \ldots K_n$ of size 2^{δ}. Thus the probability of a given key K_α being valid can be calculated using Eq (1).

$$P(K_\alpha) \geq P(K_e i) \geq \frac{1}{\|K|} \tag{1}$$

Where $|K|$ is the cardinality of K. As we know K=δ therefor we have.

$$P(K_{ei}) = \frac{1}{2^{\delta}} \tag{2}$$

Eq (2) gives us the probability of acceptance by the sink node, a random number produced by an attacking node. Also, we assume that a key S_δ is attacked by the attacking node from the pool of pi keys. lets assume the N number of nodes attacks a network. To calculate the probability of success of k attacking node out of N nodes is calculated using Eq (3).

$$P = \binom{n}{k} P^k (1-P)^{(N-k)} \tag{3}$$

This equation represents a binomial distribution, where P is the probability of an attack being successful. By combining Eq (2) and Eq (3) we get Eq (4).

$$P = \binom{n}{k} [\delta P(K_{ei})^k][1 - \delta P(K_{ei})]^{(N-k)} \tag{4}$$

Since $K_{ei} = 1/2^{\delta}$, Eq (4) becomes.

$$P = \binom{n}{k} [\delta^k \frac{1}{2^{\delta k}}][1 - \frac{\pi}{2^{\delta}}]^{(N-k)} \tag{5}$$

$$P = \binom{n}{k} \frac{\pi^k}{2^{\delta} k} [\frac{(2^{\delta} - \pi)}{2^{\delta}(N-k)}]^{(N-k)} \tag{6}$$

$$P = \binom{n}{k} \frac{(\pi^k (2^{\delta} - \pi)^{(N-k)})}{(2^{\delta n})} \tag{7}$$

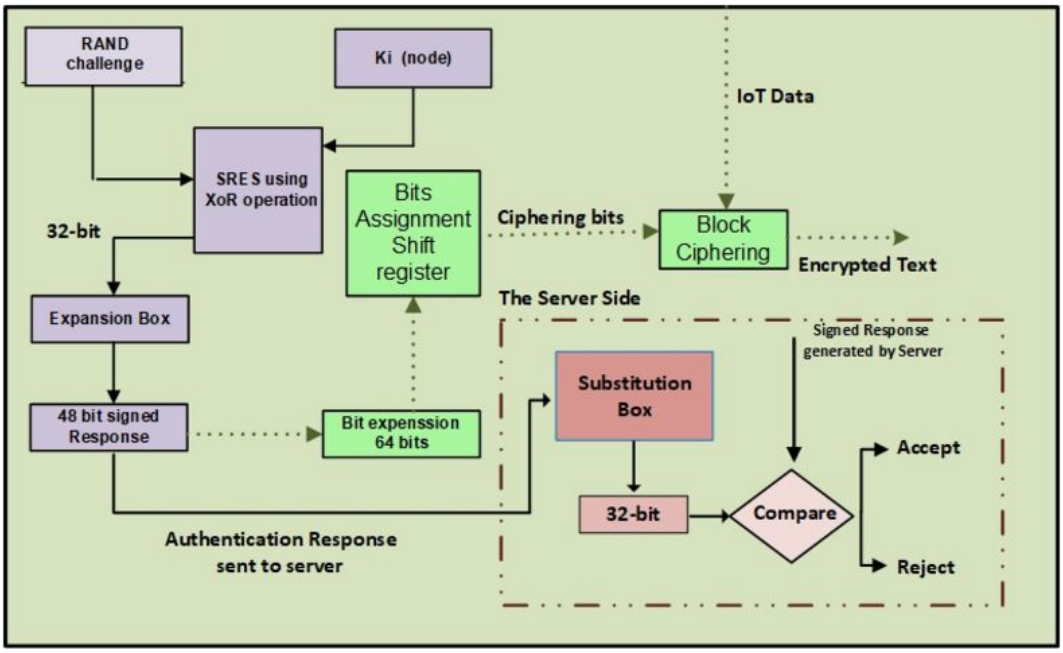

FIGURE 3. Block Diagram of proposed node authentication scheme.

If the total N number of attacking nodes attack the network the probability of successful attacks becomes.

$$P = \sum_{k=1}^{N} \binom{n}{k} \frac{(\pi^k}{(2^{\delta N}} (2^{\delta} - \pi^{K})^{(}N - k) \tag{8}$$

Equations (7) and (8) represents the total probability of success when N nodes attack the network. The sum in Eq. (8) considers all possible scenarios where k out of N nodes could be successful.

IV. EXAMPLE SCENARIO (PROOF)

Key Size (δ): 32 bits
Number of Nodes (N): 100
Number of Successful Attacks (k): 10
Total Key Space (K): 2^{32}
Attacking Nodes Key Pool Size (π): 10^6 keys
Step 1: Calculate the Probability of a Single Key
Using Eq. (2):

$$P(K_{ei}) = \frac{1}{2^{32}} = \frac{1}{4294967296} \approx 2.33 \times 10^{-10}$$

Step 2: Calculate the Probability of Successful Attacks
Using Eq. (7) and substituting the values:

$$P = \binom{100}{10} \times \frac{(10^6)^{10} \times (2^{32} - 10^6)^{(100-10)}}{(2^{32})^{100}}$$

Step 3: Simplify the Expression
First, calculate the binomial coefficient $\binom{100}{10}$:

$$\binom{100}{10} = \frac{100!}{10! \cdot (100-10)!} = 17310309456440$$

Then, plug in the values:

$$P \approx 17310309456440 \times \frac{(10^6)^{10} \times (4.294 \times 10^9)^{90}}{(2^{32})^{100}}$$

The calculated probability of P of successfull attacks is approximately $\approx 7.936 \times 10^{-24}$.

A. ATTACK MODEL AND DEFENSE STRATEGY

In order to examine the performance of proposed scheme, we developed a network of IoMT with 500 nodes. Some of the nodes are assumed to be mobile (like mounted on a patient walking around) whereas some of them are stationary. Each sensor node is assumed to be communicating with at least one of its neighboring nodes. The simulation is performed on both centralized as well as hierarchical scenarios. Here, we assume that the Sybil node in the network is highly powerful both with respect to energy and processing capability which cannot be registered to the network unless authenticated and allowed. The Sybil node can attack the network from two directions, it sends the fake IDs to the cluster head or sink node or steals an ID of a legitimate member node of the network. If a Sybil node registered itself in the network without being detected, we call it an effective node.

To verify the identity of a node, the source node (a cluster head or sink node) broadcasts a 128 bits challenge to the network. The nodes first create a 32 bit number. After a 32 bit number is produced, the expansion process is applied to expand the number into 48 bits and send it to the source node. The source node compares the value with its own generated 48 bit number and the decision is made accordingly. An illegitimate node with a fake ID will not be able to guess the correct 48 bit sequence and hence will not register itself in

the network. In order to perform the above mentioned attack strategy and defense mechanism, we emulated the proposed ESRES mechanism in a client server architecture as shown in Figure 4.

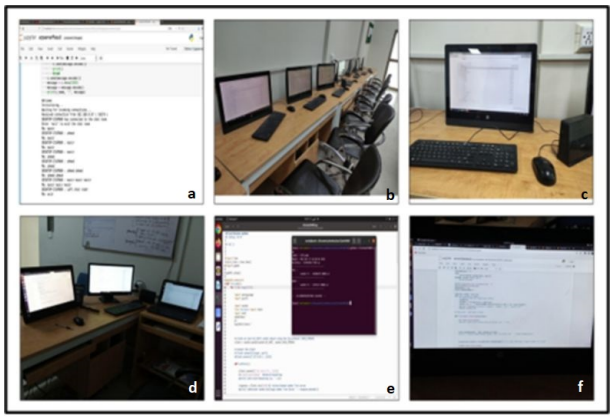

FIGURE 4. Emulation environment used for the proposed framework .(a) Generation of RAND and execution of A3 algorithm. (b)Legitimate client creating ESRES. (c)The attacking node. (d)Server monitoring the authentication process (e)process of Signed Response generated by a client node. (f) Validating a node and filtering the intruder.

In the experiments, we used a network of 10 nodes. The specifications of the systems are HP ProOne 400 G2 with Intel(R) Core(TM) i7 CPU @ 3.40 GHz processor and 8 GB physical memory, and a Dell Inspiron 3521 model with an Intel(R) Core(TM) i3 CPU @ 1.40 GHz and 4.0 GB physical memory. For wireless connectivity, we used the DLink DIR-300, a wireless broadband router supporting 802.11g WiFi with speeds up to 54 Mbps. As mentioned , the proposed framework is based in a client server architecture hence it is prone to server failure also known as single point of failure. A robust backup plan is essential in any client-server-based network to ensure continuous operations and data integrity. To address the aforementioned issue, we use a secondary server along with the primary active one. All the data and updates are replicated at secondary server so that it can take control of the network in case a primary server gets down.

To test the proposed mechanism efficiency, a network of IoT nodes in client server mode is established in anaconda Jupiter notebook 20.02. Every node is communicating with server, sink or cluster head which is responsible for authentication. We have established client server mode on board for launching and preventing attacks using python. We assume that Sybil attack node is powerful in terms of battery power and processing. The Sybil attack node is not registered until it verifies itself as member node of IoT network. To prove the proposed authentication scheme efficiency, we have evaluated client server mode. The server node or verifier challenges the identity of a node by sending the challenge towards target node residing in its neighbor. The authentication serrver generates 128 bits random number and upon receiving of challenge random number, it is encrypted by the target node with pre-distributed key using proposed dual symmetric key algorithm to generate SRES. On the other hand, authentication party i.e., server or cluster head calculates the SRES from random number using pre-distributed key Ki. When the server receives singed response key of 48 bits length from target node the values of both signed response keys are compared. If the values are same, then we say node is valid otherwise it is Sybil attack node.

V. RESULTS AND DISCUSSION

After executing the proposed framework in the above discussed emulation environment, some parameters are measured. This section presents results and discussion in terms of different parameters. Figure 5 represents the processing overhead imposed by different key sizes. The processing of overhead data is acquired by running extensive emulations. The battery level of network nodes is set to be at 100% however, the result snap is taken at the energy level equals to 70%. As depicted in result, the nodes at 48-bit key sizes has relatively more impact on processing as compared to 32 bit. It is worth mentioning here that better network security can be achieved against the little impact of processing overhead in the case of 48-bits.

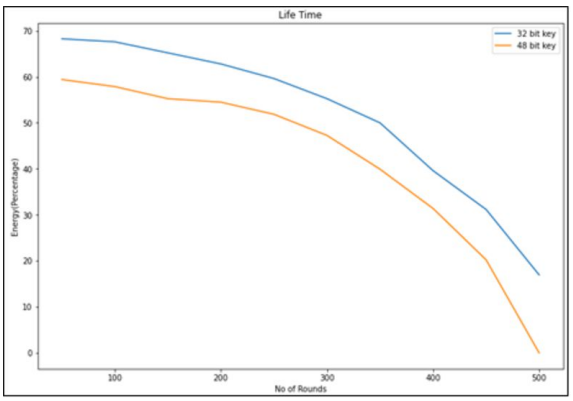

FIGURE 5. Processing overhead in terms of power consumption by the nodes under various key sizes in multiple rounds.

Similarly the Sybil attacks on any network can degrade the throughput which can be very critical in case of IoMT as the patient data transfer and retrieval is carried out by various physicians for continuous patient monitoring. Thus a robust network should have the capability of fast recovering from such type of attacks by retaining optimum throughput. Figure 6 shows the behaviour of proposed scheme under a Sybil attack with various Sybil attacking nodes. A network with no attacking nodes would obviously have desirable throughput with the increase in number of node. However it can be observed from result that the throughput decreases to 31000 and 29000 bits per-second with the attack of 10 and 30 Sybil nodes respectively however, in both cases, fast network recovery can be observed i.e., a Sybil node has been identified and isolated from the network.

Figure 7 shows the power consumption or the battery usage for authentication attempted by user using 32 bit and 48 bit key size during authentications. It is observed that both

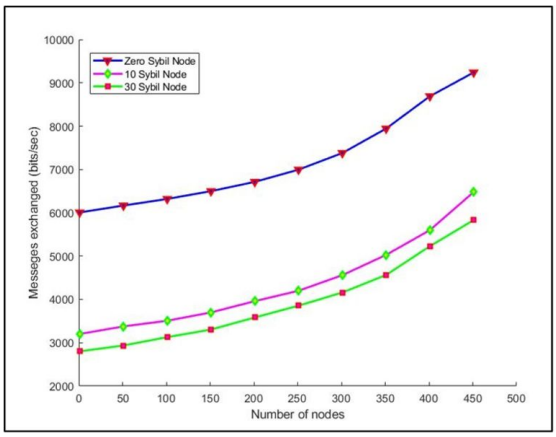

FIGURE 6. Proposed frame work response to varying number of Sybil Attacks.

the 32 bit and 48 bit based authentication process utilized the same amount of power at initial levels. However, a quick drainage of battery is noticed in case of 48 bit. This implies that a 48-bit key size proved a stronger defense against Sybil attack as compared to 32-bits with a bearable amount of power. Figure 8 shows the probability of successful attacks.

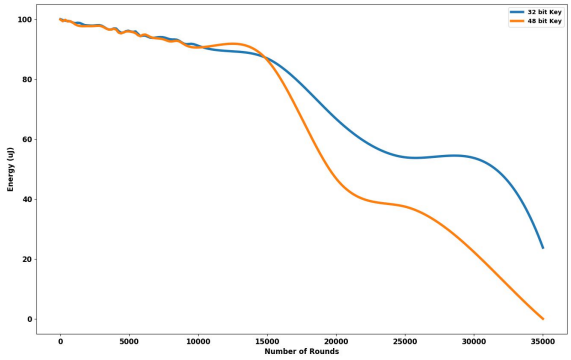

FIGURE 7. Energy consumption of attacking nodes.

If a Sybil node is injected by deceiving the cluster head or sink,it becomes an effective node as described earlier. Extensive simulations were carried out creating a strong attack scenario over the network. The attacking node picks a random key K from the pool of M total possible keys at various numbers. The result clearly shows that the probability of successful attacks can only be increased with the increase in number of Sybil nodes which implies, that a network with smaller number of attacking nodes cannot be compromised due to the high demand of energy and processing overhead by the nodes. Figure 9 shows the bar graph that represents 32-bit key in blue and 48 bits key in red color bars. This graph shows the time for authentication of both the keys. Though the 48 bit key uses a bit more time as compared to 32-bit key authentications attempts but it is negligible considering the enhanced security of the 48-bit key.

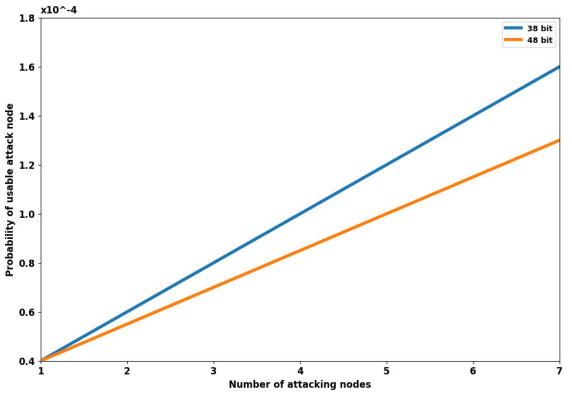

FIGURE 8. Probability of successful usable Sybil node.

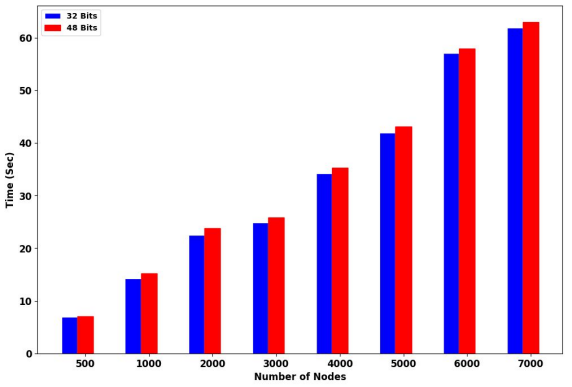

FIGURE 9. The time consumed for authentication of both the keys.

VI. CONCLUSIONS

IIn this paper, we proposed a secure and energy-efficient authentication mechanism to prevent Sybil attacks in IoMT. The proposed scheme utilizes an authentication algorithm and secure mechanism specifically designed for IoMT. The scheme involves node authentication, where each sensor node generates a key in response to a message from the governing nodes like the server, cluster head, or relay node. These governing nodes are also responsible for verifying the response upon receiving signals from the source node. This algorithm ensures that users are authenticated before accessing the network, applicable to both hierarchical and centralized networks. The proposed work is extensively evaluated under various Sybil attacks, considering different authentication key pool sizes. The results demonstrate a high probability of preventing Sybil attacks with lower computational power compared to existing schemes. We have demonstrated the effectiveness of the mechanism in dynamically changing networks, with its low power consumption and linear complexity making it suitable for modern requirements. In the future, we intend to integrate the proposed ESRES scheme with other security protocols, such as blockchain-based authentication, to enhance data integrity and transparency in IoMT environments. Moreover, we also plan to test the scheme in various IoT set-

tings, including smart cities, smart farming, etc. where secure communication between devices becomes. Additionally, we will implement and evaluate the ESRES scheme in real-world healthcare environments to have insights into its performance and reliability in practical scenarios.

DATA AVAILABILITY

The datasets used are available publicly.

CONFLICT OF INTEREST

There is no conflict of interest to report

ACKNOWLEDGEMENTS

The Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support (QU-APC-2024-9/1)

REFERENCES

[1] , Shinde, S and Phalle, V A survey paper on internet of things based healthcare system Int. Adv. Res. J. Sci. Eng. Technol volume 4,2017

[2] Mazhar, T.; Talpur, D.B.; Shloul, T.A.; Ghadi, Y.Y.; Haq, I.; Ullah, I.; Ouahada, K.; Hamam, H. The Internet of Things (IoT) in healthcare: Taking stock and moving forward, journal=Internet of Things, Volume 22, 2023, 100721, ISSN 2542-6605, https://doi.org/10.1016/j.iot.2023.100721.

[3] Abderahman Rejeb, Karim Rejeb, Horst Treiblmaier, Andrea Appolloni, Salem Alghamdi, Yaser Alhasawi, Mohammad Iranmanesh, Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence, journal=Brain Sciences, 2023, 13, 683

[4] , Hwang, Tzonelih and Gope, Prosanta, Provably secure mutual authentication and key exchange scheme for expeditious mobile communication through synchronously one-time secrets, Wireless personal communications, volume=77, year 2014, publisher Springer, 197-224

[5] Al-Fuqaha, Ala and Guizani, Mohsen and Mohammadi, Mehdi and Aledhari, Mohammed and Ayyash, Moussa Internet of things: A survey on enabling technologies, protocols, and applications, IEEE communications surveys & tutorials, volume17(4), 2347—2376, 2015, IEEE

[6] , Singh, Amit Kumar and Kumar, Basant and Singh, Ghanshyam and Mohan, Anand. Medical image watermarking, 2017, Springer

[7] Anand, Ashima and Singh, Amit Kumar Watermarking techniques for medical data authentication: a survey. Multimedia Tools and Applications, volume=80, 30165–30197, 2021 , Springer

[8] Anand, Ashima and Singh, Amit Kumar,
An improved DWT-SVD domain watermarking for medical information security, Computer Communications Volume 152, 72—80, 2020, Elsevier

[9] Aslam, Muhammad Design of sampling plan for exponential distribution under neutrosophic statistical interval method, IEEE Access, volume6, 64153–64158, 2018, IEEE

[10] , Li, Mingyan and Poovendran, Radha and Narayanan, Sreeram. Protecting patient privacy against unauthorized release of medical images in a group communication environment, Computerized Medical Imaging and Graphics, volume29(5),367–383, 2005,Elsevier

[11] Burke, Wendy and Oseni, Taiwo and Jolfaei, Alireza and Gondal, Iqbal.
Cybersecurity indexes for ehealth, Proceedings of the australasian computer science week multiconference,1–8, 2019

[12] Singh, Amit Kumar and Kumar, Chandan
Encryption-then-compression-based copyright protection scheme for E-governance, IT Professional, volume22(2), 45–52, 2020, IEEE

[13] Anand, Ashima and Singh, Amit Kumar,
Joint watermarking-encryption-ECC for patient record security in wavelet domain,
IEEE MultiMedia, volume 27(3), 66–75, 2020, IEEE

[14] Gupta, Brij B and Perez, Gregorio Martinez and Agrawal, Dharma P and Gupta, Deepak
Handbook of computer networks and cyber security. Springer, volume10, 978–993, year 2020, Springer

[15] , Salameh, Jamal N Bani
A new approach for securing medical images and Patient's information by using a hybrid system, Int Journal of Computer Sci Netw Secur, volume 19(4), 28–39, 2019

[16] Arunkumar, S and Subramaniyaswamy, V and Vijayakumar, V and Chilamkurti, Naveen and Logesh SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images, Measurement, volume 139, 426–437, 2019, Elsevier

[17] Wu, Chia-Chun and Kao, Shang-Juh and Hwang, Min-Shiang A high quality image sharing with steganography and adaptive authentication scheme, Journal of Systems and Software, volume 84(12), 2196–2207, 2011, Elsevier

[18] Kanan, Hamidreza Rashidy and Nazeri, Bahram, A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm,
Expert systems with applications, volume 41(14), pages 6123–6130, 2014 Elsevier

[19] Kumar, B Vinoth and Ramaswami, M and Swathika, P Data security on patient monitoring for future healthcare application, International Journal of Computer Applications volume 163(6), 20–23, 2017 Foundation of Computer Science

[20] Sujatha, S and Govindaraju, R A secure crypto based ECG data communication using modified SPHIT and modified quasigroup encryption,
International Journal of Computer Applications, volume 78(6), 2013, Citeseer

[21] M. Masud, G. S. Gaba, K. Choudhary, M. S. Hossain, M. F. Alhamid and G. Muhammad, "Lightweight and Anonymity-Preserving User Authentication Scheme for IoT-Based Healthcare," in IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2649-2656, 15 Feb.15, 2022, doi: 10.1109/JIOT.2021.3080461.

[22] Sun, Jinyuan and Zhu, Xiaoyan and Zhang, Chi and Fang, Yuguang HCPP: Cryptography based secure EHR system for patient privacy and emergency healthcare,
book 2011 31st International Conference on Distributed Computing Systems, 373–382, 2011, IEEE

[23] Bin Hu, Wen Tang, Qi Xie, A two-factor security authentication scheme for wireless sensor networks in IoT environments, Neurocomputing, Volume 500, 2022, Pages 741-749, ISSN 0925-2312

[24] A Shankar; A Kannammal A Hybrid Of Watermark Scheme With Encryption To Improve Security Of Medical Images, 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), 10.1109/ICICV50876.2021.9388616, IEEE

[25] Sharma, Abhilasha and Singh, Amit Kumar and Ghrera, SP
Secure hybrid robust watermarking technique for medical images, Procedia Computer Science, volume 70, 778–784, 2015, Elsevier

[26] Mian Ahmad Jan, Fazlullah Khan, Muhammad Alam, Muhammad Usman, "A payload-based mutual authentication scheme for Internet of Things",ELSEVIER, Future Generation Computer Systems, Volume 92 , March 2019, Pages 1028-1039

[27] Nagamani, S and Nagaraju, DR A mobile cloud-based approach for secure m-health prediction application,
International Journal for Innovative Engineering & Management Research, volume 7(12), 2018

[28] Chirakkarottu, Siyamol and Mathew, Sheena A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography, journal SN Applied Sciences, volume2, 1–10, 2020, Springer

[29] Mian Ahmad Jan, Fazlullah Khan, Muhammad Alam, Muhammad Usman A payload-based mutual authentication scheme for Internet of Things, Future Generation Computer Systems, Volume 92, 2019, Pages 1028-1039, ISSN 0167-739X, https://doi.org/10.1016/j.future.2017.08.035.

[30] Ali Haj-Hassan, Youcef Imine, Antoine Gallais, Bruno Quoitin, Consensus based mutual authentication scheme for Industrial IoT, Ad Hoc Networks,Volume 145,2023, 103162, ISSN 1570-8705

[31] Jahan, Sharmin and Chowdhury, Mozammel and Islam, Rafiqul Robust fingerprint verification for enhancing security in healthcare system, 2017 International Conference on Image and Vision Computing New Zealand (IVCNZ), 1—5, 2017, IEEE

[32] Ramli, Dzati Athiar and Hooi, Man Y and Chee, Kai Jye Development of heartbeat detection kit for biometric authentication system,
Procedia Computer Science, volume 96, 305–314, 2016, Elsevier

[33] , Lee, Jae-Neung and Pan, Sung Bum and Kwak, Keun-Chang Individual identification based on cascaded PCANet from ECG signal,
2019 International Conference on Electronics, Information, and Communication (ICEIC), 1–4, 2019, IEEE

[34] Thanki, Rohit and Borisagar, Komal Biometric watermarking technique based on CS theory and fast discrete curvelet transform for face and fingerprint protection,
Advances in Signal Processing and Intelligent Recognition Systems: Proceedings of Second International Symposium on Signal Processing and Intelligent Recognition Systems (SIRS-2015), 2015, Trivandrum, India, 133–144, Springer
[35] Shanthini, B and Swamynathan, S Genetic-based biometric security system for wireless sensor-based health care systems,
2012 International Conference on Recent Advances in Computing and Software Systems, 180–184, 2012, IEEE
[36] Ali, Rifaqat and Pal, Arup Kumar Cryptanalysis and biometric-based enhancement of a remote user authentication scheme for e-healthcare system,
Arabian Journal for Science and Engineering, volume 43, 7837–7852, 2018, Springer
[37] Hamidi, Hodjat An approach to develop the smart health using Internet of Things and authentication based on biometric technology, Future generation computer systems, volume 91, 434—449, 2019, Elsevier
[38] Hathaliya, Jigna J and Tanwar, Sudeep and Tyagi, Sudhanshu and Kumar, Neeraj Securing electronics healthcare records in healthcare 4.0: A biometric-based approach,
Computers & Electrical Engineering, volume 76, 398–410, 2019, Elsevier
[39] Casino, Fran and Dasaklis, Thomas K and Patsakis, Constantinos A systematic literature review of blockchain-based applications: Current status, classification and open issues,
Telematics and informatics, volume 36, 55–81, 2019, Elsevier
[40] Li, Xiaoqi and Jiang, Peng and Chen, Ting and Luo, Xiapu and Wen, Qiaoyan A survey on the security of blockchain systems, Future generation computer systems, volume 107, 841–853, 2020, Elsevier
[41] Agbo, Cornelius C and Mahmoud, Qusay H and Eklund, J Mikael Blockchain technology in healthcare: a systematic review,
Healthcare, volume7(2), pages=56,2019, MDPI
[42] , Lin, Iuon-Chang and Liao, Tzu-Chun A survey of blockchain security issues and challenges.,
Int. J. Netw. Secur, volume 19(5), 653–659, 2017
[43] , Kaur, Harleen and Alam, M Afshar and Jameel, Roshan and Mourya, Ashish Kumar and Chang, Victor A proposed solution and future direction for blockchain-based heterogeneous medicare data in cloud environment,
Journal of medical systems, 42, 1–11, 2018, Springer
[44] Chen, Yi and Ding, Shuai and Xu, Zheng and Zheng, Handong and Yang, Shanlin Blockchain-based medical records secure storage and medical service framework,
Journal of medical systems, volume 43, 1–9, 2019, Springer
[45] Wu, Sihua and Du, Jiang Electronic medical record security sharing model based on blockchain, Proceedings of the 3rd International Conference on Cryptography, Security and Privacy 13–17, 2019
[46] Zhu, Liehuang and Dong, Hui and Shen, Meng and Gai, Keke An incentive mechanism using shapley value for blockchain-based medical data sharing 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), 113—118, 2019, IEEE
[47] Brunese, Luca and Mercaldo, Francesco and Reginelli, Alfonso and Santone, Antonella A blockchain based proposal for protecting healthcare systems through formal methods, Procedia Computer Science, volume 159, 1787–1794, 2019, Elsevier
[48] Ichikawa, Daisuke and Kashiyama, Makiko and Ueno, Taro and others Tamper resistant mobile health using blockchain technology, JMIR mHealth and uHealth, volume=5(7), 2017, JMIR Publications Inc, Toronto
[49] Zhang, Cheng and Liu, Yuxuan and Guo, Xiaoming and Liu, Yanan and Shen, Yane and Ma, Jing Digital Cognitive Behavioral Therapy for Insomnia Using a Smartphone Application in China: A Pilot Randomized Clinical Trial, =JAMA Network Open, volume 6(3),866–886, 2023, American Medical Association
[50] Saud Khan, M and Khan, Noor M Low complexity signed response based sybil attack detection mechanism in wireless sensor networks, journal=Journal of Sensors, volume 2016, 2016, Hindawi

MUHAMMAD SAUD KHAN holds PhD in Cyber Security from the Capital University of Science and Technology, Islamabad, Pakistan. He completed his MS in Multimedia & Communication in 2010 from Mohammad Ali Jinnah University, Islamabad, and earned his BS in 2005 from Allama Iqbal Open University, Islamabad.
With 17 years of teaching experience at well-reputed universities across Pakistan, Dr. Saud is currently serving as an Assistant Professor in the Cyber Security Program at Air University, Islamabad. His research interests are focused on Cyber Physical Systems, Drone Fleet Security, the Internet of Things (IoT), and the development of secure routing and authentication mechanisms in computer and wireless networks.
Dr. Saud's extensive academic background and commitment to advancing the field of cyber security are reflected in his numerous contributions to research and education, making him a distinguished member of the academic community.

MUHAMMAD SARDARAZ received his master's degree in computer science from Foundation University Islamabad. He completed his Ph.D. in Computer Science in 2016 from Iqra University Islamabad, Pakistan. He worked as Lecturer in the Department of Computer Science, The University of Wah, Wah Cantt. Dr. Sardaraz worked as Assistant Professor in the Department of Computer Science COMSATS University Islamabad, Attock, Pakistan for six years. Presently Dr. Sardaraz is working as Tenured Associate Professor in the same department. His research interests are cloud computing, cluster and grid computing, and bioinformatics.

MUHAMMAD TAHIR Muhammad Tahir completed Ph.D. (Computer Science) from the Department of Computing & Technology, Iqra University in 2016. He worked as Lecturer in the Department of Computer Science, The University of Wah, Wah Cantt. Dr. Tahir worked as Assistant Professor in the Department of Computer Science COMSATS University Islamabad, Attock Campus from 2016 to 2023. He is working as Tenured Associate Professor in the same Department. His research interests are in parallel and distributed computing, Hadoop MapReduce framework, bioinformatics algorithms design and analysis and sequence alignment, cloud computing.

ABDULLAH ALOURANI is Assistant Professor at the Department of Management Information Systems, Qassim University, Saudi Arabia. He received his Ph.D. in Computer Science from the University of Illinois at Chicago, his master's degree in computer science from DePaul University in Chicago, and his bachelor's degree in computer science from Qassim University, Saudi Arabia. His current research interests are in the areas of Software Engineering, Security, and Artificial Intelligence. He is a member of ACM and IEEE.