sensors

MDPI

Article

A Secure Mutual Batch Authentication Scheme for Patient Data Privacy Preserving in WBAN

Martin Konan * and Wenyong Wang

Department of Computer Science and Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu 611731, China; wangwy@uestc.edu.cn

* Correspondence: martin_konan@live.fr

Received: 1 March 2019; Accepted: 26 March 2019; Published: 3 April 2019

Abstract: The current advances in cloud-based services have significantly enhanced individual satisfaction in numerous modern life areas. Particularly, the recent spectacular innovations in the wireless body area networks (WBAN) domain have made e-Care services rise as a promising application field, which definitely improves the quality of the medical system. However, the forwarded data from the limited connectivity range of WBAN via a smart device (e.g., smartphone) to the application provider (AP) should be secured from an unapproved access and alteration (attacker) that could prompt catastrophic consequences. Therefore, several schemes have been proposed to guarantee data integrity and privacy during their transmission between the client/controller (C) and the AP. Thereby, numerous effective cryptosystem solutions based on a bilinear pairing approach are available in the literature to address the mentioned security issues. Unfortunately, the related solution presents security shortcomings, where AP can with ease impersonate a given C. Hence, this existing scheme cannot fully guarantee C's data privacy and integrity. Therefore, we propose our contribution to address this data security issue (impersonation) through a secured and efficient remote batch authentication scheme that genuinely ascertains the identity of C and AP. Practically, the proposed cryptosystem is based on an efficient combination of elliptical curve cryptography (ECC) and bilinear pairing schemes. Furthermore, our proposed solution reduces the communication and computational costs by providing an efficient data aggregation and batch authentication for limited device's resources in WBAN. These additional features (data aggregation and batch authentication) are the core improvements of our scheme that have great merit for limited energy environments like WBAN.

Keywords: batch authentication; certificate less scheme; data aggregation; data privacy; elliptic curve cryptography (ECC); wireless body area networks (WBAN)

1. Introduction

Recall that recent innovations are done in the wireless sensor network (WSN), which have cleared the route for smart sensors that can be embedded on the human body to monitor glucose and respiratory rate, for example [1–5]. This interconnectedness of various advanced handheld gadgets worn or embedded in human systems is referred to as a wireless body area network (WBAN). WBAN commonly incorporates a cell phone at the client's side that acts as a center point/controller, obtaining the client's information and transferring it to a remote server or Application Provider (AP).

Despite the fact that WBAN has enhanced the e-Care administration system, the security and privacy of client's data remain a tremendous challenge to address [3–16]. For instance, a client should know about the AP dealing with his/her related information before asking for further data processing (data accountability issue). Therefore, there is a paramount need for the client, as well as the e-Care system agents (doctors, medical attendants, etc.), to authenticate each other to preserve data confidentiality.

Thereby the physician can ascertain the correctness of physiological information diagnostic that may have cataclysmic consequences on a patient in case of wrong authentication. Hence developing a new cryptosystem that ensures integrity, authentication, accountability, accessibility, non-repudiation, and secrecy is considered a hot topic by the information security research community [3–16]. A cryptosystem that provides mutual authentication scheme between the controller (C) and AP is crucial in order to preserve data security. For this reason, several valuable contributions have been introduced to securely transmit data from a given C to AP [3–23]. Note that those existing authentication schemes use different approaches that can be classified as: (i) physiological value based, (ii) channel based, (iii) proximity based, and (iv) cryptographic based [4].

Our proposed solution uses the cryptographic technique tools. Likewise, various cryptosystem schemes are presented among the research community [3–16]. However, the traditional asymmetric encryption (public key infrastructure PKI) technique that acts as primary solution to provide security is an inefficient option for optimized lightweight cryptosystem design in constrained resource environments (WBAN). This reason is due to the inherent PKI database administration issues, i.e., capacity, data transfer, and annulment and confirmation of certificates. To address this certificate administration issue, researchers [5] presented a new idea of an identity-based encryption (IBE) cryptosystem. This novel identity-based public key cryptographic (IB-PKC) model allows the client's secret key to be an element of his real identity, which is generated by a trusted outsider called a private key generator (PKG). In this way, a genuine public key does not require certificates [6]. However, the fact that PKG exclusively generates private keys for clients raises a security shortcoming known as a key escrow issue. With a specific end goal to tackle this mentioned issue, researchers in [7] presented a certificate-less (CL) cryptography scheme, generally denoted as CL-PKC.

Recall that WBAN is based on remote wireless sensors that can transmit only within short ranges, with low handling power and energy [7]. To address this short communication range issue of medical records to a longer distance, a smart intermediate mobile device (e.g., a cell phone, also named a controller) is used inside the WBAN's communication range (refer to Figure 1). Therefore, all cryptosystems with high computation cost to guarantee a high data security level are inappropriate. Hence various efficient authentication models other than the traditional PKI are presented in the literature [3,4,8–16,18,20]. Security insurance issues have started to draw escalated consideration among researchers and, lately, authors in [4] raised the shortcoming of an impersonation attack in a related scheme [8]. This security shortcoming resulted from saving the encryption and decryption keys on an unreliable AP database, and therefore introduced a novel secured authentication solution [4]. Furthermore, authors in [9] also proved that the existing cryptosystem [8] could not address the well-known stolen verifier–table attack. Thus, they proposed an authentication protocol based on elliptic curve cryptography (ECC) [9], notwithstanding that researchers in [10] proved that a related model [9] could not provide genuine anonymous data, while client's pseudo attributes could be utilized to track the corresponding clients. Therefore, an improved cryptosystem based on a user's identity was presented [10] to securely authenticate the different entities using bilinear pairing.

Due to the openness and mobility of WBAN, the transmission must be anonymous and unlinkable as well. In this way, authors in [11] designed a scheme that allowed sensor nodes appended in a patient's body to authenticate with a local server/hub node and establish a session key in an anonymous and unlinkable way. This scheme [11] was proposed to as efficient as possible, by using only two types of operations: the cryptographic hash function and the exclusive OR operation (XOR). Likewise, Aneesh and Deepthi [12] presented a hybrid anonymous authentication and key agreement scheme, which was an improvement based on Li et al.'s scheme [11] using the physiological signal to overcome the node impersonation issue [8]. In this proposed solution [12], authors provided additional security features to effectively address the node impersonation and key escrow issues [6,8]. Aneesh and Deepthi [12] highlighted some security shortcomings in Li et al.'s scheme [11] and used physiological signals to resolve them. This made the proposed scheme a hybrid scheme. Practically, the related schemes [11,12] security proofs used Burrows–Abadi–Needham (BAN) logic and the Automated

Validation of Internet Security Protocols and Applications (AVISPA). However, the use of physiological signals implies that all sensors nodes measure the same physiological signal and introduce additional costs for the collecting and transforming of data, as well as maintaining all sensors synchronized.

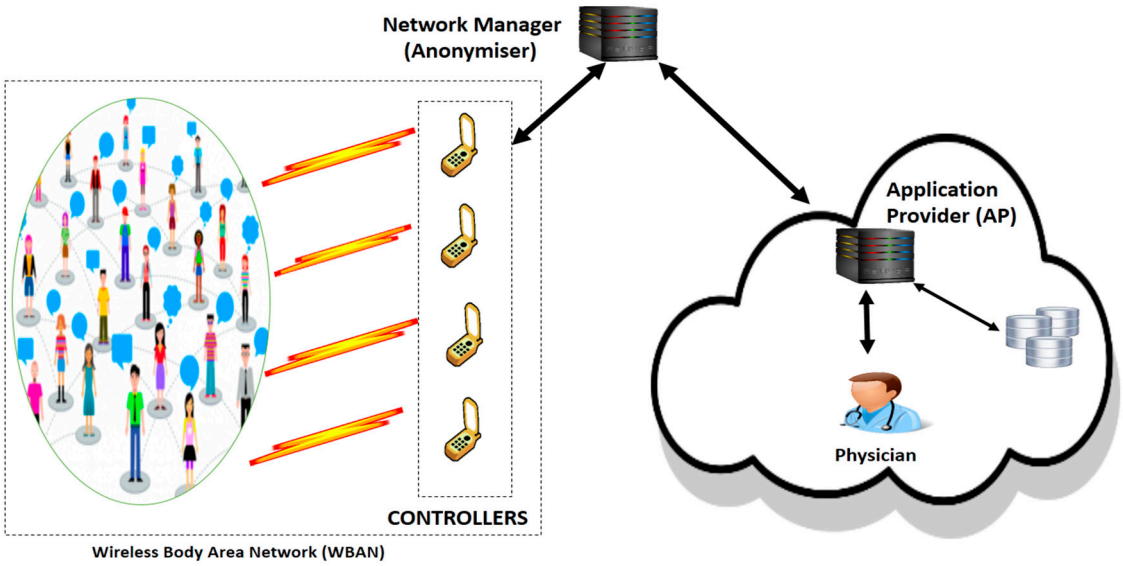

Figure 1. Proposed scenario.

Therefore, Marko et al.'s model [13] showed that the schemes [11,12] fell short of their goals, and, in fact, did not provide untraceability of the communicating sensor nodes. Based on that, the goal was to provide a solution [13] with anonymous participants without session linkability/ traceability. This new scheme achieved the untraceability property, while retaining computational complexity and reducing the communication costs. By achieving untraceability, the proposed solution could be a good candidate to improve Koya et al.'s scheme [12]. However, this scheme increased the required storage space. Furthermore, the security proof of the new scheme was discussed informally with some well-known attacks and was formally provided using the BAN logic, the AVISPA, and Scyther tool.

A new view of achieving user anonymity property has been introduced by using a Smartcard instead of traditional authentication scheme method to address the security and privacy issues in wireless multimedia sensor networks (WMSNs). Thereby, Ashok et al.'s [14] reviewed Li et al.'s scheme [11] and proved that their solution was still vulnerable to privileged-insider attack and sensor node capture attack, and failed to provide user anonymity properties. In order to address these security shortcomings found in Li et al.'s scheme [11], they proposed a secure biometrics-based user authentication scheme in WMSNs using a smartcard. This new scheme has been rigorously proven secure against possible known attacks and efficient in computation and communication as compared to Li et al.'s scheme [11]. As a further matter, a fresh approach has been tackled with the emergence of quantum computers to achieve the anonymity property. So far, most of the above-mentioned solutions are based on bilinear pairing and an elliptic curve cryptosystem. However, their security is based on the discrete logarithm on the elliptic curve, which has been proven to be limited by the development of quantum computers. To address the issue, Rui et al. [15] presented a new lightweight anonymous handover authentication (AHA) scheme based on the Number Theory Research Unit (NTRU) public key cryptosystem for wireless networks. Security analysis and experimental results showed that this scheme achieved mutual authentication with a greater security level to address known attacks. The advantages of the proposed scheme are the low computation cost, high efficiency, and ease of implementation as compared to related works like [11,12]. However, the disadvantage is that this scheme [15] cannot predict the misbehaving nodes and avoid the collusion attacks due to the lack of trust and reputation evaluation mechanism. Its correctness is only based on the certification results

of both parties. Therefore, this proposed solution [15] is only suitable for the scenario of a single authentication model with a few participants.

In this paper, our contribution will be first to identify and propose a certificate-less mutual authentication scheme that addresses the impersonation issue in the related works [8–10]. Second, we design a lightweight cryptographic algorithm using an effective combination of ECC and bilinear pairings operation for limited devices in WBAN. Furthermore, our proposed solution is more efficient than the existing works [8–10,15] by providing a batch authentication process that reduces considerably the computation and communication costs for constrained resource devices in WBAN.

The rest of this work is sectioned as follows. Section 2 presents the background work, while Section 3 gives the detailed design of the proposed solution. Section 4 analyzes and evaluates the performance and security level of the proposed contribution. Then, we end this work in Section 5.

2. Proposed Solution Construction

2.1. Preliminaries

2.1.1. Elliptic Curve Cryptography (ECC)

ECC is an asymmetric key encryption scheme based on elliptic curve theory that generates faster, smaller, and efficient cryptosystem keys. It was introduced by Koblitz [24] and Miller [25]. A fixed curve E over a field K can be described in a non-homogeneous manner by the following equation (Weierstrass equation) [26]:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$, and where Δ is the discriminant of E and is defined as follows:

$$\begin{cases} \Delta = -{d_2}^2 d_8 - 8{d_4}^3 - 27{d_6}^2 + 9d_2d_4d_6 \\ d_2 = {a_1}^2 + 4a_2;\ d_4 = 2a_4 + a_1a_3;\ d_6 = {a_3}^2 + 4a_6 \\ d_8 = {a_1}^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2{a_3}^2 - {a_4}^2 \end{cases} \quad (2)$$

Based on the literature review, ECC can provide a strong secured cryptosystem with a 164-bit key, while others cryptographic schemes require a 1024-bit key. Therefore, ECC is more appropriate to achieve the desired security level with the lowest computation power cost and device battery usage. Thus, it is a suitable and efficient solution for limited mobile device applications. The security advantage of ECC lies in its competitive short security key size and the strong assumption to solve the elliptic curve discrete logarithm problem (ECDLP).

2.1.2. Bilinear Pairings

Bilinear maps explained in [27] can be presented as follows: Let two cyclic groups E_1 (additive) and E_2 (multiplicative) of order p (prime number). Let g be a generator of E_1, and e a bilinear mapping; then,

e: $E_1 \times E_1 \rightarrow E_2$. The bilinear mapping e satisfies these properties:

- Bilinearity: $\forall$ A, B $\in E_1$, $\forall$ d, f $\in \mathbb{Z}_p^*$, $e(dA, fB) = e(A, B)^{df}$
- Non-Degeneracy: $\exists$ A, B $\in E_1$ such that e (A, B) $\neq 1$, and 1 is the identity element of E_2.
- Computation: For any A, B $\in E_1$, we have an efficient algorithm to compute e.

Recall that a group that has such a mapping e is defined as a bilinear group on which the Decisional Diffie–Hellman issue can be easily solved, while the Computational Diffie–Hellman (CDH) issue is considered very hard. Therefore, our proposed solution is based on the below security computational assumptions.

2.2. Security Assumption

We propose an efficient mutual batch authentication solution relying on strong security computation assumptions.

Problem 1: *Consider a multiplicative cyclic group G of order p, with generator g. A probabilistic polynomial–time adversary has a negligible chance to compute* g^{ab}, *from* g, g^a, g^b *for random* a, $b \in Z_p^*$.

Problem 2: *Elliptic curve discrete logarithm problem (ECDLP). Let E be elliptic curve over a finite field K. Suppose points* P, $Q \in E(K)$, *it is difficult to determine k such that* $Q = [k]P$, *with* $Q \in E(K)$.

Here, we propose an architecture that is depicted by Figure 1, which is comprised of the WBAN, the controller/client (C), the network manager (NM), and the application provider (AP). WBAN is a particular environment where a sensor is organized to work self-sufficiently by connecting to different medicinal sensors, situated inside and outside of a human body system. The sensors transmit medical information to a remote AP server via C. Therefore, in our proposed solution we focus on the mutual authentication between C and AP to guarantee data integrity and confidentiality. The main steps in this mutual authentication scheme, i.e., initialization, registration, and authentication between C and AP [4,7,28,29], are done via a reliable outsider NM as depicted in Figure 2. In this scenario, C and AP register with NM to get the different partial cryptographic keys. Thereby, NM assumes the duty of the key generator center (KGC). Contrary to related works in the literature, where NM is completely trustworthy, we assume in this paper that NM could be curious and dishonest. Therefore, C and AP register with NM to obtain not the full key but partial cryptographic key parameters for stronger data privacy protection. In order to address the various attacks (passive or active) [30], our scheme provides the following security requirements:

(i) Mutual authentication: It will ensure that exclusive genuine and approved C gets access privileges from AP and similarly just approved AP will receive and process data from C.
(ii) Anonymity: This prerequisite guarantees that an attacker does not have access to the genuine partaker's identity (C and AP) in their identification procedure.
(iii) Unlinkability: This condition guarantees that an attacker cannot interface C's identity to a particular session while asking for computations from AP.
(iv) Furthermore, our proposed solution provides resilience to replay and impersonation attack. Further, used keys cannot be recovered by an attacker, and our solution does not use verification table.

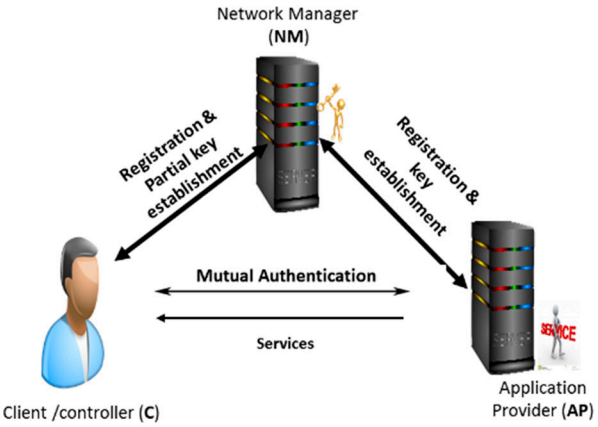

Figure 2. Mutual authentication overview.

Recall that the principal objective of this work is to design an efficient batch mutual certificate-less authentication scheme between C and AP that ascertains their identity in the communication process.

Thereby a passive attacker (eavesdropper) should have a slight chance to impersonate either C or AP. Further, by providing anonymity, we upgrade the client's privacy protection since the unlinkability property is guaranteed.

2.3. Related Work

Wang and Zhang proposed a new anonymous authentication scheme for WBAN [7] to overcome the security weaknesses of Zhao's model [9]. We can describe the different steps, i.e., Initialization, Registration, and Authentication phases of their model as follows.

- **Initialization phase:** It mainly consists of generating keys and system parameters and it is done by the NM shown below.

  (i) NM computes a large prime number q, two groups G_1, G_2, a pairing map $e : G_1 \times G_1 \rightarrow G_2$.
  (ii) NM selects two secured hashing maps h and H, where $h : \{0, 1\}* \rightarrow Zq$ and $H : \{0, 1\}* \rightarrow G_1$.
  (iii) NM generates randomly a number $s_{NM} \in Z_q$ as its secret key and compute $Q = s_{NM}P$ as its public key.
  (iv) Finally, NM provides as public parameters $params = \{q, G_1, G_2, e, P, h, H, Q_{NM}\}$.

- **Registration phase:** It is during this step that C and AP get registered with NM to get their different partial private key.

  (i) The entity C/AP transmits his identity ID_O to NM.
  (ii) With ID_O, NM computes the partial secret key $S_O = s_{NM}Q_O$, where $Q_O = H(ID_O)$. NM then sends secret key S_O to *O* through a secure channel.
  (iii) C/AP secretly stores its partial private key S_O.

- **Authentication phase:** At this phase *C*/AP mutually authenticates each other and computes secured keys to encrypt patient records as follows:

  (i) C generates a random number $r_C \in Z_q{}^*$, calculates $Q_{AP} = H(ID_{AP}), Q_C = H(ID_C)$, $R_C = r_C Q_C, K_C = e(S_C, r_C Q_{AP})$, and $Auth_C = E_{KC}(ID_C||T_C||R_C)$. With, T_C the current timestamp. Then, C sends a message $M_1 = \{R_C, T_C, Auth_C\}$ to AP.
  (ii) With $M_1 = \{R_C, T_C, Auth_C\}$, AP verifies the freshness of T_C and rejects if it is not fresh. AP computes $K_{AP} = e(S_{AP}, R_C)$ and gets $(ID_C||T_C||R_C)$ by decrypting $Auth_C$. Then AP compares if T_C and the decrypted one are equal. If not matching, AP cancels the access process. Else, AP computes randomly a number $r_{AP} \in Z_q{}^*$ and computes Q_C, Q_{AP}, $R_{AP} = r_{AP}Q_C$, $L_{AP} = r_{AP}R_C$ $Auth_{AP} = h(T_C||R_C||R_{AP}||K_{AP}||L_{AP})$ session key $sk_{AP} = h(T_C||R_C||T_{AP}||R_{AP}||L_{AP})$, where T_{AP} is the actual time stamp. Then, AP transfers message $M_2 = \{R_{AP}, T_{AP}, Auth_{AP}\}$ to C.
  (iii) Receiving M_2, C verifies the freshness of T_{AP}. If not, C stops the access demand. Otherwise, C computes $L_C = r_C R_{AP}$, and checks the correctness of the equation $Auth_{AP} = h(T_C||R_C||R_{AP}||K_{AP}||L_{AP})$. Then, C computes session key $Sk_C = h(T_C||R_C||T_{AP}||R_C||L_C)$, else the answer is rejected.

2.4. The Security Shortcoming

Based on the above description of Wang and Zhang's model (WZ) [7], a given AP can simulate a client ($K_C = K_{AB}$). Therefore, a malicious AP could impersonate C as following: the attacker picks $r_C \in_R Z_q{}^*$, sets $Q_C = H_1(ID_C)$, and computes $R_C = r_C Q_C$. Thereby the attacker can compute his/her own $K^*{}_{AB} = e(S_{AP}, R_C) = K_C$ and then generate a correct login $\{M_1 = R_C, Auth_C, T\}$,

and $Auth_C = h(T||K_C||R_C)$. This security weakness is due to the absence of an authenticator in the generated K_C. Therefore, the WZ solution presents a security shortcoming during the C/AP authentication process. To address this shortcoming, authors in [29] proposed an effective remote identity validation scheme. Based on their experiment results [29], this existing solution can provide a malignant insider security, as well as reduce running time of C by 51% when contrasted with Wang and Zhang's model [7]. However, those related works do not provide data aggregation and batch mutual identity validation processes to reinforce the data privacy protection.

3. Proposed Solution

Authentication issues related to patients in the e-Care system have begun to draw intense attention in the literature [31]. Therefore, we present in this section our contribution by designing a strong mutual certificate-less authentication scheme between C and AP. The Table 1 summarizes the different abbreviations used in this paper.

Table 1. Notations.

Symbols	Description
NM	Network manager
AP	Application provider
C	WBAN client/controller
q	Large prime number
G_1	Additive group with order q
H_i	Secure hash function with i = 1, 2
s_{NM}	Network manager private key
E/Fq	Elliptic curve over prime field
Fq	Prime field
e || f	Concatenation of strings *e* and *f*
P	Generator of group G
pid_{cj}	Client pseudo-ID, with j = 1, 2, 3
ID_{AP}	Application identity
PK_{NM}	Network manager public key

Our proposed solution satisfies the following security requirements to guarantee that an attacker cannot impersonate either AP or C and modifies the transmitted data (integrity of data and privacy of the client C assurance).

(1) Subscriber authentication: AP should confirm the various C's identity to guarantee their authenticity.
(2) Provider validation: A client C is permitted to verify the different AP's identity it visits to keep away from potential forgery and various malevolent attacks.
(3) Key generation: A different encryption key is generated each time C and AP initiate a session to ensure the protection of the transferred data.
(4) Anonymous Client: Apart NM, the client C is unknown and its operations are unlinkable to anybody including the AP.

3.1. Security System Settings

NM sets the entire system (sets parameters) and computes the partial secret keys by running the following steps based on elliptic curve E/Fq and random generator P for G_1 (cyclic additive group).

NM randomly selects a number $S_{NM} \in Z_q^*$ as master private key and calculates his related public key $PK_{NM} = S_{NM}P$.

Then, NM picks below hashing mappings:

$H_1 : \{0,1\}^l \times {G_1}^2 \rightarrow {Z_q}^*$, $H_2 : {G_1}^2 \times \{0,1\}^{2l} \rightarrow {Z_q}^*$, with l and k specifying identity's length and size in ${Z_q}^*$. NM publishes system public parameters $params = \{P_{NM}, H_1, H_2, P, E/Fq, G_1\}$

3.2. Registration Phase

We use data privacy preserving tools relying on pseudonyms. C usually has enough storage backup to handle a huge quantity of preloaded pseudonyms from NM. An effective work [32] addresses the data backup issue related to preload anonymous cryptosystem keys (pseudonyms). In this paper, the proposed scheme requires a pool of pseudonyms with short live times (based on expiry date), where the memory consumption is limited to the related work's results [32]. This approach is used by several existing models and has been proven efficient, especially for wireless environments.

The NM then provides a list of pseudonyms (pseudo identity/pseudo-ID) for C and generates partially the secret keys for both AP and C, respectively, like in [28] with some modifications in the registration phase.

3.2.1. The Client C Registration

C with its identity $ID_c \in \{0,1\}^l$ picks randomly $x_C \in {Z_q}^*$ as its secret value, computes its public key as $PK_C = x_C\, P$, then C transfers ID_c, PK_C to NM that first verifies the C's identity validity. If ID_c is genuine, then NM randomly picks a family of unlinkable pseudo-ID:

$PID_C = \{pid_{c1}, pid_{c2}, \ldots\}$ With a specified-lived valid period. Then NM generates a secret random number $r_c \in {Z_q}^*$, and computes $P_C = r_c P$.

For each pseudo-ID $pid_{cj} \in PID_C$, NM computes the secret value $S_C = (r_c + H_1\left(pid_{cj}, PK_C, P_C\right)S_{NM})$ mod q and sets C's partial private key as $S_{NM}.H_1(S_C)$. Then NM sends securely all the tuples ($S_{NM}.H_1(S_C)$, $P_C, S_C P$) back to C. Thereby C can ascertain the validation of its partial secret key by verifying if the equation $S_C P = P_C + H_1\left(pid_{cj}, PK_C, P_C\right)PK_{NM}$ holds for each $pid_{cj} \in PID_C$. Therefore, the full private key of C is generated and known by C only with the value equal to $(x_C, S_{NM}.H_1(S_C))$. Doing so, C can change its pseudo-ID $\left(pid_{cj}\right)$, in the valid time period to achieve identity privacy in mutual authentication process with AP.

3.2.2. Application Provider AP Registration

Similarly, AP and its identity $ID_{AP} \in \{0,1\}^l$ sets $x_{AP} \in {Z_q}^*$ as secret key, computes its public key as $PK_{AP} = x_{AP}\, P$, then transfers ID_{AP}, PK_{AP} to NM. Again, NM chooses random number $r_{AP} \in {Z_q}^*$, computes $P_{AP} = r_{AP}P$, $S_{AP} = (r_{AP} + H_1(ID_{AP}, PK_{AP}, P_{AP})S_{NM})$mod q.

Then NM sets as partial private key $S_{NM}.H_1(S_{AP})$ for AP and secretly (e.g., using a secure transmission protocol) sends ($S_{NM}.H_1(S_{AP})$, P_{AP}, $S_{AP}P$) to AP. In order to verify the correctness of S_{AP}, AP verifies if $S_{AP}P = P_{AP} + H_1(ID_{AP}, PK_{AP}, P_{AP})PK_{NM}$ holds and keeps this value. Likewise, AP sets its full private key as $(x_{AP}, S_{NM}.H_1(S_{AP}))$.

In the above registration process, NM appends Expire Date into each $pid_{cj} \in PID_C$. The validity of the partial private keys is then set before a specific date. Thus, the partial secret keys are automatically removed after that date, and fresh partial secret keys with new validity date are generated by NM. This key management approach securely can be given to C (even damaged, hacked, or stolen) without compromising seriously the system security. More, we avoid key and certificate management like in the traditional PKI environment and provide user revocation.

3.3. Authentication Phase

The focus here is to provide a secured mutual authentication scheme between C and AP that ascertains their identity to guarantee the physiological data's privacy during their communication process. Below are the different steps involved in this authentication process between C and AP depicted by the Figure 3:

(1). C picks a random unused pseudo-ID (pid_{cj}) and its corresponding partial private key $S_{NM}.H_1(S_C)$. Then C chooses randomly $\alpha \in {Z_q}^*$ and compute $U_C = x_C\, P$, and a session verifier $V_C = (U_C)^{\alpha}$.

(2). C computes $h_{C1} = H_1(U_C, ID_{AP}, PK_{AP})$, $h_{C2} = H_1\left(pid_{cj}, h_{C1}\right)$ and composes message $M_C = \left(pid_{cj}||h_{C2}||t_1\right)$.

(3). The client C computes a signature $\sigma_C = H_2(M_C).S_{NM}H_1(S_C)$ and sends a request message to AP: $Req = \{M_C, \sigma_C, V_C\}$ with Δt the valid transmission delay calculated by C.

(4). Upon receiving the request message (Req) at time t_2 from C, AP first verifies the expiry date in pid_{cj}. If the expiry date is valid, AP then checks the freshness of t_1 by verifying if $t_2 - t_1 \leq \Delta t$. If t_1 is fresh, AP with the public parameters params, verifies the validity of C's signature σ_C by checking if the Equation (3) holds.

$$e(\sigma_C, P) = e(H_2(M_C).H_1(S_C), PK_{NM}) \tag{3}$$

Verification:

$$\begin{aligned} e(\sigma_C, P) &= e(H_2(M_C).S_{NM}H_1(S_C), P) \\ &= e(H_2(M_C).H_1(S_C), S_{NM}P) \\ e(\sigma_C, P) &= e(H_2(M_C).H_1(S_C), PK_{NM}) \end{aligned}$$

(5). AP selects randomly $\beta \in Z_q^*$ and computes: $U_{AP} = x_{AP}P$, $V_{AP} = (U_{AP})^{\beta}$ (session verifier), and $L_{AP} = V_{AP}.V_C$.

(6). Then AP computes a private session key $PK_{AP-C} = e\left(L_{AP}.H_1(ID_{AP}), H_1\left(pid_{cj}\right)\right)$ and generates an authentication code $auth_1 = H_2\left(PK_{AP-C}\left|\left|pid_{cj}\right|\right|ID_{AP}\right)$ and sends $\{auth_1, V_{AP}, t_3, ID_{AP}, pid_{cj}\}$ to C.

(7). Upon receiving $\{auth_1, V_{AP}, t_3, ID_{AP}, pid_{cj}\}$ at t_4 from AP, the client C verifies the freshness of t_3 by checking if $t_4 - t_3 \leq \Delta' t$, with $\Delta' t$ the valid transmission delay calculated by AP. If t_3 is fresh, C computes $L_C = V_C.V_{AP}$, and a private symmetric session key with AP like: $PK_{C-AP} = e\left(L_C.H_1\left(pid_{cj}\right), H_1(ID_{AP})\right)$. Furthermore, C generates an authentication verification $auth_2 = H_2\left(PK_{C-AP}\left|\left|pid_{cj}\right|\right|ID_{AP}\right)$ code and compares with $auth_1$. If $auth_2 = auth_1$, then C can ascertain the identity of AP as legitimate; otherwise, C stops the communication process with AP and reports it to NM. In this scenario C can verifies if $auth_2 = auth_1$ if and only if $PK_{C-AP} = PK_{AP-C}$:

$$\begin{aligned} PK_{C-AP} &= e\left(L_C.H_1\left(pid_{cj}\right), H_1(ID_{AP})\right) \\ &= e\left(V_C.V_{AP}.H_1\left(pid_{cj}\right), H_1(ID_{AP})\right) \\ &= e\left(V_{AP}.V_C.H_1\left(pid_{cj}\right), H_1(ID_{AP})\right) \\ &= e\left(L_{AP}.H_1\left(pid_{cj}\right), H_1(ID_{AP})\right) \\ PK_{C-AP} &= PK_{AP-C} \end{aligned}$$

We thereby enable explicit mutual authentication between legitimate C and AP. Our proposed solution additionally empowers one-sided anonymous identity validation for C. Further, after successful authentication process, AP and C also can set secured symmetric cryptosystem for future data exchange process. Each data exchange session will be solely identified by (pid_{cj}, ID_{AP}).

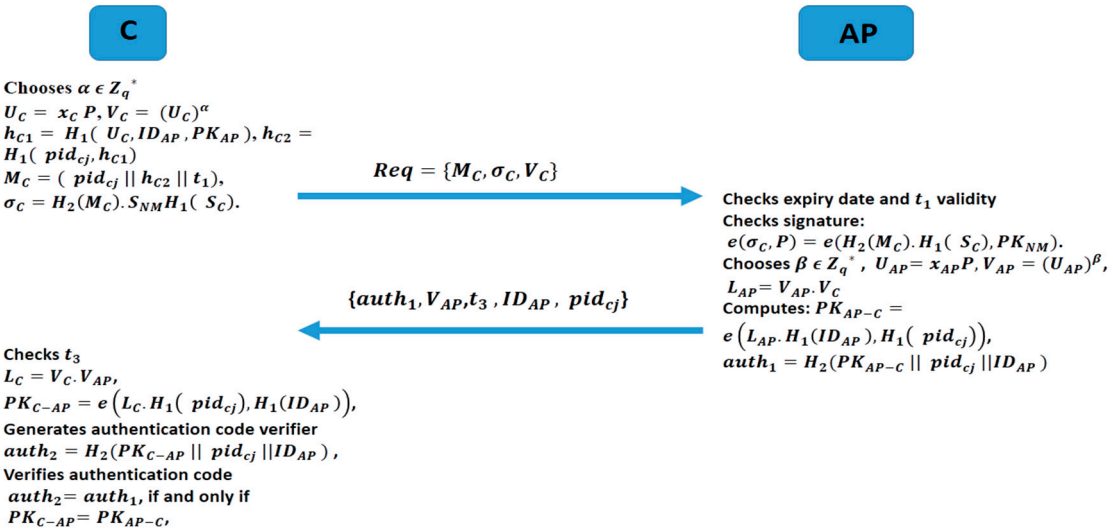

Figure 3. C and AP authentication process overview.

4. Security and Performance Analysis

4.1. Security Analysis

We tackle the proposed system security level to verify whether the requirements mentioned in subsection security assumption have been satisfied. We will show how our scheme provides secure mutual authentication between C and AP, anonymity for C, leaked key security, unlinkability, and impersonation attack. Moreover, aggregated values in our proposed solution hide the contained accumulated individual records, which empower individual C's data privacy protection. Recall the definition of the Decisional Bilinear Diffie–Hellman (DBDH) assumption in the random oracle model.

Definition (DBDH assumption): *The bilinear decisional Diffie–Hellman (*BDDH*) problem is defined in such a way that for known values* g, g^x, g^y, g^z *and unknown random values* x, y, z ∈ R Z_P, and T ∈ R, G_T, *it is considered difficult to set* $T = e(g, g)^{xyz}$ *from any random element in the target group. The (t, ϵ)–*BDDH *assumption is verified in G, if no t time algorithm has the probability of at least* $\frac{1}{2} + \epsilon$ *to solve the* BDDH *problem for non-negligible* ϵ.

- **Anonymity:** Each C gets a set of pseudo-identity $pid_{cj} \in PID_C$ and its related partial secret key $S_{NM}.H_1(S_C)$, uring registration process from NM. These pseudo-identities, rather than C's real identity, provide strong privacy protection. Not any involved entity, not even AP, can identify C or recollect different transactions launched by the same C except NM. In practice, C sends a random message request $Req = \{M_C, \sigma_C, V_C\}$ each time to AP. This message request contains secret values (x_C, α) and pseudo-ID pid_{cj} that are random (not constant) values each time that C initiates an authentication process with AP. Only C can compute $V_C = (U_C)^{\alpha}$ and $\sigma_C = H_2(M_C).S_{NM}H_1(S_C)$ since these values require both secret values (x_C, α) and partial private keys $S_{NM}H_1(S_C)$ for their calculation. Therefore, an attacker including NM, in order to compute V_C must solve the inherited CDH problem; that is, he should perform $U_C = x_C P$ and then $V_C = (U_C)^{\alpha}$ for unknown random secret values x_C, α which contradicts the CDH assumption. Therefore, C is anonymous and cannot be impersonated through our scheme. Therefore, our scheme guarantees data anonymity and identicalness (aggregated values) based on BDBH assumption in random oracle to resist chosen-plaintext attacks.
- **Mutual Authentication:** The client C's signature $\sigma_C = H_2(M_C).S_{NM}H_1(S_C)$ is in fact a signed based pseudo-identity. Therefore, it is impracticable to fake a genuine signature without prior access to the secret values $S_C = (r_c + H_1\left(pid_{cj}, PK_C, P_C\right)S_{NM})$ mod) and $U_C = x_C P$ due to the NP-hard calculation complexity of the Diffie–Hellman assumption in G_1. Thereby it is very hard

to deduce the partial private key $S_{NM}H_1(S_C)$ using pid_{cj}, and PK_{NM}. Similarly, an attacker with no prior knowledge of AP's partial private key $S_{NM}.H_1(S_{AP})$ and secret values $U_{AP} = x_{AP}P$ and β cannot make a legitimate authentication code $auth_1$. Further an adversary cannot compute $auth_2$ and verify the equation $auth_2 = auth_1$ since he cannot solve CDH (definition 1) as described in the section above. Furthermore, only legitimate C and AP can compute $L_C = L_{AP} = V_C.V_{AP}$, due to the randomness and secrecy of U_C and U_{AP} respectively. Therefore, a secured authentication process between C and AP is achieved by our scheme.

- **Unlinkability:** Recall that C uses different pseudo-identity $pid_{cj} \in PID_C$ during each authentication process with an AP. Furthermore, only NM is aware of the relation between a given pseudo-identity and its original C's identity. For that reason, excluding NM and C, no other entity is able to determine C or relate different authentication processes launched by the same C.
- **Leaked key security:** As described in Section 3, our scheme provides a random distinct session key each time an authentication process is initiated by C with AP. It is due to the randomness of the choice of secret values α, $\beta, x_{AP}, x_C \in Z_q^*$ by C and AP. Doing so, an attacker with a used key has a very slight chance to compromise succeeding sessions.
- **Impersonation attack:** To impersonate C or AP, an adversary should generate the correct values of $auth_1$ and $auth_2$, respectively, which is practically infeasible, as explained above (mutual authentication process section). Further an AP cannot generate a correct C's signature $\sigma_C = H_2(M_C).S_{NM}H_1(S_C)$ and V_C in the message request, since he cannot access S_C and x_C otherwise the attack can be detected by C in verifying $auth_1$. Likewise, an adversary that intercepts the message $M_C = \left(pid_{cj} ||h_{C2}||t_1\right)$ and tries to impersonate AP has a negligible chance of success due to the CDH assumption (mutual authentication process section) that is believed to be difficult. The performance analysis section highlights the security functional results comparison between our scheme and related works [7–9].
- **Data Aggregation:** Moreover, aggregated values in our proposed solution hide the accrued single value that enforces the privacy preservation of single C compared to related works [7–9]. To achieve this additional aggregated data feature, we designed a modified additively homomorphic IBE scheme from the Boneh–Franklin IBE cryptosystem [33]. The security proof lies on BDDH assumption in a random oracle (refer to security analysis section). This cryptosystem [33] is appropriate for our proposed solution (small sensing data reading) to achieve data aggregation and batch authentication. Our modified IBE scheme has four algorithms and we use G_1, G_2 of prime order q, P as generator of G_1, and a bilinear mapping e: $G_1 \times G_1 \rightarrow G_2$, such that $e\left(P^a, Q^b\right) = e(P, Q)^{ab}$, $\forall$ P, Q $\in G_1$, $\forall$ a, b $\in \mathbb{Z}_q^*$, and $e(P, Q) \neq 1_{G_2}$ whenever P, Q $\in G_1$.

Setup: NM randomly picks as master private key (msk) a number $S_{NM} \in Z_q^*$ and calculates its related public encryption key $PK_{NM} = S_{NM}P$. Then NM chooses a hash function defined as $H_1 : \{0,1\}^l \rightarrow G_1^*$, where the message space is $\mathcal{M} = \{0, \ldots, l-1\} \subseteq Z_q^*$ with $l = p(n) < q$ for some polynomial p and the cipher-text space is $C = G_1^* \times G_2$.

Extract (PK_{NM}, msk, pid_{ci}): NM computes and sets $k = P^{S_{NM}}$. Output $SK_{pid_{ci}} = H_1\left(pid_{ci}\right)^{S_{NM}}$ and k.

Enc (PK_{NM}, pid_{ci}, m). C randomly picks $b \in Z_q^*$; outputs $C_{mpid_{ci}} = \left(P^b, P^{-m}.e\left(H_1\left(pid_{ci}\right), k\right)^b\right)$.

Dec (PK_{NM},$SK_{pid_{ci}}$,$C_{mpid_{ci}}$). AP parses $C_{mpid_{ci}}$ as (c_1, c_2) and compute

$m^* = c_2/e\left(SK_{pid_{ci}}, c_1\right)$ and $m = \log_{\overline{P}} m^*$. The verification of our modified IBE lies on the fact that

$$\log_{\overline{P}}(m^*) = \log_{\overline{P}}\left(c_2/e\left(SK_{pid_{ci}}, c_1\right)\right)$$

$$\log_{\overline{P}}(m^*) = \log_{\overline{P}}\left(\frac{P^{-m}.e\left(H_1\left(pid_{ci}\right), k\right)^b}{e\left(H_1\left(pid_{ci}\right)^{S_{NM}}, P^b\right)}\right)$$

$$\log_{\overline{P}}(m^*) = \log_{\overline{P}}\left(\frac{P^{-m}.e\left(H_1(pid_{ci}), P^{S_{NM}}\right)^b}{e\left(H_1(pid_{ci})^{S_{NM}}, P^b\right)}\right) = m \tag{4}$$

We prove that our proposed homomorphic cryptosystem is additive in message space by multiplying cipher texts:

$$C_1 \times C_2 = (P^b \times P^{b'},\ P^{-m}.e\left(H_1(pid_{ci}), k\right)^b \times P^{-m'}.e\left(H_1(pid_{ci}), k\right)^b)$$

$$C_1 \times C_2 = (P^{b+b'},\ P^{-m+m'}.e\left(H_1(pid_{ci}), k\right)^{b+b'})$$

$$C_1 \times C_2 = Enc\left(PK_{NM}, pid_{ci}, m + m' \bmod q\right)$$

Note that the two disadvantages that come along with our modified additively homomorphic IBE scheme (i.e., the limited messages backup capacity and computing a discrete logarithm function to decrypt the data) are acceptable in many practical areas and especially in the e-Care system. Therefore, it does not affect the performance of our proposed solution. Table 2 shows clearly that our scheme is a good candidate to address the security shortcomings in the related works [7–9,29].

Table 2. Security comparison analysis.

Scheme	Wang and Zhang [7]	Liu [8]	Zhao [9]	Omala, A.A. et al. [29]	Our Scheme
Data aggregation	×	×	×	×	√
Mutual authentication	√	√	√	√	√
Anonymity	√	√	×	√	√
Impersonation attack	×	√	√	√	√
Unlinkability	√	×	√	√	√
Leaked key security	√	√	√	√	√
Batch authentication	×	×	×	×	√

4.2. Performance Analysis

We describe our proposed solution performance analysis in comparison with related works [7–9]. First our scheme provides batch authentication between different client C and AP, which reduces efficiently the communication and computation cost. Upon receiving a gain access demand from C, AP checks the message's signature authenticity in order to ascertain its related C (as described in Section 3). Further our scheme provides batch authentication, i.e., an AP can verify at the same time different message requests from various Cs securely through the help of NM. Thus, each C_i sends its message requests $\{M_{Ci}, \sigma_{Ci}, V_{Ci}\}$ to NM, which collects and forwards them as aggregated data to AP. Therefore upon receiving n distinct message requests denoted $\{M_{C1}, \sigma_{C1}, V_{C1}\}, \{M_{C2}, \sigma_{C2}, V_{C2}\}, \{M_{C3}, \sigma_{C3}, V_{C3}\}, \ldots, \{M_{Cn}, \sigma_{Cn}, V_{Cn}\}$, respectively, from n different C_i denoted as $C_1, C_2, C_3, \ldots, C_n$, with their respective signature $\sigma_{C1}, \sigma_{C2}, \sigma_{C3}, \ldots, \sigma_{Cn}$, AP checks the correctness of this equation:

$$e\left(\sum_{i=1}^{n} \sigma_{Ci}, P\right) \stackrel{?}{=} e\left(\sum_{i=1}^{n} H_2(M_{Ci}).H_1(S_{Ci}), PK_{NM}\right). \tag{5}$$

Verification

$$e\left(\sum_{i=1}^{n} \sigma_{Ci}, P\right) = e\left(\sum_{i=1}^{n} H_2(M_{Ci}).S_{NM}H_1(S_{Ci}), P\right)$$

$$e\left(\sum_{i=1}^{n} \sigma_{Ci}, P\right) = e\left(\sum_{i=1}^{n} H_2(M_{Ci}).H_1(S_{Ci}), S_{NM}P\right)$$

$$e\left(\sum_{i=1}^{n}\sigma_{Ci}, P\right) = e\left(\sum_{i=1}^{n}H_2(M_{Ci}).H_1(S_{Ci}), PK_{NM}\right)$$

This data aggregation support in our model at the NM side has significant practical advantages for sensor networks. It facilitates efficiently keeping down the communicating cost between C and AP and empowers the privacy protection of a single C_i. Our proposed solution keeps down the number of transmitted data by sending one aggregated assessment (almost the size of a single report) instead of distinct individual message requests. Furthermore, this data aggregation feature hides the accrued single value, which enforces the privacy preservation of a single C compared to related works [7–9], and [29].

Note that the two disadvantages that come along with our modified additively homomorphic IBE scheme (i.e., the limited messages backup capacity and computing a discrete logarithm function to decrypt the data) are acceptable in many practical areas and especially in the e-Care system. Therefore, it does not affect the performance of our proposed solution (see Functioning Evaluation section). Based on this data aggregation and batch authentication support, the computing cost that AP needs to validate n signatures is largely composed of n point multiplications and two pairing calculations. Thus, the required time for AP to authenticate a large number of signatures from distinct C is obviously brought down. Therefore, it reduces the transmission loss proportion imputable to a possible bottleneck of digital signature authentication at the AP side. Recall that this batch verification operation has great merit for a limited power environment like WBAN.

For efficiency purposes, the multiprecision integer and rational arithmetic cryptographic library (MIRACL) [34] and cost-efficient pairing based cryptography (PBC) libraries are implemented into our proposed solution's experiments to yield a 1024-bit security level. Experimental platforms are PCs with different computational power: Pentium(R) Dual-Core E6700 CPU 3.20 GHz, 4 GB RAM and 64-bit Intel®, 624 MHz processor, and 128MB memory to simulate AP and C, respectively. In the experiment, G_1 and G_2 are depicted by 160, 161, and 960 bits, respectively, and pid_{cj}, Timestamp, and ID_{AP} by 32 bits. A Miyaji-Nakabayashi-Takano (MNT) curve is implemented with 160 bits, $k = 6$, depicting the order and embed degree, respectively, in $Z_q{}^*$. The performance evaluation is done based on related work experimental conclusions [8] depicted in Table 3. We focus on computations with expensive calculation costs, like modular exponentiation (TSM), ECSM (TSM), Hashing to point in G_1 (TGH) and bilinear pairing (TP) operations. Therefore, a computing time-based comparison study is done with the exiting related models as shown in Table 4.

Table 3. Cryptography running time operation based on results in [8].

	AP (ms)	**C (ms)**
TME	13.21	63.51
TSM	6.38	30.67
TP	20.04	96.35
THG	3.04	14.62

Table 4. Functioning Evaluation (Execution Time).

Schemes	**AP (ms)**	**C (ms)**
Wang and Zhang [7]	$2TSM + 1TP \approx 32.80$	$3TSM + 1Tp \approx 188.36$
Liu [8]	$1TME + 1TSM + 1Tpq \approx 39.63$	$1TME + 4TSM \approx 186.19$
Zhao [9]	$6TSM \approx 38.28$	$3TSM \approx 92.01$
Our Scheme	$\mathbf{1TSM + 2TP \approx 46.46}$	$\mathbf{1TSM + 1Tp \approx 127.02}$

Note that the computation cost for AP and C is one point multiplication for both two and one pairing calculations, respectively. Recall that the computing cost for a pairing function is much more expensive than a multiplication calculation. The client C may be a limited device; this low computation cost is a significant advantage for our scheme compared to the related work [7].

Based on Table 4 analysis, we can highlight our scheme efficiency on the obvious reduction of computation and communication costs for verifying n different signatures (batch authentication) from multiple clients by AP that consists of n point multiplications and two pairing calculations only. We also reduce the computation cost of C, which is a limited resource device in comparison to Wang and Zhang's Model. This result is a desirable attribute for constrained power environments like WBAN.

5. Conclusions

This work presents a novel batch mutual authentication cryptosystem between WBAN's controller/client C and an application provider AP. This proposed solution empowers the cryptosystem security level by providing batch authentication and data aggregation supports. We keep low the data transmission and computing over heads of C and AP using a lightweight ECC and efficient cryptographic pairing tools. Additionally, our solution needs only two handshakes between C and AP, without key certificate management like in the original asymmetric cryptography environment (PKI). Furthermore, our scheme efficiently provides an additive homomorphic IBE operation, in which a given AP can compute securely aggregated values from various WBAN clients. Our scheme reinforces privacy protection and reduces the running time on the client side. This is a great benefit for limited devices in environments like WBAN. However, we will improve the performance and security level by designing in our future work, a lightweight additive homomorphic IBE scheme with auxiliary input to address the side-channel attacks at the end user's side.

Author Contributions: Conceptualization, M.K.; Methodology, M.K.; Software, M.K.; Validation, M.K., and W.W.; Formal Analysis, M.K.; Investigation, M.K.; Resources, M.K., and W.W.; Data Curation, M.K.; Writing—Original Draft Preparation, M.K.; Writing—Review & Editing, M.K., and W.W.; Visualization, M.K., and W.W.; Supervision, W.W.; Project Administration, W.W.; Funding Acquisition, W.W.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bourouis, A.; Feham, M.; Bouchachia, A. Ubiquitous mobile health monitoring system for elderly (UMHMSE). *arXiv* **2011**, arXiv:1107.3695. [CrossRef]
2. Latre, B.; Braem, B.; Moerman, I.; Blondia, C.; Demeester, P. A survey on wireless body area networks. *Wirel. Netw.* **2011**, *17*, 1–18. [CrossRef]
3. Wang, D.; He, D.; Wang, P.; Chu, C.H. Anonymous two- factor authentication in distributed systems: Certain goals are beyond attainment. *IEEE Trans.* **2015**, *12*, 428–442. [CrossRef]
4. He, D.; Zeadally, S.; Kumar, N.; Lee, J.H. Anonymous authentication for wireless body area networks with provable security. *IEEE Syst. J.* **2016**, *99*, 1–12. [CrossRef]
5. Shamir, A. Advances in cryptology. In *Proceedings of the CRYPTO 84, Chap. Identity-Based Cryptosystems and Signature Schemes*; Springer: Berlin, Germany, 1985; pp. 47–53. [CrossRef]
6. Li, F.; Zheng, Z.; Jin, C. Secure and efficient data transmission in the internet of things. *Telecommun. Syst.* **2016**, *62*, 111–122. [CrossRef]
7. Wang, C.; Zhang, Y. New authentication scheme for wireless body area networks using the bilinear pairing. *J. Med. Syst.* **2015**, *39*, 1–8. [CrossRef] [PubMed]
8. Liu, J.; Zhang, Z.; Chen, X.; Kwak, K.S. Certificate-less remote anonymous authentication schemes for wireless body area networks. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 332–342. [CrossRef]
9. Zhao, Z. An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. *J. Med. Syst.* **2014**, *38*, 1–7. [CrossRef] [PubMed]
10. Abi-Char, P.E.; Mhamed, A.; El-Hassan, B. A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications. In Proceedings of the International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST 2007), Cardiff, UK, 12–14 September 2007; pp. 235–240. [CrossRef]

11. Li, X.; Hamada Ibrahim, M.; Kumari, S.; Kumar Sangaiah, A.; Gupta, V.; Raymond Choo, K. Anonymous Mutual Authentication and Key Agreement Scheme for Wearable Sensors in Wireless Body Area Networks. *Comput. Netw.* **2017**, *129*, 429–443. [CrossRef]
12. Koya, A.; Deepthi, P.P. Anonymous hybrid mutual authentication and key agreement scheme for wireless body area network. *Comput. Netw.* **2018**, *140*, 138–151. [CrossRef]
13. Kompara, M.; Islam, S.K.H.; Hölbl, M. A Robust and Efficient Mutual Authentication and Key Agreement Scheme with Untraceability for WBANs. *Comput. Netw.* **2018**, *148*, 196–213. [CrossRef]
14. Das, A.K.; Kumar, S.A.; Odelu, V.; Goswami, A. A Secure Smartcard-Based Anonymous User Authentication Scheme for Healthcare Applications Using Wireless Medical Sensor Networks. *Wirel. Pers. Commun.* **2017**, *94*, 1899–1933. [CrossRef]
15. Chen, R.; Peng, D. A Novel NTRU-Based Handover Authentication Scheme for Wireless Networks. *IEEE Commun. Lett.* **2017**, *22*, 586–589. [CrossRef]
16. Jiang, C.; Li, B.; Xu, H. An efficient scheme for user authentication in wireless sensor networks. In Proceedings of the 21st International Conference on Advanced Information Networking and Applications Workshops, Niagara Falls, ON, Canada, 21–23 May 2007; pp. 438–442. [CrossRef]
17. Li, F.; Han, Y.; Jin, C. Practical access control for sensor networks in the context of the internet of things. *Comput. Commun.* **2016**, *89*, 154–164. [CrossRef]
18. Xiong, H. Cost-effective scalable and anonymous certificate-less remote authentication protocol. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 23–39. [CrossRef]
19. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. A survey on sensor networks. *IEEE Commun. Mag.* **2002**, *40*, 102–114. [CrossRef]
20. Cherukuri, S.; Venkatasubramanian, K.K.; Gupta, S.K.S. Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In Proceedings of the International Conference on Parallel Processing Workshops, Kaohsiung, Taiwan, 6–9 October 2003; pp. 432–439. [CrossRef]
21. Aydos, M.; Sunar, B.; Koc, C.K. An elliptic curve cryptography based authentication and key agreement protocol for wireless communication. In Proceedings of the Second International Workshop on Discrete Algorithm and Methods for Model Computation and Communication, Dallas, TX, USA, 30 October 1998.
22. Al-Riyami, S.S.; Paterson, K.G. Advances in Cryptology. In Proceedings of the ASIACRYPT 2003: 9th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, 30 November–4 December 2003; pp. 452–473. [CrossRef]
23. Kim, S.J.; Chung, J.Y. Eeg encryption scheme with junk data using chaos maps. In Proceedings of the 6th International Conference on Intelligent Systems, Modelling and Simulation, Kuala Lumpur, Malaysia, 9–11 February 2015; pp. 132–134. [CrossRef]
24. Koblitz, N. Elliptic curve cryptosystems. *Math. Comput.* **1987**, *48*, 203–209. [CrossRef]
25. Miller, V.S. Use of Elliptic Curves in Cryptography. In *Advances in Cryptology—CRYPTO '85 Proceedings. CRYPTO 1985*; Lecture Notes in Computer Science, 218; Williams, H.C., Ed.; Springer: Berlin/Heidelberg, Germany, 1985.
26. Hankerson, D.; Menezes, A.J.; Vanstone, S. *Guide to Elliptic Curve Cryptography*; Springer: Berlin/Heidelberg, Germany, 2006.
27. Dong, C. Jpair: A Quick Introduction. Available online: https://personal.cis.strath.ac.uk/changyu.dong/jpair/intro.html (accessed on 20 June 2010).
28. Islam, S.H. Design and analysis of an improved smartcard-based remote user password authentication scheme. *Int. J. Commun. Syst.* **2016**, *29*, 1708–1719. [CrossRef]
29. Omala, A.A.; Kibiwott, K.P.; Li, F. An Efficient Remote Authentication Scheme for Wireless Body Area Network. *J. Med. Syst.* **2016**, *41*, 1–9. [CrossRef] [PubMed]
30. Dolev, D.; Yao, A.C. On the security of public key protocols. In Proceedings of the 22nd Annual Symposium on Foundations of Computer Science (sfcs 1981), Nashville, TN, USA, 28–30 October 1981; pp. 350–357. [CrossRef]
31. Dimitrakakis, C.; Gkoulalas-Divanis, A.; Mitrokotsa, A.; Verykios, S.V.; Saygin, Y. *Privacy and Security Issues in Data Mining and Machine Learning*; Springer-Verlag: Berlin/Heidelberg, Germany; Barcelona, Spain, 2010.
32. Raya, M.; Hubaux, J.-P. Securing vehicular ad hoc networks. *J. Comput. Secur.* **2007**, *15*, 39–68. [CrossRef]

33. Boneh, D.; Franklin, M.K. Identity-Based Encryption from the Weil Pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, CA, USA, 19–23 August 2001; pp. 213–229.
34. Scott, M. *Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL)*; Shamus Software Ltd. Available online: http://urlm.co/www.shamus.ie (accessed on 16 November 2018).