ISSN: 2584-0495 Vol. 2, Issue 2, pp. 591-597

International Journal of Microsystems and IoT

ISSN :(Online) Journal homepage: https://www.ijmit.org

# Cryptanalysis of a Biometric based Anonymous Authentication Approach for IoT Environment

**Khushboo Jha, Sumit Srivastava and Aruna Jain**

**Cite as:** Jha, K., Srivastava, S., & Jain, A. (2024). Cryptanalysis of a Biometric based Anonymous Authentication Approach for IoT Environment. International Journal of Microsystems and IoT, 2(2), 591-597. https://doi.org/10.5281/zenodo.10804461

© 2024 The Author(s). Published by Indian Society for VLSI Education, Ranchi, India

Published online: 20 February 2024.

Submit your article to this journal:

Article views:

View related articles:

View Crossmark data:

**DOI:** https://doi.org/10.5281/zenodo.10804461

Full Terms & Conditions of access and use can be found at https://ijmit.org/mission.php

International Journal of Microsystems and IoT
Vol. 2, Issue 2, pp. 591-597; DOI: https://doi.org/10.5281/zenodo.10804461

# Cryptanalysis of a Biometric-based Anonymous Authentication Approach for IoT Environment

Khushboo Jha, Sumit Srivastava and Aruna Jain

Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi, India.

**ABSTRACT**
Network-based services place significant emphasis on user authentication as a critical security concern. Li et al. have proposed a user authentication method for wireless sensor networks in IoT environments, utilising a three-factor authentication approach. They claimed that their approach has numerous advantages and is capable of enduring different types of attacks. However, this study examines the weaknesses of the aforesaid technique and identifies many types of the attacks, including sensor node capture assault, user impersonation attack, sensor node impersonation attack, session key leak attack, and gateway node impersonation attack. Hence, it is demonstrated that the suggested method is unsuitable for applications based on wireless sensor networks in an IoT environment. In addition, a reliable multimodal biometric system using face and speech modality, is suggested as a solution to tackle with the aforesaid vulnerable authentication scheme.

**KEYWORDS**
Cryptographic attacks; Cryptanalysis; Internet of Things (IoT); Biometrics; Security; Wireless Sensor Networks (WSN)

## 1. INTRODUCTION

In the present era, the network has become ubiquitous, with an increasing number of services and applications being delivered through it. Due to the network's intrinsic openness, attackers have the ability to eavesdrop on, intercept, and manipulate with messages delivered across the public channel. Ensuring safe communication on an insecure route has become a significant concern. The user authentication system is a straightforward and efficient method for addressing this security concern. It enables the remote server to authenticate the user's identity when the user seeks access to the remote server. Following Lamport's initial proposal [1] for a user authentication mechanism in an unsecured channel, other researchers have made significant contributions [2] and achieved notable advancements in this field. In password-based systems, the user provides their identity and password to the distant server. The server then verifies the user's validity by comparing their identity and password with the stored information. Consequently, in the majority of user authentication systems that rely on passwords, the server must maintain a verification table in order to authenticate users. However, this practice can make the system vulnerable to a leak-of-verifier attack [3]. Integrating a biometric authentication [4-5] approach can enhance the effectiveness of password-based methods.

Moreover, since the IoT-based application [6, 16] involves every device with networking and data exchange capabilities, a special concern should be dedicated to security. Recently, an IoT based three factor authentication scheme was proposed by Li et al. [7]. However, few researchers [8] have pointed out some flaws, such as violations of forward secrecy, smart card loss attack and mistakes in BAN logic proof. Also, in this paper some more pitfalls are identified, like sensor node capture, user impersonation, session key leak, sensor node impersonation and gateway node impersonation attacks. Therefore, it has been demonstrated that it is unsuitable for the IoT environment. So, in this work, at first the aforesaid scheme is reviewed, then cryptanalysis is carried out and at last, a solution is suggested to decimate the above vulnerabilities.

The paper is structured as described. In Section 2 revisits Li et al.'s approach. The security threats of the aforesaid scheme is elaborated in Section 3. The section 4 suggests a user authentication solution to tackle this vulnerable scheme. At last section 5 summarizes the complete research.

## 2. REVISIT OF LI ET AL.'S MUTUAL AUTHENTICATION APPROACH

This is a biometric based authentication approach designed for Wireless Sensor Networks (WSN) in an Internet of Things (IoT) settings, in which fuzzy commitment approach [9] is implemented to deal with human's biometric data. This scheme contains three entities i.e. user as $U_i$ , the gateway node as GWN and a sensor node as $S_j$ where GWN is regarded as a trustworthy party through which $U_i$ exchange information with $S_j$. The scheme comprises of a few phases such as sensor node registration; user registration; login and authentication and the password change phases.

© 2024 The Author(s). Published by Indian Society for VLSI Education, Ranchi, India

Initially some parameters are produced by GWN. The additive group says G for the finite field $F_p$ over an elliptical curve [9, 10] is chosen via the GWN, also a point P of order large prime n is a generator. A nonce $x \in Z_n^*$ is chosen as the master key and the GWN computes the public key X as xP. The GWN selects a master secret key as $K_{GWN}$ and x. The $K_{GWN}$ is kept privately, the components $\{E(F_p), G, X, P\}$ are broadcast by the GWN.

## 2.1 The sensor node registration phase:

In offline mode, GWN chooses an identity as SID for every sensor node, evaluates the private key as $K_{GWN-S} = h(K_{GWN} \parallel SID_j)$, say for $S_j$. GWN saves $\{SID_j, K_{GWN-S}\}$ in the sensor node's memory and disperse them in respective location.

## 2.2 The user registration phase:

To access sensor node's data, at first user has to register to GWN as shown in Figure 1 and also described as follows:

1. A user say $U_i$ choose an identity as $ID_i$, a password as $PW_i$, a nonce as $a_i$. Computes $RPW_i = h(a_i \parallel PW_i)$. The $U_i$ stamps i.e., gives biometric on a specific gadget and receives the biometric data as bi . And then $U_i$ delivers the registration request message as $\{ID_i, b_i, RPW_i\}$ to the GWN via a private channel.

2. GWN on receipt of registration request, choose a random codeword as $c_i \subseteq C$ (for $U_i$), evaluates $F(c_i, b_i) = (\alpha, \delta)$, here $\delta = (c_i \oplus b_i)$ and $\alpha = h(c_i)$. Moreover, GWN evaluates $A_i = h(ID_i \parallel c_i \parallel RPW_i)$ as well as $B_i = h(ID_i \parallel K_{GWN}) \oplus h(c_i \parallel RPW_i)$. Finally, GWN stores the $\{\alpha, B_i, A_i, X, f(\cdot), \delta\}$ into the smart card. Send to the $U_i$ through a safe medium and saves the $ID_i$ in its database and removes other data.

3. $U_i$ receives the smart card and saves ai into it. Now, smart card consists of $\{\alpha, A_i, \delta, B_i, f(\cdot), X, a_i\}$.

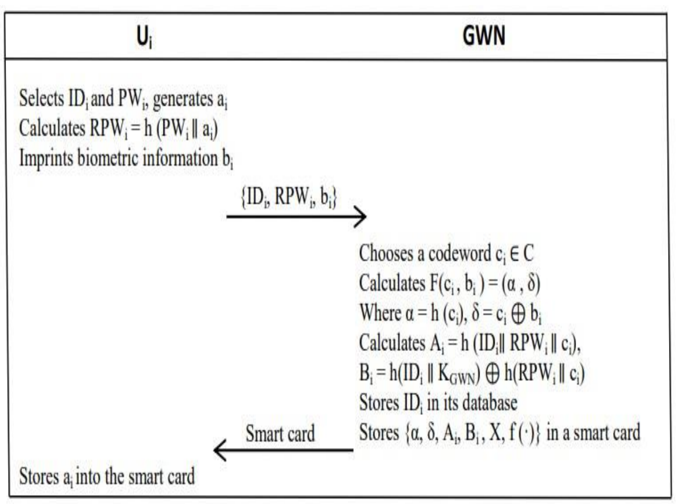


**Fig. 1** User registration phase

## 2.3 The login-authentication phase:

1. A smart card is put into a specific gadget by the $U_i$, stamps biometric $b'_i$ upon a gadget. SC evaluates $c'_i = f(c_i \oplus (b_i \oplus b'_i)) = f(\delta \oplus b'_i)$ and verifies $h(c'_i) ?= \alpha = h(c_i)$. If it is unequal, session is dispersed by SC. Else, the biometric verification is successful for user $U_i$. Then $U_i$ inputs the identity as $ID_i$ and password as $PW_i$ to evaluate $A'_i = h(a_i \parallel h(ID_i \parallel PW_i) \parallel c'_i)$, also verifies $A'_i ?= A_i$. If it is unequal, session is dispersed by the SC. Else the identity as well as password of the user is successfully tested by the SC. Then generates a random number $r_i$ and $s \in Z_n^*$, and evaluates $M_1 = B_i \oplus h(h(a_i \parallel PW_i) \parallel c'_i)$; $M_2 = sP$; $M_3 = sxP = sX$; $M_4 = M_3 \oplus ID_i$; $M_5 = r_i \oplus M_1$; $M_6 = h(ID_i \parallel r_i) \oplus SID_j$ as well as $M_7 = h(M_3 \parallel SID_j \parallel M_1 \parallel r_i)$. At last, a login request via messages $\{M_2, M_4, M_5, M_6, M_7\}$ is submitted by the $U_i$ to the GWN.

2. GWN on receiving the above request evaluates $M'_3 = xsP = xM_2$; $ID'_i = M'_3 \oplus M_4$; verifies if the $ID'_i$ is present in database or not. If it's not present in the database then session is rejected else GWN evaluates $M'_1 = h(ID'_i \parallel K_{GWN})$; $r'_i = M'_1 \oplus M_5$, $SID'_j = M_6 \oplus h(ID'_i \parallel r'_i)$ also, $M'_7 = h(M'_1 \parallel SID'_j \parallel M'_3 \parallel r'_i)$; verifies $M'_7 ?= M_7$. Authentication process gets terminated incase it is unequal otherwise GWN chooses a nonce $r_g$; computes $K'_{GWN-S} = h(SID'_j \parallel K_{GWN})$, $M_8 = ID'_i \oplus K'_{GWN-S}$, $M_9 = r_g \oplus h(ID'_i \parallel K'_{GWN-S})$, $M_{10} = r'_i \oplus r_g$, $M_{11} = h(SID'_j \parallel ID'_i \parallel K'_{GWN-S} \parallel r_g \parallel r'_i)$. Finally, GWN send the message $\{M_8, M_9, M_{10}, M_{11}\}$ to $S_j$ i.e., $SID_j$ through public channel.

3. $S_j$ receives the message and computes $ID''_i = M_8 \oplus K_{GWN-S}$, $r'_g = h(ID''_i \parallel K_{GWN-S}) \oplus M_9$; $r''_i = M_{10} \oplus r''_g$, $M'_{11} = h(ID''_i \parallel SID_j \parallel K_{GWN-S} \parallel r'_g \parallel r''_i)$ and verifies $M'_{11} ?= M_{11}$. The $S_j$ rejects the session if it is unequal. Else, $S_j$ chooses a nonce $r_j$, to evaluate $M_{12} = r_j \oplus K_{GWN-S}$, $SK_j = h(ID''_i \parallel r''_i \parallel SID_j \parallel r'_g \parallel r_j)$, $M_{13} = h(K_{GWN-S} \parallel SK_j \parallel r_j)$. And then $S_j$ send the response as $\{M_{12}, M_{13}\}$ to the GWN through public channel.

4. GWN receives the above response from $S_j$, computes $r'_j = M_{12} \oplus K'_{GWN-S}$, $SK_{GWN} = h(SID'_j \parallel ID'_i \parallel r'_j \parallel r_g \parallel r'_i)$ also, $M'_{13} = h(K'_{GWN-S} \parallel SK_{GWN} \parallel r'_j)$; verifies $M'_{13} ?= M_{13}$. Authentication process gets terminated if it is unequal. Else, GWN evaluates $M_{14} = r_g \oplus M'_1$, $M_{15} = r'_j \oplus r'_i$, $M_{16} = h(SK_{GWN} \parallel ID'_i \parallel r'_j \parallel r_g)$. Atlast, GWN send the messages $\{M_{14}, M_{15}, M_{16}\}$ to the $U_i$ through public channel.

5. Following receipt of the GWN messages, the $U_i$ computes $r''_g = M_1 \oplus M_{14}$; $r''_j = r_i \oplus M_{15}$; $SK_i = h(ID_i \parallel SID_j \parallel r_i \parallel r''_j \parallel r''_g)$, $M''_{16} = h(r''_g \parallel SK_i \parallel ID_i \parallel r''_j)$; verifies $M'_{16} ?= M_{16}$. A session is terminated if it is unequal. Else, the mutual authentication is said to be successful between these legitimate parties, as shown in Figure 2.

At last, $U_i$ is permitted to access data of the $S_j$ through GWN as well as the session key as $SK_i$ (= $SK_j$ = $SK_{GWN}$) is shared between all i.e., $U_i$, GWN and the $S_j$.

## 3. SECURITY THREATS IN LI ET AL. SCHEME

The cryptanalysis of [7] scheme is performed here. As a result, some weaknesses like sensor node capture attack; session key leak attack; sensor node impersonation attack; user impersonation attack and gateway node impersonation attack are found and described as follows:

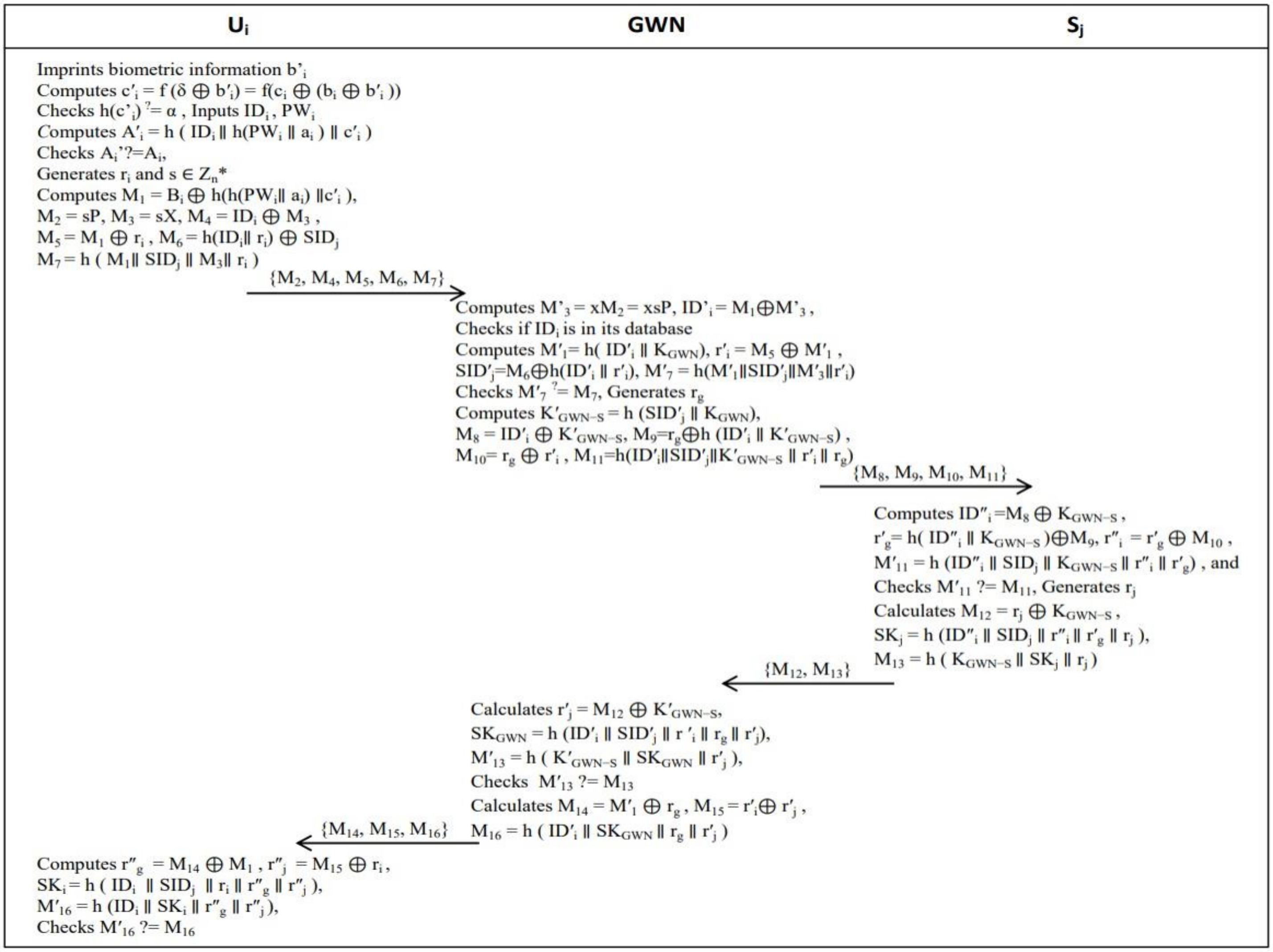


**Fig. 2** Login-authentication phase

### 3.1 Sensor node capture attack:

In a network when an attacker $\hat{A}$ directly takes control over the targeted sensor node [11, 12] he gets all the stored information like encryption key, data collected and received from different user or gateway nodes. An attacker can later destroy or change the malicious node to perform the desired operation.

1. When user $U_i$ accesses the data of sensor node $S_j$ then all the information exchanged during authentication process involving $S_j$ gets stored in it's memory like $SID_j$ , $K_{GWNSj} = h(SID_j \parallel K_{GWN})$, $SK_j$ , messages $\{M_8, M_9, M_{10}, M_{11}\}$ sent by GWN to $S_j$ and $\{M_{12}, M_{13}\}$ sent by $S_j$ to GWN .

2. Later when the above sensor node $S_j$ gets captured by $\hat{A}$, he is able to retrieve: $M_8 \oplus K'_{GWN-Sj} = ID'_i$ , $M_9 \oplus h(ID'_i \parallel K'_{GWN-Sj}) = r_g$, $M_{10} \oplus r_g = r'_i$ , $M_{14} \oplus r_g = M'_1 = h(ID_i \parallel K_{GWN})$. Therefore, from above, legal user's $ID_i$ , $h(ID_i \parallel K_{GWN})$ , nonce of user ($r'_i$ ) and GWN ($r_g$) along with sensor node's session key ($SK_j$ ) is disclosed to $\hat{A}$ which he uses for further attacks.

### 3.2 Session key leak attack:

Proper communication starts after establishment of session key at both sides (as it is computed after different levels of verification). When an attacker successfully retrieves the necessary information to compute the session key then an attacker is able to break the system [9].

1. Here $U_i$ (previously accessed $S_j$) now sends request to GWN to access another node $S_k$ then, smart card chooses a nonce $r_{inew}$ and $s_{new} \in Z_n^*$ and evaluates $M_1 = h(h(a_i \parallel PW_i) \parallel c'_i) \oplus B_i$ ; $M_2 = s_{new}P$, $M_3 = s_{new}X = s_{new}xP$, $M_4 = M_3 \oplus ID_i$ ; $M_5 = M_1 \oplus r_{inew}$, $M_6 = h(r_i \parallel ID_i) \oplus SID_k$; $M_7 = h(M_1 \parallel SID_k \parallel M_3 \parallel r_{inew}) = h(h(ID_i \parallel K_{GWN}) \parallel SID_k \parallel s_{new}xP \parallel r_{inew})$ and $U_i$ transmits login request messages as $\{M_2, M_4, M_5, M_6, M_7\}$ to the GWN via public channel to access $S_k$.

2. From captured sensor node $S_j$, $\hat{A}$ knows $ID_i$ of legal user $U_i$ and also $M_1 = h(ID_i \parallel K_{GWN})$ as from $M_4 \oplus ID_i$ , $ID_i \oplus M_3 \oplus ID_i = M_3 = s_{new}xP$. From $M_5 \oplus M_1$, $M_1 \oplus r_{inew} \oplus M_1 = r_{inew}$. From $M_6 \oplus h(ID_i \parallel r_{inew})$, $h(ID_i \parallel r_{inew}) \oplus SID_k \oplus h(ID_i \parallel r_{inew}) = SID_k$. Therefore, $U_i$ is trying to access $SID_k$ is revealed to $\hat{A}$.

3. GWN receives the messages $\{M_2, M_4, M_5, M_6, M_7\}$ from the $U_i$ and after some computation sends the message $\{M_8, M_9, M_{10}, M_{11}\}$ to $SID_k$ via public channel.

4. As the above messages are send via public medium, $\hat{A}$ is able to compute: $M_8 \oplus ID'_i = ID'_i \oplus K'_{GWN-Sk} \oplus ID'_i = K'_{GWN-Sk}$, $M_9 \oplus h(ID'_i \parallel K'_{GWN-Sk}) = r_{gnew} \oplus h(ID'_i \parallel K'_{GWN-Sk}) \oplus hID'_i \parallel K'_{GWN-Sk}) = r_{gnew}$, $M_{10} \oplus r_{gnew} = r_{gnew} \oplus r'_{inew} \oplus r_{gnew} = r'_{inew}$.

5. When sensor node $SID_k$ receives message $\{M_8, M_9, M_{10}, M_{11}\}$ from GWN via public channel, performs some computation and transmits the responses as $\{M_{12}, M_{13}\}$ to the GWN through the public channel.

6. Now, $\hat{A}$ computes: $M_{12} \oplus K_{GWN-Sk} = r_{jnew} \oplus K_{GWN-Sk} \oplus K_{GWN-Sk} = r_{jnew}$, $SK_k = h(ID''_i \parallel SID_k \parallel r''_{inew} \parallel r'_{gnew} \parallel r_{jnew})$ and verify $SK_k$ through $M_{13}$ i.e. $M_{13} = h(K_{GWN-Sk} \parallel SK_k \parallel r_{jnew})$. Since attacker $\hat{A}$ got all parameters to compute $SK_k = h(ID''_i \parallel SID_k \parallel r''_{inew} \parallel r'_{gnew} \parallel r_{jnew})$, thus it can be inferred that an uncaptured sensor node $SID_k$ is vulnerable to session key leak attack.

### 3.3 Sensor node impersonation attack:

As a registered sensor node, an attacker impersonate [14] to a legal user and gateway node, based on some disclosed secret data from previous conversation. Here legal user $U_a$ sends login request to GWN to access $SID_k$. In continuation of previous attack now $\hat{A}$ knows $SID_k$ and $K_{GWN-Sk}$ of a $S_k$. So, now it will be illustrated how $\hat{A}$ will be able to impersonate as $S_k$ to $U_a$.

1. As per Login phase: Smart card generates nonce $r_a$ and $b \in Z_n^*$ and computes, $M_1 = h(ID_a \parallel K_{GWN})$, $M_2 = bP$, $M_3 = bX = bxP$, $M_4 = ID_a \oplus M_3$, $M_5 = M_1 \oplus r_a$, $M_6 = h(ID_a \parallel r_a) \oplus SID_k$ and $M_7 = h(M_1 \parallel SID_k \parallel M_3 \parallel r_a) = h(h(ID_a \parallel K_{GWN}) \parallel SID_k \parallel bxP \parallel r_a)$. $U_a$ sends login request messages $\{M_2, M_4, M_5, M_6, M_7\}$ to the GWN via public channel.

2. GWN receives $\{M_2, M_4, M_5, M_6, M_7\}$ and evaluates: $M'_3 = xM_2 = xbP$, retrieves $ID'_a = M_4 \oplus M'_3 = ID_a \oplus xbP \oplus xbP = ID_a$ evaluates $M'_1 = h(ID_a \parallel K_{GWN})$, retrieves $r_a = M'_1 \oplus M_5 = M_1 \oplus r_a \oplus M'_1$ , $SID_k = M_6 \oplus h(ID_a \parallel r_a) = h(ID_a \parallel r_a) \oplus SID_k \oplus h(ID_a \parallel r_a) = SID_k$, checks $M'_7 = h(M_1 \parallel SID_k \parallel M_3 \parallel r_a)$, $M'_7 ?= M_7$. If unequal then session is dismissed by the GWN else computes $K_{GWN-Sk} = h(SID_k \parallel K_{GWN})$ for $S_k$ and generates a nonce $r_{gnew}$ to computes: $M_8 = ID_a \oplus K_{GWN-Sk}$, $M_9 = r_{gnew} \oplus h(ID_a \parallel K_{GWN-Sk})$, $M_{10} = r_{gnew} \oplus r_a$, $M_{11} = h(ID_a \parallel SID_k \parallel K_{GWN-Sk} \parallel r_a \parallel r_{gnew})$. GWN submits the messages $\{M_8, M_9, M_{10}, M_{11}\}$ to $SID_k$ but received by $\hat{A}$ via public channel.

3. $\hat{A}$ impersonating as $SID_k$ : When $\hat{A}$ receives message $\{M_8, M_9, M_{10}, M_{11}\}$ he already knows $SID_k$ and $K_{GWN-Sk}$ (from previous attack), retrieve the user ID from $M_8 \oplus K_{GWN-Sk} = ID_a \oplus K_{GWN-Sk} \oplus K_{GWN-Sk} = ID_a$. Retrieves, $r_{gnew} = h(ID_a \parallel K_{GWN-Sk}) \oplus M_9$. From $r_a = M_{10} \oplus r_{gnew} = r_{gnew} \oplus r_a \oplus r_{gnew} = r_a$ verify through $M_{11} = h(ID_a \parallel SID_k \parallel K_{GWN-Sk} \parallel r_a \parallel r_{gnew})$. Chooses a nonce $r''_k$ and computes $SK_A = h(ID_a \parallel SID_k \parallel r_a \parallel r_{gnew} \parallel r''_k)$, $M_{12} = r''_k \oplus K_{GWN-Sk}$, $M_{13} = h(K_{GWN-Sk} \parallel SK_A \parallel r''k)$. $\hat{A}$ as $S_k$ sends response $\{M_{12}, M_{13}\}$ to GWN via public channel.

4. GWN receives response message $\{M_{12}, M_{13}\}$ from $\hat{A}$ and retrieves, $r''_k = M_{12} \oplus K'_{GWN-Sk} = r''_k \oplus K_{GWN-Sk} \oplus K'_{GWN-Sk}$ and computes: $SKG = h(ID_a \parallel SID_k \parallel r_a \parallel r_{gnew} \parallel r''_k)$, $M'_{13} = h(K_{GWN-Sk} \parallel SK_G \parallel r''_k)$. Checks $M'_{13} ?= M_{13}$ if not then session is rejected by the GWN else computes: $M_{14} = M'_1 \oplus r_{gnew} = h(ID_a \parallel K_{GWN}) \oplus r_{gnew}$, $M_{15} = r_a \oplus r''_k$ , $M_{16} = h(ID_a \parallel SK_G \parallel r_{gnew} \parallel r''_k)$. GWN delivers the messages $\{M_{14}, M_{15}, M_{16}\}$ to $U_a$ via public channel.

5. $U_a$ receives the message $\{M_{14}, M_{15}, M_{16}\}$ from the GWN and evaluates, $r_{gnew} = M_{14} \oplus M_1 = M_1 \oplus r_{gnew} \oplus M_1$, $r''_k = M_{15} \oplus r_a = r_a \oplus r''_k \oplus r_a$, $SK_{aA} = h(ID_a \parallel SID_k \parallel r_a \parallel r_{gnew} \parallel r''_k)$, $M'_{16} = h(ID_a \parallel SK_a \parallel r_{gnew} \parallel r''_k)$ and verifies $M'_{16} ?= M_{16}$. Session gets terminated if the above values are unequal else authentication process is said to be completed. Therefore, it can be conclude that, after getting ($SID_k$, $K_{GWN-Sk}$) $\hat{A}$ successfully impersonate as sensor node Sk to GWN and $U_a$.

NOTE: In past computation $\hat{A}$ has retrieved $ID_a$ and from $M_{14} = M_1 \oplus r_{gnew} = h(ID_a \parallel K_{GWN}) \oplus r_{gnew} \oplus r_{gnew} = h(ID_a \parallel K_{GWN})$. Now, it will be checked for user impersonation attack on the basis of $ID_a$ and $h(ID_a \parallel K_{GWN})$.

### 3.4 User impersonation attack:

An attacker impersonate [13] as a registered user to a legal sensor node and gateway node, based on some disclosed secret parameters from previous communication. Here $\hat{A}$ impersonate as a legal user $U_a$ and sends login request message to GWN to access sensor node $S_t$. In continuation of previous attack now $\hat{A}$ knows $ID_a$ and $h(ID_a \parallel K_{GWN})$ of a $U_a$ and so now it will be proven how $\hat{A}$ will impersonate as $U_a$ to $S_t$ and GWN.

1. $\hat{A}$ as $U_a$ choose a nonce $r_{adv}$ and $s_{adv} \in Z_n^*$ and computes: $M_2 = s_{adv}P$, here P is public and fixed. $M_3 = s_{adv}X = s_{adv}xP$, here X is public and fixed, $M_4 = ID_a \oplus M_3$, $\hat{A}$ knows the $ID_a$ from previous calculations. $M_5 = M_1 \oplus s_{adv}$, $\hat{A}$ knows the $M_1 = h(ID_a \parallel K_{GWN})$ from previous calculations. $M_6 = h(ID_a \parallel r_{adv})$

$\oplus$ $SID_t$ and $M_7 = h(M_1 \| SID_t \| M_3 \| r_{adv}) = h(h(ID_a \| K_{GWN}) \| SID_t \| s_{adv}xP \| r_{adv})$. $\hat{A}$ (as $U_a$) send login request messages as $\{M_2, M_4, M_5, M_6, M_7\}$ to the GWN to access $SID_t$ through public channel.

2. On reveiving the login request messages, GWN evaluates $M'_3 = xM_2 = xs_{adv}P$ and retrieves $ID'_a = M_4 \oplus M'_3 = ID_a \oplus xs_{new}P \oplus xs_{new}P = ID_a$, verifies $ID'_a$ exists in the database or not, if not then GWN rejects session else computes, $M'_1 = h(ID'_a \| K_{GWN})$. From, $r'_{adv} = M_5 \oplus M'_1 = M_1 \oplus r_{adv} \oplus M'_1 = r_{adv}$, $SID'_t = M_6 \oplus h(ID'_a \| r'_{adv}) = h(ID'_a \| r'_{adv}) \oplus SID_t \oplus h(ID_a \| r_{adv}) = SID_t$ and checks $M'_7 = h(M'_1 \| SID'_t \| M'_3 \| r'_{adv})$ ?= $M_7 = h(M_1 \| SID_t \| M_3 \| r_{adv})$. If unequal then session is rejected by the GWN otherwise chooses a nonce $r'_g$ and computes: $K'_{GWN-St} = h(SID'_t \| K_{GWN})$, $M_8 = ID'_a \oplus K'_{GWN-St}$, $M_9 = r'_g \oplus h(ID'_a \| K'_{GWN-St})$, $M_{10} = r'_g \oplus r'_{adv}$, $M_{11} = h(ID'_a \| SID'_t \| K'_{GWN-St} \| r'_{adv} \| r'_g)$. The GWN then delivers the messages $\{M_8, M_9, M_{10}, M_{11}\}$ to $SID_t$ through public channel.

3. St sensor node ($SID_t$) receives messages $\{M_8, M_9, M_{10}, M_{11}\}$ and computes: $ID''_a = M_8 \oplus K_{GWN-St} = ID'_a \oplus K'_{GWN-St} \oplus K_{GWN-St} = ID'_a$ . Retrieve, $r''_g = h(ID''_a \| K_{GWN-St}) \oplus M_9 = h(ID''_a \| K_{GWN-St}) \oplus r'_g \oplus h(ID'_a \| K'_{GWN-St}) = r'_g$ , $r''_{adv} = r''_g \oplus M_{10} = r''_g \oplus r'_g \oplus r'_{adv} = r'_{adv}$ and checks $M'_{11} = h(ID''a \| SID_t \| K_{GWN-St} \| r''_{adv} \| r''_g)$, $M'_{11}$ ?= $M_{11}$, if not session is terminated by St else, a nonce rt is generated and computes: $M_{12} = r_t \oplus K_{GWN-St}$, $SK_t = h(ID''_a \| SID_t \| r''_{adv} \| r''_g \| rt)$, $M_{13} = h(K_{GWN-St} \| SK_t \| r_t)$. St sends response message $\{M_{12}, M_{13}\}$ to GWN through public channel.

4. GWN receives response message $\{M_{12}, M_{13}\}$ and retrieves $r'_t = M_{12} \oplus K'_{GWN-St} = r_t \oplus K_{GWN-St} \oplus K'_{GWN-St}$ and computes: $SK_{GWN} = h(ID'_a \| SID'_t \| r'_{adv} \| r'_g \| r'_t)$ and checks $M'_{13} = h(K'_{GWN-St} \| SK_{GWN} \| r'_t)$ ?= $M_{13}$, if yes, computes: $M_{14} = M'_1 \oplus r'_g = h(ID'_a \| K_{GWN}) \oplus r'_g$ , $M_{15} = r'_{adv} \oplus r'_t$ , $M_{16} = h(ID'_a \| SK_{GWN} \| r'_g \| r'_t)$ and GWN transmit the messages $\{M_{14}, M_{15}, M_{16}\}$ to $\hat{A}$ (as $U_a$).

5. $\hat{A}$ impersonating as a legal user receives message $\{M_{14}, M_{15}, M_{16}\}$. Since $\hat{A}$ has choosen radv so he can easily retrieve the nonce of $S_t$ and GWN as $r'_t = M_{15} \oplus r_{adv} = r'_{adv} \oplus r'_t \oplus r_{adv}$, $r''_g = M_{14} \oplus M_1 = h(ID'_a \| K_{GWN}) \oplus r'_g \oplus h(ID_a \| K_{GWN})$. Therefore, $\hat{A}$ can easily compute session key as $SK\hat{A} = h(ID_a \| SID_t \| r_{adv} \| r''_g \| r''_t)$. Thus $\hat{A}$ successfully impersonate as a legal user to gateway node (GWN) and sensor node ($S_t$) and gets all the essential data to the compute session key. Thereby able to access sensor data of $S_t$.

### 3.5 Gateway node impersonation attack:

1. A legitimate user $U_a$ sends login request as $\{M_2, M_4, M_5, M_6, M_7\}$ to the GWN to access sensor node $S_k$ as $SID_k$ via insecure channel.

2. $\hat{A}$ impersonating as GWN receives $\{M_2, M_4, M_5, M_6, M_7\}$. Evaluates few messages $\{M_8, M_9, M_{10}, M_{11}\}$ and forward them to $SID_k$ through public channel.

3. Sensor node $SID_k$ receives the messages $\{M_8, M_9, M_{10}, M_{11}\}$ and computes $ID''_a = M_8 \oplus K_{GWN-Sk} = ID'_a \oplus K'_{GWN-Sk} \oplus K_{GWN-Sk} = ID'_a$ . Retrieves, $r''_g = h(ID''_a \| K_{GWN-Sk}) \oplus M_9 = h(ID''_a \| K_{GWN-Sk}) \oplus r'_g \oplus h(ID'_a \| K'_{GWN-Sk})$. Retrieves, $r''_a = r''_g \oplus M_{10}$. Computes $M'_{11} = h(ID''_a \| SID_k \| K_{GWN-Sk} \| r''_a \| r''_g)$ and verifies $M'_{11}$ ?= $M_{11}$. If unequal then session is terminated by sensor node $S_k$ else a nonce $r_k$ is generated and computes: $M_{12} = r_k \oplus K_{GWN-Sk}$, $SK_t = h(ID''_a \| SID_k \| r''_a \| r''_g \| r_k)$, $M_{13} = h(K_{GWN-Sk} \| SK_k \| r_k)$. $S_k$ sends response message $\{M_{12}, M_{13}\}$ to $\hat{A}$ impersonating as GWN through public channel.

4. $\hat{A}$ receives the response message $\{M_{12}, M_{13}\}$ from $SID_k$ and retrieves $r'_k = M_{12} \oplus K'_{GWN-Sk}$. Computes: $SK\hat{A} = h(ID'_a \| SID'_k \| r'_a \| r'_g \| r'_k)$ also, $M_{14} = M'_1 \oplus r'_g = h(ID'_a \| K_{GWN}) \oplus r'_g$ , $M_{15} = r'_a \oplus r'_k$ , $M_{16} = h(ID'_a \| SK\hat{A} \| r'_g \| r'_k)$ . $\hat{A}$ transmit messages $\{M_{14}, M_{15}, M_{16}\}$ to $U_a$ through public channel.

5. $U_a$ receives the message $\{M_{14}, M_{15}, M_{16}\}$ and computes $r_g = M_{14} \oplus M_1 = M''_1 \oplus r_g \oplus M_1$, $r''k = M_{15} \oplus r_a = r'_a \oplus r'_k \oplus r_a$, $SK_{aA} = h(ID_a \| SID_k \| r_a \| r_g \| r''_k)$, $M'_{16} = h(ID_a \| SK \| r_g \| r''_k)$. Cross verify with $M_{16} = h(ID_a \| SK \| r_g \| r''_k)$ as true so the session is accepted and hence authentication process is successfully completed.

Therefore, it is inferred that for a pair $U_a$ and $S_k$, $\hat{A}$ is able to impersonate as a legal GWN [14] since sensor node capture results in disclosure of legitimate user's $ID_a$ and $M_1 = h(ID_a \| K_{GWN})$ and the non trapped sensor node's $SID_k$ and $K_{GWN-Sk} = h(SID_k \| K_{GWN})$.

## 4. SUGGESTION FOR IMPROVEMENT

Three factor authentication approach has some limitations, including challenging setup and integration, reliance on third parties when problems arise, significant administration resources and large database management costs. Furthermore, the safety of a smart card is precarious, given that anyone in control of the card can use it to authenticate. Users also have difficulty remembering their passwords. To address the aforementioned problems, a smart multimodal biometric system-based authentication [17] is suggested as an alternative. The fundamental advantage of multimodal biometrics is that they can identify the person based on who they are rather than what they know or have. Thus, the multimodal biometric system that is recommended includes facial (physiological) [4] and speech (physiological and behavioural) [5, 15, 18, 19] modalities being concatenated at the feature level [18, 19] using a deep neural network-based classifier [20] for user authentication as shown in Figure 3. For any application requiring increased accuracy, security and widespread user acceptability, this can be regarded as a preferred solution over three factor authentication.

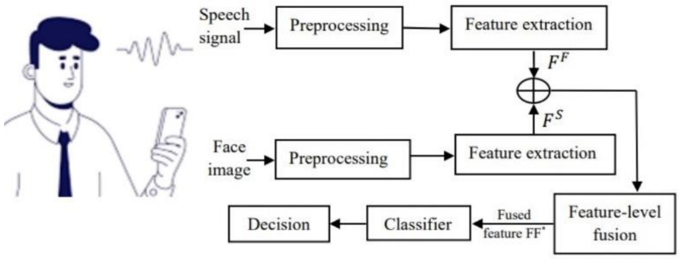


**Fig. 3** Suggested multimodal biometric system-based user authentication approach

## 5. CONCLUSION

This research investigates the pitfalls of Li et al.'s approach for WSNs in an IoT environment. As a result, it was identified that their strategy is exposed to sensor node capture attack, sensor node impersonation attack, user impersonation attack, session key leak attack and gateway node impersonation attack. Thus, it is unsuitable for a WSN based IoT environment. Additionally, an enhanced multimodal biometric user authentication system is suggested. It will effectively eliminate all attacks and it will be highly compatible with IoT-based applications.

## REFERENCES


1. Praveen Kumar, E., & Priyanka, S. (2023). A password less authentication protocol for multi-server environment using physical unclonable function. The Journal of Supercomputing, 1-33. https://doi.org//10.1007/s11227- 023-05437-3

2. Soni, P., Pal, A. K., & Khushboo, K. (2019, July). A User Convenient Secure Authentication Scheme for Accessing e-Governance Services. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-7). IEEE. https://doi.org//10.1109/ICCCNT45670.2019.8944393

3. Li, X., Xiong, Y., Ma, J., & Wang, W. (2012). An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards. Journal of Network and Computer Applications, 35(2), 763-769. https://doi.org/10.1016/j.jnca.2011.11.009

4. Jha, K., Srivastava, S., & Jain, A. (2023, March). Integrating Global and Local Features for Efficient Face Identification Using Deep CNN Classifier. In 2023 International Conference on Device Intelligence, Computing and Communication Technologies,(DICCT) (pp. 532-536). IEEE. https://doi.org//10.1109/DICCT56244.2023.10110170.

5. Jha, K., Jain, A., & Srivastava, S. (2023, March). An Efficient Speaker Identification Approach for Biometric Access Control System. In 2023 5th International Conference on Recent Advances in Information Technology (RAIT) (pp. 1-5). IEEE. https://doi.org//10.1109/RAIT57693.2023.10127101

6. Sobh, T. S., & Khalil, A. H. (2023). Securing Hybrid Architecture of Cloudlet Computing in 5G Networks Enabling IoT and Mobile Wireless Devices. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science), 16(2), 14-29. https://doi.org/10.2174/2666255815666220513100257

7. Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A. K., & Choo, K. K. R. (2018). A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. Journal of Network and Computer Applications, 103, 194-204. https://doi.org/10.1016/j.jnca.2017.07.001

8. Li, W., Li, B., Zhao, Y., Wang, P., & Wei, F. (2018). Cryptanalysis and security enhancement of three authentication schemes in wireless sensor networks. Wireless Communications and Mobile Computing, 2018. https://doi.org//10.1155/2018/8539674

9. Soni, P., Pal, A. K., & Islam, S. H. (2019). An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. Computer methods and programs in biomedicine, 182, 105054. https://doi.org/10.1016/j.cmpb.2019.105054

10. Chilveri, P. G., & Nagmode, M. S. (2020). A novel node authentication protocol connected with ECC for heterogeneous network. Wireless Networks, 26, 4999-5012. https://doi.org/10.1007/s11276-020-02358-4

11. Chang, C. C., & Le, H. D. (2015). A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks. IEEE Transactions on wireless communications, 15(1), 357-366. https://doi.org//10.1109/TWC.2015.2473165

12. Li, X., Niu, J., Bhuiyan, M. Z. A., Wu, F., Karuppiah, M., & Kumari, S. (2017). A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things. IEEE Transactions on Industrial Informatics, 14(8), 3599-3609. https://doi.org//10.1109/TII.2017.2773666

13. Thakur, G., Prajapat, S., Kumar, P., Das, A. K., & Shetty, S. (2023). An Efficient Lightweight Provably Secure Authentication Protocol for Patient Monitoring Using Wireless Medical Sensor Networks. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3325130

14. Kumar, P., & Om, H. (2023). An anonymous and authenticated V2I communication with a simplified user revocation and re-registration strategy. The Journal of Supercomputing, 79(7), 8070-8096. https://doi.org/10.1007/s11227-022-04978-3

15. Srivastava, Sumit, Mahesh Chandra, G. Sahoo, "Speaker identification and its application in automobile industry for automatic seat adjustment," Microsystem Technologies, vol. 25-6, pp. 2339-2347, 2019. https://doi.org//10.1007/S00542-018-4111-Z

16. Quazi Warisha Ahmed, & Shruti Garg. (2023). IoT based Smart Healthcare System in Cloud Environment. International Journal of Microsystems and IoT, 1(2), 73– 81. https://doi.org/10.5281/zenodo.8288243

17. Byeon, H., Raina, V., Sandhu, M., Shabaz, M., Keshta, I., Soni, M., & Lakshmi, T. R. (2024). Artificial intelligence-Enabled deep learning model for multimodal biometric fusion. Multimedia Tools and Applications, 1-24. https://doi.org/10.1007/s11042-024-18509-0

18. Freire-Obregon, D., Rosales-Santana, K., Marin-Reyes, P. A., Penate-Sanchez, A., Lorenzo-Navarro, J., & Castrillon-Santana, M. (2021). Improving user verification in human-robot interaction from audio or image inputs through sample quality

assessment. Pattern Recognition Letters, 149, 179-184. https://doi.org/10.1016/j.patrec.2021.06.014

19. Abozaid, A., Haggag, A., Kasban, H., & Eltokhy, M. (2019). Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion. Multimedia tools and applications, 78, 16345-16361. https://doi.org/10.1007/s11042-018-7012-3

20. Agrawal, S. S., Jain, A., & Sinha, S. (2016). Analysis and modeling of acoustic information for automatic dialect classification. International Journal of Speech Technology, 19, 593-609. https://doi.org/10.1007/s10772-016-9351-7

## Authors:

**Khushboo Jha** received her BTech degree in Information Technology from Techno India College of Engineering & Management (Techno Main Saltlake), Kolkata, India in 2012 and MTech degree in Computer Science and Engineering (Spec. in Information Security) from Indian Institute of Technology (IIT), Dhanbad, India in 2019. She is currently pursuing PhD at the Department of Computer Science and Engineering, Birla Institute of Technology, Mesra, India. Her areas of interest are biometrics, speech processing, speaker recognition, face recognition, deep neural networks and multimodal biometric system.

Corresponding author Email: kjha.phd@gmail.com

**Sumit Srivastava** is working as an Assistant Professor in the department of Computer Science and Engineering, Birla Institute of Technology, Mesra, Ranchi, India. He has done his PhD in Computer Science and Engineering from the Birla Institute of Technology, Mesra, India. He has ten years of experience in teaching and research. His areas of interest are speech processing, signal processing, cryptography and network security, embedded systems, and machine learning. He has received several patents. He has also published several papers in various international/national journals and the proceedings of prestigious international/national conferences.

Email: sumit.srivs88@gmail.com

**Aruna Jain** is working as Associate Professor in the department of Computer Science & Engineering, Birla Institute of Technology, Mesra, India. She has done her PhD in Computer Science and Engineering from the Birla Institute of Technology, Mesra, India. She has more than 32 years of experience in teaching and research. Her areas of research are cryptography & network security, blockchain technology, speech processing and optical networks. She has published several papers in various international/national journals and the proceedings of prestigious international/national conferences. She is also regular writer in various Educational and Spiritual magazines.

Email: arunajain@bitmesra.ac.in