IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Productive Get to Control Conspire with Certificate less Signcryption for Remote Body Zone Systems

[1]Dr. R. Bagavathi Lakshmi,[2] PN Shiammalaame,[3]MKrithika,[4]S. Jayashree

[1]Associate Professor,[2]Assistant Professor,[3]Assistant Professor, [4]Assistant Professor
[1]Department of Information Technology,
[1]VELS Institute of Science Technology and Advanced Studies(VISTAS), Chennai.

Abstract: Remote body range systems (WBANs) can collect clients' imperative information on body parameters and environment parameters using little wearable or implantable sensors. To guarantee the security of crucial information, a productive get-to-control conspire with certificate less encryption (CLSC) is planned. The rightness of the plot is demonstrated by scientific calculation. It too indicates that the plot offers secrecy and enforceability within the irregular or-acle show on the premise of the hardness of the Computational Diffie-Hellman (CDH) issue and Discrete Logarithm (DL) issue individually. Compared with the existing three get-to-control plans utilizing encryption, the Conspire can fulfill more security properties and has the most limited computational time and the slightest vitality utilization for the controller..
Keywords: Access Control; Certificate less; Signcryption; Wireless Body Area Networks.

I. INTRODUCTION

Wireless body area networks (WBANs) can acquire the human body's vital signals through a network of intelligent and low-power micro-and nano-sensors and actuators. These sensors for collecting timely data can be placed on the body or implanted in the human body (or even in the bloodstream). In addition to saving lives, WBANs are prevalent in reducing healthcare costs by removing the costly in-hospital monitoring of patients. In IEEE 802.15.6 [13], WBAN applications are classified into two types: medical and non-medical applications. In the study, we focus on the technological requirements of medical WBANs.

Security and privacy are two important considerations in WBANs. Since the patient-related data in the WBANs plays a critical role in medical diagnosis and treatment, it is necessary to ensure the security of these data in such a way that only authorized users can access these data [4, 18, 19]. Another aspect that should be considered in WBANs is the limitation of the controller's sources, especially storage space and computational- ability. To protect data privacy and reduce the energy consumption of computation and communication, lightweight access control schemes are needed. The certificates public key cryptography (CL-PKC) [5] does not require the use of a certificate which brings the burden of certificate management, and CL-PKC avoids the key escrow problem because the user's private key is not generated by himself but by the user and the key generation center (KGC). Signcryption [3], as a cryptographic technique, can provide both the functions of public key-encryption and digital signature in a logically single step at a significantly lower cost compared to traditional signature-then-encryption methods. A signcryption scheme can achieve confidentiality, authentication, integrity, and non-repudiation simultaneously at a lower cost. Therefore, we design an efficient access control with certificateless encryption (CLSC) to protect the data privacy of WBANs while reducing the computational overhead and storage overhead of resource-constrained controllers. Many certificateless cryptosystems [1, 9, 10], such as certificateless encryption schemes, certificates encryption schemes, and certificates access control schemes were proposed.

Access control is an important part of the defense for the security of network systems, which protects data security and user privacy through only authorized users who can access the WBANs. Some important progress has been made in the access control for the WBANs. In2011, Cagalaban and Kim [2] proposed a novel efficient access control scheme for the WBANs based on identity-based encryption (IBSC) [12] (hereafter called CK). The encryption method adopted in the CK scheme can simultaneously authenticate the users and protect the request messages. The scheme effectively solves the problem of a single point of failure in the traditional public-key infrastructure-supported system (PKI) by providing key generation and key management services without any sumption of the pre-fixed trust relationship between network devices. However, CK has the key escrow problem since it is based on the IBSC. In 2016, Li and Hong [8] demonstrated an efficient certificateless access control scheme for the WBANs by using certificateless encryption (CLSC) with public verifiability and ciphertext authenticity (hereafter called LH). The scheme can solve the key escrow problem and avoid the use of public key certificates. The controller could verify the validity of a ciphertext before decryption. Then Li et al. [7] proposed a novel certificate-less encryption scheme and designed a cost-effective and anonymous access control scheme for the WBANs with the novel encryption (hereafter called LHJ). They re-reported that the proposed access control scheme achieved various securities and

had the least computational cost and total energy consumption of the controller. However, the above two schemes may not be good choices since they require some costly bilinear pairing operations. The computational cost of a bilinear pairing operation is approximately twenty times higher than that of scale multi-plication [6]. These costly operations are a heavy burden for resource-limited sensor nodes.

In this paper, we proposed an efficient access control scheme with certificateless signcryption for WBANs.The main contributions are:

1. A CLSC scheme without using a bilinear pairing operation is proposed, and an efficient access control scheme for WBANs is constructed. The use of CL-PKC eliminates the burden of certificate management and solves the key escrow problem.
2. The correctness of the CLSC scheme is verified from the aspects of the partial key, the ciphertext, and the signature.
3. It is formally proved that the scheme is semantically secure against indistinguishability-certificate less signcryption adaptive chosen ciphertext attacks(IND-CLSC-CCA2) based on the hardness of the Computational Diffie-Hellman (CDH) problem and existential enforceabilitycertificateless signcryption-chosen message attack (EUF-CLSC-CMA) based on the hardness of the Discrete Logarithm (DL) problem.
4. The security attributes of the scheme are analyzed.
5. Compared with three other access control schemes utilizing encryption, the scheme is characterized bythe lowest computational cost and energy consumption for the controller.

2. Preliminary

In this section, we present some mathematical assumptions, the security model, and the network model.

2.1 Computational Assumptions

Definition 1. Computational Diffie-Hellman (CDH). Given a 3-tuple (p, aP, bP) for two unknown elements, b Zq∗, here G is a group with prime order q and P is a generator of G, the CDH problem is to compute the value abP from aP and bP. The advantage of any probabilistic polynomial time algorithm A in solving the CDH problem in G is defined as AdvCDH = Pr[A(p, aP, bP) =abP |a, b ∈Zq∗]. The CDH assumption is that the advantage AdvCDH is negligibly small for any probabilistic poly-nominal time algorithm A.

Definition 2. Discrete Logarithm (DL). Given a 2-tuple (P, μP) for an unknown element μ Zq∗, here G is a group with prime order q and P is a generator of G, the DL problem is to find the value μ. The advantage of any probabilistic polynomial time algorithm A in solving the DL problem in Zq∗ is defined as AdvDL = Pr[A(P, μP) =|μ ∈ Zq∗]. The DL assumption is that the advantageAAdvDL is negligibly small for any probabilistic polynomial time algorithm A.

2.2 Security Model

All CLSC schemes may be subjected to two types of attacks [20]: Type-I adversary A1 and Type-II adversary A2.

Type-I adversary: The adversary A1 is not accessible to the master key, but he can replace public keys at his will. Therefore, the adversary A1 is also called malicioususer.

Type-II adversary: Adversary A2 is accessible to the master key, but it cannot replace the user's public keys. It represents a malicious KGC that generates partial private keys of users.

Definitio 3. Confidentiality. A certificateless signcryption scheme is semantically secure against indistinguishability-certificateless signcryption-adaptive chosen ciphertext attacks (IND-CLSC-CCA2) if there is not a probabilistic polynomial time adversary Ai(i=1,2) that has the non-negligible advantage in winning the game [20].

Definition 4. Unforgeability. A certificate sign- encryption scheme is semantically secure against existing- trial unforgeability-certificateless signcryption-chosen message attack (EUF-CLSC-CMA) if there is not a probabilistic polynomial time adversary Ai(i=1,2) with the non-negligible advantage in winning the game [20].

2.3 Network Model

The IEEE 802.15.6 working group has considered WBANs to operate in a one-hop or two-hop star topology. The node being placed in a location like the waist is the center of the star topology and controls the communication in WBANs [13]. Here we consider the one-hop star topology and all nodes in the WBANs are directly connected to the controller which all nodes talk. The WBANs contain some sensor nodes and a controller. Sensor nodes in, on, or around the body collect vital signals of the patient and regularly transfer them to the corresponding controller. The controller aggregates information from the sensor nodes and communicates with the Internet. Figure 1 shows the overview of the network model of our WBANs applications. The framework is mainly composed of three entities: a Server Provider (SP), the WBANs of a patient, and a user (e.g. a physician, a researcher, or an emergency). The SP deploys the WBANs and is re- responsible for the registration both of users and patients. The SP plays the role of KGC in the CLCS scheme and produces the partial key for any entity that registers at the SP. We suppose that the SP is honest. However, in practice, we do not need to fully trust the SP since it only knows the partial private key of the entity.

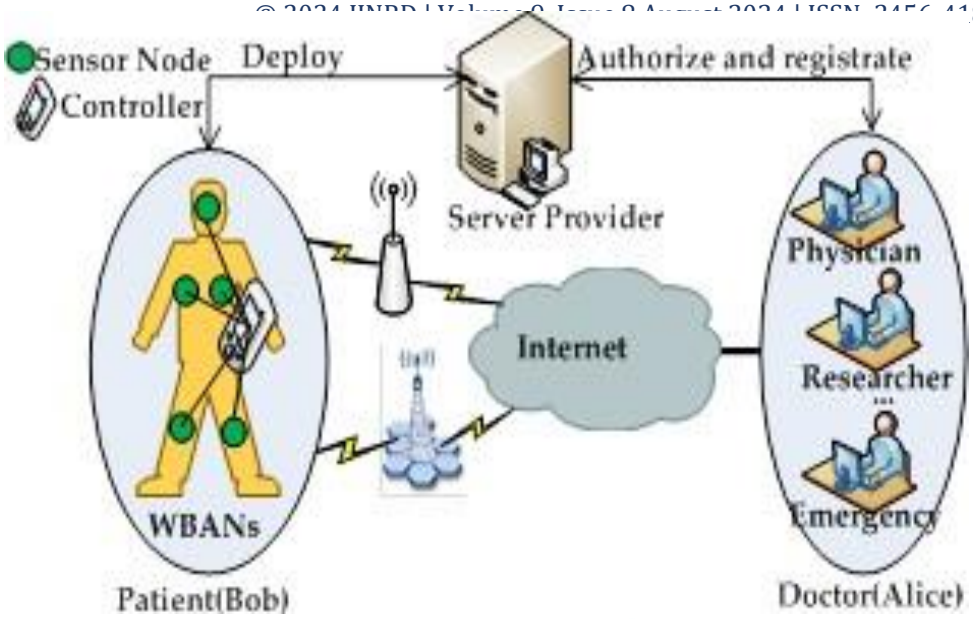


Figure 1: Network model of our WBANs applications

Here's a practical example. We assume that a patient Bob is hospitalized and the SP has deployed the WBANs of Bob. Bob's private key was generated when he registered at the SP. Sensor nodes in WBANs collect profile and medical records and transfer them to the controller. Doctor Alice has registered at the SP, and the SP has allocated expired data for Alice. When Alice needs to access the data of Bob, she first sends an access request message to Bob. Then Bob checks whether Alice has the access privilege to his medical data. If Alice is authorized, Alice communicates with Bob to get the vital sign data to provide better medical care service. Otherwise, Bob refuses the access request.

3.1 Our Access Control Scheme

In this section, with the proposed CLSC scheme, we de- sign an efficient access control scheme with certificate- less signcryption for the WBANs. The scheme has four phases: the initialization phase, the registration phase, the authentication and authorization phase, and the re- vocation phase. We define ED as an expiration date. The access control scheme is summarized in Figure 2.

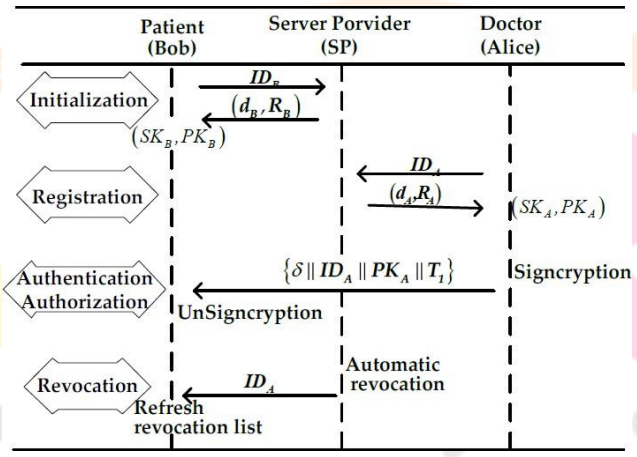


Figure 2: Certificateless access control scheme

3.1.1 Initialization Phase

During this phase, the Service Provider (SP) executes the Setup algorithm to deploy Wireless Body Area Networks (WBANs) and generate system parameters. Patient Bob, identified as IDB, receives his/her public key PKB = (XB, RB) and private key SKB = (xB, dB). Notably, all of Bob's communications with the Internet are managed by the WBANs' controller, to whom Bob also refers. The SP may execute both the Setup algorithm and the PartialKeyGen algorithm.

3.1.2 Registration Phase

Doctor Alice can access patient Bob's data only if she is a registered user with the Service Provider (SP). Alice submits her identity IDA to the SP, which verifies its validity. If the identity is valid, the SP sets an expiration date ED and executes the PartialKeyGen algorithm to generate a partial private key (dA, RA). Once Alice receives (dA, RA), she uses the KeyGen algorithm to obtain her full private key SKA = (dA, xA) and full public key PKA = (RA, XA).

3.1.3 Authentication and Authorization Phase

When Doctor Alice, identified by IDA, needs to access the monitoring data from the Wireless Body Area Networks (WBANs), she begins by generating a request message m and applies the Sign algorithm to create a ciphertext δ = (s, C, T). To prevent replay attacks, Alice concatenates the request message with a timestamp to form a new signed and encrypted message.

Alice then sends the concatenated message {δ || IDA || PKA || T1} to Bob, where T1 represents the current timestamp. Upon receiving Alice's access request, Bob checks if T2 - T1 < ΔT holds true, where T2 is the current timestamp. If this condition is not satisfied, Bob terminates the session. Otherwise, Bob uses the Unsign algorithm to decrypt and verify the message.

If the result of the Unsign algorithm is empty, Bob rejects the request. Otherwise, the request is deemed valid, and Alice and Bob can communicate using the session key established between them, denoted as H3(VA) or H3(VB). This session key ensures secure communication between Alice and Bob during their interaction.

3.1.4 Revocation

Access privileges are automatically revoked upon reaching the expiration date ED. For instance, if ED is set to "2017-12-31", users can only access the WBANs before December 31, 2017. After this date, the Service Provider (SP) revokes Alice's partial private key and partial public key, rendering her access unauthorized.

In cases where access privileges need to be revoked before the expiration date for specific reasons, the SP submits Alice's identity to Bob. Bob maintains a list of revoked identities to verify the validity of users. Upon receiving Alice's identity, Bob adds a record to his revocation list, thereby categorizing Alice as an unauthorized user. This ensures that Alice's access is terminated promptly, even before the designated expiration date.

4. Efficiency Comparisons

In this section, we analyze the performance of our access control scheme in regard to energy consumption and communication overhead. Firstly, we compare the scheme with other three schemes of CK [2], LH [8] and LHJ [7] in computation efficiency and communication efficiency. The computation efficiency is determined by the computational cost of algorithm and the communication efficiency is determined by the length of ciphertext and public key. The symbol P denotes pairing operation, the symbol Edenotes and exponentiation operation, the symbol M de- notes a point multiplication operation. Let |∗| denote thelength of element . For example, G denotes the lengthof element in group G and m denotes the length of message space. As can be seen from Table 2, our scheme has the lower computational cost than the other three schemesforbothAliceandBob.Here,weneglectthecostofother operations because they are much smaller than the above three operations.

Table1:Comparisons of security properties

	CK[2]	LH[8]	LHJ[7]	Ourscheme
Confidentiality	√	√	√	√
Unforgeability	√	√	√	√
Authentication	√	√	√	√
Non-repudiation	√	√	√	√
Nocertificate		√	√	√
Nokeyescrow	×			√
Withoutbilinearpairing	×	×	×	

Abbreviations: √ :Schemepreventsthisattackorsatisfiestheattribute,
×:Schemefailstopreventtheattackordoesnotsatisfytheattribute.

Table2: Performance valuation of the four schemes

Schemes	ComputationalCost(Alice)	ComputationalCost(Bob)	CommunicationCost(Bob)
CK[2]	1P+3M	3P+M	$2\|G_1\|+\|ID\|+\|m\|$
LH[8]	2E	1P+1M+1E	$\|G_1\|+\|G_2\|+3\|Z_p^*\|+\|ID\|+\|m\|$
LHJ[7]	1E+4M	2P+2M+1E	$3\|G_1\|+\|ID\|+\|m\|$
Ours	3M	4M	$5\|Z_q^*\|+\|ID\|+\|m\|$

Here's a rewritten version of the quantitative evaluation results for the four schemes, focusing on Bob's overhead:

The evaluation is based on the MICA2 mote, which utilizes an ATmega128 8-bit processor operating at 7.3728 MHz, with 128KB ROM and 4KB RAM. The cryptographic operations are performed using a super singular curve \(E \) (F2271) with an embedding degree of 4 and implementing a ηT pairing, ensuring an 80-bit security level.

Computational Time:

- CK [2] Scheme: 6.51 seconds
- LH [8] Scheme: 3.61 seconds
- LHJ [7] Scheme: 6.32 seconds
- Our Scheme: 3.24 seconds

These times are calculated based on specific operations:

- Pairing operation: 1.9 seconds

- Exponentiation operation: 0.9 seconds
- Point multiplication: 0.81 seconds

The formulas used to calculate the computational time for each scheme are detailed in the original text.

Energy Consumption:

Assuming a power level of 3.0 V for the MICA2 mote:

- Pairing operation consumes 45.6 mJ
- Point multiplication consumes 19.44 mJ
- Exponentiation operation in G2 consumes 21.6 mJ

Energy consumption on the controller of each scheme:

- CK [2] Scheme: 156.24 mJ
- LH [8] Scheme: 86.64 mJ
- LHJ [7] Scheme: 151.68 mJ
- Our Scheme: 77.76 mJ

These calculations are based on the number of operations and their respective energy costs, as specified in the original analysis.

This evaluation provides a comparative view of the computational time and energy consumption for each cryptographic scheme on the specified platform.

Figure 3 and Figure 4 respectively describe the computational time and energy consumption of the controller. It is clear that our scheme has the shortest computational time and least energy consumption among the four schemes.

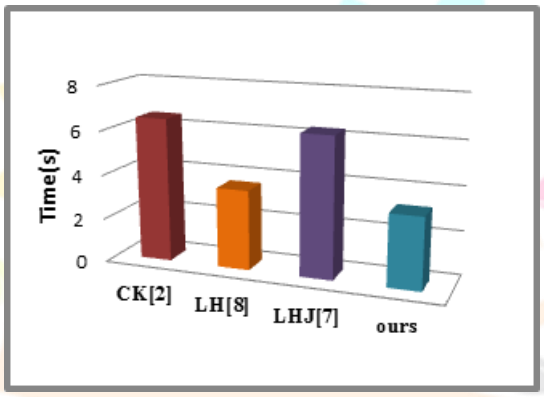


Figure 3: The computational time of the controller

Schemes	Computationalenergy consumption(mJ)	Communicationenergy consumption(mJ)	Totalenergy consumption(mJ)
CK[2]	156.24	1.86	158.1
LH[8]	86.64	5.62	92.26
LHJ[7]	151.68	2.51	154.19
Ours	77.76	3.61	81.37

Table3:Energy consumption of the four schemes

Here's a rewritten version of the energy consumption analysis for the four schemes, focusing on both computation and communication costs:

The MICA2 mote consumes 0.019 mJ to receive a one-byte message. Based on this, the communication energy consumption values for each scheme are calculated as follows:

- CK [2] Scheme: $0.019 \times 98 = 1.86$ mJ
- LH [8] Scheme: $0.019 \times 296 = 5.62$ mJ
- LHJ [7] Scheme: $0.019 \times 132 = 2.51$ mJ
- Our Scheme: $0.019 \times 190 = 3.61$ mJ

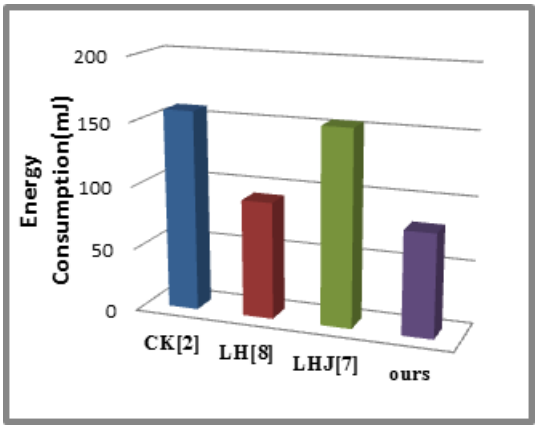
The total energy consumption for each scheme, combining computational and communication costs, is summarized below:

- CK [2] Scheme: $156.24 + 1.86 = 158.1$ mJ
- LH [8] Scheme: $86.64 + 5.62 = 92.26$ mJ
- LHJ [7] Scheme: $151.68 + 2.51 = 154.19$ mJ
- Our Scheme: $77.76 + 3.61 = 81.37$ mJ

Comparing these totals, it's noted that while the communication cost of our scheme is higher than that of CK [2] and LHJ [7], the overall energy consumption of our scheme is lower than the other three schemes. Specifically, the combined energy consumption of computation and communication in our scheme is almost half that of CK [2] and LHJ [7].

This analysis is essential for evaluating the efficiency of each cryptographic scheme on the limited-resource platform of the MICA2 mote.

Figure4:Theenergyconsumptionofthecontroller



5 Conclusions

In our paper, we introduced a novel CLSC scheme that does not rely on bilinear pairing operations. This scheme was specifically designed for efficient access control in Wireless Body Area Networks (WBANs). We rigorously verified the mathematical correctness of our CLSC scheme, focusing on the partial key generation, ciphertext construction, and signature processes.

Furthermore, we provided formal proofs demonstrating that our proposed scheme achieves confidentiality and enforceability within the random oracle model. These proofs were grounded in the computational hardness of the Computational Diffie-Hellman (CDH) problem and the Discrete Logarithm (DL) problem, respectively.

Security analysis revealed that our scheme satisfies a broader range of security properties compared to three existing access control schemes employing signcryption. Specifically, we highlighted superior performance metrics in terms of computational efficiency and energy consumption. Our access control scheme demonstrated the shortest computational time and the least energy consumption among the compared schemes.

Overall, our paper contributes a novel CLSC scheme tailored for WBANs, offering robust security properties and efficient performance characteristics.

References

[1] S. K. Balakrishnan and V. P. Jagathy Raj, “Practical implementation of a secure email system using cer- tificateless cryptography and domain name system”, International Journal of Network Security, vol. 18, no. 1, pp. 99-107, 2016.

[2] G. Cagalaban and S. Kim, “Towards a secure patient information access control in ubiquitous healthcare systems using identity-based signcryption”, in Pro- ceedings of 13th International Conference on Adv. Commun. Technol. (ICACT’11), pp. 863-867, 2011.

[3] L. Cheng and Q. Wen, “An improved certificateless signcryption in the standard model”, International Journal of Network Security, vol. 17, no. 5, pp. 597- 606, 2015.

[4] G.Gao, X. Peng, Y. Tian and Z. Qin, “A chaotic maps-based authentication scheme for wireless body area networks”, International Journal of Distributed Sensor Networks, vol. 12, no. 7, pp. 2174720-2174720, 2016.

[5] M. Hassouna, B. Barry, and E. Bashier, “A new level 3 trust hierarchal certificateless public key cryptog- raphy scheme in the random oracle model”, Interna- tional Journal of Network Security, vol. 19, no. 4, pp. 551-558, 2017.

[6] D. He, J. Chen, and J. Hu, “An ID-based proxy sig- nature schemes without bilinear pairings”, Annals of Telecommunications, vol. 66, no. 11-12, pp. 657-662, 2011.

[7] F. Li, Y. Han, and C. Jin, “Cost-effective and anony- mous access control for wireless body area networks”,IEEE Systems Journal, vol.12, no. 1, pp. 747-758, 2018.

[8] F. Li and J. Hong, “Efficient certificateless access control for wireless body area networks”, IEEE Sen- sors Journal, vol. 16, no. 13, pp. 5389-5396, 2016.

[9] F. Li, J. Hong, and A. A. Omala, “Efficient cer- tificateless access control for industrial Internet of things”, Future Generation Computer Systems, vol. 76, pp.285-292, 2017.

[10] M. Luo, Y. Wan, and D. Huang, “Certificateless hybrid signcryption scheme with known session- specific temporary information security”, Interna- tional Journal of Network Security, vol. 19, no. 6, pp. 966-972, 2017.

[11] C. Ma, K. Xue, and P. Hong, “Distributed access control with adaptive privacy preserving property for wireless sensor networks”, Security and Communica- tion Networks, vol. 7, no. 4, pp. 759-773, 2014.

[12] M. Mandal, G. Sharma, and A. K. Verma, “A computational review of identity-based signcryption schemes”, International Journal of Network Security, vol. 18, no. 5, pp. 969-977, 2016.

[13] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, “Wireless body area networks: a survey”, IEEE Communication Surveys & Trtorials, vol. 16, no. 3, pp. 1658-1686, 2014.

[14] L. B. Oliveira, D. F. Aranha, et al., “TinyPBC: Pair- ings for authenticated identity-based non-interactive key distribution in sensor networks”, Computer Communications, vol. 34, no. 3, pp. 485-493, 2011.

[15] Z. Shao, Y. Gao, “A provably secure signature scheme based on factoring and discrete logarithms”, Applied Mathematics & Information Sciences, vol. 8, no. 4, pp. 1553-1558, 2014.