Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.028536
Article

Tech Science Press

A Multi-Stage Secure IoT Authentication Protocol

Khalid Alhusayni[1], Raniyah Wazirali[1], Mousa AlAkhras[1,2], Marwah Almasri[1,*] and Samah Alhazmi[1]

[1]College of Computing and Informatics, Saudi Electronic University, Riyadh, 11673, Saudi Arabia
[2]King Abdullah II School for Information Technology, The University of Jordan, Amman, 11942, Jordan
*Corresponding Author: Marwah Almasri. Email: m.almasri@seu.edu.sa
Received: 12 February 2022; Accepted: 19 April 2022

Abstract: The Internet of Things (IoT) is a network of heterogeneous and smart devices that can make decisions without human intervention. It can connect millions of devices across the universe. Their ability to collect information, perform analysis, and even come to meaningful conclusions without human capital intervention matters. Such circumstances require stringent security measures and, in particular, the extent of authentication. Systems applied in the IoT paradigm point out high-interest levels since enormous damage will occur if a malicious, wrongly authenticated device finds its way into the IoT system. This research provides a clear and updated view of the trends in the IoT authentication area. Among the issues covered include a series of authentication protocols that have remained research gaps in various studies. This study applies a comparative evaluation of authentication protocols, including their strengths and weaknesses. Thus, it forms the foundation in the IoT authentication field of study. In that direction, a multi authentication architecture that involves secured means is proposed for protocol authentication. Informal analysis can affect the security of the protocols. Burrows-Abadi-Needham (BAN) logic provides proof of the attainment of mutual authentication. NS3 simulator tool is used to compare the performance of the proposed protocol to verify the formal security offered by the BAN logic.

Keywords: Internet of Things (IoT); security; authentication; BAN logic; sensor networks

1 Introduction

Internet of Things (IoT) is one of the fast-growing technologies with intelligent features that use resources efficiently [1–4]. It combines physical objects with Internet connectivity for forming cyber-physical networks. Smart devices have a vital role in applications of IoT in the healthcare field as medical tools with IoT characteristics can perform several functionalities through their basic abilities, like sensing to collect information associated with health, process, and communication [5]. IoT permits sensing or controlling objects remotely through the present network infrastructure, generating opportunities to integrate the physical world into computerized systems directly, enhancing efficiency, improving accuracy, and achieving economic advantages with decreased human intervention [6–8].

The unique features of IoT depend on whether sensors are used or not. Sensors convert IoT from a standard network of passive devices into a more active network that can be integrated with the real world. An ecosystem consisting of constantly connected devices over the networks is created by IoT [9,10]. The system provides less control, regardless of any security measures; this leads to several attacker types being exposed to users. Due to the rapid introduction of IoT in the market and millions of IoT devices, security and other services are still challenges [11–14].

There are numerous threats to IoT security [15,16]. The main challenges include user privacy, confidentiality in business, and third-person trust. In addition to existing issues in other networks, IoT faces both passive and active attacks, which can easily interrupt its operation and decrease IoT's advantages and services. Attacks in passive mode can recover data from the network, and its behavior is unaffected. Attacks in active mode directly block the provided services [17,18]. Further, these threats can be broadly classified as either external threats originating from outside the network or internal threats generated from inside the network. Internal threats have access to confidential and valuable data accessible to services, making them more dangerous than external threats.

Various attacks in IoT are categorized based on attack vulnerabilities utilized in compromising the network [19–21]. Attacks can be classified based on the chances of being detected and how they influence the network. Attacks in the network can be classified as physical attacks, network attacks, software attacks, and encryption attacks.

A physical attack, which uses injected malicious nodes, was the most dangerous attack because it modifies the information and stops the services. In a network attack, a high-risk attack is the attack of a sinkhole [22]. This type of attack attracts the entire traffic to the base station and also initiates additional threats like chosen forwarding, modification, or packet dropping. A worm attack is a dangerous attack from the types of software attack since they can be the more destructive and unsafe format of the malware on the Internet [23]. A worm is a program that generates copies of itself to affect computers by utilizing security holes present in the software and hardware of networks. Also, system files can be erased, some data such as passwords can be robbed, passwords can be altered to become unknown to the user and further cause computer interruptions. Encryption attacks are the most difficult to handle. They occur through the usage of side-channel to make their detection difficult.

Other attacks include Man-in-the-middle attack, Denial of Service (DoS) attack, password guessing in the offline attack, impersonation of user attack, and the smart card is stolen attack [24]. A man-in-the-Middle attack interrupts communication among two nodes. They acquire sensitive information through eavesdropping. When a similar attack occurs on an encrypted line, the attacker interrupts the communication when keys are interchanged and acquires the key.

In a DoS attack, significant traffic floods the networks to stop its services from reaching the intended users [25]. When this attack takes place on the software side, the attacker restricts a user from an application layer by rejecting services. Since IoT networks have a similar architecture to a traditional network in the way devices are connected, imperfections of the traditional architecture of the network have been inherited in an IoT architecture.

Researchers proposed many solutions for handling the above attacks. Applying all available security measures and methods consumes computational power on devices, which is intolerable for IoT technology and their devices with limited resources. Security mechanisms are required for handling extreme security issues. At the same time, they must be lightweight and robust to fit IoT characteristics. Some IoT attacks can be eliminated by placing a few security precautions when the application is developed. Some attacks are challenging to detect or prevent. A secure and efficient solution is required [26].

IoT is applied in the healthcare field. A precise understanding of human anatomy permits healthcare experts to handle emergencies. Patient monitoring remotely by healthcare experts or doctors using

Wireless Sensor Network (WSN) provides a solution for the shortage issues [5]. To monitor remotely with WSN, termed as Wireless Body Area Network (WBAN) or Wireless Medical Sensor Network (WMSN), uses several sensors that gather data from the human body that is later sent to a central device to process and store. WSN applications in healthcare can be divided into monitoring patients and monitoring by care centers for long-term databases [27].

Many limitations exist in WSN because sensor nodes are limited in power, storage, and process. That needs appropriate management of resources, especially in insecure communication in the wireless mode because of the lack of infrastructure [12,15]. Compromise of sensor nodes is carried out at ease due to: its heterogeneous nature and frequent change in topology because of failure in nodes, merging, and mobility.

The desired security characteristics include authentication, privacy, integrity, anti-playback, and non-repudiation. A large volume of data is transmitted over the network channels; this presents a high risk. Consequently, many cryptographic approaches, steganography methods, and additional techniques are widely used [17]. Security and authentication are the major issues facing IoT and wireless networks, and these requirements are the focus of this paper. A multi authentication architecture is proposed in this paper.

The proposed multi authentication architecture involves a secured means for protocol authentication. It can prevent IoT cyberattacks and data breaches by adding an extra layer of authentication.

The proposed Multi authentication architecture uses five steps: Initialization, user and sensor registration, login, authentication, and password renewal. The initialization phase describes the system setup. The registration phase involves sensor registration and user registration phases. The login phase explains how the authenticated user can access the sensor using the terminal's user ID, password, and biometric recognition. The authentication phase describes two authentication models; the first model will be selected if the Database has the sensor index number; if not, it will choose the second model. The password renewal phase describes how the user can renew the password. It is the only way, even if the user forgets the password and knows the rest of the authentication details, still, the user cannot access the secured gateway.

The rest of this paper is organized as follows: Section 2 reviews the relevant literature and methods related to the secure authentication protocols in IoT. Section 3 describes the proposed multi-authentication method architecture. The performance of the proposed method is analyzed in Section 4 by several metrics and compared with other existing methods using the NS3 simulation tool. Finally, Section 5 provides the conclusions and possible avenues for future work.

2 Literature Review

Body Sensor Networks (BSN) framework is applied through the IoT-based healthcare system to operate securely [28]. To ensure confidentiality in transmitting data and authentication of entities provided to smart objects, a backend BSN server, a local processing unit, and two communication processes are created by robust crypto primitives. The IoT-based healthcare system and its communication through the BSN servers help to achieve efficiency and robustness in transmission. A Raspberry PI platform was implemented on this proposed healthcare system and highlighted the feasibility and practicability. When crypto-hash modules replaced the traditional SHA-2 methods, acceptable computational cost and improved efficiency were achieved. From the results, the proposed method guaranteed practicability and robustness.

Yeh [29] developed an IoT healthcare system to focus on unbiased decision-making. Patient health parameters monitoring based on healthcare system using core IoT technologies such as BSN-based tiny and lightweight wireless sensor nodes. This proposed method is used in the healthcare system for strokes and coronary heart disease. This study is helpful to monitor the pulse rate, and its differentiation and panic situation has been alerted. This method is sensitive and could reduce the loss of lives.

In [30], the authors proposed a unique method for authenticating the exchange of information in WSN distinct from earlier existing authentication research for resisting attacks by capturing nodes in the network. The objective was to add an authentication scheme to exchange information in the earlier authentication method but does not offer a new approach. This method was developed with associated ideas of Home Gateway Node (HGWN) and other native sensor nodes. The home gateway network contacts every native sensor node and performs the authentication process to exchange information to resist security threats. The mechanism with dynamic contact was designed to prevent an attacker from predicting the period of communication between the sensor and the HGWN. Validation was done in three ways with detailed explanations of the offered scheme: security evaluation, BAN logic, and overall performance. These evaluations proved that the proposed authentication scheme for exchanging information could attain features of security and its goals. Though few benefits were offered, practical implementation was not performed to transfer data with novel security authentication to the sensor. Thus, this proposed scheme provided a new way to design a better scheme to enhance the original key agreement and authentication protocol.

Another study offered a novel and enhanced scheme for user authentication and the key agreement protocol for the heterogeneous WSN [31]. This scheme was designed for the IoT environment and was reliant on a proposed unique method of Turkanovic. Whereas the novelty of both the offered approach and Turkanovic were related to the primary authentication model of sensor node of four steps, all registered users in IoT contact directly with sensor node from WSN that does not get involved with the Gateway Node (GWN). By cryptanalysis of the existing method, certain shortcomings were identified based on security, which was vulnerable to many cryptographic attacks. The existing protection scheme of traceability and privacy of sensor nodes was not offered. Also, the method was exposed to attacks by breaching smart cards, impersonation attacks of sensor nodes, and man-in-the-middle attacks.

Further, the method tackled and eliminated all shortcomings of security and the susceptibilities of the existing method to preserve the novel framework and its functionalities. The method was analyzed using BAN logic and utilized a simulation tool, Automated Validation of Internet Security-sensitive Protocols and Applications (AVISPA), to automatically analyze the security of the cryptographic protocols; it assured the specified security of the proposed protocol. The performance results show that the proposed scheme consumed less storage and enabled unlimited and dynamic network growth without disturbing registration or the authentication functionality for sensor and user nodes.

The authors in [32] reviewed the existing method of 2-factor authentication. They later offered a 3-factor unspecified authentication method for wireless networks in an IoT environment. A fuzzy commitment method was implemented to handle the information from the user's biometrics. Analyzing the performance and thorough comparison of obtained results shows better computation efficiency with better security and functional characteristics. Additional processes related to simulation were not performed, and the offered scheme's efficiency still needs better evaluation. Various security approaches for applications of IoT were also studied. Such applications include smart environments like smart grid, healthcare with smart technology, and smart transportation system.

The authors in [33] developed an encoding technique based on XOR manipulation, rather than complicated encoding like hash function usage, to anti-counterfeit and protect privacy. In an IoT environment, the present security mechanisms of the Radio-frequency Identification (RFID) system can be improved using cryptography protocols. The drawbacks of RFID protocols can also be enhanced with lightweight cryptography protocols. Hardware implementation for lightweight cryptography protocol was also demonstrated. Additionally, the offered protocol may also be utilized for establishing a process of mutual authentication in the unique system of RFID for IoT implementations.

The authors in [34] proposed a highly secured healthcare system based on IoT with BSN termed BSN-care that accomplished the requirements efficiently. BSN authoritative technologies were utilized in the

modern healthcare system. It needs less power and lightweight wireless sensors nodes, which were used to monitor the functions of the human body and the surrounding environment. BSN nodes were utilized for collecting complex data and operating in an unfriendly environment and need firm security methods that prevent interaction of malicious nodes with the system. Security and confidentiality were described based on the implementation of BSN in the healthcare field. Many researches were based on trending BSN attempted to solve the security problems but failed to offer more robust security services such as preserving the privacy of the patient's data. To solve such issues, the proposed framework of BSN-care resulted in better efficiency concerning the needs of the healthcare system.

The authors in [35] offered a novel authentication of crucial establishment based on a signature for the IoT environment. The proposed security solution was tested using BAN logic, analysis of the informal security, and formal verification of the security using the AVISPA tool. The proposed method was also applied with the NS2 simulation tool. The results of the simulation illustrate the real-time implementation of the scheme. Higher security, efficient computation, and reduced costs for communication proved that the proposed method outperforms existing approaches. The model for authenticating the upcoming applications with IoT was discussed, and later challenges and needs for better security were also illustrated.

The authors in [36] proposed a lightweight and mutually reliant authentication protocol with a unique public key encoding method for the applications in a smart city. The protocol is a hybrid solution that considers communication cost and efficiency without sacrificing security. The proposed protocol was comparatively better than other earlier protocols, such as Elliptic-Curve Cryptography (ECC) and RSA-based. The authors also analyzed the security of the offered encoding approach and the mutual authentication protocol. The protocol was evaluated using Powerful Wireless Microcontroller System-On-Chip for 2.4-GHz IEEE 802.15.4 (CC2538) and Contiki Operating System (OS) modules. The experiments' results showed that the offered protocol on the level of 112 bits security was around 88 and seven times faster than ECC and RSA, respectively. The time for mutual authentication can also be decreased if offline or online methods are enabled. Evaluation of the protocol in a real-time hardware environment was not carried out, and instead, only software evaluation was done. The protocol can be further optimized when the size of the message is at maximum without altering the size of ciphertext.

Security and authentication are the major security issues facing IoT and wireless networks. These drawbacks and requirements are the primary focal points of the proposed method in this paper.

3 The Proposed Methodology

This section highlights the architecture of the proposed method. It also describes the multi-authentication process using five steps of Initialization, user and sensor registration, login, authentication, and password renewal implemented on the two Gateway nodes, HGWN and Foreign Gateway Node (FGWN).

3.1 Basic Concepts

In WSN, the gateway node GWN is authoritative and an essential part between the users and the sensors, and it is essential for information exchange. The data from sensors initially reach the GWN through the Internet and is sent to the user. Once they work, the sensors and GWN tend to be static. While communication occurs, the distance between the user and a particular sensor may change. GWN continuously shows the power and communication resource so that the user contact reduces the sensor energy cost, as shown in Fig. 1 [31]. Preference is given for transmitting messages from the user to the GWN to the sensor and vice versa. The multi-gateway authentication process implemented in this study meets the farther sensors' access requirement and solves only one GWN problem, which leads to packet collisions issues.

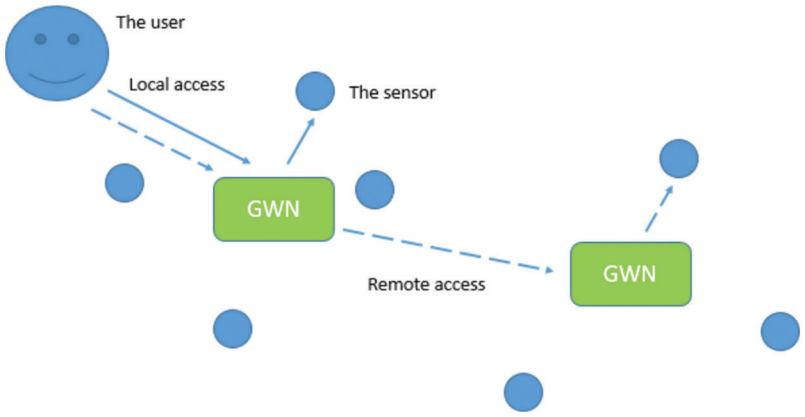

Figure 1: Multi-gateway sensor nodes access [31]

In the Multi-Gateway Sensor Nodes Access technique, the user is registered with a nearby GWN, and the data is obtained from the sensors. If the sensor is registered in the registered GWN's location, the user can access the sensor through GWN, and it is named a Home GWN or shortly an HGWN. Alternatively, if the sensor is near another GWN, it is called a Foreign GWN (FGWN), and the user can get the data through the FGWN.

The WSN communication environment is vulnerable [37,38], and security and privacy must be ensured. Mutual authentication and user tracking attacks are noted. Secret keys are generated using the BAN logic approach to share the information with the gateway nodes. The user and the sensors must register themselves. While entering into authentication, if it is not present in the HGWN database, it performs model 1 format, and if it is present, it performs model 2 based FGWN. Finally, the security system is verified using the multi-search tree algorithm.

3.2 Proposed Method Architecture

For a multi-gateway WSN architecture, a new authentication scheme named a three-factor authentication technique is used. The system needs to initialize the user identity, password, and biometrics [39]. The user and sensor nodes must be registered to share the information with the gateway nodes GWN. In this study, two Gateway nodes have been implemented, as shown in Fig. 2.

To reach the gateway nodes, the sensors and users must register themselves using the BAN logic approach in an HGWN and using the BAN logic hashing inference rule in FGWN. Then the system has to log in to send the secret messages, and for that, the pseudo-identity number and other parameters are generated and sent to the HGWN. After that, the authentication phase exhibited nonce value. The user identity should be present in the Database for access, and if it is present in the HGWN database, it performs the model 1 procedure. If it is not present, then it performs model 2 procedure. For the verification, the multi-search-based encryption and decryption method is used. Both multi-search tree-based encryption and decryption were implemented to check the robustness of the model. Against simulation attacks, this scheme ensures security. This proposed study is based on security properties and performance as expected to be efficient compared to other techniques. Tab. 1 shows the notation used in the proposed protocol.

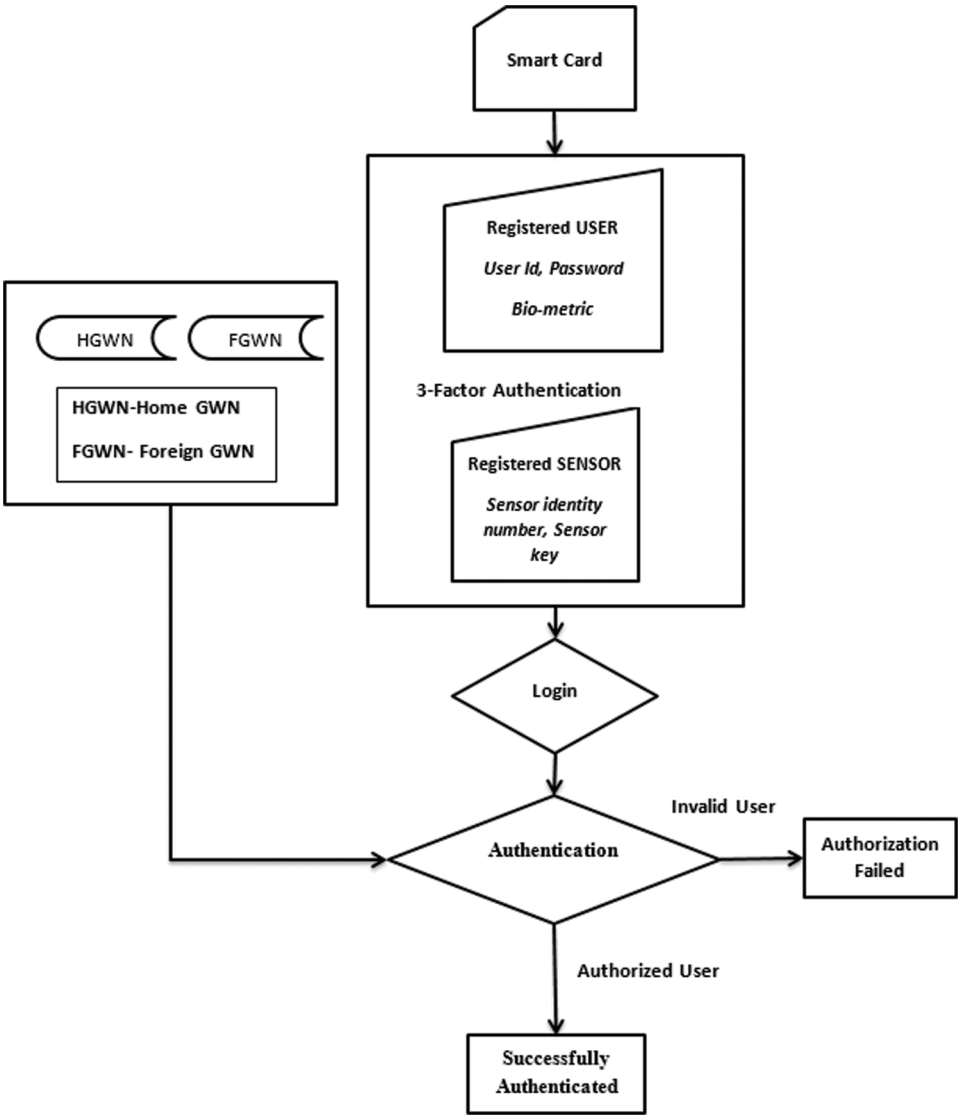

Figure 2: The multi-authentication process in GWN

Table 1: Notations used in the proposed multi-stage secure IoT authentication protocol

Notation	Description
S_{idx}	Deploy the Sensor with an index
$user_i, ID_i^u, PW_i^u, Bio_i^u$	i^{th} user and identity, password and biometric of the users
HG_{id}	home gateway node with an identity that is used to send secret information between users and sensors
FG_{id}	Identity Foreign Gate Way Node, which is used to send secret information between users and sensors
$K_{user_i}^H$	i^{th} User secret key for HGWN

(Continued)

Table 1 (continued)

Notation	Description
$K^{H}_{Sensor_j}$	j^{th} Sensor secret key for HGWN
$K^{F}_{user_i}$	i^{th} User secret key for FGWN
$K^{F}_{Sensor_j}$	j^{th} Sensor secret key for FGWN
K^{HF}	HGWN & FGWN paired secret Key
H_{S_K}	Sensor Secret key
F_{S_K}	The secret key of FGWN
S_j	Sensor coordinates
rd_i	pseudo-identity number
Sp^{H_1} and Sp^{H_2}	pseudo strings which the user generates
Sp_1, Sp_2, Sp_3	Computed string values
$nonce^{u}_{i}$	Secret message of i^{th} user
$B_{PW^{u}_{i}}$	Hashing interference rule between a password and secret message based on BAN Logic
$HBio^{u}_{i}$	Hashing interference rule for given biometric based on BAN Logic
c_1, c_2, c_3, and c_4	Computed parameters during the login process
rd^{new}_{i}	New pseudo-random identity of the i^{th} user
mg_1, mg_2, mg_3, mg_4, mg_5,mg_6,mg_7	A message which comprises a set of parameters and transmits from the user
$nonce_{uhg}$	The nonce secret message which is generated by HGWN for the i^{th} user
c_5, c_6, c_7	Computed parameters during the authentication process
$nonce^{s}_{i}$	The nonce secret message which is generated by the sensor for the i^{th} user
mg_2	The message comprises a set of parameters and is transmitted by HGWN
$Sess_k$	Session key
$Sess^{hg}_{k}$	Session key or HGWN
$c_8, c_9, c_{10}, c_{11}, c_{12}$	Parameters during the authentication process are computed at the HGWN
$Sess_{k_u}$	Session key or User
$sess^{fg}_{k_2}$	Session key or FGWN
$c_{13}, c_{14}, c_{15}, c_{16}, c_{17}$	Computed parameters during the authentication process by FGWN
$c_{18}, c_{19}, c_{20}, c_{21}, c_{22}$	Parameters during the authentication process that are computed at the FGWN
$c_{23}, c_{24}, c_{25}, c_{26}$	Parameters during the authentication process for sensor

There are several assumptions for the multifactor authentication process against the adversary. The security property analysis rule has been demonstrated below:

1. Both Identity and Password identification are in relatively small sets. Searching for both is hard and takes time, and is considered a false premise. An assumption has been made that both can be guessed in polynomial time simultaneously. The adversary cannot identify or guess the hash values or nonce or secret key numbers because it has a greater secure length.
2. The three-factor authentications are considered robust because the last one is unidentified. Since an adversary can find out the user identity and password but still not the third authentication. Through side-channel attacks, the user identity can be identified. The false-positive issue even exists in biometric recognition.
3. Through the private and public channels, the messages have been transmitted. The adversary can damage the public channel until the three-factor authentication is cracked. However, the adversary could not damage the private channel. On the GWN side, the suspected system administrator's presence can crack the registered information sent to the GWN, but it is not happening in a private channel.

The methods followed in the multifactor authentication include the five phases developed in this study: system initialization, Registration, Login, Authentication, and Password renewal.

3.2.1 System Initialization Phase

For WSN, efficient system initialization has to be designed [40]. Every GWN has its own identity, shown in the below initialization. For the HGWN, an identity HG_{id} is established, and for the FGWN, an identity FG_{id} is established. The sensor has its position recorded with a sensor index S_{idx}. Here three-way multi authentication processes are implemented. As explained below, identity, password, and biometrics have been established for every user. Between the users and sensors, secret information is sent through every identity. $K^H_{user_i}$, $K^H_{Sensor_j}$, $K^F_{user_i}$, $K^F_{Sensor_j}$ are the user's secret keys and sensors for the HGWN and the FGWN, respectively. K^{HF} is the paired secret key for both HGWN and FGWN. Hence the shared key is allocated for each GWN. The algorithm of the initialization phase is shown in Algorithm 1. Sensors are randomly deployed with generated coordinates S_j.

1. If S_{idx} is required to communicate with HGWN, it should generate a secret key using the BAN Logic approach $H_{S_K} \rightarrow hash\left(S_{idx_j} \middle\| K^H_{Sensor_j} \middle\| \|HG_{id}\|\right)$
2. If S_{idx} needs to communicate with FGWN, it should generate a secret key $F_{S_K} \rightarrow hash\left(S_{idx_j} \middle\| K^F_{Sensor_j} \middle\| \|FG_{id}\|\right)$
3. Finally, S_{idx} information is saved in both the gateway node and S_j next, the secret key is stored by S_j.

Algorithm 1: System initialization phase

$S_{idx} \rightarrow$ Deploy the Sensor with index.

$user_i, ID^u_i, PW^u_i, Bio^u_i$ –ith user and identity, password, and biometric of the users.

$HG_{id} \rightarrow$ *home gate way node with identity*

$FG_{id} \rightarrow$ *indentity Foreign Gate Way Node*

send secret information between users and sensors

$K^H_{user_i} \rightarrow i^{th}$ *User secret key for HGWN*

(Continued)

Algorithm 1: (continued)

$K^{H}_{Sensor_j} \rightarrow j^{th}$ *Sensor secret key for HGWN*

$K^{F}_{user_i} \rightarrow i^{th}$ *User secret key for FGWN*

$K^{F}_{Sensor_j} \rightarrow j^{th}$ *Sensor secret key for FGWN*

$K^{HF} \rightarrow$ *HGWN & FGWN paired secret Key*

3.2.2 Registration Phase

In this phase, after the sensor nodes are deployed in the target field, the information in the sensor nodes is sent to the legally registered user. Each sensor node has access using a secret key shared between the gateway nodes with authentication and key agreement. The registration phase involves sensor registration and user registration.

Sensor Registration

The sensor nodes are randomly deployed with general coordinates S_j. The sensor index S_{idx} generated a secret key H_{S_K} using the BAN Logic approach for communication with HGWN and also to communicate with the FGWN, a secret key F_{S_K} is generated. The secret key information is stored in both gateway nodes HGWN ad FGWN and S_j. Only S_j stores the secret key. Sensor registration steps are shown in Algorithm 2.

Algorithm 2: Sensor registration

Deploy sensor randomly with generated coordinates S_j

If S_{idx} required to communicate with that HGWN, it should generate a secret key using the BAN Logic approach $H_{S_K} \rightarrow hash\left(S_{idx_j} \middle\| K^{H}_{Sensor_j} \middle\| \|HG_{id}\|\right)$

If S_{idx} needs to communicate with FGWN, it should generate a secret key $F_{S_K} \rightarrow hash\left(S_{idx_j} \middle\| K^{F}_{Sensor_j} \middle\| \|FG_{id}\|\right)$

Finally, S_{idx} information is saved in both the gateway node and S_j next, the secret key is stored by S_j.

User Registration

The user registration undergoes three main steps to send the secret messages.

First: the ith user $User_i$ selected the user-id ID^{u}_{i} and the password PW^{u}_{i} and biometric recognition $Bio^{u}_{i}is$ marked as an input into the terminal. In the terminal, the pseudo-identity and nonce can generate the random string. The hash reference rule-based BAN logic approach generates password and secret key messages. Meanwhile, the secret message is converted to a secret number for security purposes. The user identity ID^{u}_{i} and pseudo-identity number rd_i are encrypted with the help of a multi-search tree and sent to the HGWN gateway identity HG_{id} securely.

Second: the user identification number and pseudo-identity number retrieved data through decryption with the help of a multi-search tree and stored in the Database. The two pseudo strings $Sp^{H_1} and Sp^{H_2}$ are generated. These strings are transmitted to the user $User_i$ through the BST encryption method.

Third: then the value Sp_1, Sp_2, Sp_3 have been calculated through these pseudo strings. In the smart card, the three values of Sp_1, Sp_2, Sp_3 and the pseudo-identity rd_i is stored. User registration is shown in Algorithm 3.

Algorithm 3: User registration

1. i[th] User chooses the user-id ID_i^u, password PW_i^u and give biometric Bio_i^u input
2. Produce a random string that is generated by pseudo-identity rd_i and secret message $nonce_i^u$ by the terminal.
3. Compute BAN logic based on the hashing inference rule between a password and secret message $B_{PW_i^u} \rightarrow hash\left(PW_i^u||nonce_i^u\right)$ & logic applied to convert the secret number from a secret message $HBio_i^u \rightarrow hash\left(Bio_i^u\right)$
4. Then user-id ID_i^u and rd_i are encrypted and formed codebook, which is computed by the multi-search tree and sent to HG_{id} in a secure manner.
5. At the HG_{id} the received data decrypted by a multi-search tree and ID_i^u and rd_i information is saved in the Database.
6. Also, compute two pseudo strings using the BAN logic hashing inference rule at the HG_{id}, i.e., $Sp^{H_1} \rightarrow hash\left(rd_i \middle\| K_{user_i}^H \middle\| HG_{id}\right)$
7. $Sp^{H_2} \rightarrow hash\left(ID_i^u \middle\| K_{user_i}^H \middle\| HG_{id}\right)$
8. Now the Sp^{H_1} & Sp^{H_2} are transmitted to the $user_i$ via a secured way by BST encryption
9. Then $user_i$ compute the $Sp_1 \rightarrow Sp^{H_1} \oplus B_{PW_i^u}, Sp_2 \rightarrow Sp^{H_2} \oplus HBio_i^u$,

   $Sp_3 \rightarrow hash\left(ID_i^u \middle\| PW_i^u \middle\| HBio_i^u\right) \oplus Bio_i^u$
10. Store the (Sp_1, Sp_2, Sp_3, rd_i) in the $user_i$ smart card

3.2.3 Login Phase

The login phase describes the authenticated user $User_i$ access the sensor index number S_{idx} using the user id $user_i$, password, PW_i^u and biometric recognition Bio_i^u in the terminal. After selecting these three inputs, a new pseudo-identity number rd_i^{new} and an arbitrary value $nonce_i^u$ are generated by the smart card and select the S_{idx_j}. Then the $HBio_i^u$ value is calculated, and pseudo code strings here $Sp^{H_1} and Sp^{H_2}$ are measured from the results obtained. With the help of these values and secret messages, the parameters c_1, c_2, c_3, and c_4 are figured out. Finally, the user $User_i$ can send the secret message with a new pseudo-identity number, secret index number, and parameters to the HGWN. The login phase algorithm is shown in Algorithm 4.

Algorithm 4: Login phase

When $user_i$ needs to access some sensor S_{idx}

1. Select $user_i$, PW_i^u and Bio_i^u
2. The smart card creates pseudo-identity rd_i^{new}, $nonce_i^u$ and select S_{idx_j}
3. Calculates $HBio_i^u \rightarrow hash\left(PW_i^u||Bio_i^u\right)$
4. From the obtained $HBio_i^u$, it calculates the following information, $Sp^{H_1} \rightarrow hash\left(Sp_1||HBio_i^u\right), Sp^{H_2} \rightarrow hash\left(Sp^{H_1}||HBio_i^u\right)$
5. Next, use the generated pseudo information and secret message to compute the following parameters, $c_1 \rightarrow Sp^{H_1} \oplus nonce_i^u$

(Continued)

Algorithm 4: (continued)

6. $c_2 \rightarrow hash\left(nonce_i^u||S_{idx_j}\right)||ID_i^u$
7. $c_3 \rightarrow Sp^{H_2} \oplus hash\left(nonce_i^u||ID_i^u\right) \oplus rd_i^{new}$
8. $c_4 \rightarrow hash\left(ID_i^u||rd_i||rd_i^{new}\left|\right|S_{idx_j}\left|\right|nonce_i^u\right)$
9. Now $user_i$ send the $mg_1 \rightarrow \left\{rd_i, S_{idx_j}, c_1, c_2, c_3, c_4\right\}$ to HGWN

3.2.4 Authentication Phase

In the authentication phase, the HG_{node} measures the nonce value $nonce_i^u$ and user identity ID_i^u. Then check the user identity in the Database. If it is not present, the sensor allocation process is immediately aborted, and a non-registered user caption is declared. If the sensor index number found in the HGWN Database proceeds to model 1 that defines the process of secret message, and if it is not present, it proceeds to model 2, where it is in search of a foreign gateway node FGWN. Algorithm 5 shows the procedure of the authentication process.

Algorithm 5: Authentication phase

Initially HG_{node} estimate the $nonce_i^u \rightarrow c_1||hash\left(rd_i\left|\right|K_{user_i}^H\left|\right|HG_{id}\right)$ and $ID_i^u \rightarrow c_2||hash\left(nonce_i^u||S_{idx_j}\right)$ compute user-id ID_i^u is in Database

If the ID_i^u is not in the Database, then the sensor allocation process will be aborted and declared as not registered user.

H-GWN compute $Sp^{H_2} \rightarrow hash\left(ID_i^u\left|\right|K_{user_i}^H\left|\right|HG_{id}\right)$

$rd_i^{new} \rightarrow c_3||hash\left(nonce_i^u||ID_i^u\right)$

Check c_4 is equal to $hash\left(ID_i^u||rd_i||rd_i^{new}\left|\right|S_{idx_j}\left|\right|nonce_i^u\right)$

If it is satisfied according to the deployment place of S_{idx_j}. There are 2 cases here.

If S_{idx} founded in H-GWN in Database

Perform model 1

Else

Perform model 2

End

- ***Model 1:***

If the HGWN database has the sensor index number S_{idx} value, then it performs model 1, and it comprises four steps.

Step 1: In this step, the HGWN chooses the nonce secret message $nonce_{uhg}$ and calculates the HGWN secret key H_{S_K} and also c_5, c_6, c_7 parameters, and finally, the message scheme mg2 contains the parameters sent to the S_j by HGWN.

Step 2: calculate the nonce value and nonce secret message computed by sensor S_j. Furthermore, check whether the c_7 value equals the hash value. If it equals, then select the $nonce_i^s$ by S_j. and also calculate the session key $Sess_k$, and parameters c_8 and c_9. Finally, send the mg3 containing c_8 and c_9 to HGWN by sensor node S_j.

Step 3: In this step the $nonce_i^s$, $Sess_k^{hg}$ the nonce value and session key of HGWN. Then verify the c_9 value equals the hash value, and if it equals, then it calculates the pseudo number $Sp_{new}^{H_1}$ and the parameters c_{10}, $c_{11,}$ and c_{12} values are measured. Then the message mg4 contains c_8, c_{10}, $c_{11,}$ and c_{12} are sent to $User_i$.

Step 4: The smart card calculates the pseudo number and nonce values from the parameters and hash values after the mg4 is received. Then session value is computed, and if c12 equals the hash value of respected identity values and pseudo number values, then the new values of pseudo number and pseudo-identity are measured by the card. Finally, replace the rd_i, Sp_1 to the rd_i^{new}, Sp_1^{new}.

- ***Model 2:***

If the HGWN database does not have the sensor index number S_{idx} value, then it performs model 2, and it is comprised of the following steps:

Step 1- The HGWN transmits the mg5 message containing the pseudo-identity number, sensor identity number S_{idx_j} and home gateway identity to other gateways GWNs. FGWN checks for the existence of the sensor identity number, and if it is present, then FGWN measures the F_{S_K}, c_{13} and c_{14}. The parameter and FGWN identity c_{14}, FG_{id} contained in mg6 are sent to HGWN.

Step 2- The HGWN computed the new pseudo-identity number, c_{15}, $c_{16,}$ and c_{17} values. Then the message mg7 is sent to $User_i$ contains c15, c16, c17, and FG_{id}.

Step 3- After receiving the mg7 value, the smart card measures the $Sp_{new}^{H_1}$ and verifies c17 equals to hash values of the set; then, it creates another secret message for the user and $nonce_{i_2}^u$. Then calculates c18 and c19 and at last mg 8 contains rd_i, c_{18}, c_{19} sent to FGWN.

Step 4- Now FGWN calculates the $nonce_{i_2}^u$ value. Checking the c19 value equals hash values, it created the $nonce_{ufg}$, c_{20}, $c_{21,}$ and c_{22}. Then the mg9 contains c_{20}, $c_{21,}$ and c_{22} sent to the sensor identity number from FGWN.

Step 5- the sensor node S_j estimated the nonce value $nonce_{ufg}$, $nonce_{i_2}^u$ and verifies c22 equals hash values, then send Sj created a random number $nonce_{ufg}^2$.

Step 6- $nonce_{ufg}^2$ value has been generated. Then FGWN session key $sess_k^{fg}$ is computed with hash values. C24 verified if it equals hash values and c25 and c26 formed. Nonce values exhibited and $sess_{k_2}^{fg}$ are created. After verification with c26 and finally updates (S_{idx_j}, Sp_1) with $\left(S_{idx_j}^{new}, Sp_1^{new}\right)$.

3.2.5 Password Renewal

If the user forgets the password and knows the rest of the authentication details, still the user cannot access the secured gateway. The only option to change or renew the password is to follow the steps of password renewal by the user. The multi-search tree used the binary search concept for cipher values. It encrypts the message and decrypts the message at the receiver side to check the system's security. Algorithm 6 illustrates the password renewal steps.

Algorithm 6: Password renewal

1. Secret Key Generation

$key_{Sec} \rightarrow [K_{s0}, K_{s1}, \ldots K_{s15}]$

key_{Sec} is an 8-bit character to create a weight matrix W_0

$$W_0 = \left(\frac{K_{s0} \oplus K_{s1} \oplus \ldots K_{s15}}{2^8} + \frac{\sum_{i=8}^{15} K_{si}}{2^{64}}\right)/2$$

(Continued)

Algorithm 6: (continued)

2. Determine the depth of Candidate value in the weight matrix,

$N_{candidate} \rightarrow round(W_0 * inp)$

inp–input value

3. Creating Multi-Search Tree candidate

$can_{bst} \rightarrow round(W_i \times 255) \cdots\cdots i = 1 \ldots n$

4. $BST_{rule} \rightarrow round(can_{bst} \times 7) + 1$

5. $p = N + 1, \ldots, 2N$

6. Convert value in cipher with the help of BST_{rule}

7. For decryption, it will perform a reverse manner

4 Research Results and Discussion

The proposed method used multi-stages to authenticate users. Home and foreign gateways are used like HGWN and FGWN. The user registration and sensor registration are performed through the BAN logic approach. It has been evaluated through several experiments. The performance of the proposed IoT authentication method is evaluated in terms of metrics such as authorized and unauthorized sensors, energy utilization, network lifetime, misdetection probability, false-positive rate, and packet loss. These performance metrics results have been compared with other existing methods like Trust-Based Monitoring (TBM), Multi-Source Feedback Trust (MFTM), Software-defined networking-based (SDN-MG), and SMER. Trust-Based (TBM) follows the spoof detection, and trust construction and authenticates the message [39]. Multi-Source Feedback Trust (MFTM) depends on the lightweight trust mechanism reliable methodology. Software-defined networking-based (SDN-MG) security mechanism ensures data transfer security and continuous data flow. SMER is a secure method to exchange resources based on administering security in IoT environments resource exchange. The above traditional methods are used for analysis purposes since they are based on trust-based analysis and authentication.

4.1 NS3 Tool

NS-3 simulator tool was used to evaluate the proposed protocol. NS-3 provides an open, extensible network simulation platform. NS-3 simulates data packet networks, provides high performance, simulates the user's engine, and provides a highly controlled system behavior and a reproducible learning network environment. It focuses on the protocols of the Internet and the working of the network. Moreover, the NS-3 tool can also be used for non-Internet-based systems.

4.2 Performance Analysis

The performance of this proposed method is analyzed by several metrics and compared with other existing methods using the NS3 tool as follows.

4.2.1 Sensors in the GWN

Sensors near the gateway node share the secret message after proper authentication in HGWN. If the sensor presents and shares the message to another gateway node but is still near, the sensor is FGWN. In Fig. 3, 100 sensors represented as green dots are around the HGWN, and sensors around FGWN are represented as blue dots.

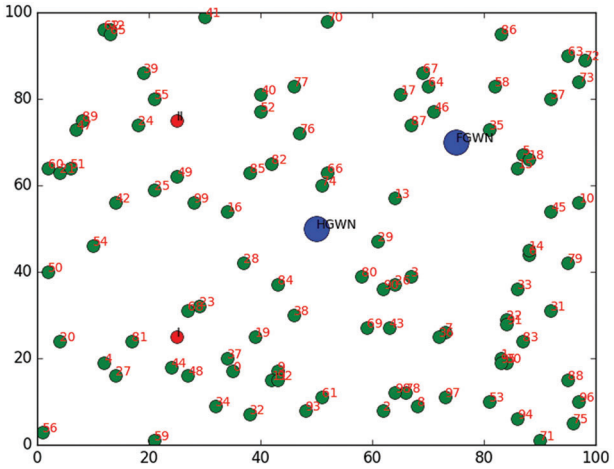

Figure 3: Authenticated sensors around the HGWN and FGWN

Fig. 4 shows the unauthenticated sensors as black dots. The sensor is considered unauthenticated if any authentications fail in the three-way authentication.

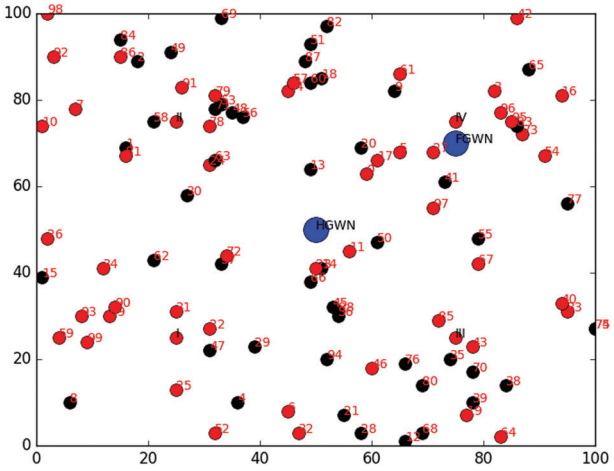

Figure 4: Unauthenticated sensors around HGWN and FGWN

4.2.2 Energy Utilization Comparison

The energy utilization of the proposed method is evaluated and compared with other existing methods, TBM [39], MFTM, SDN-MG, and SMER. If the message byte increases, the required energy to share the message increases. In Fig. 5, the proposed method increases energy utilization as the message bytes increase. Compared with other methods like SDN-MG, it shows a higher energy utilization than MFTM and SMER. In the case of TBM, energy utilization is sometimes better compared to others. The energy consumption has to be minimized concerning the message bytes.

4.2.3 Network Lifetime Comparison

The network lifetime depends on the energy consumption for sharing the message. If the network lifetime is high, then the processing and computational time are optimized, leading to efficiency in the whole process. Hence, more energy remaining leads to extra process time and a prolonged network

lifetime. The comparison of a network lifetime with other existing methods is shown in Fig. 6. The proposed method shows a higher network lifetime under the same number of iterations. In case of energy loss, the data transmission decreases, and the remaining sensors used for the process are considered network failure. In the 4 cases of iterations, the network lifetime shows better results with the proposed protocol.

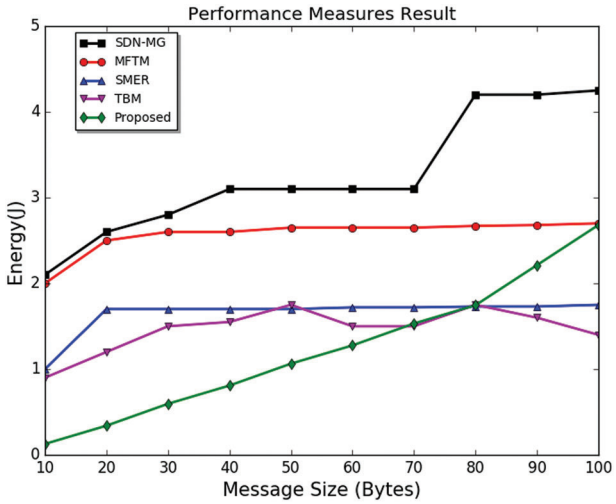

Figure 5: Comparison of energy utilization

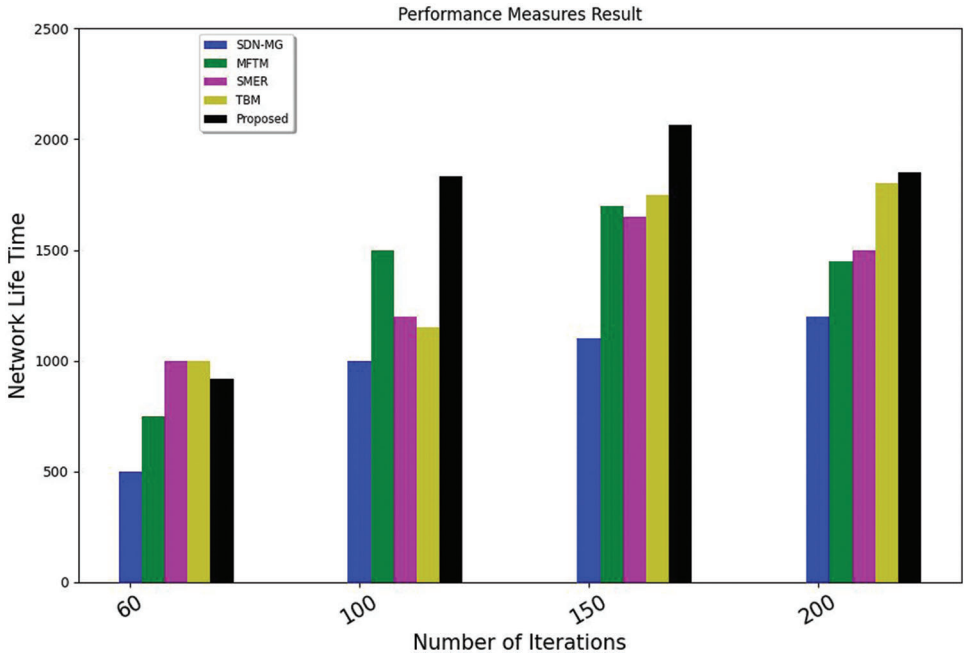

Figure 6: Comparison of network lifetime

4.2.4 Probability of Misdetection

The verification and trust monitoring levels are followed in the misdetection rate measurement. The misdetection may be present during the communication process. It is expected to be detected at an early stage, and even though it passed through initial analysis, it is detected at another stage by the evaluation

factors. The misdetection probability rate is low when false alarm probability is low. The malicious sensor based on the BAN logic approach detection is called misdetection. In Fig. 7, the proposed method shows a decreased misdetection rate and a decreased false alarm rate. Compared to other existing approaches, the SDN-MG shows the highest malicious detection, followed by MFTM, SMER, and TBM, respectively [39].

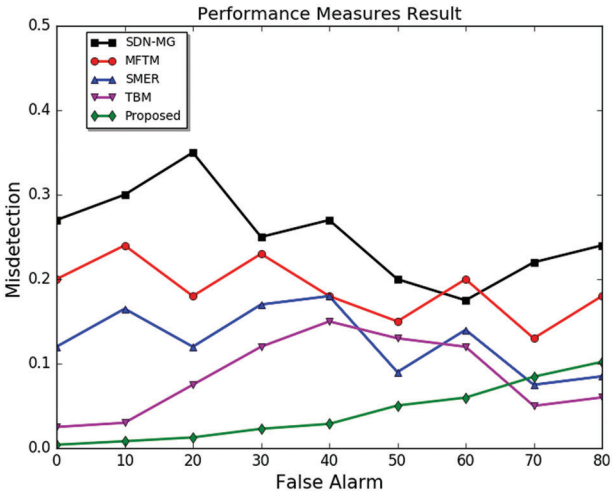

Figure 7: Probability of misdetection comparison

4.2.5 False Positive Rate

With the increase in distance, the false-positive rate varies. The device becomes illegal when the proximity between the devices increases. The false-positive rate is decreased by detecting the malicious threats accurately in the network. Fig. 8 compares the false-positive rate values with other approaches under different distances. Previous methods show a higher false-positive rate compared to the proposed method.

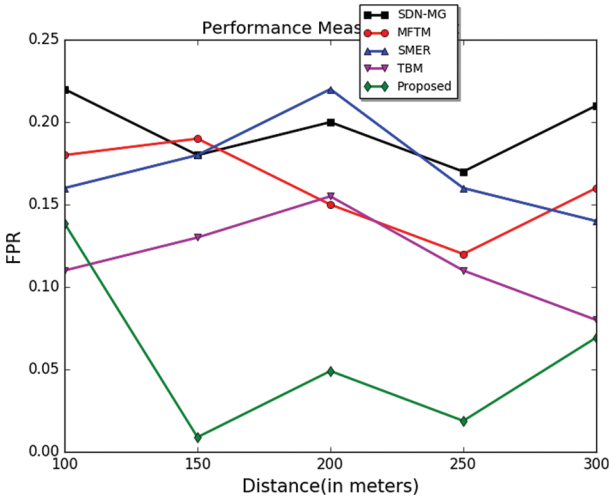

Figure 8: False positive rate comparisons

4.2.6 Packet Loss

The authenticated packets should be delivered correctly to lead to a decrease in packet loss. If the sent packets are not delivered to the desired destination, packet loss is termed. It is considered a reduction in the accuracy of delivering the packets. Fig. 9 compares the packet loss of the proposed method with previous methods. SDN-MG has the highest packet loss rate, followed by MFTM, SMER, and TBM [39]. The packet loss rate slightly increased with the increase in the number of devices.

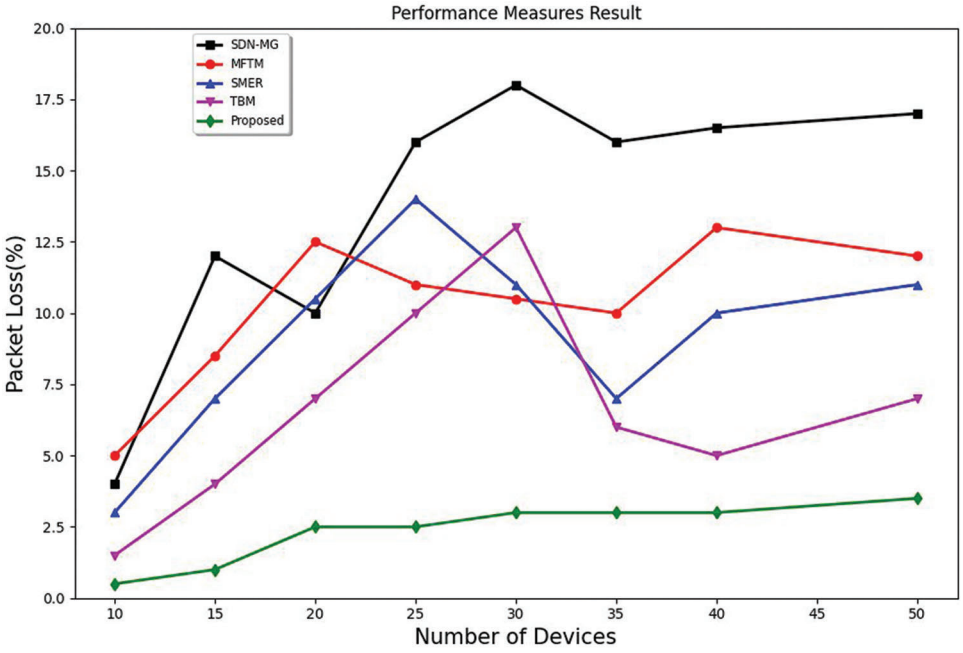

Figure 9: Packet loss comparisons

4.2.7 Communication Cost

Fig. 10 compares the communication cost of the authentication process to other protocols with the increase in the message size. For acceptable packets, the authentication signature is placed in message authentication. The comparisons were also made to ensure that communication security improves reliability. The transmission process determines the communication message rate after the authentication process. It can be noticed that under the same message size, the proposed method's communication cost is less than the cost of the TBM method, which has a medium communication cost rate. The LSS method shows the highest communication cost value [39]. The communication rate increases for all three methods by increasing the message size rate.

4.2.8 Measurement of Time consumption, throughput, and End-to-End delay

Different schemes are compared in terms of time consumption, throughput, and End-to-End Delay. Based on the network transmission message rate, the time taken to share and receive the message has been measured in ms, as shown in Fig. 11. The throughput value is measured in bps and is shown in Fig. 12, and the End-to-End delay is measured in seconds and shown in Fig. 13.

From Fig. 11, the proposed method's time consumption decreases compared to other studies, indicating performance improvement. From Fig. 12, it can be noticed that the proposed method throughput value is less compared to other existing studies. From Fig. 13, it can be seen that the end-to-end delay value decreased compared to other methods, which improves the accuracy and reliability of the proposed method.

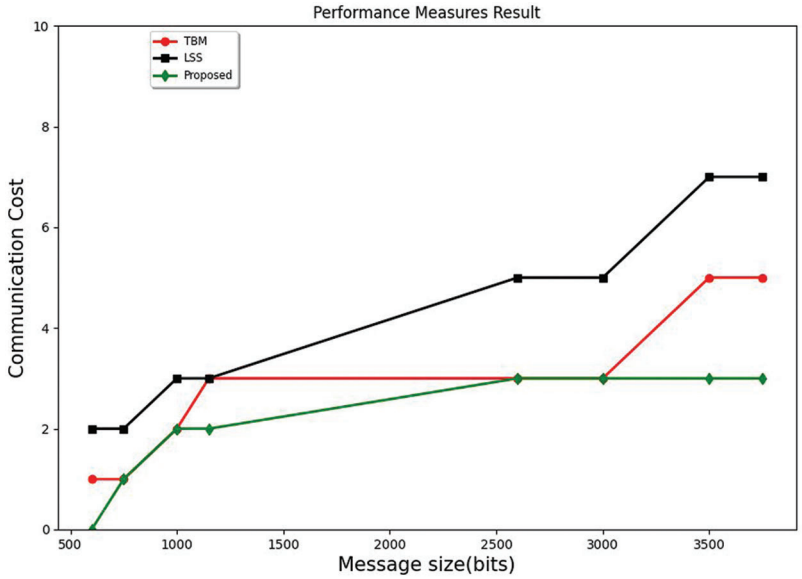

Figure 10: Communication cost comparison

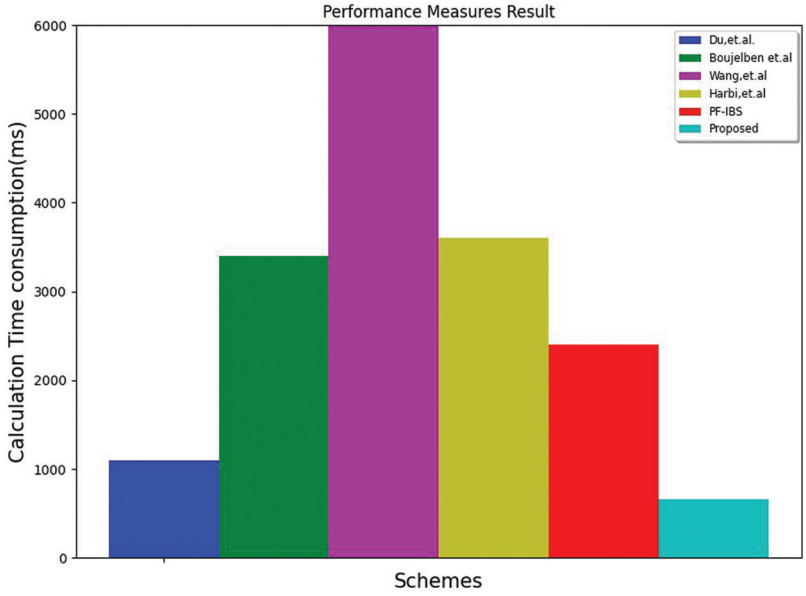

Figure 11: Time consumption calculation comparison

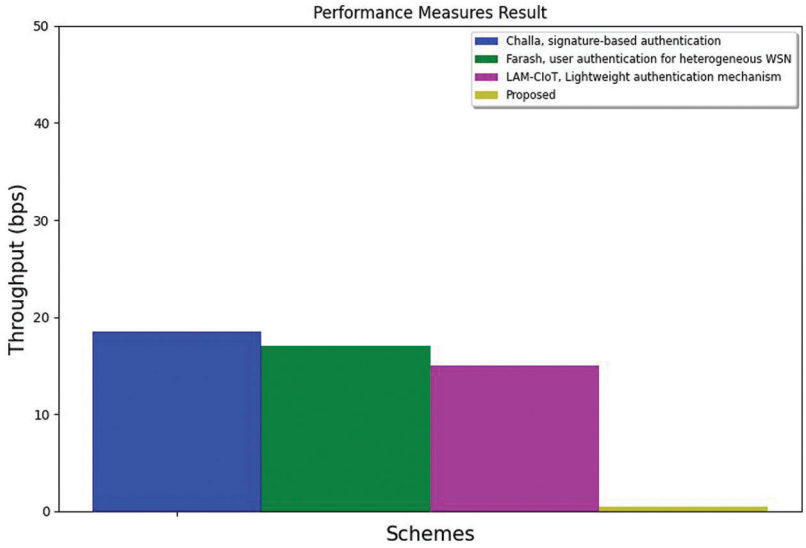

Figure 12: Throughput comparison

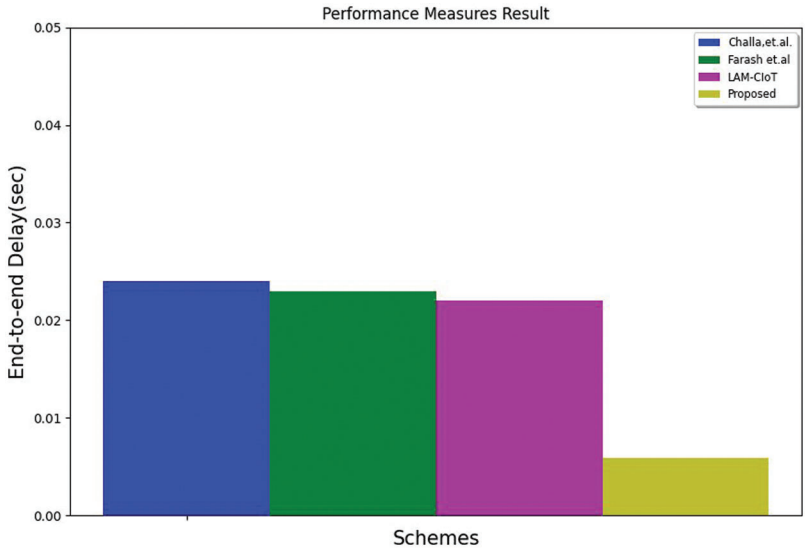

Figure 13: End-to-end delay comparison

5 Conclusions and Future Work

This study proposes a multi-authentication scheme using five steps: Initialization, user and sensor registration, login, authentication, and password renewal. The proposed scheme has been implemented on the Home Gateway Node (HGWN) and Foreign Gateway Node (FGWN). The 3-way authentication of user identity number, Password, and biometric recognition is followed. BAN logic approach of the hash inference rule is used to register the user and the sensor in a secure and trustworthy way. The proposed method ensures that secret message sharing and registration information sharing are done in an authenticated manner. If any one of the authentications fails, it is considered an unauthorized user. The proposed method has been evaluated in terms of performance metrics like False-Positive Rate (FPR), Network lifetime, packet loss, communication cost, and energy consumption and compared with other existing methods. The time consumption and End-to-End delay have been reduced, and the throughput

value increased slightly. The loss of message packets, False positive rate value, and misdetection rate have been reduced. The energy consumption increased with the increase in the size of the messages. The network lifetime also increased in this proposed method. The communication cost is slightly high concerning the processing and message sharing rates. The main drawback is that BAN logic-based protocols sometimes have to be insecure and cannot be distinguished, and these variations tend to be critical. This protocol provides high security and robustness. Because of the inconsistency and insecurity in BAN logic, the log-regularly varying distribution protocol can be implemented and considered a possible avenue for future work.

Acknowledgement: Thanks to the Saudi Electronic University for sponsoring this work.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] P. Sarwesh, N. S. V. Shet and K. Chandrasekaran, "Energy efficient network design for IoT healthcare applications," in *Internet of Things and Big Data Technologies for Next Generation Healthcare*, Cham, Switzerland, Springer, pp. 35–61, 2017.

[2] A. Tiwary, M. Mahato, A. Chidar, M. K. Chandrol, M. Shrivastava *et al.,* "Internet of Things (IoT): Research, architectures and applications," *International Journal on Future Revolution in Computer Science & Communication Engineering*, vol. 4, no. 3, pp. 23–27, 2018.

[3] P. Sanmartin, A. Rojas, L. Fernandez, K. Avila, D. Jabba *et al.,* "Sigma routing metric for RPL protocol," *Sensors*, vol. 18, no. 4, pp. 1–18, 2018.

[4] M. Conti, P. Kaliyar, M. Rabbani and S. Ranise, "Attestation-enabled secure and scalable routing protocol for IoT networks," *Ad Hoc Networks*, vol. 98, no. 3, pp. 102054, 2020.

[5] K. Haseeb, A. Almogren, N. Islam, I. U. Din and Z. Jan, "An energy-efficient and secure routing protocol for intrusion avoidance in IoT-based WSN," *Energies*, vol. 12, no. 21, pp. 354–369, 2019.

[6] A. O. A. Salem and N. Shudifat, "Enhanced LEACH protocol for increasing a lifetime of WSNs," *Personal and Ubiquitous Computing*, vol. 23, no. 5-6, pp. 901–907, 2019.

[7] H. Kim, J. Ko, D. E. Culler and J. Paek, "Challenging the IPv6 routing protocol for low-power and lossy networks (RPL): A survey," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 4, pp. 2502–2525, 2017.

[8] F. A. Khan, M. Khan, M. Asif, A. Khalid and I. U. Haq, "Hybrid and multi-hop advanced zonal-stable election protocol for wireless sensor networks," *IEEE Access*, vol. 7, pp. 25334–25346, 2019.

[9] C. Nakas, D. Kandris and G. Visvardis, "Energy efficient routing in wireless sensor networks: A comprehensive survey," *Algorithms*, vol. 13, no. 3, pp. 1–65, 2020.

[10] E. Bertino, V. Casola, A. Castiglione and W. Susilo, "Security and privacy protection vs. sustainable development," *Computer Security*, vol. 76, pp. 250–251, 2018.

[11] D. N. Serpanos and A. G. Voyiatzis, "Security challenges in embedded systems," *ACM Transactions on Embedded Computing Systems*, vol. 12, no. 1, pp. 1–10, 2013.

[12] B. Aboushosha, R. A. Ramadan, A. D. Dwivedi, A. El-Sayed and M. Dessouky, "SLIM: A lightweight block cipher for internet of health things," *IEEE Access*, vol. 8, pp. 203747–203757, 2020.

[13] C. G. García, E. R. Núñez-Valdez, V. García-Díaz, C. P. García-Bustelo and M. Cueva Lovelle, "A review of artificial intelligence in the internet of things," *International Journal of Interactive Multimedia and Artificial Intelligence*, vol. 5, no. 4, pp. 9–20, 2019.

[14] D. Saeed, R. Iqbal, H. H. R. Sherazi and U. G. Khan, "Evaluating near-field communication tag security for identity theft prevention," *Internet Technology Letters*, vol. 2, no. 5, pp. e123, 2019.

[15] Z. Hong, W. Chen, H. Huang, S. Guo and Z. Zheng, "Multi-hop cooperative computation offloading for industrial IoT-edge-cloud computing environments," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 12, pp. 2759–2774, 2019.

[16] A. Yousefpour, G. Ishigaki, R. Gour and J. P. Jue, "On reducing IoT service delay via fog offloading," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 998–1010, 2018.

[17] M. S. Hossain, C. I. Nwakanma, J. M. Lee and D. S. Kim, "Edge computational task offloading scheme using reinforcement learning for IIoT scenario," *ICT Express*, vol. 6, no. 4, pp. 291–299, 2020.

[18] H. W. Kim, J. H. Park and Y. S. Jeong, "Adaptive job allocation scheduler based on usage pattern for computing offloading of IoT," *Future Generation Computer Systems*, vol. 98, no. 2, pp. 18–24, 2019.

[19] B. Jan, H. Farman, H. Javed, B. Montrucchio, M. Khan *et al.,* "Energy efficient hierarchical clustering approaches in wireless sensor networks: A survey," *Wireless Communications and Mobile Computing*, vol. 2017, pp. 1–14, 2017.

[20] H. Wei, H. Luo, Y. Sun and M. S. Obaidat, "Cache-aware computation offloading in IoT systems," *IEEE Systems Journal*, vol. 14, no. 1, pp. 61–72, 2020.

[21] H. R. Ghorbani and M. H. Ahmadzadegan, "Security challenges in internet of things: Survey," in *2017 IEEE Conf. on Wireless Sensors (ICWiSe)*, Miri, Malaysia, IEEE, pp. 1–6, 2017.

[22] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *2017 Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), 2017*, Palladam, India, IEEE, pp. 32–37, 2017.

[23] D. S. David and A. Jeyachandran, "A comprehensive survey of security mechanisms in healthcare applications," in *2016 Int. Conf. on Communication and Electronics Systems (ICCES)*, Coimbatore, India, IEEE, pp. 1–6, 2016.

[24] N. A. El-mawla, M. Badawy and H. Arafat, "Security and key management challenges over WSN (A Survey)," *International Journal of Computer Science & Engineering Survey (IJCSES)*, vol. 10, no. 1, pp. 15–34, 2019.

[25] P. Nalajala and S. B. Lakshmi, "A secured IoT based advanced health care system for medical field using sensor network," *International Journal of Engineering & Technology*, vol. 7, no. 2. 20, pp. 105–108, 2018.

[26] R. S. Harry and R. Joseph, "Enhancements in anomaly detection in body sensor networks," in *2019 IEEE Int. Conf. on Computational Science and Engineering (CSE) and IEEE Int. Conf. on Embedded and Ubiquitous Computing (EUC)*, New York, NY, USA, IEEE, pp. 384–389, 2019.

[27] F. T. Zuhra, K. A. Bakar, A. Ahmed and M. A. Tunio, "Routing protocols in wireless body sensor networks: A comprehensive survey," *Journal of Network and Computer Applications*, vol. 99, pp. 73–97, 2017.

[28] R. Gravina, P. Alinia, H. Ghasemzadeh and G. Fortino, "Multi-sensor fusion in body sensor networks: State-of-the-art and research challenges," *Information Fusion*, vol. 35, no. 3, pp. 68–80, 2017.

[29] K. H. Yeh, "A secure IoT-based healthcare system with body sensor networks," *IEEE Access*, vol. 4, pp. 10288–10299, 2016.

[30] A. J. Abraham, A. Thomas and J. Pradeep, "IoT based real time cardiac activity monitoring system using body sensor network," *International Journal of Pure and Applied Mathematics*, vol. 120, no. 6, pp. 1455–1464, 2018.

[31] S. K. Yang, Y. M. Shiue, Z. Y. Su, I. H. Liu and C. G. Liu, "An authentication information exchange scheme in WSN for IoT applications," *IEEE Access*, vol. 8, pp. 9728–9738, 2020.

[32] M. S. Farash, M. Turkanović, S. Kumari and M. Hölbl, "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment," *Ad Hoc Networks*, vol. 36, no. 6, pp. 152–176, 2016.

[33] X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah *et al.,* "A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments," *Journal of Network and Computer Applications*, vol. 103, pp. 194–204, 2018.

[34] J. Y. Lee, W. C. Lin and Y. H. Huang, "A lightweight authentication protocol for internet of things," in *2014 Int. Symp. on Next-Generation Electronics (ISNE)*, Kwei-Shan Tao-Yuan, Taiwan, IEEE, pp. 1–2, 2014.

[35] P. Gope and T. Hwang, "BSN-Care: A secure IoT-based modern healthcare system using body sensor network," *IEEE sensors journal*, vol. 16, no. 5, pp. 1368–1376, 2015.

[36] S. Challa, M. Wazid, A. K. Das, N. Kumar, A. G. Reddy *et al.,* "Secure signature-based authenticated key establishment scheme for future IoT applications," *IEEE Access*, vol. 5, pp. 3028–3043, 2017.

[37] N. Li, D. Liu and S. Nepal, "Lightweight mutual authentication for IoT and its applications," *IEEE Transactions on Sustainable Computing*, vol. 2, no. 4, pp. 359–370, 2017.

[38] W. Teepe, "On BAN logic and hash functions or: How an unjustified inference rule causes problems," *Autonomous Agents and Multi-Agent Systems*, vol. 19, no. 1, pp. 76–88, 2009.

[39] F. Alqahtani, Z. Al-Makhadmeh, A. Tolba and O. Said, "TBM: A trust-based monitoring security scheme to improve the service authentication in the internet of things communications," *Computer Communications*, vol. 150, no. 15, pp. 216–225, 2020.

[40] L. Chan, K. Gomez-Chavez, H. Rudolph and A. Hourani, "Hierarchical routing protocols for wireless sensor network: A compressive survey," *Wireless Networks*, vol. 26, no. 5, pp. 3291–3314, 2020.