Open Access
Full Length Article

ORIGINAL ARTICLE

Enhanced Biometric-Based User Authentication Scheme for Wireless Sensor Networks Using Fuzzy Extraction and Elliptic Curve Cryptography

Rabia Riaz[1], Sana Shokat[2], Sanam Shahla Rizvi[3], Musarat Shaheen[4]

[1]Department of CS & IT, University of Azad Jammu and Kashmir, Muzaffarabad, Pakistan
[2]Department of CS & IT, University of Azad Jammu and Kashmir, Muzaffarabad, Pakistan
[3]Raptor Interactive (Pty) Ltd, Eco Boulevard, Witch Hazel Ave, Centurion, South Africa
[4]Department of CS & IT, University of Azad Jammu and Kashmir, Muzaffarabad, Pakistan

ABSTRACT

Wireless sensor networks are used to monitor physical and environmental conditions. User authentication is required to achieve a consistent access control. However, authenticating a user or sensor in a network is a challenging task owing to the limited resources of the sensor nodes. Therefore, to provide secure and efficient communication, numerous authentication schemes have been designed. Traditional schemes have several security vulnerabilities and significant computational overhead. In this paper, we propose an Enhanced biometric based user Authentication Scheme using Fuzzy extraction and Elliptic curve cryptography (EBAS-FeEcc) for wireless sensor networks to achieve high security level and improve the performance as well as life time of entire network. Presented technique consists of easy operations and light computations. Analysis shows that previous schemes have various security weaknesses such as a biometric recognition error, user verification problem, lack of anonymity, session key exposure by the gateway node, and perfect forward secrecy. Our proposed technique overcomes these network security issues. Our scheme additionally increases performance of the network by reducing network traffic, defending sensor network against DOS attack and increasing nodes battery life. Therefore, the functionality and performance of the entire network improves.

Keywords: WSN; Security; Authentication; Biometrics; Fuzzy Extraction; Elliptic Curve Cryptography

Author`s Contribution
[1,2] Manuscript writing, Data Collection Data analysis, interpretation, Conception, synthesis, ,[3,4]planning of research, and discussion

Address of Correspondence
Rabia Riaz
rabia.riaz@ajku.edu.pk

Article info.
Received: September 11,2019
Accepted: March 28,2020
Published: June 30,2020

Cite this article: *Riaz R, Shokat S, Rizvi SS, Shaheen M. Enhanced Biometric-Based User Authentication Scheme for Wireless Sensor Networks using Fuzzy Extraction and Elliptic Curve Cryptography. J. Inf. commun. technol. robot. appl.2020; 11(1):1-14*

Funding Source: *Nil*
Conflict of Interest: *Nil*

INTRODUCTION

Wireless sensor networks (WSNs) contain devices having sensors for any specific purpose [1]. Tiny sensor nodes in network process information after sensing from its surroundings. These networks have lots of applications such as structural monitoring, environmental control, health care systems asnd battlefield surveillance [2]. In most of these applications, user can directly receive data through gateway node.

Sometimes data access from gateway node is difficult or the gateway node is inaccessible [3]. In such cases, data is obtained through sensor nodes directly [4]. Data that is sensed can be confidential [5]. However, sensor nodes cannot often authenticate request messages. Consequently, a malicious user can easily access sensitive data by sending requests to a sensor node. This can lead to leakage of sensitive information as well as unnecessary depletion of network resources like nodes energy and network bandwidth [6]. All these problems affect network's lifetime, performance and make the system unavailable for legitimate users. Thus, user authentication and access control are required services to prevent unauthorized use of network data and its resources [7]. To accomplish this, for sensor nodes, we need a mechanism to identify and authenticate the users such that only authenticated users can join the network. However, providing authentication in WSNs is tremendously challenging due to resource limitation of tiny sensor devices including energy and memory limitation, computational capabilities and communication capacities [8]. Various protocols have been proposed but their authentication process is still insecure [9]. Ultimately there is need for a protocol with stronger and smarter mechanism to make WSNs safer. Based on our study of previous security techniques, in this paper we offer a competent user authentication technique for WSN applications.

The remainder of this paper is organized as follows. User authentication problems identified in literature review are discussed in Section 2. Section 3 describes related work to emphasize the need for this research. In Section 4, we propose the biometric-based authentication scheme using fuzzy extraction and ECC with improved security. Section 5 presents a security analysis of various security properties for proposed scheme. We compare proposed scheme with several previous protocols using performance evaluation in Section 6. Section 7 concludes the paper.

LITERATURE REVIEW

Wong et al [10] proposed a user authentication scheme based on password of user and cryptographic hash operations. Wong's protocol consists of three phases, first user registration then login, third user authentication. It permits only authenticated users to request for data. This scheme is vulnerable to various security attacks such as forged attack, replay attack, stolen-verifier attack as gateway and login-node maintains tables containing information of registered users. Passwords may be exposed by any of the sensor nodes and user is unable to alter password [8]. Das [11] proposed user authentication scheme for WSNs which overcame the security flaws of the scheme proposed by Wong [10]. The author exposed numerous security weaknesses in Wong's user authentication technique and proposed a scheme based on smart card and user's password. This authentication technique consists of only two phases, user registration and authentication phase. In the phase of registration, gateway node generates a private secret key and this key is shared among sensor nodes. User has no idea about this key. Authentication phase consists of login and verification phase. This scheme overcomes weaknesses of Wong's scheme but it also suffers from several security threats. For transmission of data, no secure medium is provided therefore transmitted data can be easily altered by an attacker. Also this protocol is not robust because its robustness depends on that secret parameter that is preinstalled in sensor nodes and smart card. If node is compromised then security of entire network will be destroyed [12]. In addition, an attacker can eavesdrop on entire conversations of all entities in a network. Node compromise is major problem in this scheme and it is also defenseless against various attacks like replaying and impersonation attack. It also faces problems from attacks like node compromise, password guessing, and denial of service (DOS) attacks.

Khan and Alghathbar [13] have shown that scheme proposed by Das [11] does not provide mutual authentication and is also defenseless against privileged insider attacks. They also identified that Das's scheme does not allow changing of passwords freely. Khan and Alghathbar proposed a security technique that attempts to overcome these security flaws. In their proposed protocol, they added a user password changing phase in the Das scheme so that users can change their password easily. Whenever any

user wishes to modify the password, the smart card overwrites the password's old contents with the new ones. To overcome problems an insider attack, their proposed work is based on hashed value of plain text (password). Simple password without using any hash value is sent to gateway node in Das scheme which causes various insider attacks in a network. So hash value of password decreases the probability of insider attack in a network. To some extent, their proposed work offers security to a network but this scheme also has some security flaws. In this scheme, the session key is not established between two entities, for instance the sensor node and the user. Therefore, mutual authentication along with message confidentiality is not ensured. Recently a new authentication mechanism is proposed that's helps users for easy password memorization [14]. An authentication scheme that adopts computable dynamic password is proposed in [15]. They have designed a custom password computation algorithm to make the password confidential and dynamic for each login round. A lightweight password based authentication scheme has been proposed to prove protection from Insider attacks in [16]. Their evaluation shows better results than other existing protocols in terms of computational cost and communication overhead with high level of security.

Yuan et al proposes the protocol based on biometrics of users. Password and smart card is also used in their work [17]. Transmitted data is not encrypted in this scheme; if any of sensor nodes is captured by an unauthorized user then he can easily view the messages. Moreover, an attacker can exchange messages as an authorized entity between sensor node and user and gather all the information. Since no secure channel is provided, message confidentiality and data integrity are major problems in this scheme. Yoon et al [18] proposes a protocol that is enhancement of Yuan protocol [17] based on biometrics but without password. In this protocol two secret parameters are used. Through these secret parameters all entities verify legitimacy of each other in the network. Data integrity is considered in this protocol. But this scheme still has security flaws as response message of user sent by sensor node is not encrypted therefore confidentiality issues can still arise. Moreover, this protocol is susceptible to various DOS attacks. To overcome flaws in Yoon protocol, Debiao introduced another protocol that was based on user's biometrics. This protocol needs complicated hardware and is computationally intensive and thus consumes a lot of energy [19]. Additional hardware, like smart card, based biometric schemes have been proposed by [20, 21] for wireless sensor networks, especially big data environments. Multifactor user authentication protocol for data access in wireless sensor networks has been proposed that provide forward secrecy [22]. Similarly, another study has proposed a lightweight security-improved smart card based three-factor authentication scheme for WSNs to overcome the weaknesses of previous schemes [23].

As per our observation the above-mentioned protocols are susceptible to various types of attacks including DOS attack, guessing and replay attack [24]. Node compromise, message confidentiality and data integrity are major problems in existing protocols and some of these protocols also require complicated hardware. The security of previous user authentication protocols is based on password. Short length passwords are broken without difficulty with the help of password guessing attacks. Additionally, a user password can be shared with others or stolen and there is no way to differentiate between the actual user and an impersonator. Similarly other authentication protocols require special hardware support. Biometric authentication can overcome these security limitations [25]. It is more secure as well as reliable than conventional password based authentication. Althobaiti et al pointed out numerous security vulnerabilities in traditional user authentication protocols and proposed an efficient biometric based user authentication scheme for WSNs [26]. It is feasible for resource constraint devices in WSNs because it is based on hash function and biometric encryption without using any complicated equipment. However, Das [27] described that Althobaiti's scheme is efficient in terms of computation but it is not secure against several common attacks such as man-in-the-middle attack, impersonation attack, and is not resilient against node capture attack [12].

Srikanth designed a new biometric based user

authentication mechanism for heterogeneous WSNs. This mechanism provides stronger authentication than traditional password based protocols [28]. Moreover, provides mutual authentication and defends WSNs against several security attacks. This protocol is efficient in terms of computation cost but requires special hardware. A privacy-preserving authentication scheme for multi-server architecture using elliptic curve cryptography (ECC) has been proposed by [29]. They used identity-based cryptography for providing certificate less authentication. A user authentication scheme for multi-server environments is proposed in [30]. Server mutual verification is used in this scheme to provide robustness to a malicious server. Their scheme can protect from malicious insiders attacks in multi-server environments. It also requires special hardware due to use of smart cards.

Das proposed a new biometric based remote user authentication scheme for WSNs. This protocol uses biometric verification along with password based verification in order to provide strong authentication [31]. This scheme provides mutual authentication and low cost as compared to existing related protocols. This scheme is secure against active and passive attacks but still insecure against some common attacks such as network traffic attack and DOS attacks.

Authentication in wireless sensor networks has become an attractive research area in the domain of IOT and Smart homes. Light weight three factor authentication schemes have been proposed of Smart homes in [32] and IOT and 5G in [33] and [34]. All these schemes require smart card to store user biometric information and provide authentication. Their proposed scheme provides desirable attributes for IoT environments and show that the computation and communication costs are suitable for extremely low-cost IoT devices. Need for smart card was removed by scheme proposed in [35].

Health care monitoring is another emerging application of wireless sensor networks. The most important aspect of healthcare applications is to provide access to sensitive documents [35]. Authentication is thus vital for secure health care provision. A secure authentication scheme for multi-server based E-health system is provided in [37]. Cancelable transformation of the raw biometric data is used to provide the privacy to biometric data in this scheme. Biometric and smartcard based authentication schemes have been proposed for health care in [38] and [39].

All these schemes have several security vulnerabilities such as sensor node impersonation attack, poor repair ability, biometric recognition error, user verification problem, and session key exposure by the gateway node, lack of anonymity, insecure against DOS attack [40-47]. Smart card based schemes are prone to smart card stolen attack [48, 49]. To address the limitations of schemes based on integration of password, smart card and biometrics, a Secure User's Biometric Based Authentication Scheme (SUBBASe) was proposed by Riaz [50]. The scheme provides mutual authentication, defends network against several common security attacks such as stolen verifier attack, message confidentiality, replay attack, guessing attack and network traffic attack. We found that although this scheme enhances the network security significantly, it suffers from several security vulnerabilities such as biometric recognition error, user anonymity, perfect forward secrecy, and gateway node impersonation attack.

Hence existing user authentication protocols based on biometric are still facing several security vulnerabilities and decrease the overall performance of WSNs. Therefore, only biometric based user authentication protocol for resource constraint devices is not sufficient to increase the effectiveness and efficiency of the entire WSN. To solve these problems, we first suggest appropriate countermeasures and then propose enhanced biometric based user authentication scheme for wireless sensor networks using fuzzy extraction and elliptic curve cryptography. Our proposed scheme conforms to the proposed countermeasures.

RELATED WORK

Fuzzy Extraction

We use an efficient fuzzy extractor that converts non-uniform biometrics data into a uniform random string. Using this random string makes it possible to provide biometrics security by applying cryptographic mechanisms. The fuzzy extractor can reliably extract

uniform randomness pair (R_i, P_i) from user's biometrics information. It is an error tolerant mechanism because R_i will be the same in the assistance of helping string P_i even if the new user's biometrics has some little difference from the original biometrics [51]. The fuzzy extractor consists of two algorithms (Gen and Rep).

- **Gen (B_i) = (R_i, P_i)** Gen is a probabilistic generation algorithm that takes a user's biometrics as the input, and extracts a random string Ri and a helping string Pi as the output.
- **Rep(B_i*,P_i)=R_i** Rep is a deterministic reproduction algorithm, which permits Ri to be recovered from the corresponding helping string and newly captured user's biometrics as long as both the original biometrics and the newly captured biometrics are similar to each other.

Elliptic Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) is a public key encryption method based on elliptic curves which have an algebraic structure in the form $y^2=x^3+ax+b$. ECC provides equivalent security but with reduced key size when compared to other public key cryptography methods. Therefore ECC is useful for resource-constrained devices. [52]

Let P>3 be a large prime number and select two elements a,b∈ FP that satisfy $4a^3+27b^2=0$ mod P to describe the equation of no super singular curve $E:y^2=x^3+ax+b$ mod P over FP. Select a generator point P=(x×P, y×P) having order in large prime number q over E(FP). The subgroup G of the elliptic curve group E(Ep) having order q is built in the same manner. There are three mathematical problems in ECC.

- Elliptic Curve Discrete Logarithm Problem (ECDLP): If Q is the point element in G, find x ∈ z* such that Q=x×P, where x×P indicates that point P is x time added to itself through an operation with an elliptic curve.
- Elliptic Curve Computational Diffie-Hellman Problem (ECCDHP): For a∈zq*, given two point elements a×P and b×P, compute a×b×P in G.
- Elliptic Curve Decisional Diffie-Hellman Problem (ECDDHP): For a∈zq*, given three point elements a×P, b×P, and c×P in G, verify whether c×P = a×b×P.

In the proposed scheme for the protection of a random number generated by user (ru) and sensor (rs), we use ECDLP in the following way:

The user sends $X_i = r_u \times P$ to the gateway, and the sensor sends $Y_i = r_s \times P$ to the user for a session key agreement and authentication. If an adversary obtains r_u and r_s, he can attempt different types of attacks. But in the proposed scheme, if an adversary captures Xi and Yi, the adversary cannot compute r_u and r_s owing to the use of ECDLP. In proposed scheme ECCDHP is used to protect $KUS = KSU = r_u \times r_s \times P$ from an attacker. Only authorized user and sensor can calculate KUS and KSU by using own random number.

Proposed Scheme (EBAS-FeEcc)

This section introduces our proposed scheme that provides Enhanced Biometric based user Authentication Scheme using Fuzzy extraction and Elliptic curve cryptography (EBAS-FeEcc). All the symbols that are used in this paper are described in Table 1. In our proposed scheme user ID, secret value xo is preloaded at each node and one master key h(x‖y) is preloaded at the gateway node in the network before their deployment. EBAS-FeEcc consists of two phases; registration phase, and login and authentication phase.

Table 1. Symbols used in Secure Authentication Technique.

Notations	Comments
TN	Trusted node
SN	Sensor node
ID_u	Identity of user
h(.)	One-way hash function
Esk()	Encryption of message
Dsk()	Decryption of message
||	Concatenation operator
Δt	Time interval for transmission delay
x_0	Secret value known to TN
RI	Requested information of user
Bio_u	Biometrics of user
AE	All participating entities
P_{fe}	Helping strings generated by fuzzy extractor
P_{ec}	Base point on the elliptic curve

Registration Phase

The registration phase of the EBAS-FeEcc is described in Fig. 1. The user performs its registration with the gateway node using a secure channel. User computes Bi by using a biometrics scanning device and R_i and P_{fe} using fuzzy extraction. Then, the user's information is sent to the gateway for registration. However, the gateway will not store the user's biometrics information. The detailed steps of this are as follows.

The user selects ID_u and captures their own biometrics Bi using a scanning device (PC or PDA).

User computes a uniform random string Ri and a helper string P_{fe} using a fuzzy extractor, i.e., $<R_i,P_{fe}>=Gen(B_i)$ and $A_i=h(R_i)$. Then user sends $<ID_u,A_i>$to the gateway node.

After receiving $<ID_u,A_i>$, the gateway node computes the authentication parameters for user by using the received hash value; ID_u and secret parameter xo, which are preloaded at each node in the network before executing the scheme as follows:

$$s = h(ID_u||A_i||x_0)$$

$$N_i = h(x\|y) \oplus A_i$$

The gateway node broadcasts a secret message containing these parameters, i.e., $M1=<s,N_i>$, to everyone in the network, after successful registration, it will be helpful for authentication purpose.

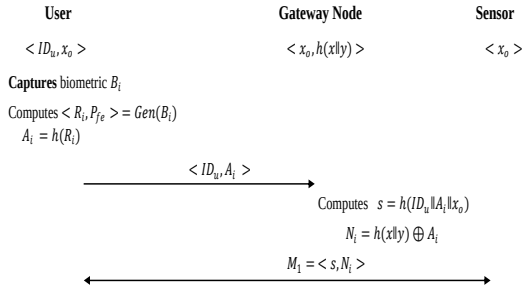


Figure 1. Registration phase of proposed scheme.

Login and Authentication Phase

The login and authentication phase of EBAS-FeEcc scheme is shown in Fig. 2. The detailed steps are as follows:

- The user again captures his own biometric information B_i*; reproduces a random string R_i* using a fuzzy extractor, i.e., $R_i*=Rep(B_i*,P_{ec})$; computes the hash value of the random string, i.e., $A_i*=(R_i*)$; and calculates h*(x||y) to provide user anonymity:

$$h*(x\|y) = Ai* \oplus Ni$$

$$ID_u^* = ID_u \oplus h^*(x\|y)$$

- User generates a random number ru and computes X_i, which is used as a session key between the user and sensor:

$$Xi = r_u \times Pec$$

- The user takes the current time stamp T_0, and sends a message containing request for the required information and some parameters X_i, ID_u*,A_i*,T_0 for authentication with the gateway node:

$$M_2 =< X_i, ID_u^*, A_i^*, RI, T_o >$$

- After receiving M2 from the user, the gateway node retrieves the current timestamp T_0 and checks the freshness of time. If $T_1-T_0 \geq \Delta T$, the request is rejected; otherwise, a hash value of the random string is computed, i.e., $A_i*=(R_i*)$, and h*(x||y) is calculated to provide user anonymity:

$$h^*(x\|y) = A_i^* \oplus N_i$$

$$ID_u^* = ID_u \oplus h^*(x\|y)$$

The following are verified: (i) A_i and A_i^* and (ii) ID_u and ID_u^*

- If $A_i \neq A_i^*$and $ID_u \neq ID_u^*$then gateway node sends a reject message M_3= [Reject] to the user otherwise it sends M_4= [In-Progress] and also takes a new time stamp $T_2$and forwards a message to sensor node containing request for desired information along with some parameters i.e. $ID_u^*, s^*, A_i^* X_i, T_2$ to authenticate with sensor node:

$$M_5 =< IDu*, s*, RI, Ai*, Xi, T_2 >$$

- After receiving the message M_5 from the gateway node, sensor node checks timestamp if $T_3 - T_2 \geq \Delta T$ then request rejected and authentication phase is stopped else sensor node
- compares S and S* to authenticate the gateway

node if S ≠S* then reject request and

- authentication phase stopped.
- Otherwise sensor node generates a random number r_s to compute a session key. This session key is only computed by user and sensor node due to the mathematical problem inherent to ECC. Then sensor node takes a new time stamp T_4 and computes vi and encrypts the required information by using this key.

$$Yi \times Pec$$

$$ksu = rs \times Xivi = h(IDu * \|s\|ksu\|T_4)$$

$$e = Evi(RI)$$

Sensor node uses v_i as session key which is shared between user and sensor node. $E_{Vi}(RI)$ is encryption of requested information (RI) of user.

- After encryption, the sensor node sends the secured requested information to the user in the following manner.

$$M_6 = (Accpt, e, Yi, T_4)$$

- After receiving the message from the sensor node, the user verifies if T5-T4≥ΔT and then computes k_{us}. If user is legal, then the user computes the session key v_i using the secret parameters s and k_{us}. Finally, it decrypts the message using vi and obtains the required information in this way:

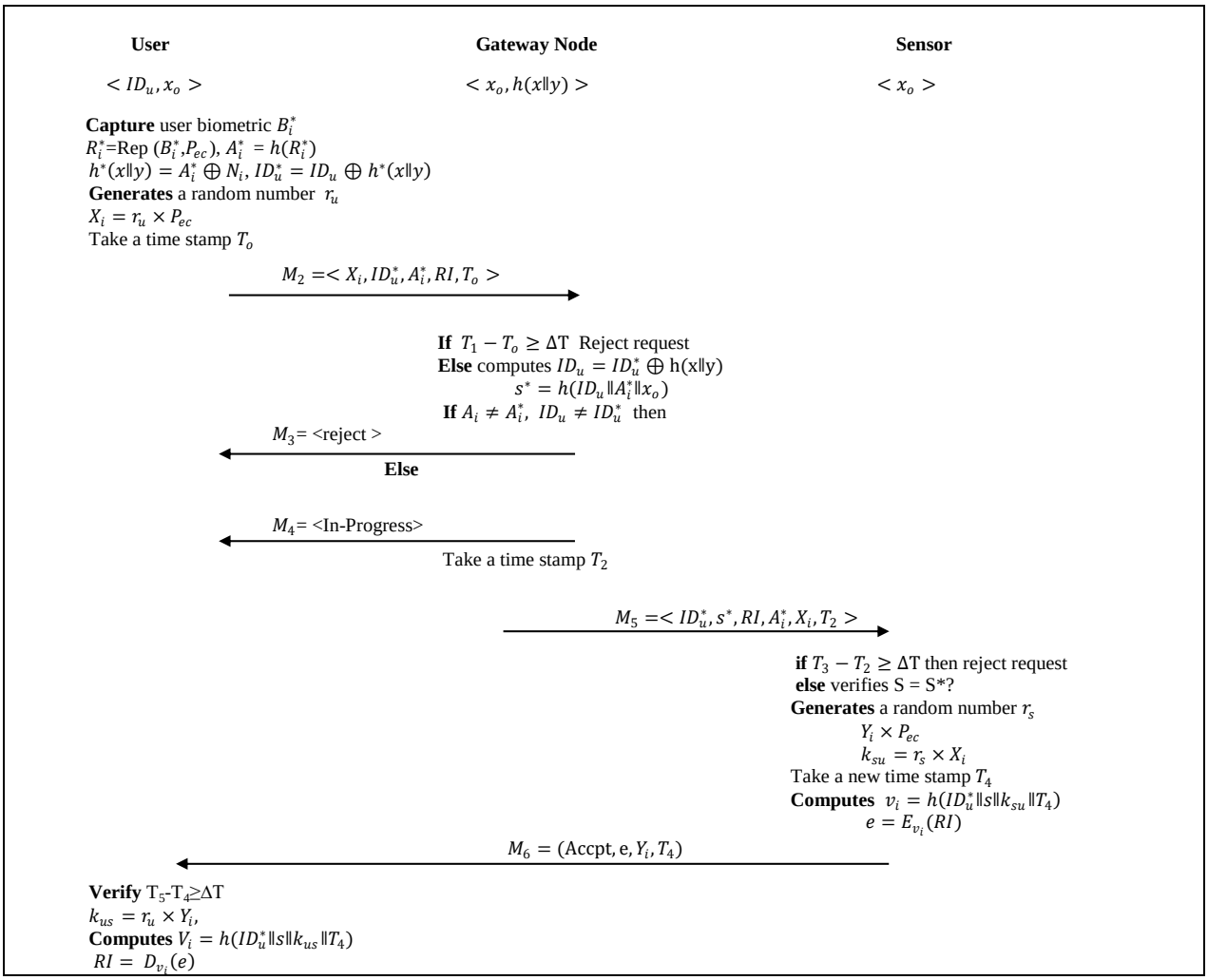
$$k_{us} = r_u \times Y_i$$

$$v_i = h(ID_u^* \| s \| k_{us} \| T_4)$$

$$RI = D_{vi}(e)$$

- From now on, the user can communicate securely with the sensor node using the following session key:

$$\boldsymbol{v_i = h(ID_u^* \| s \| k_{us} \| T_4)}$$



Security Analysis

This section describes the security analysis to demonstrate the security properties of our proposed scheme EBAS-FeEcc.

Eliminate need for Complicated Equipment

To provide a high level of security, numerous storage devices such as smart cards are used for identification purpose. Such storage devices cannot be supported by everyone because of the need for specialized and often expensive hardware. In our proposed scheme the users don't require any additional hardware. Only a recognition interface that provides the additional security benefits to the users and merchants is needed. This will enhance the efficiency of network and provide more accessibility to the users.

Prevent Guessing Attack

This kind of attack occurs in password based systems. The proposed scheme defends against this type of attack because each user uses own biometrics features in registration, login and authentication phases instead of a password. An attacker cannot steal user's biometrics.

Resist Replay Attack

If an attacker captures previous communication and starts communication between two entities pretending to be a legal user, proposed scheme prevents this attack by adding timestamps T_0, T_2, T_4 into authentication messages M1, M4, M5, respectively. Even if the attacker obtains messages, and starts communication with the current timestamps, he will not be able to verify ΔT.

Resist Integrity Threat

If an attacker captures the message during transmission and alters the contents of that message among communicating entities, the proposed protocol assures data integrity by using a one way hash function i.e. $M_2 =< X_i, ID_u^*, A_i^*, RI, T_o >$ where $A_i^* = h(R_i^*), ID_u^* = ID_u \oplus h^*(x\|y)$. All messages are sent in the same way so an attacker cannot alter these messages.

Resist Insider Attack

Typically, malicious insiders want to capture private user information such as their biometrics. In proposed scheme the user imprints own biometrics B_i and generates a random string by using fuzzy extraction i.e. $< R_i, P_{fe} >= Gen(B_i)$ and calculates $A_i = h(R_i)$, then sends A_i to gateway node. The gateway node cannot obtain B_i from A_i due to the properties of one way hash function and fuzzy extraction method. Therefore, the proposed scheme is secure against insider attacks.

Provide Mutual Authentication

In the proposed scheme all entities authenticate each other before starting the communication so it provides mutual authentication. When user sends request to the gateway node it verifies user's authenticity and then forwards request to the sensor node. The sensor node checks the legality of sender and then sends requested information to the user.

Provide User Anonymity

In proposed scheme the user's ID is protected by using hash function i.e. $ID_u^* = ID_u \oplus h^*(x\|y)$. An attacker cannot obtain user's ID without knowing the $h(x\|y)$. The gateway node can calculate ID_u because they store a master key $h(x\|y)$ before executing the scheme. User can also compute the $h(x\|y)$ by using his biometrics and parameters received from the gateway node i.e. $N_i = h(x\|y) \oplus A_i$.

Robust Against Biometric Recognition Error

The proposed scheme is robust against biometric recognition error by using fuzzy extraction. Fuzzy extractor generates a uniform random string R_i and a helper string P_{ec}. Even if a user's biometric B_i^* is slightly different from a previous biometric reading for the same user due to sensitivity of the biometric sensor, R_i remains the same with the assistance of helper string P_{ec}.

In registration phase user captures own biometrics B_i and computes P_{ec}, R_i and A_i in this way:

$$< \mathrm{R_i}, \mathrm{P_{fe}} >= Gen(\mathrm{B_i})$$

$$< \mathrm{R_i}, \mathrm{P_{fe}} >= Gen(\mathrm{B_i})$$

$$\mathrm{A_i} = \mathrm{h(R_i)}$$

In login and authentication phase user again captures own biometric B_i^* and performs following step:

$$\mathrm{R_i^*}=\mathrm{Rep}\ (\mathrm{B_i^*}, \mathrm{P_{ec}}),\ \mathrm{A_i^*} = \mathrm{h(R_i^*)}$$

Fuzzy extractor computes constant value of A_i^* even if new user's biometric is slightly different from

previous biometric. Hence EBAS-FeEcc resists biometric recognition errors.

Table 2 provides a summary and comparison of the security provided by the proposed scheme EBAS-FeEcc and that provided by other schemes including SUBBASe.

Table 2. Security comparison of Authentication Schemes Against various Attacks

Resists Attacks	Debiao [19]	Yoon [18]	Althobaiti et al [26]	SUBBASe [50]	F.Wei [40]	Yoon & Kim [18]	EBAS-FeEcc
Replay Attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Guessing Attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Stolen-verifier Attack	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Impersonation Attack	Yes	No	Yes	Yes	Yes	Yes	Yes
Complicated Hardware Needed	Yes	Yes	No	No	Yes	Yes	No
Insider Attack	Yes	No	Yes	Yes	Yes	Yes	Yes
Biometric Recognition Error	No	No	No	No	Yes	No	Yes

Performance Evaluation

The proposed scheme EBAS-FeEcc is evaluated and compared with SUBBASe, Yoon and Kim, F.Wei, Yoon and Kim, Althobaiti and Debiao's schemes for different metrics like time computation, energy consumption and different attacks. By applying all these schemes on mica2 nodes of WSNs, we evaluate the performance of proposed scheme. We use mathematical model to examine the performance. Our algorithm uses RC5 and ECDH [40] as these are most suitable for implementation on resource constraint devices. Time to encrypt and decrypt messages using RC5 is 0.26ms on mica2 node. Similarly we choose SHA-1, time to perform one way hash function on mica2 is 3.636ms [50]. Our scheme uses ECC and fuzzy extractor to provide strong security in WSNs. The total amount of energy needed per node to perform ECDH key exchange is approximately 57mj and it takes around 2.375ms [53]. The computational cost of an efficient fuzzy extractor is not greater than the computational cost of one hash operation [54, 55].

In SUBBASe, one hash operation is needed by user in enrollment phase, and two hash operations and time to decrypt message, three hash operations and time to encrypt a message is required by sensor node and three hash operations are required by trusted node for authentication.

In proposed EBAS-FeEcc one hash operation and one fuzzy extraction operation is required by the user in registration phase. Two hash operations, one fuzzy extraction operation, one ECDH (two elliptic curve point multiplication) and one decryption operation is needed by the user in login and authentication phase. Gateway node requires one hash operation in registration phase and one hash operation in authentication phase. One hash operation, one ECDH operation (two elliptic curve point multiplication and one encryption operation) is required by the sensor node in authentication. Table 3 shows the computation time comparison for login, authentication and registration phases of different authentication schemes.

Table 3. Computational time Comparison			
Protocols	**Registration**	**Login + Authentication**	**Total computational time**
Yoon protocol [18]	$3\ T_H$	$10\ T_H$	$13\ T_H$
Debiao protocol [19]	$3\ T_H$	$8\ T_H + 4T_{sym}$	$11\ T_H + 4\ T_{sym} = 15\ T_H$
Althobaiti protocol [26]	$2\ T_H$	$6T_H + 4T_{RC5} + 2T_{MAC}$	$8T_H + 4T_{RC5} + 2T_{MAC}$
SUBBASe protocol [50]	$2T_H$	$7T_H + 2T_{RC5}$	$9\ T_H + 2T_{RC5}$
Yoon&Kim protocol [19]	$3T_H$	$11T_H + 4T_{sym}$	$17T_H$
F.Wei protocol [40]	$4T_H$	$11T_H + 4T_{sym}$	$19T_H$
EBAS-FeEcc	$2T_H + Tf_e$	$2T_{RC5} + T_{fe} + 2EC_{DH} + 4T_H$	$8T_H + 2T_{RC5} + 2f_e + 2EC_{DH}$

Our protocol's aim is to reduce the computation cost at sensor node as energy of tiny sensor nodes is inadequate and it directly affects network life time. We calculated time taken and energy consumed for authentication of one user by our proposed protocol as well as existing schemes, which is shown in Table 4. For calculating energy we used equation E=v*Q where Q= i*t. For mica2 node v=3.0, I=8mA. E denotes consumption of energy, Q is charge, I is current, V is voltage and t is time [25]. We compared total energy consumption during registration, login and authentication phase between proposed and other previous schemes based on their computation time as calculated in Table 3.

Table 4.Computational Over head in terms of Time and Energy consumption for One User		
Protocols	**Time (ms)**	**Energy Consumption (mJ)**
Yoon protocol [18]	47.26	1134.42
Debiao protocol [19]	54.54	1308.96
Althobaiti protocol [26]	36.37	872.83
SUBBASe protocol [50]	33.24	797.76
Yoon and Kim protocol [18]	65.44	1570.56
F.Wei protocol [40]	69.052	1657.25
EBAS-FeEcc	34.358	824.59

Thus the analysis clearly indicates that proposed scheme improves the network performance and its life time by reducing time and computational overhead. In addition, our scheme also enhances the security of WSNs by protecting it against various security attacks (Table 2).

We use simulation for evaluating the strength and performance of the proposed security technique EBAS-FeEcc. When users increase, the computational overhead for authentication also increases. This is because more number of nodes gets involved in the authentication process (Fig. 3). As time complexity of existing schemes increases the energy consumption also increases. We noticed that the energy consumption of proposed scheme is a bit more than SUBBASe because it required more energy due to fuzzy extraction method and ECC in order to provide strong authentication and high security. But energy consumption of proposed scheme is minimum as compared to all other compared schemes (Fig. 4). Since in our approach only authorized users can access information from the network so nodes (sensor nodes/base station) do not send redundant packets and only few packets are exchanged during transmission which decreases the network traffic overhead. Therefore our scheme increases the network's performance and life time by saving battery power of its nodes. So network becomes sustainable for authorized users through easy operations and less calculations.

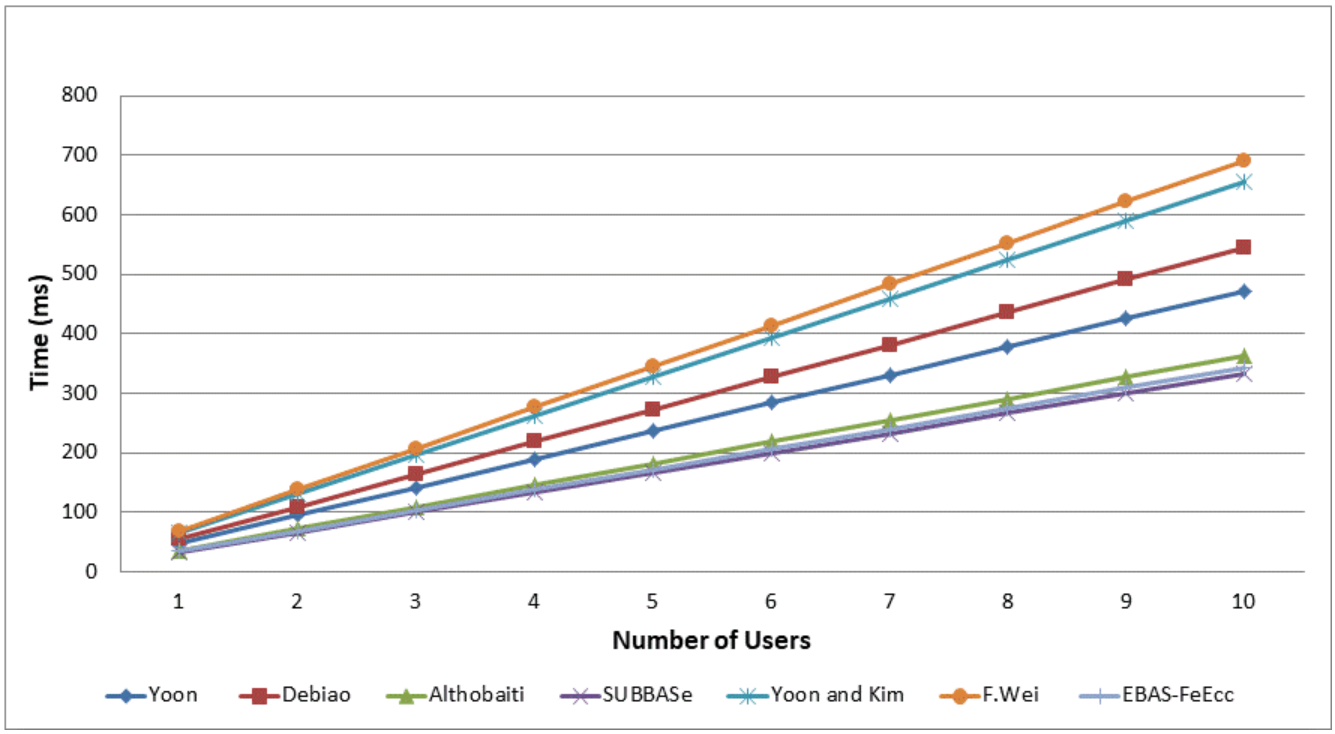


Figure 3. Computational overhead with respect to number of users

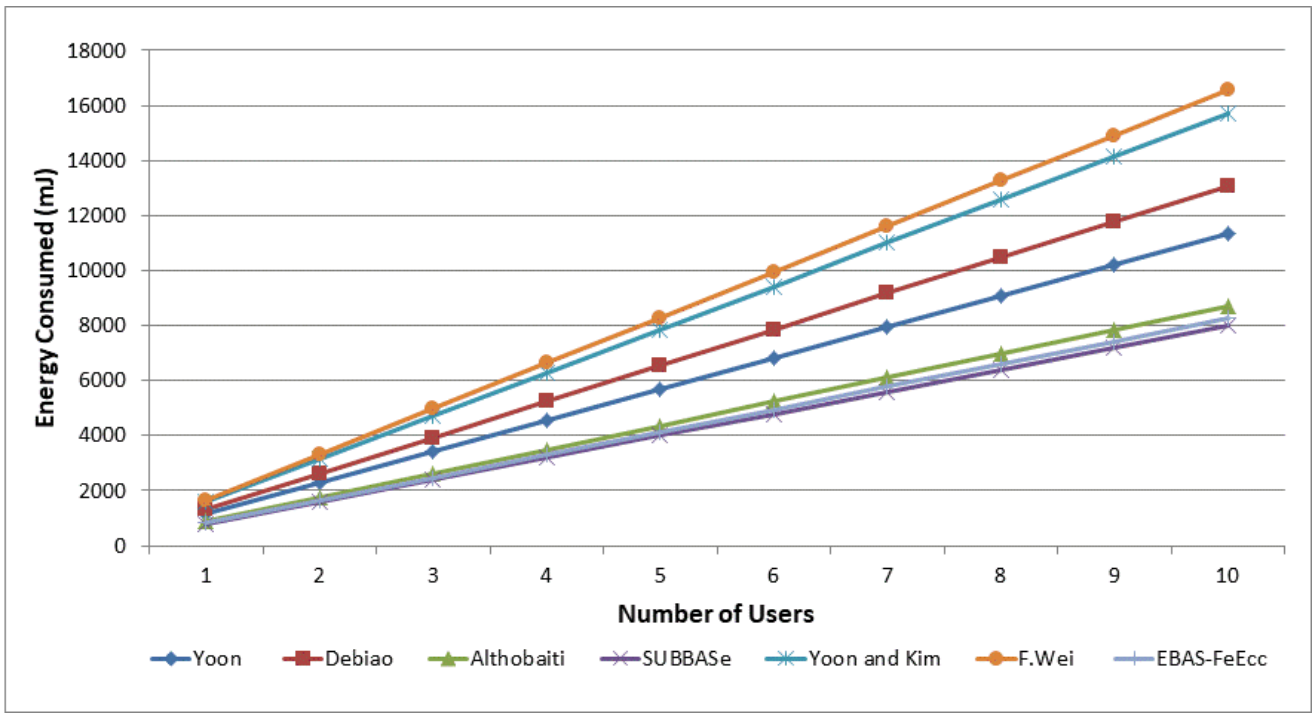


Figure 4.Energy consumption with respect to number of users

CONCLUSION

A large number of authentications schemes have been designed for WSNs that provide security to wireless sensors and users. To overcome the limitations of schemes based on integration of password, smart card and biometrics, a secure user's biometric based authentication scheme (SUBBASe) was proposed. In this paper, we have identified vulnerabilities in SUBBASe scheme in terms of a biometric recognition error, lack of anonymity, lack of perfect forward secrecy, and session key exposure by the gateway node. To solve these security vulnerabilities, we have used fuzzy extraction and ECC. During the registration phase, fuzzy extraction imprints biometrics consisting of error tolerant cryptographic primitives for biometric security. During the authentication phase, sensor node's random number and ECC are used to exchange a random number between a user and the sensor node. ECC maintain the same degree of security with a smaller key size than other forms of public-key cryptography thus making it suitable for use in wireless devices with limited resources. In accordance with these countermeasures, we proposed an enhanced biometrics-based authentication scheme using fuzzy extraction and ECC (EBAS-FeEcc) with improved security. In addition, we conducted a security analysis and performance evaluation to show that the proposed scheme is more secure and efficient not only in comparison to SUBBASE but also to other authentication schemes.

REFERENCES

1. M. T. Raza, S. Lu and M. Gerla, "vEPC-sec: Securing LTE Network Functions Virtualization on Public Cloud," IEEE Transactions on Information Forensics and Security, vol. 14, no. 12, pp. 3287-3297, 2019.
2. J. Mo, Z. Hu and Y. Lin, "Cryptanalysis and Security Improvement of Two Authentication Schemes for Healthcare Systems Using Wireless Medical Sensor Networks." Security & Communication Networks, https://doi.org/10.1155/2020/5047379, 2020.
3. M. J. Gul, A. Rehman, A. Paul, S. Rho, R. Riaz and J. Kim, "Blockchain Expansion to secure Assets with Fog Node on special Duty," Soft Computing, pp. 1-13, https://doi.org/10.1007/s00500-020-04857-0, 2020.
4. L. Yang and Z. Zheng, "Cryptanalysis and improvement of a biometrics-based authentication and key agreement scheme for multi-server environments,". PLoS ONE, vol 13, no. 3, 2018.
5. R. Riaz, S. S. Rizvi, H. M. Minhas, and S. Shokat, "Analysssis and Evaluation of Privacy Issues in Online Social Networks", Journal of Information Communication Technologies and Robotic Applications (JICTRA), vol. 10, no. 2, pp. 59-69, Dec. 2019.
6. B. Bhushan and G. Sahoo, "E2SR2: An acknowledgement-based mobile sink routing protocol with rechargeable sensors for wireless sensor networks," Wireless Networks, vol. 25, no. 5, pp. 2697-2721, 2019.
7. R. Riaz, S. S. Rizvi, E. Mushtaq and S. Shokat, "OSAP: Online Smartphone's User Authentication Protocol," International Journal of Computer Science and Network Security (IJCSNS), vol. 17, no. 3, pp. 7-12, Mar. 2017.
8. S. S. Rizvi and T. S. Chung, "PIYAS-Proceeding to intelligent service oriented memory allocation for flash based data centric sensor devices in wireless sensor networks," Sensors, vol. 10, no. 1, pp. 292-312, 2010.
9. M. A. Ferrag, L. Maglaras and A. Derhab, "Authentication and Authorization for Mobile IoT Devices Using Biofeatures: Recent Advances and Future Trends," Security and Communication Networks, https://doi.org/10.1155/2019/5452870, 2019.
10. K. H. Wong, Y. Zheng, J. Cao and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," In IEEE International Conference on Sensor Networks, Ubiquitous, and Trustsworthy Computing (SUTC'06), vol. 1, pp. 8-pp, IEEE, 2006.
11. M. L. Das, "Two-factor user authentication in wireless sensor networks," IEEE Transactions on Wireless Communications, vol. 8, no. 3, pp. 1086-1090, 2009.
12. C. Wang, D. Wang, Y. Tu, G. Xu and H. Wang, "Understanding Node Capture Attacks in User Authentication Schemes for Wireless Sensor Networks," IEEE Transactions On Dependable And Secure Computing, pp. 1-17, 2020.
13. M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of two-factor user authentication in wireless sensor networks". Sensors, vol. 10, no. 3, pp. 2450-2459, 2010.
14. S. S. Woo, R. Artstein, E. Kaiser, X. Le and J. Mirkovic, "Using Episodic Memory for User Authentication," ACM Transactions on Privacy and Security, vol. 22, no. 2, pp. 11-46, 2019.
15. X. Liu, R. Zhang and M. Zhao, "A robust authentication scheme with dynamic password for wireless body area networks," Computer Networks, vol. 161, pp. 220-234, 2019.
16. S. Rajamanickam, S. Vollala, R. Amin and N. Ramasubramanian, "Insider Attack Protection: Lightweight Password-Based Authentication Techniques Using ECC," in IEEE Systems Journal, doi: 10.1109/JSYST.2019.2933464 , 2019.

17. J. Yuan, C. Jiang, and Z. Jiang, “A biometric-based user authentication for wireless sensor networks,” Wuhan University Journal of Natural Sciences, vol. 15, no. 3, pp. 272-276, 2010.
18. E. J. Yoon and K. Y. Yoo, “A new biometric-based user authentication scheme without using password for wireless sensor networks.” IEEE 20th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 279-284, IEEE , 2011 .
19. D. He, Y. Zhang and J. Chen, “Robust Biometric-Based User Authentication Scheme for Wireless Sensor Networks,” IACR Cryptology ePrint Archive 2012, p 203, 2012.
20. T. Maitra, D. Giri and R. N. Mohapatra, "SAS-SIP: A secure authentication scheme based on ECC and a fuzzy extractor for session initiation protocol," Cryptologia, vol. 43, no. 3, pp. 212-232, 2019.
21. S. Nashwan, "AAA-WSN: Anonymous access authentication scheme for wireless," Egyptian Informatics Journal, pp. 1-12, 2020.
22. D. Wang, P. Wang and C. Wang, "Efficient Multi-Factor User Authentication Protocol with Forward Secrecy for Real-Time Data Access in WSNs," ACM Transactions on Cyber-Physical Systems, vol. 4, no. 3, pp. 30-56, 2020.
23. J. Mo and H. Chen, "A Lightweight Secure User Authentication and Key Agreement," Security and Communication Networks, pp. 1-17, 2019.
24. D. G. Padmavathi and M. A. Shanmugapriya, “Survey of attacks, security mechanisms and challenges in wireless sensor networks,” International Journal of computer Science and Information Security, pp. 69-80, 2009.
25. D. Bhattacharyya, R. Ranjan, F. Alisherov and Choi, “Biometric authentication: A review,” International Journal of u-and e-Service, Science and Technology, vol. 2, no. 3, pp. 13-28, 2009.
26. O. Althobaiti, M. Al-Rodhaan and A. Al-Dhelaan, “An efficient biometric authentication protocol for wireless sensor networks,” International Journal of Distributed Sensor Networks, vol. 9, no. 5, pp. 407971, 2013.
27. A. K. Das, “On the Security of An Efficient Biometric Authentication Protocol for Wireless Sensor Networks,” IACR Cryptology ePrint Archive 2014, p. 643, 2014.
28. S. P. Srikanth and D. S. Haliyal, “Two Way User Authentication Using Biometric Based Scheme for Wireless Sensor Networks,” International Journal of Engineering and Innovative Technology, vol. 3, no. 10, pp. 2277-3754, 2014.
29. M. Shuai, B. Liu, N. Yu, L. Xiong and C. Wang, "Efficient and Privacy-preserving Authentication scheme for Wireless Body Area Networks," Journal of Information Security and Applications, vol. 52, p. 102499, 2020.
30. Y. Park, K. Park and Y. Park, "Secure user authentication scheme with novel server mutual verification for Multiserver Environments," International Journal of Communication Systems, vol. 32, no. 7, p. 3929, 2019.
31. A. K. Das, S. Chatterjee and J.K. Sing, “A New Biometric-Based Remote User Authentication Scheme in Hierarchical Wireless Body Area Sensor Networks,” Adhoc and Sensor Wireless Networks, 28, 2015.
32. S. Shin and T. Kwon, "A Lightweight Three-Factor Authentication and Key Agreement Scheme in Wireless Sensor Networks for Smart Homes," Sensors, vol. 9, no. 2, pp. 1-24, 2019.
33. H. Lee, D. Kang, J. Ryu, D. Won, H. Kim and Y. Lee, "A three-factor anonymous user authentication scheme for Internet of Things environments," Journal of Information Security and Applications, vol. 52, p. 102494, 2020.
34. S. Shin and T. Kwon, "A Privacy-Preserving Authentication, Authorization, and Key Agreement Scheme for Wireless Sensor Networks in 5G-Integrated Internet of Things," IEEE Access, vol. 8, pp. 67555-67571, 2020.
35. M. Wazid, A. K. Das, S. Shetty, J. J. P. C. Rodrigues and Y. Park, "LDAKM-EIoT: Lightweight Device Authentication and Key Management Mechanism for Edge-Based IoT Deployment," Sensors, vol. 19, no. 24, p. 5539, 2019
36. T. Ali, “Z Notation Formalization of Blockchain Healthcare Document Sharing Based on CRBAC”, JICTRA, pp. 16-29, Jun. 2018.
37. S. Barman, H. P. H. Shum, S. Chattopadhyay and D. Samanta, "A Secure Authentication Protocol for Multi-Server-Based E-Healthcare Using a Fuzzy Commitment Scheme," IEEE Access, vol. 7, pp. 12557- 12573, 2019.
38. B. D. Deebak, F. AL-Turjman, M. AloQaily and O. Alfandis, "An Authentic-Based Privacy Preservation Protocol for Smart e-HealthcareSystems in IoT," IEEE Access, vol. 7, pp. 135632- 135648, 2019.
39. Z. Ali, A. Ghani, I. Khan, S. A. Chaudhry, S. H. Islam and D. Giri, "A Robust Authentication and Access Control Protocol for Securing Wireless Healthcare Sensor Networks," Journal of Information Security and Applications, vol. 52, pp. 2214-2126, 2020.
40. J. Jung, D. Kang, D. Lee, D. Won, “An Improved and Secure Anonymous Biometric-Based User Authentication with Key Agreement Scheme for the Integrated EPR Information System”. PLoS ONE, vol. 12, no. 1,e0169414. https://doi.org/10.1371/journal.pone.0169414, 2017.
41. R. Riaz, T. S. Chung, S. S. Rizvi, N. Yaqub, “BAS: The Bi-phase Authentication Scheme for Wireless Sensor Networks,” International Journal of Security and Communication Networks (IJSCN), 2017.
42. J. Moon, D. Lee, Y. Lee and D. Won, “Improving Biometric-Based Authentication Schemes with Smart Card Revocation/Reissue for Wireless Sensor Networks,” Sensors, vol. 17, p. 940, 2017.
43. S. Yu, J. Lee, K. Lee, K. Park and Y. Park, “Secure Authentication Protocol for Wireless Sensor Networks in

Vehicular Communications," Sensors, vol. 18, no. 10, p. 3191, https://doi.org/10.3390/s18103191, 2018.
44. B. Yang and J. Zhang, "Physical Layer Secret-Key Generation Scheme for Transportation Security Sensor Network," Sensors, vol.17, no. 7, p. 1524, https://doi.org/10.3390/s17071524, 2017.
45. A. Ometov, S. Bezzateev, N. Voloshina, P. Masek and M. Komarov, "Environmental Monitoring with Distributed Mesh Networks: An Overview and Practical Implementation Perspective for Urban Scenario". Sensors, vol. 19, no. 24, p. 5548, https://doi.org/10.3390/s19245548, 2019.
46. F. Wang, G. Xu, C. Wang and J. Peng, "A Provably Secure Biometrics-Based Authentication Scheme for Multiserver Environment," Security and Communication Networks, https://doi.org/10.1155/2019/2838615, 2019.
47. A. Diaz and P. Sanchez, "Simulation of Attacks for Security in Wireless Sensor Network". Sensors, vol. 16, no. 11, p. 1932, https://doi.org/10.3390/s16111932 , 2016.
48. H. Guo, Y. Gao, T. Xu, X. Zhang and J. Ye, "A Secure And Efficient Three-Factor Multi-Gateway Authentication Protocol For Wireless Sensor Networks," Ad Hoc Networks, vol. 95, p. 101965, 2019.
49. M. Hussain, A. Mehmood, S. Khan, M. A. Khan and Z. Iqbal, "A Survey on Authentication Techniques for Wireless Body Area," Journal of Systems Architecture, p. 101655, 2019.
50. R. Riaz, N. U. A. Gillani, S. S. Rizvi, S. Shokat and S. J. Kwon, "SUBBASE: An Authentication Scheme for Wireless Sensor Networks Based on User Biometrics," Wireless Communications and Mobile Computing 2019, 2019.
51. R. Czabanski, M. Jezewski and J. "Introduction to fuzzy systems." In Theory and Applications of Ordered Fuzzy Numbers, pp. 23-43. Springer, Cham, 2017.
52. D. Hankerson, S. Vanstone and A. Menezes, "Guide To Elliptic Curve Cryptography," New York: Springer.2011
53. C. Lederer, R. Mader, M. Koschuch, J. Großschädl, A. Szekely and S. Tillich,"Energy-efficient implementation of ECDH key exchange for wireless sensor networks," In IFIP International Workshop on Information Security Theory and Practices, pp. 112-127, Springer, Berlin, Heidelberg, 2009.
54. Y. Dodis, B. Kanukurthi, J. Katz, L. Reyzin and A. Smith, "Robust fuzzy extractors and authenticated key agreement from close secrets," IEEE Transactions on Information Theory, vol. 58, no. 9, pp. 6207-6222, 2012.
55. Y. Choi, J. Nam, D. Lee, J. Kim, J. Jung and D. Won, "Security Enhanced Anonymous Multiserver Authenticated Key Agreement Scheme Using Smart Cards And Biometrics," The Scientific World Journal, 2014, 2014.
56.