An efficient authentication and key agreement scheme for e-health applications in the context of Internet of Things

Hamza Khemissa, Djamel Tandjaoui, Samia Bouzefrane

An efficient authentication and key agreement scheme for e-health applications in the context of Internet of Things

Hamza Khemissa, Djamel Tandjaoui, Samia Bouzefrane

An efficient authentication and key agreement scheme for e-health applications in the context of internet of things

Hamza Khemissa*

LSI Laboratory,
USTHB: University of Sciences and Technology Houari Boumediene,
Algiers, Algeria
and
Computer Security Division,
CERIST: Research Center on Scientific and Technical Information,
Algiers, Algeria
Email: h.khemissa@usthb.dz
Email: hkhemissa@cerist.dz
*Corresponding author

Djamel Tandjaoui

Computer Security Division,
CERIST: Research Center on Scientific and Technical Information,
Algiers, Algeria
Email: dtandjaoui@cerist.dz

Samia Bouzefrane

CEDRIC Laboratory,
CNAM: National Conservatory of Arts and Crafts,
Paris, France
Email: samia.bouzefrane@lecnam.net

Abstract: E-health applications are one of the most promising applications in the context of internet of things (IoT). Nevertheless, resource constraints and security issues in IoT are the main barriers for their deployment. Among security issues, authentication and data confidentiality are required to secure e-health applications. In this paper, we propose a new authentication and key agreement scheme for e-health applications in the context of IoT. This scheme allows a sensor node, a gateway node, and a remote user to authenticate each other and secure the collection of health-related data. The proposed scheme is based on lightweight symmetric cryptography since it uses nonces, exclusive-or operations, and simple hash functions. Besides, it takes into consideration the sensors location to provide an efficient authentication. To assess the proposed scheme, we conduct a theoretical and an automated security analysis using AVISPA tool. The results show that our scheme preserves the security properties, and ensures resilience against different types of attacks. In addition, we evaluate

and compare both communication and computational costs with some existing authentication schemes. The obtained results prove that it provides authentication with low energy cost.

Keywords: internet of things; IoT; e-health; identity; location; authentication; session key agreement.

Reference to this paper should be made as follows: Khemissa, H., Tandjaoui, D. and Bouzefrane, S. (xxxx) 'An efficient authentication and key agreement scheme for e-health applications in the context of internet of things', *Int. J. Information and Computer Security*, Vol. x, No. x, pp.xxx–xxx.

Biographical notes: Hamza Khemissa is a PhD student at the University of Sciences and Technology Houari Boumediene (USTHB), and research member of Computer Security Division at the Research Center on Scientific and Technical Information (CERIST) in Algiers, Algeria. He obtained his Master's in Networks and Distributed Systems in 2013 and graduation in Computer Science in 2011 from the same university. His current research activities are focused on security, identity management, and authentication in the context of internet of things.

Djamel Tandjaoui is a researcher at the Research Center on Scientific and Technical Information (CERIST). He received his PhD from the University of Sciences and Technology Houari Boumediene (USTHB) in 2005. He obtained his Master's in Computer Science from the same university. His research interest includes mobile networks, sensor networks, and security.

Samia Bouzefrane is an Associate Professor and has accreditation to conduct research (HDR) at the Conservatoire National des Arts et Metiers (CNAM) of Paris. She received her PhD in Computer Science from the University of Poitiers (France) in 1998. After four years at the University of Le Havre (France), she joined in 2002 the CEDRIC Lab of CNAM. She is the co-author of many books (*Operating Systems, Smart Cards, and Identity Management Systems*). Her current research areas cover security in cloud computing and internet of things, resource allocation in cloud computing, and new paradigms for networking such as NFV and NDN.

1 Introduction

Nowadays, internet of things (IoT) is considered as one of the main communication progress in the area of wireless communications. This novel paradigm allows the interaction of heterogeneous objects such as sensors, radio-frequency identification (RFID) tags, mobile phones, etc. to reach common goals (Atzori et al., 2010; Sicari et al., 2015). In the IoT, each object has a locatable, addressable, and readable counterpart on the internet. Thus, it can be connected to other objects and to different networks.

IoT makes possible the development of a huge number of applications that can be grouped into four domains: transportation and logistics domain, healthcare domain, smart environment domain, and personal and social domain (Atzori et al., 2010). E-health applications are one of actual and effective applications in the healthcare domain. An e-health application aims generally to monitor patients, and to anticipate emergency

situations by a fast and an efficient healthcare intervention (Patel and Wang, 2010). However, the low capabilities in both energy and computing resources make difficult the implementation of complex security schemes. Also, IoT is extremely vulnerable to several attacks since most communications are wireless which cause eavesdropping (Atzori et al., 2010). In order to reach the goal of such applications, security issues should be taken seriously.

Among security issues in the IoT, Authentication is an important concept that should be addressed efficiently since it allows the identity verification of each connected object (Sicari et al., 2015). Nevertheless, the implementation of an authentication scheme must be tailored to the constrained environment of IoT. In an e-health application, an authentication scheme aims to avoid any wrong health data transmission by a malicious node. Indeed, any modification in the transmitted data could lead to a disaster, since it could engender wrong medical prescription or delay an emergency intervention. Therefore, identity authentication of the connected objects should be addressed efficiently on e-health applications (Li et al., 2010).

Location of connected objects is an important aspect since IoT supports mobility. Checking location is to know the position of an object. Thus, we verify if an object can begin a local or remote communication (Roman et al., 2013; Al-Fuqaha et al., 2015). There are several proposals for managing the location of objects in IoT (Atzori et al., 2010; Roman et al., 2013; Al-Fuqaha et al., 2015). In this work, we take into consideration the location of communicating objects in the authentication scheme. To our knowledge, there are no prior works that consider this aspect during the authentication phase.

According to Xue et al. (2013), there are five models of authentication for wireless sensor networks (WSNs), and each model achieves authentication through four messages. In only one of the five models, the user initiates the authentication scheme by directly contacting the concerned object. In our proposed e-health network, we use this authentication model when developing the proposed authentication scheme, but it is the sensor node who initiates the authentication scheme (see Figure 1).

In the literature, different authentication schemes have been proposed for the IoT environment. The common challenges of these research works were energy cost and security (Sicari et al., 2015). Authentication schemes based on public key cryptography (PKC) have been proposed in Kothmayr et al. (2013) and Porambage et al. (2014b, 2014a). As a result of the analysis of these protocols, we notice that they have a high level of security. Nevertheless, the high energy consumption is their main weakness. In order to save energy, Das and Goswami (2013), Turkanović et al. (2014), Amin et al. (2015), Farash et al. (2016) and Gope and Hwang (2016) proposed certificateless authentication schemes based on symmetric cryptography.

Inspired by the energy saving of the certificateless authentication schemes, we propose in this paper an efficient authentication and key agreement scheme for e-health applications in the context of IoT. For this purpose, we:

- choose a secure method to protect the sensor identity from disclosure and impersonate attacks.
- design a new authentication and key agreement scheme using nonces, hash functions, and the location of involved sensors.
- demonstrate that the proposed scheme saves energy and offers a high level of security.

To assess the proposed scheme, we conduct a theoretical security analysis that is validated with an automated analysis using AVISPA (http://www.avispa-project.org) tool. The obtained results show that the scheme protects the sensor node identity from disclosure, ensures the integrity of exchanges, and offers a high security level against several attacks. Furthermore, we study both communication and computational costs, we estimate the energy cost on sensor nodes, and we compare with recent authentication schemes. The results show that using the aforementioned security mechanisms, the proposed scheme provides authentication and key agreement with a low energy cost.

The remainder of the paper is organised as follows. In Section 2, we briefly introduce e-health applications in the context of IoT. Section 3 presents a state of the art on authentication in the context of IoT. In Section 4, we present in details the network and authentication model, and the proposed authentication scheme. Then, we carry out an analysis of the proposed scheme both in terms of security and performance in Section 5. Finally, Section 6 and Section 7 conclude the paper.

2 E-health applications in the context of IoT

E-health applications are one of important IoT supported applications (Atzori et al., 2010). An e-health system is a radio frequency-based wireless networking technology. It is built by different objects with some more computational and energy capabilities, such as contextual and wearable sensors planted in, on, or around a human body, a network gateway node, etc. Thus, it often aims to collect health-related data and then achieve a personal healthcare (Dohr et al., 2010).

To secure an e-health application, we have to consider the main security problems and challenges of the IoT. The most important issues, applications, and researches in the IoT have been identified in Medaglia and Serbanati (2010), Roman et al. (2011) and Miorandi et al. (2012). Based on these studies, object authentication is considered as an important aspect that must be implemented to maintain a secure communication. To collect sensitive health-related data from sensor nodes, we have to create a secure communication channel through an authentication scheme adaptable to the vulnerabilities and the scarcity of both power and computation resources of the IoT environment.

3 Related work

In the recent years, the research community has focused its attention on security aspect in different IoT applications. Indeed, it is considered as an important challenge to overcome. Due to the limitation of both energy and computation resources in the IoT, classic security protocols cannot be applied. Thus, several research works aim to propose new lightweight security protocols for constrained environments. In our discussion of related work, we present and discuss several proposed authentication and key agreement schemes in the context of IoT.

Authentication of objects is a critical security issue in several IoT applications. Indeed, authentication ensures the validity of each communication party identity (Sicari et al., 2015). IoT offers mobility to connected objects to reach application goals (e.g., healthcare applications, etc.). Thus, we distinguish two cases of authentication namely: remote and local authentication.

Traditional authentication schemes usually interact with centralised authentication servers and identity providers to achieve authentication (El Maliki and Seigneur, 2007; Mangle and Patel, 2014). Consequently, such schemes require certain energy, storage, and computation capabilities which is unsuitable for IoT. Nowadays, many research works aim to propose tailored and new lightweight authentication and key agreement schemes for IoT. Several research works on authentication in the context of IoT are cited in Atzori et al. (2010) and Sicari et al. (2015). Recent proposed authentication schemes can be divided into two classes namely.

3.1 Authentication with certification

In this class of schemes, authentication is achieved using digital certificates such as each object must have its digital certificate. Among these schemes, datagram transport layer security (DTLS) (Rescorla and Modadugu, 2012) authentication handshake has been proposed for the IoT (Kothmayr et al., 2013). It provides a secure authentication between objects. Furthermore, the scheme can be deployed in both of remote and local authentication cases. However, its main weakness is the high energy cost caused by the use of asymmetric encryption-based RSA and the PKI certificates exchanges in the authentication phase. For this reason, elliptic curve cryptography (ECC) has raised as an interesting approach compared to RSA-based algorithms. Indeed, it offers the same level of security with less key size and energy cost (Szczechowiak et al., 2008).

In order to reduce the energy consumption of the authentication process, Porambage et al. (2014b, 2014a) have proposed an authentication scheme using ECC-based implicit certificate (SEC4, 2013) for WSNs in distributed IoT applications. This scheme achieves authentication and key agreement with less energy cost and computation overhead. In addition, it can be deployed in both of remote and local authentication cases.

3.2 Certificateless authentication

This class of schemes is based on cryptographic operations such as exclusive-or operation (XOR), and symmetric cryptography. Also, certificateless authentication schemes do not use digital certificate for authentication. Hence, this class of authentication schemes saves energy.

In Xue et al. (2013) have proposed a lightweight temporal credential-based mutual authentication and key agreement scheme for WSNs. It uses only hash functions, concatenation and XOR operations. Unfortunately, Wang and Wang (2014) demonstrated that the scheme cannot ensure user anonymity and untraceability. Also, Jiang et al. (2015) observe that Xue et al. (2013) scheme is vulnerable to identity guessing attack, tracking attack, privileged insider attack and weak stolen smart card attack. In order to fix the mentioned drawbacks, they proposed an efficient two-factor user authentication scheme with unlinkability for WSNs. However, their scheme is vulnerable to denial of service (DoS) attacks.

In 2014, Das (2016) analyses Jiang et al.'s (2015) scheme and shows its several drawbacks. In order to withstand the weakness found in Jiang et al. (2015) scheme, he proposed a three-factor user authentication scheme for WSNs. This scheme is efficient as compared to Jiang et al.'s (2015).

In Das (2015) has proposed a secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed WSNs. This scheme uses only concatenation and XOR operations, hash functions, and symmetric key encryption and decryption operations. The security analysis demonstrates that the scheme is secure against passive and active adversaries. Nevertheless, the scheme is also vulnerable to DoS attacks.

Turkanović et al. (2014) have proposed a user authentication and key agreement scheme based on the IoT notion for heterogeneous ad hoc WSNs. Also, it uses only hash functions, concatenation and XOR operations between a user, a gateway, and a sensor node. In 2015, Farash et al. (2016) reviewed the previous proposed scheme and show its security weakness. Then, they proposed a new and efficient user authentication and key agreement scheme. The security analysis of this scheme by BAN-logic and AVISPA tools confirm that it ensures the security properties.

In the same year, Amin et al. (2015) have proposed a remote user mutual authentication and session key agreement scheme for e-health care systems. This scheme uses only cryptographic operations between a user and a medical server. Authors reviewed Das and Goswami (2013) scheme and demonstrated the security weakness of the scheme against several security attacks such as user anonymity problem, user impersonation attack, server impersonation attack, and session key disclosure attack. Hence, their work overcame the mentioned security problems by preserving the anonymity of the remote patient.

Khemissa and Tandjaoui (2015) have proposed a new lightweight authentication scheme for e-health applications in the context of IoT. The scheme introduces a new method to securely send messages in the authentication phase between two objects. In 2016, they proposed a remote authentication scheme for heterogeneous WSNs in Khemissa and Tandjaoui (2016). In both schemes, analyses prove that the proposed schemes can be classified as lightweight due to their low energy cost.

In Tewari and Gupta (2016) have proposed an ultralightweight authentication protocol that uses only bitwise operations for IoT devices using RFID tags. The security of this scheme has been compared with other ultralightweight authentication schemes, which shows its resistance against several possible attacks. However, Safkhani and Bagheri (2016) have studied this authentication protocol, and showed that it does not provide a resistance against different attacks. The authors presented an efficient passive attack that retrieves all secret parameters of the tag by only eavesdropping a session of protocol between the target tag and the legitimate reader. In addition, the attack has a negligible computational complexity and can be executed in a very short-time.

Sood (2016) have proposed a dynamic identity-based authentication protocol using smart card. They propose an improvement of the scheme proposed by Hsiang and Shih (2009), and prove that it is secure against all well known security attacks with a low computational cost.

Gope and Hwang (2016) have proposed a lightweight anonymous authentication protocol for securing real-time application data access in WSNs, such as healthcare applications. The authors showed that their protocol provides different security features with a high security level. Nevertheless, the sensor identity is not protected during the authentication process. The performance analysis shows that the proposed scheme has low costs of communication and computation, and that is suitable for resource constrained environments.

In Shen et al. (2018), proposed an efficient multilayer authentication protocol and a secure session key generation method for wireless body area networks (WBANs). They design a one-to-many group authentication protocol and a group key establishment

algorithm between personal digital assistance (PDA) and each of sensor nodes. The proposed certificateless authentication protocol using ECC algorithm. The security and performance analysis shows that it provides a high security level with low computational cost.

In Gope et al. (2017) have proposed a lightweight RFID-based authentication scheme for distributed IoT applications. The scheme is based on lightweight cryptography. The analysis shows that it is suitable for smart city and resource constrained environments. The scheme provides forward secrecy, anonymity and untraceability of RFID-tag, and secure localisation. Furthermore, it has a reasonable execution time compared to existing schemes.

Wu et al. (2017) have proposed a robust and lightweight authentication scheme for wireless medical sensor networks (WMSNs). The tool proverif Blanchet and Smyth (2011) is employed to validate the security of proposed scheme against different attacks. In addition, the analysis and the comparison of the scheme show that is suitable for personalised healthcare systems (PHSs).

Recently, Ali et al. (2017) proposed a new remote user authentication scheme using WSNs for agriculture monitoring. The scheme is validated through Burrows-Abadi-Needham (BAN) logic, and simulated using AVISPA tool. The security analysis shows that the proposed scheme is secure and resists different possible attacks. Thus, their proposed scheme is applicable in a real life application.

Our proposed scheme introduces a new way to achieve authentication using nonces, XORs, and simple hash functions. Moreover, it takes into consideration the sensors location to provide an efficient authentication. In the next section, we present in detail our proposed scheme that aims to provide mutual authentication and key establishment between the sensor node and the remote user to maintain a secure channel. Then, we prove through a detailed analysis that the proposed scheme achieves authentication with a high level of security and low energy cost.

4 The proposed scheme

This section presents the proposed authentication and key agreement scheme for e-health applications in the context of IoT. Firstly, we describe the network architecture of the e-health application and some assumptions. Secondly, we define the notations used throughout the paper. Finally, we present the functioning of the proposed scheme in details.

4.1 Network architecture

The network architecture is mainly composed of: the patient side and the caregiver side (see Figure 1). The most appropriate e-health scenario is the case of a patient who has one or more critical illnesses, such as health-related data are collected from sensors and transmitted to the caregiver. The latter sends the right medical prescriptions to the patient.

- *The patient side*

  The mobile and contextual sensors, and the gateway node are in the patient side.

  1 *Mobile and contextual sensor nodes*: the sensors are planted in, on, or around a patient body to collect health-related data (e.g., electrocardiogram sensor, blood glucose level, body temperature level, etc.).

2 *The gateway node*: the gateway node is used to gather and process data from each sensor node, send commands to the sensor network, facilitate authentication schemes, etc. (Ozdemir and Xiao, 2009). In addition, it plays the role of a trusted third party in the mutual authentication and key agreement process (Xue et al., 2013). The gateway node is supposed as a trusted device. It can be in a fixed position such as, an asymetric digital subscriber line (ADSL) box, etc. Also, it might be played by the personal smartphone of the patient in case of mobility.

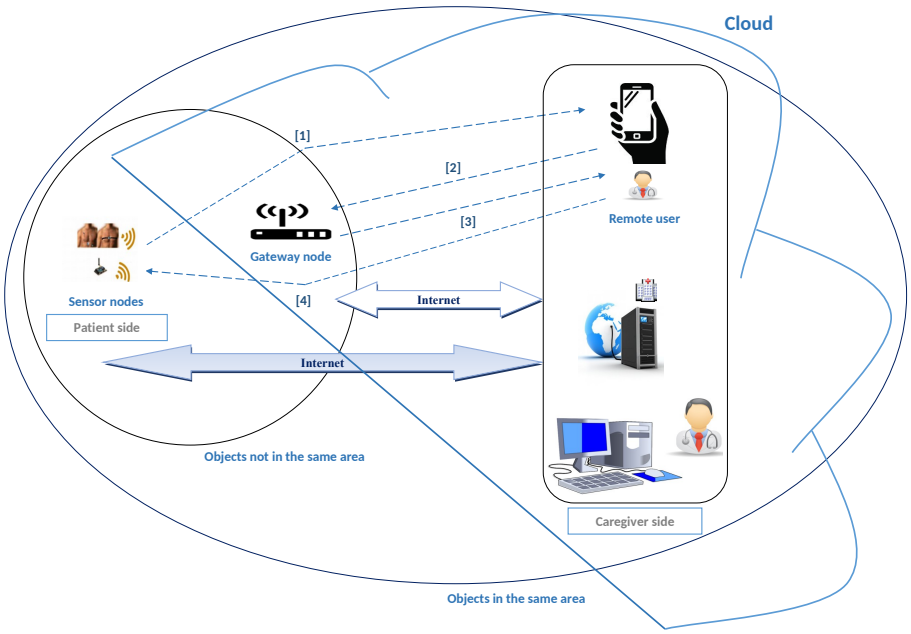
- *The caregiver side*

  The remote user as a caregiver can receive the gathered heath-related data using his desktop computer in the hospital, or his mobile device. In our network architecture, we consider the case of a mobile caregiver (see Figure 1).

  1 *The remote user*: the remote user receives the collected health-related data. Also, it could also be used by the caregiver to take appropriate decisions for the patient.

As shown in Figure 1, the caregiver devices and the gateway node are connected to a private cloud of the hospital. The latter is usually used to store collected health-related data and healthcare prescriptions. Furthermore, it facilitates the statistical analyses of the hospital.

Figure 1 Network architecture (see online version for colours)



According to involved devices in the network architecture, we make some assumptions:

- Objects can be divided into two categories: sensor nodes as constrained on both of computational and energy resources. The gateway node and the remote user are non-constrained since they have more computational and energy capabilities.
- Each sensor has an identity Id_i and a masked identity $MSId_i$. Also, it has an IPv6 address that gives its location in the IPv6 network (Perkins et al., 2011; Martinez-Julia and Skarmeta, 2013).
- Each sensor has the capacity to perform symmetric encryption. The gateway node and the remote user are able to perform classical PKI to secure transmission outside the WSN since they are non-constrained.
- The gateway node knows the secret key of the sensor node X_i, and the public key of the remote user PK_j on the pre-deployment of the network.

After a successful registration phase, the used authentication model allows a specific sensor to reach a remote user directly through the internet without connecting first with the gateway node (see Figure 1). Also, once a successful mutual authentication between a sensor node and the remote user, it enables collected health-related data from a sensor to be securely transmitted to the remote user.

4.2 Notations used in the proposed scheme

For the convenience of the reader, the notations used in the proposed authentication and key agreement scheme are defined in Table 1.

Table 1 Used notations

Notation	*Description*
$\|\|$	Concatenation
$\oplus$	Exclusive-or operation (XOR)
N	Nonce value of the sensor node
M	First nonce value of the remote user
S	Nonce value of the third party
W	Second nonce value of the remote user
T	Value used by the third party
Z	Value used by the remote user
K1	First value used for the session key computation
K2	Second value used for the session key computation
K	Shared symmetric session key
H()	A one way hash function
Enc(N, X_i)	AES-128 encryption of the value N using the secret key X_i
F(N)	If (N != 16 bytes): the function F applies an hash function h() that returns 16 bytes

4.3 Functioning of the proposed scheme

The proposed scheme aims to provide a secure communication in the e-health application. For this purpose, mutual authentication between the different sensor nodes and the remote

user is performed. Besides, it terminates by a session key agreement between each sensor and the remote user. The proposed scheme is divided into three phases:

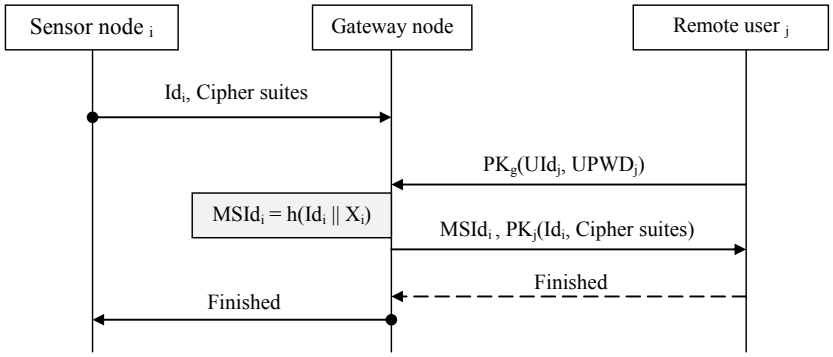
- *The registration phase* where new sensor nodes have to register. First, a registration part with the gateway node. Then, a second registration part with the remote user.
- *The authentication phase* between the sensor nodes, the gateway node, and the remote user to achieve mutual authentication between the sensor nodes and the remote user.
- *The key establishment phase* where a shared key is established, and then used as a session key between each sensor node and the remote user.

In the following, we will present each phase in details and by functional diagrams.

4.3.1 Registration phase

This phase is important in the functioning of the proposed scheme. In fact, each sensor must be registered in order to be integrated to the network system. The registration phase between the sensor nodes, the gateway node, and the mobile remote user is divided into two parts (see Figure 2).

Figure 2 Registration phase



First, registration part between the sensor node and the gateway node. We assume that the channel between the sensor node and the gateway node has been secured. Hence, the sensor node sends its identity Id_i and a list of supported cipher suites to the gateway node through a secure channel.

Second, the registration part between the gateway node and the remote user. The remote user connects to the gateway node using its identity UId_j and password $UPWD_j$ by an encrypted message ($PK_g(UId_j, UPWD_j)$) using the public key of the gateway node PK_g. The gateway node selects the used cipher suites, and calculates the masked identity of the sensor $MSId_i$ using the sensor identity Id_i and its secret key X_i. Then, the gateway node sends to the remote user a message containing the masked identity of the sensor node $MSId_i$, an encryption of both of the identity of the sensor Id_i and the selected cipher suites using the public key of the remote user PK_j.

As a response from the remote user, it sends an encrypted message *finished* with the secret key of the sensor containing the selected cipher suite. Finally, the gateway node transmits the *finished* message to the sensor node, and the registration phase terminates.

After a successful registration phase, both of the gateway node and the remote user store the security related information as shown in Table 2.

Table 2 Security related information

Node	*Cipher suite*	*Masked Identity:* $MSId_i = \mathrm{h}\ (Id_i \| X_i)$
Id_1	Cipher1 and X_1	$MSId_1$
Id_2	Cipher2 and X_2	$MSId_2$
Id_3	Cipher3 and X_3	...

4.3.2 Authentication phase

The authentication phase aims to mutually authenticate both of the sensor nodes and the remote user. To communicate the health-related data to the remote user, each sensor must execute the authentication process. The proposed scheme supports two cases of sensors authentication. The first case when the sensor nodes are not in the same location as the remote user, and in the second case, they are in the same location. The proposed authentication and key agreement scheme is as follows (see Figure 3):

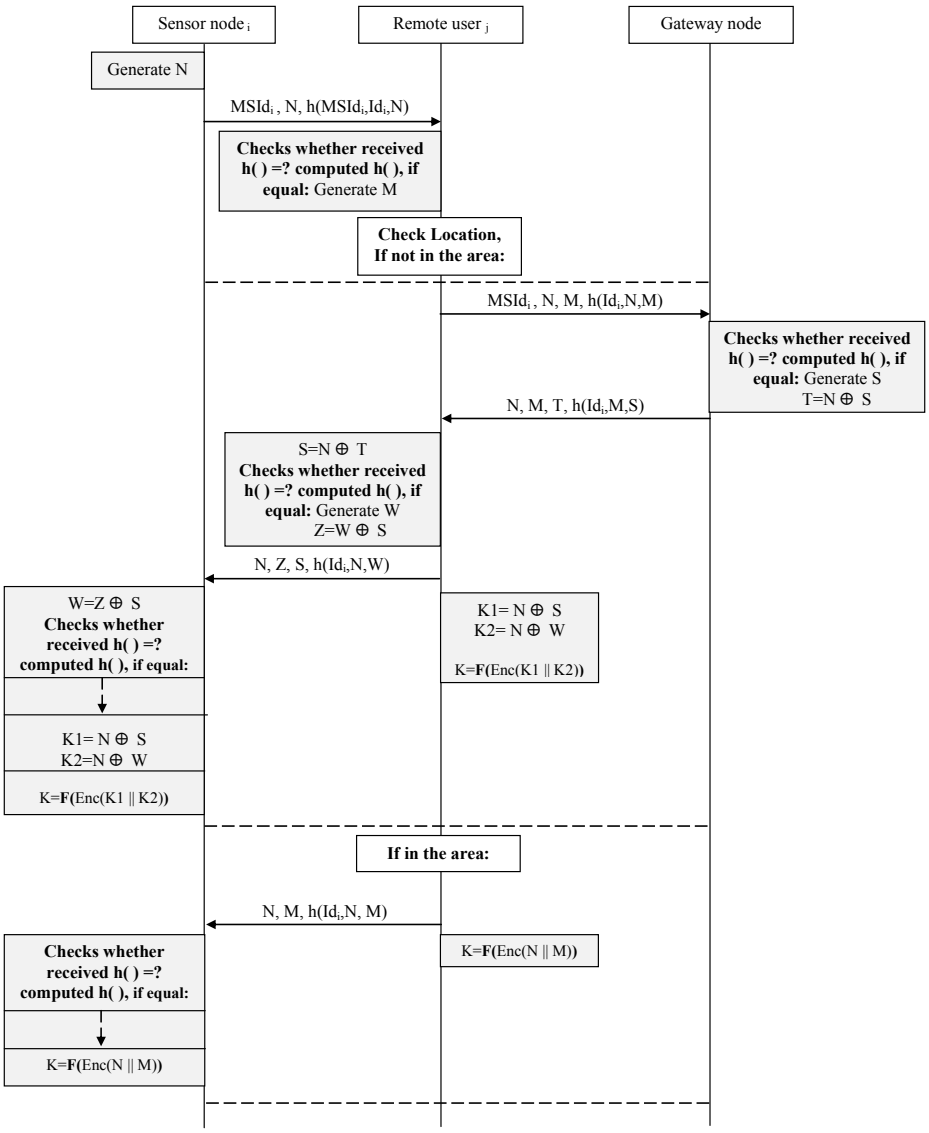
- The sensor node initiates the authentication phase, it generates a random nonce N on 8 bytes and sends a message composed of the generated nonce N, its masked identity $MSId_i$, and a h($MSId_i$, N, Id_i) to the remote user.
- Upon receiving the message by the remote user, the message is verified by checking whether received hash is equal to the computed hash. If the matching is successful, the remote user generates a random nonce M on 8 bytes, else it is an authentication failure.
- The remote user checks the location of the sensor node. If the remote user cannot reach the sensor node in his Wi-Fi covered area, then:

  Case 'not in the area':

- The remote user transmits to the gateway node a message composed by the masked identity of the sensor node $MSId_i$, the received nonce N, the nonce M, and a h($MSId_i$, N, M).
- Upon receiving the message by the gateway node, it verifies the message by checking whether the received hash is equal to the computed hash. If the check is successful, the gateway node generates a random nonce S on 8 bytes, and applies an XOR with the received nonce N: (T = N $\oplus$ S). Then, it sends to the remote user a message composed of the received nonces N and M, the computed value T and a h(M, Id_i, S), otherwise the authentication fails.
- When the remote user receives the message, the nonce value S is computed as follows: (S = N $\oplus$ T) and the message is verified by checking whether the received hash is equal to the computed hash. If the check is successful, the remote user also generates a random nonce W on 8 bytes, applies an XOR with value S as:

(Z = W ⊕ S), and sends to the sensor node a message composed by: the received nonce N, the value Z, the nonce value S, and a h(N, Id_i, W), otherwise it is an authentication failure.

Figure 3 Authentication scheme



- Upon receiving the message by the sensor node, the nonce value W is computed as follows: (W = Z ⊕ S), and the message is verified by checking whether received hash is equal to the computed hash. If the check is successful, a successful mutual authentication between objects terminates successfully.

Else, case 'in the area':

- The remote user transmits to the sensor node a message composed by the received nonce N, the nonce M, and a h($MSId_i$, N, M).
- When the sensor node receives the message, it verifies the message by checking whether the received hash is equal to the computed hash. If the check is successful, the random values are well received and the mutual authentication between objects terminates successfully, otherwise the authentication fails.

4.3.3 Key establishment phase

After a successful authentication phase, a shared symmetric key K on 16 bytes is established in order to secure the communication channel, such as in:

1 Case 'not in the area': the shared key is computed using a personalised function as: K = F(Enc(K1 || K2, X_i)). First, the values K1 and K2 are computed by applying respectively an XOR of the nonce value N with the nonces S and W. Then, the concatenation of the two values K1 and K2 is done to apply an encryption with the associated secret key of the sensor node X_i. Thus, the key establishment phase terminates.

2 Else, case 'in the area': the shared key is computed using a personalised function. First, the concatenation of the nonce values N and M, and then apply an encryption with the associated secret key of the sensor node X_i as K = F(Enc(N || M, X_i)). Consequently, the key establishment phase terminates.

5 Analysis

In this section, we provide in details the analysis of the proposed scheme in both of security and performance. First, we present a theoretical security analysis of the scheme concerning properties and resilience against different possible attacks. The security analysis is validated using an automated validation tool called AVISPA (http://www.avispa-project.org). Second, we evaluate and compare both communication and computational costs of the proposed scheme. In order to prove the energy saving of the scheme, we use energy models to estimate the energy cost consisting of both computational and communication costs.

5.1 Security analysis

5.1.1 Informal security analysis

Theoretical security analysis

The proposed authentication scheme provides a resistance to different possible attacks. In our analysis, we are interested in:

- *Replay attack*: the replay attack can be dangerous for such a scheme. In fact, a replay attack occurs when an attacker intercepts a previous message exchanged by a sensor node, and tries to replay it in order to impersonate the sensor node, respectively the gateway node, or the remote user. For this reason, we must take seriously the

resilience against this attack. In the proposed scheme, if an attacker intercepts a previous message exchanged in the authentication phase and tries to replay it in order to impersonate the sensor identity respectively the gateway node or the remote user, then in:

Case 'not in the area':

New nonces are generated for each authentication to provide mutual authentication. Therefore, the nonce intercepted in the previous exchange is not accepted, and the message is considered as an old replayed message. As a result, the attacker cannot impersonate the sensor node, the gateway node or the remote user. So, the proposed authentication scheme is resistant against replay attack.

Case 'in the area':

New nonces N and M are generated for each authentication to provide mutual authentication. If an attacker intercepts the previous exchanged message and tries to replay, the nonce intercepted in the message is not accepted and the message is considered as an old replayed one. Hence, the attacker cannot impersonate the sensor node, or the remote user. Thus, the proposed authentication scheme is resistant against replay attack.

- *Impersonation attacks*: in both cases, an attacker cannot impersonate a sensor node since the identity is masked by the value $MSId_i$. Moreover, the attacker cannot impersonate the remote user or the gateway node without computing a correct hash using the sensor identity Id_i. Consequently, the proposed scheme is resistant against impersonate attack.
- *DoS attack*: the DoS is also a very dangerous attack, given that IoT is generally based on resources constrained components. There are different types of DoS attacks (Wood et al., 2002). In particular, we are interested in the threat of flooding attack, that can affect the proposed scheme. In both cases of the proposed scheme, a received message is checked by the use of random nonces, and it indicates the acceptance or rejection of the message (Rejection in the case of an authentication failure). Therefore, we confirm that it is an authentic received message, and that it is not a DoS attack. Hence, the proposed authentication scheme provides resistance against DoS attacks.

The proposed scheme offers also advanced security features that improve security such as:

- *Mutual authentication*: mutual authentication is of high importance in such a scheme. In the two cases of the authentication phase, each involved object authenticates each other. This process is called mutual authentication. Hence, each involved object is sure of the identities of the others.
- *Data integrity*: in both cases of the proposed scheme, the integrity of a message is checked by the use of hash verification for each exchange. Thus, we are sure that the captured data transmitted in the authentication phase between involved objects, are not altered and are sent by legitimate objects.

- *Session key establishment*: after the key establishment phase of the proposed scheme, a shared session key is established between the sensor node and the remote user. The secret session key makes sure the communication channel.
- *Sensor identity protection*: after the registration phase of the proposed scheme, each sensor has an identity Id_i, and a masked identity $MSId_i$. In order to disallow the revelation of the sensor identity, the $MSId_i$ is also known by the gateway node and the remote user. Hence, the anonymity of the sensor node is ensured throughout the authentication process.
- *Remote user anonymity*: in both of the registration and the authentication phase, the remote user does not reveal its identity. Thus, an attacker cannot know the identity of the user that is anonymous during the authentication process.
- *Synchronisation independence*: in the two cases of the proposed scheme, we use random nonces in the different exchanges to guarantee the freshness of messages. Thus, the proposed scheme does not require synchronisation between objects. Consequently, the synchronisation independence enhances security of the proposed scheme.
- *Extensibility and scalability*: the proposed scheme allows new sensor nodes to be integrated into the network system through the registration phase. Then, new sensor nodes are added to the security related information table with their masked identity and cipher suites. Hence, The proposed scheme offers the scalability.

As a result of the theoretical informal security analysis, the proposed scheme is suitable in insecure IoT environments in which a malicious user can eavesdrop communications. A comparison between the proposed scheme and some previously proposed authentication and key agreement schemes is summarised in Table 3.

5.1.2 Formal security analysis

In this analysis, we conduct a formal security analysis to show that the proposed scheme is secure. First, we describe the scheme in algorithmic language.

As described in the algorithm, the sensor initiates the authentication scheme. It generates a random nonce N, computes an h($MSId_i$, Id_i, N), and sends to the remote user R a message composed of [$MSId_i$, N, h($MSId_i$, Id_i, N)].

The remote user receives the message. It verifies the integrity of the message by computing the hash of the message. Then, it compares with the received hash. If the check is successful, it generates a random nonce M, else it sends an authentication failure message F1 to the sensor node SN.

The remote user checks the sensor location. If the sensor node SN is not in the same covered area as the remote user, then it computes a h(Id_i, N, M), and sends to the gateway node G a message composed of [$MSId_i$, N, M, h(Id_i, N, M)]. Upon receiving the message by the gateway node, it verifies the integrity of the message by computing the hash of the message. Then, it compares with the received hash. If the check is successful, the gateway node generates a random nonce S, computes $T = N \oplus S$, computes h(Id_i, M, S), and sends to the remote user a message composed of [N, M, T, h(Id_i, M, S)]. In the case of a unsuccessful check, the gateway node sends an authentication failure message F2 to the remote user.

The remote user receives the message, it computes the value S = N ⊕ T. It verifies the integrity of the message by computing the hash of the message, and compares with the received hash. If the check is successful, it generates a random nonce W, computes Z = W ⊕ S, computes a h(Id_i, N, W), and sends to the sensor node SN a message composed of [N, Z, S, h(Id_i, N, W)]. It computes the values K1 = N ⊕ S, K2 = N ⊕ W, and the session key K = F(Enc(K1 || K2)). In the case of a unsuccessful check, the remote user sends an authentication failure message F3 to the sensor node. Upon receiving the message by the sensor node, it computes the value W = Z ⊕ S. It verifies the integrity of the message by computing the hash of the message, and compares with the received hash. If the check is successful, it computes the values K1 = N ⊕ S and K2 = N ⊕ W, and computes the session key K = F(Enc(K1 || K2)). In the case of a unsuccessful check, the sensor node sends an authentication failure message F4 to the remote user.

Algorithm:

SN: Sensor node
G: Gateway node
R: Remote user

1: SN generates a random nonce N
Computes h($MSID_i$, Id_i, N)
SN ⟶ R : {$MSID_i$, N, h($MSID_i$, Id_i, N)}
2: R computes h'( ).
If (h( ) = = h'( )) then Generates a random nonce M
else return 0 (Failure)
3: R checks sensor location

If (Sensor not in the area) *then*
Computes h(Id_i, N, M)
R ⟶ G : {$MSID_i$, N, M, h(Id_i, N, M)}
3.1.1: G computes h'( ).
If (h( ) = = h'( )) then Generates a random nonce S
Computes T = N ⊕ S, h(Id_i, M, S)
G ⟶ R : {N, M, T, h(Id_i, M, S)}
else return 0 (Failure)
3.1.2: R computes S = N ⊕ T
If (h( ) = = h'( )) then Generates a random nonce W.
Computes Z = W ⊕ S, h(Id_i, N, W)
R ⟶ SN : { N, Z, S, h(Id_i, N, W)}

Computes K1 = N ⊕ S, K2 = N ⊕ W
Computes the session key K = F(Enc(K1 || K2))
else return 0 (Failure)
3.1.3: SN computes W = Z ⊕ S
If (h( ) = = h'( )) then Computes K1 = N ⊕ S, K2 = N ⊕ W
Computes the session key K = F(Enc(K1 || K2))
return 1 (Success)
else return 0 (Failure)

else

3.2.1: R computes h(Id_i, N, M)
R ⟶ SN : {N, M, h(Id_i, N, M)]}
Computes the session key K = F(Enc(N || M))
3.2.2: If (h( ) = = h'( )) then SN computes the session key K = F(Enc(N || M))
return 1 (Success)

Table 3 Comparison of security features between the proposed scheme and other schemes

Security feature	*Xue et al.'s scheme*	*Jiang et al.'s scheme*	*Das's scheme*	*Farash et al.'s scheme*	*Gope et al.'s scheme*	*The proposed scheme*
Mutual authentication	Yes	Yes	Yes	Yes	Yes	Yes
Session key establishment	Yes	Yes	Yes	Yes	Yes	Yes
Sensor identity protection	-	-	-	Yes	No	Yes
User anonymity	No	-	-	Yes	Yes	Yes
Exchanged data integrity	Yes	Yes	Yes	Yes	Yes	Yes
Synchronisation independence	No	No	No	No	No	Yes
Extensibility and scalability	No	No	Yes	Yes	Yes	Yes
Resilience against						
Replay attack	Yes	Yes	Yes	Yes	Yes	Yes
Sensor node impersonation attack	-	-	-	Yes	Yes	Yes
User impersonation attack	Yes	-	Yes	Yes	Yes	Yes
Denial of service attack	No	No	No	Yes	Yes	Yes

If the sensor node and the remote user are in the same covered area, then the remote user computes a h(Id_i, N, M) , and sends the sensor node a message composed of [N, M, h(Id_i, N, M)]. Also, it computes the session key K = F(Enc(N || M)). Upon receiving the message by the sensor node SN, it verifies the integrity of the message by computing the hash of the message, and compares with the received hash. If the check is successful, the sensor node computes the session key K = F(Enc(N || M)), otherwise the authentication fails.

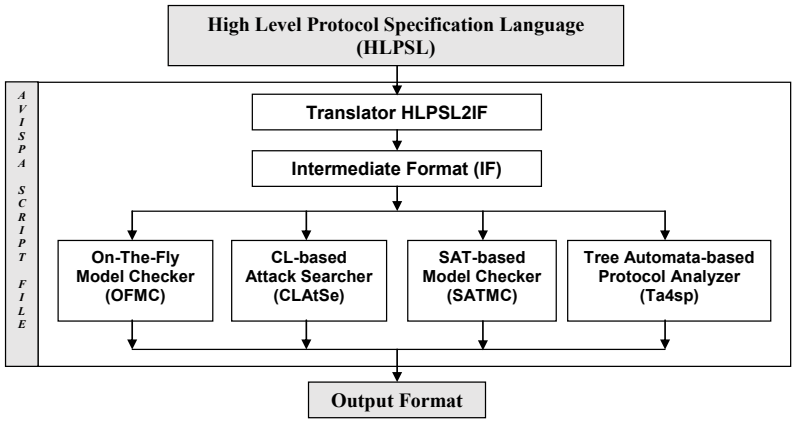
Automated security analysis

In order to validate the theoretical security analysis of the proposed scheme, we conduct an automated analysis using AVISPA tools. This latter is a simulation tool used to analyse the security of the scheme, and to confirm the non-violation of the required security properties, in particular, confidentiality, data integrity, authentication, and identity protection.

AVISPA tool

Automated validation of internet security protocols and applications (AVISPA) is a state of the art verification tool for security protocols (AVISPA, http://www.avispa-project.org). It is considered as an effective tool for the analysis of internet security protocols and applications since it verifies all security requirements, and confirms the safety of cryptographic protocols. In the past, different security protocols have been validated using AVISPA (Moedersheim et al., 2005; Chen et al., 2011). Furthermore, security protocols standardised by the internet engineering task force (IETF) have been analysed by the AVISPA tools (e.g., TLS, IKE, etc.). Figure 4 shows the architecture of AVISPA (http://www.avispa-project.org).

Figure 4 The architecture of the AVISPA



First, we have to present the scheme in a role-based language called high level protocol specification language (HLPSL) (von Oheimb, 2005). Then, the HLPSL presentation of the scheme is translated into a lower level language called intermediate format (IF) with a translator called HLPSL2IF (the translation of the HLPSL to IF presentation is transparent to the user). The IF presentation of the scheme is used as an input to the four backends

of AVISPA to verify the analysed scheme against the specified security goals (AVISPA, http://www.avispa-project.org): on-the-fly model-checker (OFMC), constraint-logic-based attack searcher (CL-AtSe), SAT-based model-checker (SATMC), and tree-automata-based protocol analyser (TA4SP). The AVISPA's back-ends perform the security analysis of the scheme, output the results, and show if the scheme is safe or not. In case of an unsafe scheme, the AVISPA tools provide a trace highlighting the reasons that have led to the attack.

As a channel model, Dolev-Yao (dy) channel model is generally used. This type of channel allows the interception or alteration of data by an intruder (Dolev and Yao, 1983). Before launching the analysis, the security goals of the analysed scheme are specified in the goal section of the HLPSL code (AVISPA, http://www.avispa-project.org).

Figure 5 Role specification of the sensor node in HLPSL (case 'not in the area')

```
role alice (A, B : agent,
X : symmetric_key,
H : hash_func,
SND_BA, RCV_BA: channel(dy))

played_by A
def=

local State : nat,
N, M, Id, MSId, S,Z,W : text,
K,K1,K2 : symmetric_key

init State := 0
transition
1. State = 0 /\ RCV_BA(start)  =|>
State':= 2 /\ N' := new()
          /\ MSId' := H(Id.X)
          /\ SND_BA(A.B.N'.MSId'.H(MSId'.Id.N'))
            /\  secret({Id},identity,{A,B})

2. State = 8 /\ RCV_BA(B.A.N.Z'.S'.H(Id.N.W'))  =|>

State' := 9  /\ W':= xor(Z', S') /\ K1':= xor(N, S') /\ K2':= xor(N, W')
                /\ K' := H({K1'.K2'}_X)
                 /\ request(A,B,alice_bob_n,N)


end role
```

HLPSL implementation of the proposed scheme

In order to model the proposed scheme, we specified a basic role to describe the actions of each involved entity. Then, we have specified the interactions of communicating entities with each other in a composed role. For more details, we present our modelling using a high level Alice-Bob (A-B) notation in both cases of authentication, where:

- *Case 'not in the area'*:

  A: Sensor node
  B: Remote user
  C: Gateway node
  A → B: $\{MSId_i, N\}$, H($MSId_i$, Id_i, N)
  B → C: $\{MSId_i, N, M\}$, H($MSId_i$, N, M)
  C → B: $\{N, M, T\}$, H(M, Id_i, S)
  B → A: $\{N, Z, S\}$, H(N, Id_i, W)

- *Case 'in the area'*:

  A: Sensor node
  B: Remote user
  A → B: $\{MSId_i, N\}$, H($MSId_i$, Id_i,N)
  B → A: $\{N, M\}$, H(N, Id_i, M)

The rest of the used notations are the same as previously presented in Table 1.

Figure 6 Role specification of the sensor node in HLPSL (case 'in the area')

```
role alice (A, B : agent,
X : symmetric_key,
H : hash_func,
SND_BA, RCV_BA: channel(dy))

played_by A
def=

local State : nat,
N, M, Id, MSId, S,Z,W : text,
K,K1,K2 : symmetric_key

init State := 0
transition
1. State = 0 /\ RCV_BA(start)  =|>
State':= 2 /\ N' := new()
          /\ MSId' := H(Id.X)
          /\ SND_BA(A.B.N'.MSId'.H(MSId'.Id.N'))
            /\  secret({Id},identity,{A,B})

2. State = 8 /\ RCV_BA(B.A.N.Z'.S'.H(Id.N.W'))  =|>

State' := 9  /\ W':= xor(Z', S') /\ K1':= xor(N, S') /\ K2':= xor(N, W')
                /\ K' := H({K1'.K2'}_X)
                 /\ request(A,B,alice_bob_n,N)


end role
```

Figure 7 Role specification of the remote user in HLPSL (case 'not in the area')

```
role bob (A, B, C : agent,
X : symmetric_key,
H : hash_func,
SND_AB, RCV_AB, SND_CB, RCV_CB  : channel(dy))

played_by B
def=

local State : nat,
N,M,S,T,W,Z, Id, MSId : text,
K,K1,K2 : symmetric_key

init State := 1
transition

1. State = 1  /\ RCV_AB(A.B.N'.MSId'.H(MSId'.Id.N'))  =|>

   State':= 3   /\ M' := new() /\ SND_CB(B.C.MSId'.N'.M'.H(Id.N'.M'))
                /\  secret({Id},identity,{B,C}) /\  witness(B,C,gwn_bob_m,M')


2. State = 6  /\   RCV_CB(C.B.N.M.T'.H(Id.M. S'))  =|>

State':= 7  /\  S':= xor(N, T')   /\ W' := new() /\  Z':= xor(W', S')
            /\  SND_AB(B.A.N.Z'.S'.H(Id.N. W')) /\ K1':= xor(N, S')   /\ K2':= xor(N, W')
            /\  K' := H({K1'.K2'}_X)   /\  secret({Id},identity,{B,A})
            /\  request(B,A,gwn_bob_w,W')  /\ request(A,B,alice_bob_n,N)

3. State = 10 /\ K1'= xor(N, S')   /\ K2'= xor(N, W')   /\  K' = H({K1'.K2'}_X)
               /\ request(A,B,alice_bob_n,N)

end role
```

In both the authentication phase and the key establishment phase of the proposed scheme, we implemented in HLPSL the role specification of the sensor node (see Figure 5 and Figure 6), the role specification of the remote user (see Figure 7 and Figure 8), the role specification of the gateway node (see Figure 9), and the specification for the roles of session and environment (see Figure 10 and Figure 11).

To clarify the HLPSL specification, basic types and important notations supported by HLPSL are presented in AVISPA (http://www.avispa-project.org) and Odelu et al. (2015). In addition, the four predefined goal predicates in HLPSL are as follows:

- Secret(A, *Id*, B): declares the information A as secret shared by the agents of set B. This secret will be identified by the constant *Id* in the goal section.
- Witness(A, B, *Id*, E): for a weak authentication property of A by B on E, declares that agent A is witness for the information E. This goal will be identified by the constant *Id* in the goal section.
- Request(B, A, *Id*, E): for a strong authentication property of A by B on E, declares that agent B requests a check of the value E. This goal will be identified by the constant *Id* in the goal section.

- Wrequest(B, A, *Id*, E): it is similar to request, but for a weak authentication property.

Figure 8 Role specification of the remote user in HLPSL (case 'in the area')

```
role bob (A, B : agent,
X : symmetric_key,
H : hash_func,
SND_AB, RCV_AB   : channel(dy))

played_by B
def=

local State : nat,
N,M,Id, MSId : text,
K : symmetric_key

init State := 1
transition

1. State = 1  /\ RCV_AB(A.B.N'.MSId'.H(MSId'.Id.N'))  =|>

   State':= 3  /\ M' := new() /\ SND_AB(B.A.MSId'.N'.M'.H(Id. N'. M'))
                /\ K' := H({N.M'}_X)
                /\  secret({Id},identity,{B,A})  /\  request(A,B,alice_bob_n,N)


end role
```

Figure 9 Role specification of the gateway node in HLPSL (case 'not in the area')

```
role gwn (B, C : agent,
X : symmetric_key,
H : hash_func,
SND_BC, RCV_BC : channel(dy))



played_by C
def=

local State : nat,
N,M,S,T, Id, MSId : text,
K: symmetric_key

init State := 4
transition
1. State = 4 /\ RCV_BC(C.B.MSId'.N'.M'.H(Id.N'.M'))  =|>

   State':= 5 /\ S' := new() /\ T':= xor(N', S')  /\ SND_BC(B.C.N'.M'.T'.H(Id.M'.S'))
               /\  secret({Id},identity,{C,B}) /\  request(B,C,gwn_bob_s,S')


end role
```

Figure 10 Role specification of session and environment in HLPSL (case 'not in the area')

```
role session(A, B, C : agent,
H  : hash_func,
X : symmetric_key)

def=
local  SND_BA, RCV_BA, SND_AB, RCV_AB, SND_CB, RCV_CB, SND_BC,
RCV_BC    : channel (dy)

composition

alice (A, B, X, H, SND_BA, RCV_BA)

/\ bob (A, B, C, X, H, SND_AB, RCV_AB, SND_CB, RCV_CB)

/\ gwn (C, B, X, H, SND_BC, RCV_BC)

end role

role environment( )
def=
const a, b, c : agent,
x : symmetric_key,
h : hash_func,
k, alice_bob_n, gwn_bob_m, gwn_bob_s, gwn_bob_w, identity : protocol_id
intruder_knowledge = {a, b, c, h, x}

composition

session(a,b,c,h,x)
/\ session(c,b,a,h,x)
/\ session(b,a,c,h,x)

end role

goal
secrecy_of k
secrecy_of identity
authentication_on alice_bob_n
authentication_on gwn_bob_m
authentication_on gwn_bob_s
authentication_on gwn_bob_w

end goal

environment( )
```

Figure 11 Role specification of session and environment in HLPSL (case 'in the area')

```
role session(A, B :  agent,
H  : hash_func,
X : symmetric_key)

def=
local  SND_BA, RCV_BA, SND_AB, RCV_AB    : channel (dy)

composition

alice (A, B, X, H, SND_BA, RCV_BA)

/\ bob (A, B, X, H, SND_AB, RCV_AB)

end role


role environment( )
def=
const  a, b  : agent,
x : symmetric_key,
h : hash_func,
k, alice_bob_n, identity : protocol_id
intruder_knowledge = {a, b, h, x}

composition

session(a,b,h,x)
/\ session(b,a,h,x)

end role

goal
secrecy_of k
secrecy_of identity
authentication_on  alice_bob_n

end goal

environment( )
```

Simulation results

The output format of AVISPA is generated by executing one of the four back ends: OFMC, CL-AtSe, SATMC, and TA4SP. The latter has the following important sections (AVISPA, http://www.avispa-project.org; Farash et al., 2016):

- SUMMARY section: indicates that the protocol test result is SAFE, UNSAFE, or INCONCLUSIVE.
- DETAILS section: either explains under what condition the tested protocol is declared safe or what conditions have been used for finding an attack or finally why the analysis was inconclusive.
- Other sections: PROTOCOL, GOAL, and BACKEND, are the name of the protocol, the goal of the analysis, and the name of the back end used,respectively.
- Finally: after comments and statistics. In case of unsafety, the trace of an attack is also displayed in the standard Alice-Bob format.

We have evaluated the security goals of the proposed scheme by executing the four backends of AVISPA (i.e., OFMC, CL-AtSe, SATMC and TA4SP), and using the default Dolev-Yao intruder model that allows the simulation of an intruder with a full control over the deployed network.

In the first case of authentication, the outputs of the HLPSL code execution in AVISPA tool show that the proposed scheme is 'SAFE' against OFMC (see Figure 12) and CL-AtSe (see Figure 13). Nevertheless, the result was 'INCONCLUSIVE' against SATMC (see Figure 14) and TA4SP database (see Figure 15).

In the second case of authentication, the outputs of the HLPSL code execution in AVISPA tool show that the proposed scheme is 'SAFE' against OFMC (see Figure 16), CL-AtSe (see Figure 17), and SATMC (see Figure 18). However, the result was 'INCONCLUSIVE' against TA4SP database (see Figure 19). According to AVISPA user manual, an inconclusive result does not signify that an attack has been found.

In the two cases of authentication, the obtained simulation results can safely affirm that the proposed scheme is SAFE. Thus, the theoretical security analysis results are confirmed. As a conclusion, we could confirm that our proposed scheme is secure in an IoT environment.

Figure 12 AVISPA output (OFMC) (case 'not in the area')

```
user@instant-contiki:~/Desktop$ avispa Case1.hlpsl   --ofmc
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /opt/avispa-1.1/testsuite/results/Case1.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.02s
  visitedNodes: 8 nodes
  depth: 3 plies
```

Figure 13 AVISPA output (CL-AtSe) (case 'not in the area')

```
user@instant-contiki:~/Desktop$ avispa Case1.hlpsl   --cl-atse

SUMMARY
    SAFE

DETAILS
    BOUNDED_NUMBER_OF_SESSIONS
   TYPED_MODEL

PROTOCOL
  /opt/avispa-1.1/testsuite/results/Case1.if

GOAL
    As Specified

BACKEND
    CL-AtSe

STATISTICS

    Analysed   : 6 states
    Reachable  : 0 states
    Translation: 0.08 seconds
    Computation: 0.00 seconds
```

Figure 14 AVISPA output (SATMC) (case 'not in the area')

```
user@instant-contiki:~/Desktop$ avispa Case1.hlpsl  --satmc


% WARNING: The term xor(Z,S) requires algebraic equation on the xor operator.

SUMMARY
    INCONCLUSIVE

DETAILS
    NOT_SUPPORTED

PROTOCOL
    Case1.if

BACKEND
    SATMC

COMMENTS
    The security protocol analyzed required support for some
    algebraic equations specified in the prelude file, while
    SATMC currently assumes free-algebra. Hence if operators
    like exp or xor occur in the IF specification, then the
    analysis is inconclusive and it is not performed.
```

Figure 15 AVISPA output (TA4SP) (case 'not in the area')

```
user@instant-contiki:~/Desktop$ avispa Case1.hlpsl  --ta4sp
SUMMARY
      INCONCLUSIVE

DETAILS
     NOT_SUPPORTED

PROTOCOL
     /opt/avispa-1.1/testsuite/results/Case1.if

GOAL
      SECRECY

BACKEND
      TA4SP

COMMENTS
       Sorry, currently TA4SP does not support XOR operator

STATISTICS
     Translation: 0.03 seconds
```

Figure 16 Avispa output (OFMC) (case 'in the area')

```
user@instant-contiki:~/Desktop$ avispa Case2.hlpsl   --ofmc
% OFMC
% Version of 2006/02/13
SUMMARY
    SAFE
DETAILS
    BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
   /opt/avispa-1.1/testsuite/results/Case2.if
GOAL
    as_specified
BACKEND
    OFMC
COMMENTS
STATISTICS
   parseTime: 0.00s
   searchTime: 0.00s
   visitedNodes: 4 nodes
   depth: 2 plies
```

Figure 17 Avispa output (CL-AtSe) (case 'in the area')

```
user@instant-contiki:~/Desktop$ avispa Case1.hlpsl   --cl-atse

SUMMARY
    SAFE

DETAILS
   BOUNDED_NUMBER_OF_SESSIONS
   TYPED_MODEL

PROTOCOL
   /opt/avispa-1.1/testsuite/results/Case2.if

GOAL
    As Specified

BACKEND
    CL-AtSe

STATISTICS

    Analysed   : 2 states
    Reachable  : 0 states
    Translation: 0.00 seconds
    Computation: 0.00 seconds
```

5.2 Performance analysis

Our contribution consists on proposing an efficient lightweight authentication and key agreement scheme for e-health applications as a constrained environment in the IoT. In this section, we provide a performance analysis of the proposed scheme. Firstly, we conduct an analysis of communication cost, execution time, and storage overhead of the proposed scheme. Secondly, we focus on the energy consumption of the sensor node as a constrained object. We compute the energy required for computation (execution of the cryptographic primitives), along with the energy required for communication. Finally, we compare the energy cost of the proposed scheme with some recent authentication schemes.

5.2.1 Communication cost analysis of the proposed scheme

In a constrained environment, we must seriously consider the impact of communication in the total energy cost of an authentication and key agreement scheme. In fact, transmission consumes more energy than computation, such as 1 bit transmitted equals an execution of about 900 CPU instructions (Simplicio et al., 2013). In the proposed scheme, the nonce value and the secret key X_i are generated through a trusted platform module (TPM) (Morris, 2011). We consider that the length of the nonce value is 8 bytes, the identity of the sensor node is 8 bytes, and the masked identity is 16 bytes. However, each hash value sent in the different messages has 8 bytes instead of 16 bytes. We divide the result of the hash value

(16 bytes) into two values of 8 bytes, and we apply an XOR operation between the two parts. Thus, the result of the XOR operation is sent as an hash value.

In order to show the efficiency of the proposed scheme, we study the communication cost of the different exchanged messages (see Table 4). Then, we compare the sensor communication cost with Xue et al.'s (2013) scheme, Jiang et al.'s (2015) scheme, Das's (2016) scheme, Farash et al.'s (2016) scheme, and Gope et al.'s scheme (Gope and Hwang, 2016) (see Table 5).

As a result from the communication cost analysis of proposed authentication and key agreement scheme, we deduce that the proposed scheme has a low communication cost on sensor nodes in both cases of authentication. Consequently, it offers a low energy cost on communication, which enhances the scheme performance.

Figure 18 Avispa output (SATMC) (case 'in the area')

```
user@instant-contiki:~/Desktop$ avispa Case2.hlpsl   --satmc
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  BOUNDED_SEARCH_DEPTH
  BOUNDED_MESSAGE_DEPTH

PROTOCOL
  Case2.if

GOAL
  %% see the HLPSL specification..

BACKEND
  SATMC

COMMENTS

STATISTICS
  attackFound              false          boolean
  upperBoundReached        true           boolean
  graphLeveledOff          1              steps
  satSolver                zchaff         solver
  maxStepsNumber           30             steps
  stepsNumber              1              steps
  atomsNumber              0              atoms
  clausesNumber            0              clauses
  encodingTime             0.0            seconds
  solvingTime              0              seconds
  if2sateCompilationTime   0.02           seconds

ATTACK TRACE
  %% no attacks have been found..
```

Figure 19 Avispa output (TA4SP) (case 'in the area')

```
user@instant-contiki:~/Desktop$ avispa Case2.hlpsl  --ta4sp
SUMMARY
      INCONCLUSIVE

DETAILS
     NOT_SUPPORTED

PROTOCOL
     /opt/avispa-1.1/testsuite/results/Case2.if

GOAL
      SECRECY

BACKEND
      TA4SP

COMMENTS
       Some rules may be not fired so TA4SP does not do the verification.


STATISTICS
     Translation: 0.00 seconds
```

Table 4 Communication cost of exchanged messages in the proposed scheme

Message	*From-to*	*Cost (bytes)*
$MSId_i$, N, Hash	Sensor node-remote user	32
Case 1: If not in the area		
$MSId_i$,N, M, Hash	Remote user-gateway node	40
N, M, T, Hash	Gateway node-remote user	32
N, Z, S, Hash	Remote user-sensor node	32
Case 2: If in the area		
N, M, Hash	Remote user-sensor node	24

5.2.2 Execution time comparison of the proposed scheme

The execution time of an authentication and key agreement scheme is very important. We estimate and compare the execution time of the proposed scheme with Xue et al.'s (2013) scheme, Jiang et al.'s (2015) scheme, Das's (2016) scheme, Farash et al.'s (2016) and Gope et al.'s scheme (Gope and Hwang, 2016) (see Table 6).

As a result from the execution time analysis of the proposed scheme, we deduce that the scheme has also a low execution time on the sensor nodes, remote user, and gateway node. The mutual authentication is achieved in just $2T_{Hash}$ of the computational execution time, plus $1T_{Aes}$ for the computation of the session key in the key establishment phase.

Table 8 shows the total execution time of the schemes. In both cases of authentication, the execution time of the proposed scheme is 6.74 ms that is less than Farash et al.'s (2016) scheme and more than Xue et al.'s (2013) scheme, Jiang et al.'s (2015) scheme, Das's (2016) scheme, and Gope et al.'s scheme (Gope and Hwang, 2016). However, the execution time of the proposed authentication and key agreement scheme is acceptable and considered as a low cost.

Table 5 Comparison of sensor node communication cost of the proposed scheme

Scheme	*Network architecture*	*Sensor transmission cost (bytes)*	*Sensor reception cost (bytes)*
Xue et al.	Remote user-gateway node-sensor node	51	67
Jiang et al.	Remote user-gateway node-sensor node	51	51
Das	Remote user-gateway node-sensor node	51	64
Farash et al.	Remote user-sensor node-gateway node	256	178
Gope et al.	Remote user-gateway node-sensor node	35	51
Case 1: If not in the area	Sensor node-remote user-gateway node	32	32
Case 2: If in the area	Sensor node-remote user-gateway node	32	24

Table 6 Execution time comparison of the proposed scheme

Scheme	*Sensor node*	*Remote user*	*Gateway node*
Xue et al.	$5T_{Hash}$	$10T_{Hash}$	$7T_{Hash}$
Jiang et al.	$5T_{Hash}$	$10T_{Hash}$	$7T_{Hash}$
Das	$6T_{Hash}$	$11T_{Hash}$	$11T_{Hash}$
Farash et al.	$7T_{Hash}$	$11T_{Hash}$	$14T_{Hash}$
Gope et al.	$3T_{Hash}$	$9T_{Hash}$	$7T_{Hash}$
Case 1: If not in the area	$2T_{Hash} + 1T_{Aes}$	$4T_{Hash} + 1T_{Aes}$	$2T_{Hash}$
Case 2: If in the area	$2T_{Hash} + 1T_{Aes}$	$2T_{Hash} + 1T_{Aes}$	-

Table 7 Estimated energy and time costs on the sensor node

Operation	*Cost (Ws)*	*Execution time (ms)*
SHA-256	0.27	1.06
128-bit AES-CBC	0.72	4.62

Source: Gope and Hwang (2016)

Table 8 Energy and execution time costs comparison of the proposed scheme on the sensor node

Scheme	*Communication cost (Ws)*	*Computational cost (Ws)*	*Execution time (ms)*
Xue et al.	61.2	1.35	5.3
Jiang et al.	61.2	1.35	5.3
Das	61.2	1.62	6.36
Farash et al.	307.2	1.89	7.42
Gope et al.	42	0.81	3.18
Case 1: If not in the area	38.4	1.26	6.74
Case 2: If in the area	38.4	1.26	6.74

5.2.3 Storage overhead analysis

Storage overhead must be taken into consideration to design efficient security schemes in the context of IoT. Thus, we study the storage cost at specific moments in the sensor node as a constrained object. First, after the registration phase, the sensor node stores (Id_i, $MSId_i$, X_i) which means 40 bytes.

Second, after the authentication phase, we have two cases:

- *Case 'not in the area'*: the sensor node has in its storage (Id_i, $MSId_i$, X_i, N, Z, S, W) which means 72 bytes.
- *Case 'in the area'*: the sensor node has in its storage (Id_i, $MSId_i$, X_i, N, M) which means 56 bytes. Third, at the end of the key establishment phase:
- *Case 'not in the area'*: the sensor node stores (Id_i, $MSId_i$, X_i, N, Z, S, W, K1, K2, K) that consumes 104 bytes, and it is the maximum used storage.
- *Case 'in the area'*: the sensor node stores (Id_i, $MSId_i$, X_i, N, M, K) that consumes 72 bytes.

Finally, after the key establishment phases, the sensor node can delete (N, Z, S, W, K1, K2) in the first case, and (N, M) in the second case. Thus, it stores only 56 bytes (Id_i, $MSId_i$, X_i, K).

As a result from the storage overhead analysis of proposed authentication and key agreement scheme, we deduce that the proposed scheme has a very low storage cost which enhances the scheme performance.

5.2.4 Energy evaluation and comparison of the proposed scheme

In this evaluation of the proposed scheme, we estimate the energy consumption of both the authentication and the key establishment phases. We use the modular sensor board MSB430 with the TI MSP430 micro controller, the temperature and relative humidity sensor Sensirion SHT11, and a CC1020 radio transceiver. The sensor node has 55 KB Flash, and 5 KB RAM. In addition to that it contains a SD-/MM card slot which supports a secondary storage of up to 4 GB (Baar et al., 2007). The MSB430 can be powered by both a battery pack containing three AAA (1.5 V) batteries and through an external power-supply interface using, e.g., an external mains-connected voltage generator, a solar panel, or a high-power capacitor (Omiyi et al., 2008).

For the energy evaluation of the proposed scheme, we use SHA-256 (Eastlake and Hansen, 2006) as an hash function, and 128-bit AES-CBC (Dworkin, 2001) as a symmetric encryption primitive. Based on the simulation outcomes of the cryptographic operations used in the proposed scheme and the other recent schemes (Gope and Hwang, 2016), Table 7 summarises the energy cost and the execution time of each used cryptographic operation. In addition, the transmission cost for each byte of data in sensor node is 1.2 Ws.

As a result of the energy cost comparison of the schemes (see Table 8), the proposed scheme has the less communication cost with 38.4 Ws in both cases of authentication. Also, it has 1.26 Ws as a computational cost that is less than Xue et al.'s (2013) scheme, Jiang et al.'s (2015) scheme, Das's (2016) scheme, and Farash et al.'s (2016) scheme. Nevertheless, it is slightly more than Gope et al.'s scheme (Gope and Hwang, 2016).

Thus, the computational cost of the proposed authentication and key agreement scheme is considered as a low cost.

The performance analysis shows the impact of the communication cost on the total energy cost of an authentication and key agreement scheme, and that we must consider communication cost, computational cost, and execution time to design a lightweight scheme.

The analysis study allowed us to validate the proposed authentication and key agreement scheme. First, we provided a theoretical analysis regarding several attacks and different security properties. Then, we validated the security of the proposed scheme using AVISPA tools. Furthermore, we confirmed the low energy cost of proposed scheme through the performance analysis.

6 Conclusions

This paper proposed an efficient authentication and key agreement scheme for e-health applications in the context of IoT. This scheme enables a mutual authentication and a session key agreement between a specific sensor node and a remote user. Since IoT is resource constrained, the proposed scheme is based on lightweight cryptography. In the authentication phase, it uses only nonces, XORs, and hash functions. Furthermore, it considers the location aspect by checking the location of the sensor nodes in the beginning of the authentication phase. Then, it uses one concatenation operation and one AES encryption primitives in the key establishment phase.

For validation purpose, the proposed scheme has been evaluated in both security and performance. First, the security analysis shows that the proposed scheme provides a resistance against several possible attacks, as well as security properties are ensured. Second, the performance analysis confirms that the proposed scheme is very lightweight as it requires low communication overhead and energy cost.

In comparison with recent authentication schemes, the proposed scheme has low costs of communication and computation with a high level of security. Thus, it is suitable to be applied in e-health applications deployed in a highly resource constrained environment.

7 Limitations and future research

In this paper, we have proposed a secure and efficient authentication and key agreement scheme for e-health applications in the context of IoT. However, the limitation of many research works is how to be sure that confidential data are securely stored in the different objects, and this is our new research challenge. As a future work, the strong development of blockchains as distributed secure databases to share and store data, give us many ideas to design a novel solution based on blockchain technology for a best confidentiality, integrity, and access control.

References

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. and Ayyash, M. (2015) 'Internet of things: a survey on enabling technologies, protocols, and applications', *IEEE Communications Surveys and Tutorials*, Vol. 17, No. 4, pp.2347–2376.

Ali, R., Pal, A.K., Kumari, S., Karuppiah, M. and Conti, M. (2017) 'A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring', *Future Generation Computer Systems*, Vol 84, pp.200–215.

Amin, R., Islam, S.H., Biswas, G., Khan, M.K. and Li, X. (2015) 'Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems', *Journal of Medical Systems*, Vol. 39, No. 11, pp.1–21.

Atzori, L., Iera, A. and Morabito, G. (2010) 'The internet of things: a survey', *Computer Networks*, Vol. 54, No. 15, pp.2787–2805.

AVISPA – A Tool for Automated Validation of Internet Security Protocols [online] http://www.avispa-project.org (accessed September 2017).

Baar, M., Köppe, E., Liers, A. and Schiller, J. (2007) 'Poster abstract: the scatterweb msb-430 platform for wireless sensor networks', in *Contiki Workshop '07*.

Blanchet, B. and Smyth, B. (2011) *Proverif: Automatic Cryptographic Protocol Verifier User Manual and Tutorial* [online] http://scholar.google.com/scholar (accessed September 2017).

Chen, C., He, D., Chan, S., Bu, J., Gao, Y. and Fan, R. (2011) 'Lightweight and provably secure user authentication with anonymity for the global mobility network', *International Journal of Communication Systems*, Vol. 24, No. 3, pp.347–362.

Das, A.K. (2015) 'A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks', *Wireless Personal Communications*, Vol. 82, No. 3, pp.1377–1404.

Das, A.K. (2016) 'A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks', *Peer-to-peer Networking and Applications*, Vol. 9, No. 1, pp.223–244.

Das, A.K. and Goswami, A. (2013) 'A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care', *Journal of Medical Systems*, Vol. 37, No. 3, pp.1–16.

Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D. and Schreier, G. (2010) 'The internet of things for ambient assisted living', in *2010 Seventh International Conference on Information Technology: New Generations (ITNG)*, IEEE, pp.804–809.

Dolev, D. and Yao, A.C. (1983) 'On the security of public key protocols', *IEEE Transactions on Information Theory*, Vol. 29, No. 2, pp.198–208.

Dworkin, M. (2001) *Recommendation for Block Cipher Modes of Operation, Methods and Techniques*, Technical Report, DTIC Document.

Eastlake III, D. and Hansen, T. (2006) *Rfc 4634-us Secure Hash Algorithms (sha and hmac-sha)*, Motorola Labs and AT&T Labs.

El Maliki, T. and Seigneur, J-M. (2007) 'A survey of user-centric identity management technologies', in *The International Conference on Emerging Security Information, Systems, and Technologies, SecureWare 2007*, IEEE, pp.12–17.

Farash, M.S., Turkanović, M., Kumari, S. and Hölbl, M. (2016) 'An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment', *Ad Hoc Networks*, Vol. 36, No. P1, pp.152–176.

Gope, P., Amin, R., Islam, S.H., Kumar, N. and Bhalla, V.K. (2017) 'Lightweight and privacy-preserving RFID authentication scheme for distributed iot infrastructure with secure localization services for smart city environment', *Future Generation Computer Systems*, Vol. 83, No. C, pp.629–637.

Gope, P. and Hwang, T. (2016) 'A realistic lightweight anonymous authentication protocol for securing real-time application data access in wireless sensor networks', *IEEE Transactions on Industrial Electronics*, Vol. 63, No. 11, pp.7124–7132.

Hsiang, H-C. and Shih, W-K. (2009) 'Weaknesses and improvements of the yoon-ryu-yoo remote user authentication scheme using smart cards', *Computer Communications*, Vol. 32, No. 4, pp.649–652.

Jiang, Q., Ma, J., Lu, X. and Tian, Y. (2015) 'An efficient two-factor user authentication scheme with unlinkability for wireless sensor networks', *Peer-to-Peer Networking and Applications*, Vol. 8, No. 6, pp.1070–1081.

Khemissa, H. and Tandjaoui, D. (2015) 'A lightweight authentication scheme for e-health applications in the context of internet of things', in *2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, IEEE, pp.90–95.

Khemissa, H. and Tandjaoui, D. (2016) 'A novel lightweight authentication scheme for heterogeneous wireless sensor networks in the context of internet of things', in *2016 Wireless Telecommunications Symposium (WTS)*, IEEE, pp.1–6.

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M. and Carle, G. (2013) 'DTLS-based security and two-way authentication for the internet of things', *Ad Hoc Networks*, Vol. 11, No. 8, pp.2710–2723.

Li, M., Lou, W. and Ren, K. (2010) 'Data security and privacy in wireless body area networks', *Wireless Communications*, IEEE, Vol. 17, No. 1, pp.51–58.

Mangle, A. and Patel, S.C. (2014) 'Issues in user authentication using security questions', *International Journal of Information and Computer Security*, Vol. 6, No. 4, pp.383–407.

Martinez-Julia, P. and Skarmeta, A.F. (2013) 'Beyond the separation of identifier and locator: building an identity-based overlay network architecture for the future internet', *Computer Networks*, Vol. 57, No. 10, pp.2280–2300.

Medaglia, C.M. and Serbanati, A. (2010) 'An overview of privacy and security issues in the internet of things', in *The Internet of Things*, pp.389–395, Springer, New York, NY.

Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. (2012) 'Internet of things: vision, applications and research challenges', *Ad Hoc Networks*, Vol. 10, No. 7, pp.1497–1516.

Moedersheim, S., Drielsma, P. et al. (2005) *Avispa Project Deliverable d6. 2: Specification of the Problems in the High-level Specification Language* (accessed September 2017).

Morris, T. (2011) 'Trusted platform module', in *Encyclopedia of Cryptography and Security*, pp.1332–1335, Springer, Boston, MA.

Odelu, V., Das, A.K. and Goswami, A. (2015) 'A secure and efficient ECC-based user anonymity preserving single sign-on scheme for distributed computer networks', *Security and Communication Networks*, Vol. 8, No. 9, pp.1732–1751.

Omiyi, E., Bür, K. and Yang, Y. (2008) *A Technical Survey of Wireless Sensor Network Platforms, Devices and Testbeds*, Technical Report.

Ozdemir, S. and Xiao, Y. (2009) 'Secure data aggregation in wireless sensor networks: a comprehensive overview', *Computer Networks*, Vol. 53, No. 12, pp.2022–2037.

Patel, M. and Wang, J. (2010) 'Applications, challenges, and prospective in emerging body area networking technologies', *IEEE Wireless Communications*, Vol. 17, No. 1, pp.80–88.

Perkins, C., Johnson, D. and Arkko, J. (2011) *Mobility Support in ipv6*, Technical Report.

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A. and Ylianttila, M. (2014a) 'Pauthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed iot applications', *International Journal of Distributed Sensor Networks*, Vol. 10, No. 7, pp.357–430.

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A. and Ylianttila, M. (2014b)'Two-phase authentication protocol for wireless sensor networks in distributed iot applications', in *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, IEEE, pp.2728–2733.

Rescorla, E. and Modadugu, N. (2012) *Datagram Transport Layer Security Version 1.2* [online] https://tools.ietf.org/html/rfc6347 (accessed September 2017).

Roman, R., Najera, P. and Lopez, J. (2011) 'Securing the internet of things', *Computer*, Vol. 44, No. 9, pp.51–58.

Roman, R., Zhou, J. and Lopez, J. (2013) 'On the features and challenges of security and privacy in distributed internet of things', *Computer Networks*, Vol. 57, No. 10, pp.2266–2279.

Safkhani, M. and Bagheri, N. (2016) *Passive Secret Disclosure Attack on an Ultralightweight Authentication Protocol for Internet of Things*, Technical Report, Cryptology ePrint Archive, Report 2016/838 [online] http://eprint.iacr.org/2016/838 (accessed August 2017).

SEC4 (2013)*SEC4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)*, version 0.97, August [online] http://www.secg.org (accessed August 2017).

Shen, J., Chang, S., Shen, J., Liu, Q. and Sun, X. (2018) 'A lightweight multi-layer authentication protocol for wireless body area networks', *Future Generation Computer Systems*, Vol. 78, No. P3, pp.956–963.

Sicari, S., Rizzardi, A., Grieco, L. and Coen-Porisini, A. (2015) 'Security, privacy and trust in internet of things: The road ahead', *Computer Networks*, Vol. 76, pp.146–164.

Simplicio, M.A., de Oliveira, B.T., Margi, C.B., Barreto, P.S., Carvalho, T.C. and Näslund, M. (2013) 'Survey and comparison of message authentication solutions on wireless sensor networks', *Ad Hoc Networks*, Vol. 11, No. 3, pp.1221–1236.

Sood, S.K. (2016) 'Advanced dynamic identity-based authentication protocol using smart card', *International Journal of Information and Computer Security*, Vol. 8, No. 1, pp.11–33.

Szczechowiak, P., Oliveira, L.B., Scott, M., Collier, M. and Dahab, R. (2008) 'Nanoecc: testing the limits of elliptic curve cryptography in sensor networks', in *Wireless Sensor Networks*, pp.305–320, Springer, Berlin, Heidelberg.

Tewari, A. and Gupta, B. (2016) 'Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for iot devices using rfid tags', *The Journal of Supercomputing*, Vol. 73, No. 3, pp.1085–1102.

Turkanović, M., Brumen, B. and Hölbl, M. (2014) 'A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion', *Ad Hoc Networks*, Vol. 20, pp.96–112.

von Oheimb, D. (2005) 'The high-level protocol specification language HLPSL developed in the EU Project AVISPA, in *Proceedings of APPSEM 2005 Workshop*, pp.1–17.

Wang, D. and Wang, P. (2014) 'On the anonymity of two-factor authentication schemes for wireless sensor networks: attacks, principle and solutions', *Computer Networks*, Vol. 73, No. C, pp.41–57.

Wood, A.D., Stankovic, J. et al. (2002) 'Denial of service in sensor networks', *Computer*, Vol. 35, No. 10, pp.54–62.

Wu, F., Li, X., Sangaiah, A.K., Xu, L., Kumari, S., Wu, L. and Shen, J. (2017) 'A lightweight and robust two-factor authentication scheme for personalized healthcare systems using wireless medical sensor networks', *Future Generation Computer Systems*, Vol. 82, pp.727–737.

Xue, K., Ma, C., Hong, P. and Ding, R. (2013) 'A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks', *Journal of Network and Computer Applications*, Vol. 36, No. 1, pp.316–323.