Journal of Information Security and Applications 000 (2017) 1–16

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A lightweight biometrics based remote user authentication scheme for IoT services

Parwinder Kaur Dhillon*, Sheetal Kalra

Department of Computer Science and Engineering, Guru Nanak Dev University, Regional Campus, Jalandhar, Punjab, 144001, India

ARTICLE INFO

Article history:
Available online xxx

Keywords:
Biometrics
IoT services
Key agreement
Remote user authentication
Security

ABSTRACT

User authentication is becoming crucial in the accelerating Internet of Things (IoT) environment. With IoT several applications and services have been emerging in the areas such as, surveillance, healthcare, security, etc. The services offered can be accessed through smart device applications by the user from anywhere, anytime and anyplace. This makes security and privacy critical to IoT. Moreover, security is paramount in IoT, to enable secure access to the services; multi-factor based authentication can provide high security. In this paper, a lightweight biometric based remote user authentication and key agreement scheme for secure access to IoT services has been proposed. The protocol makes use of lightweight hash operations and XOR operation. The security analysis proves that it is robust against multiple security attacks. The formal verification is performed using AVISPA tool, which confirms its security in the presence of a possible intruder.

1. Introduction

IoT envisions a future networking paradigm and service infrastructure in which spatially distributed physical objects will be widespread deployed to form information networks to facilitate advanced and intelligent services. This network of physical objects will include sensors, actuators, RFID tags or mobile devices, possessing the capability to sense, monitor and collect data about the user environment [1]. Using data collected by the devices, intelligent and ubiquitous services can be facilitated for the users such as surveillance, health care, security, traffic management, etc. IoT services enable interactions of the devices with the real world. Due to above scenarios, several applications for smart devices are being developed to access services offered by IoT networks. By combining IoT networks with smart devices, numerous suitable IoT services can be provided to users. For example, Lockitron can lock and unlock doors through Smartphone [2]. Likewise, most of the IoT services can be monitored and controlled through smart device applications. However, this brings with it adverse underlying effects such as invasion of privacy and information leakage. Moreover, due to the large number of applications in smart devices, these devices often store vital personal information about the user. As a result, attackers are expanding the scope of their attacks beyond the existing Internet environment into smart devices so as to extract the stored user information [3-6]. Furthermore, IoT services that are running in the background, track location based information about the user about which he/she may or may not be aware of. Such background applications might cause serious privacy issues in case if the user forgets to terminate them. On the other hand, some IoT services might record personal information about the user in the background, for example; the patient health monitoring service might track critical health factors without notifying its user. This, in turn, leads to several security problems to sensed data exchanged by *things* such as confidentiality, authenticity and integrity [7,8].

Fig. 1 shows the IoT environment, how remote users can access the different nodes of an IoT network through smart device applications. Remote users can access IoT services through smart device applications in order to connect to any node or sensing element in an unattended IoT environment. Once connected, the user can access desired information from specific nodes. This makes remote user authentication very crucial in IoT networks so that only legitimate users can access IoT nodes while using any service on his/her smart device [9,10]. Because nodes or sensors in IoT networks are resource constrained in terms of processing power, memory requirements, etc., adding resourceful gateway nodes that can support the constrained nodes or sensors, can provide quick on-demand delivery of data or information and take care of most of the processing.

Authentication has three different factors that symbolize user's identity, namely, *something user has* (ownership factor, e.g., smart cards, smart phones, tokens, etc.), *something user knows* (knowledge factor, e.g., passwords) and *something user is* (inherence factor

* Corresponding author.
E-mail address: parwindhillon@gmail.com (P.K. Dhillon).

http://dx.doi.org/10.1016/j.jisa.2017.01.003
2214-2126/

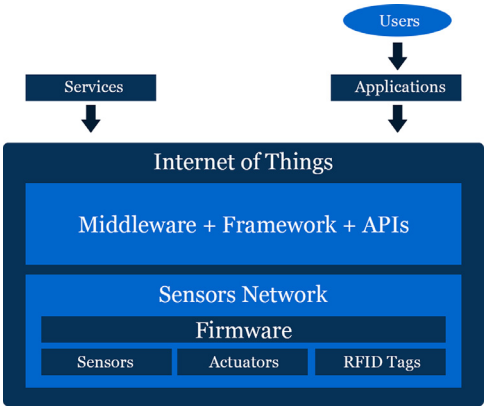

Fig. 1. Relationship between nodes and IoT.

e.g., fingerprint, iris scan, etc.) [11,13–16]. Traditional user authentication schemes are predominantly based on knowledge factor such as passwords. However, the last few years have witnessed that the Single Factor Authentication (SFA) approaches based on passwords alone are easy to breach and hence insufficient to guarantee security. Therefore, incorporating a second factor based on user's personal biometric traits can enable development of a stronger authentication scheme. Also, for user's ease and many security implications researchers have proposed several smart card based authentication protocols using biometric to provide increased security [17–19]. Adding biometrics offer several advantages such as hard to forge or distribute, cannot be lost or forgotten, difficult to copy, etc. Biometrics offers a scalable factor for strong user authentication that many organizations can use to keep them, and their users safe. Also, the speed with which "things" are getting connected to the Internet makes multi-factor authentication a viable solution for ensuring the security and privacy in IoT networks.

Kuo et al. [12] pointed following five characteristics of Biometrics:

- *Universal*: Biometrics is a universal trait possessed by every individual.
- *Distinctive*: Each individual possess distinct biometric features.
- *Persistent*: Biometric features never vary over time.
- *Collectable*: Biometric features can be measured or acquired easily using available devices, such as, fingerprint recognizer, etc.
- *Unique*: Biometric features are distinctive to each individual.

Several key requirements for developing an effective remote user authentication scheme for IoT networks include:

- *Lightweight security solution*: The nodes in the IoT networks are resource constrained in terms of processing power, battery backup, memory, speed, etc. Hence, a lightweight security solution is needed.
- *Key agreement*: A secure shared session key needs to be established between sensor nodes and the user outside the IoT network.
- *Mutual authentication*: For a secure authentication scheme both the communication parties need to be sure of the legitimacy of each other.
- *Multi-factor authentication*: Single factor schemes based only on passwords are easier to break, therefore, adding a second factor based on personal biometric can increase the security of the scheme.

The remaining paper is organized as follows. Section 2 gives an overview of the related work. Section 3 presents IoT security issues for better understanding of the topic. The proposed protocol, multi-factor biometric based mutual authentication and key agreement scheme for secure access of IoT services between the users and nodes is presented in Section 4, which is followed by the security and performance evaluation in Section 5. Section 6 concludes the paper.

2. Related work

2.1. IoT security protocols

Several studies and surveys have been conducted by several researchers relevant to the security in the IoT. Atzori et al. [3] performed a study on authentication, data integrity and privacy issues in the IoT, mostly in RFID systems and sensor networks. An ARM compliant framework for handling security and privacy in IoT-enabled smart buildings has been proposed by Hernández-Ramos et al. [6]. In order to achieve a high level of security in smart buildings, the authors have presented authentication and authorization mechanisms to access offered services. Gigli and Koo in [11] categorized IoT services on the basis of application of service into four types viz. Identity-Related Services, Information Aggregation Services, Collaborative-Aware Services and Ubiquitous Services. Li and Zhou [21] have presented various security issues for IoT. They have proposed a security architecture in which IoT security is analyzed from three dimensions, i.e., the security services, network layer and security domain. In [22], Ma et al. has discussed three main goals of IoT. Based on these goals he presented main challenges and key scientific problems that occur during IoT deployment. Thoma et al. in [23] performed a survey on usage for different IoT services and IoT service oriented architecture. In the survey they found the lack of a rational definition and categorized of IoT services, and presented a formal definition of IoT services and also gave a classification of IoT services on how a physical entity relates to its life cycle. Singh et al. [24] discussed different internet applications, services and also, proposed a model for IoT using the Semantic Fusion Model. In the proposed architecture, the authors introduced how smart semantic framework can help gathering information from sensor networks and encapsulating it for further processing. Zanella et al. [25] discussed a reference framework for urban IoT and presented a survey of technologies and protocols necessary for acceptance of urban IoT by local governments. Weber et al. [26] has highlighted the privacy risks associated with the use and access of data in IoT. They also suggested key elements that must be considered while formulating new rules and regulatory policies for ensuring security and privacy of data. A survey of several already existing IP-based Internet security protocols in wireless sensor networks that are suitable for use in IoT environments have been conducted by Nguyen et al. [27]. Ren et al. [28] studied several lightweight and attack-resistant security solutions for WSNs and IoT. These protocols have been analyzed to identify various IoT security requirements and challenges. They also classified the studied protocols based on the key bootstrapping approach. Wang et al. [29] conducted a thorough survey of different security and privacy issues of wireless sensor networks, which are relevant to IoT scenarios. The study identifies different constraints and requirements against IoT networks at different layers. They also proposed key management systems in WSN using cryptographic primitives. Kumar and Patel [30] gave a general description of diverse security threats and privacy issues encountered during processing, storage and transmission of data and information.

All these studies and surveys generally focus on identification of several challenges in IoT security and different security threats present in the IoT environments. However, since the advent of the IoT, researchers have proposed several solutions and protocols for handling security and privacy in IoT environments.

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

2.2. User authentication protocols

Numerous biometrics based remote user authentication schemes have been proposed for providing secure network access. Most of the schemes concentrate on the establishing a cryptographic key between the user and the base station or the gateway node.

Lee et al. [17] presented a multi-factor authentication scheme based on smart-card and fingerprint. The scheme required no password table searches to authenticate registered users. However, the cryptanalysis performed in [18–20] suggests that the scheme is vulnerable to conspiring attacks and masquerade attacks. Lin and Lai [19] proposed an improved version of the protocol scheme given by Lee et al. [17] to make the protocol secure to masquerade attacks, however, Khan and Zhang in [20] performed a cryptanalysis and found that the scheme does not provide mutual authentication and is also susceptible to server spoofing attacks. Chen et al. [31] proposed a highly secure two-factor user authentication and session key establishment scheme for Wireless Sensor Networks (WSN). They also studied main attacks and security needs of two-factor authentication. The proposed scheme is also resistant to stolen smart-card attack. Das and Goswami in [32] reviewed the security of An's scheme [33] and proposed a robust anonymous biometric-based remote user authentication scheme using smart cards. They conducted informal and formal security analysis to prove the security of the proposed scheme against all possible known attacks including the attacks found in An's scheme [33]. A systematic approach based on three factors - password, smart-card and biometrics for authenticating clients has been proposed by Huang et al. [34]. Kothmayr et al. [35] proposed two-way security architecture for the IoT. Authentication is carried out during a fully authenticated Datagram Transport Layer Security handshake. The proposed architecture offers message integrity, confidentiality and authenticity with reasonable energy, end-to-end latency and memory overhead. However, the proposed scheme has the drawback that the proposed architecture only supports IT, DTCT, SSR, and PP partially. Li et al. [37] reviewed Xue et al. [46] biometric-based remote user authentication protocol and proposed an improvement of Das's user authentication scheme. The proposed scheme uses only hash function and the XOR operation. The proposed multi-factor scheme offers mutual authentication and uses biometric, password as well as random nonces generated by the user and server. A biometric and smart card based remote user authentication scheme with a relatively lower computational cost has been proposed by Li et al. [36]. The multi-factor scheme uses one-way hash function, biometric verification and smart cards. Liao and Hsiao [38], the authors proposed an ECC-based mutual authentication, RFID scheme integrated with ID-verifier transfer protocol. The proposed scheme satisfies confidentiality, anonymity, forward secrecy and scalability. Ndibanje et al. [39] reviewed Jing et al.'s [40] authentication scheme for internet and their analysis showed that Jing et al.'s [40] protocol has a high cost during message exchange and the protocol lacks security. They proposed improvements to Jing et al.'s protocol to eliminate the weaknesses found. Their protocol offers user anonymity, mutual authentication, and secure session key establishment. The performance and security analysis showed resistant against popular attacks and the proposed protocol achieves better efficiency at low communication cost. Saied et al. [41] reviewed existing key establishment protocols, and assessed their applicability to the IoT paradigm. They also proposed lightweight collaborative key establishment scheme for the Internet of Things. De et al. [42] investigated the application of elliptic curve cryptography on constrained devices and performed a cost comparison between two key establishment schemes ECDH– ECDSA and Kerberos. They conclude that Kerberos is 95 times less costly than ECDH–ECDSA on a MICAz sensing platform. Turkanovic et al. [43] proposed a user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks. Their scheme allows remote users to securely share a secret session key to sensor node. Yao et al. [44] proposed an electrocardiogram-signal-based key establishment protocol to secure the communication between every sensor and the control unit. The uniqueness of ECG provides long, random, distinctive and temporal variant keys. They have applied biometric encryption technique to achieve the mutual authentication and derive a non-linkable session key between every sensor and the control unit. The correctness of the proposed key establishment protocol is formally verified based on SVO logic. The protocol provides data confidentiality, authenticity and integrity. He et al. [45] and Xue et al. [46] the authors presented a user authentication and key agreement schemes for WSN. The protocol allows a remote user to effectively and securely connect to the nodes of a WSN. Hummen et al. [52] conducted evaluation of the public-key cryptography on the certificate-based DTLS handshake and identified the different memory (RAM and ROM) requirements. They established a testbed and conducted the analysis of memory requirements.

The security requirements for connected embedded devices in IoT are different due to the restricted memory, limited processing power, small memory and low computing speed. By using the processing power of cloud computing servers, even the most secure authentication scheme can be hacked. Hackers can read, intercept, modify or remove communication messages.

3. Security in IoT environment

IoT is on the threshold of transforming the existing Internet into a fully integrated Future Internet (FI), fuelled by the presence of devices enabled by open wireless technologies such as Bluetooth, radio frequency identification (RFID), Wi-Fi as well as embedded sensors and actuator nodes [4]. IoT brings new challenges in cryptographic security, credentialing and identity management. The existing cryptographic techniques require improvements for applicability in IoT. Credentialing also poses significant challenges in the current Internet and these challenges will expand with the increasing number of smart devices [6]. As the number of connected things increases, the risk of vulnerabilities and data breaches also increases because connecting tens of billions of devices quickly escalates the prospective attack surface for attackers. This has led security and data privacy to take center stage in IoT environments. The IoT is built on different technologies, including power management, devices, sensors and microprocessors. Therefore, the performance and security requirements will differ a great deal from one application to another. Existing security strategies are not sufficient enough to guarantee the basic security level in the IoT devices due to the resource constrained nature of IoT devices. In case of machine-to-machine communications, smaller embedded devices possess no capabilities to maintain certificates. This makes securing the IoT environment more challenging. Security mechanisms devised for IoT environments must provide users with a high level of protection, and at the same time they must not be difficult to implement in small resource constrained embedded devices in IoT networks [7].

One of the most difficult and crucial aspect of any cryptographic security protocol is key management. Although several Internet protocols have been deployed with manual keys or pre-shared keys, the manual configuration of session keys in IoT devices is difficult. Moreover, due to the large number of devices having limited user interfaces, it becomes difficult to deploy meaningful security information using manual configuration. Even if the devices can be manually keyed on initial deployment, automated re-key after deployment is necessary. Hence, automated key management has

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

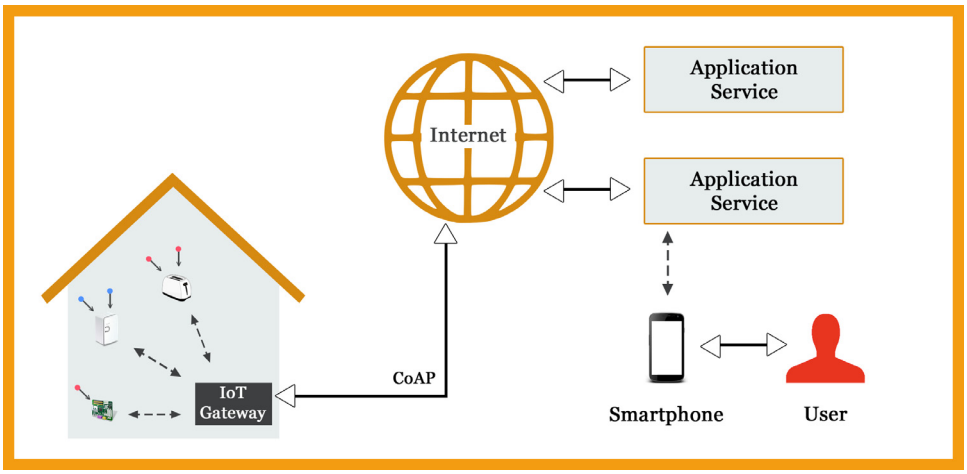

Fig. 2. Authentication model of proposed user authentication scheme.

always been a challenge, but it becomes more crucial in IoT networks.

3.1. Network scenario

Based on the application areas, the assumed network scenario for the proposed user authentication scheme is shown in Fig. 2, where users can communicate with different nodes in IoT environment, in order to obtain desired information or service. Xue et al. [46] gave five basic authentication models for Wireless Sensor Networks (WSNs). In out of the five models except for one, the user first contacts the gateway node to initiate the key agreement process. For our proposed scheme, we have selected the fifth model to fit into the notion of IoT networks. It becomes crucial in IoT networks to decrease the transmission and communication costs because the nodes in IoT are constrained in resources. Once the user and the nodes successfully authenticate each other the communication can start, without requiring the need to first connect to gateway node, thereby ensuring a more straightforward approach. The proposed network scenario has a user-centric view and consists of several heterogeneous devices ranging from highly constrained devices to powerful devices, such as the Cloud in which the IoT service can reside. The user uses his smart device to access the IoT service through an application to gain access to IoT devices through internet or cloud server. Each user in the system owns and accesses one or more IoT nodes using his/her smart device.

There are four main components in an IoT network:

a) The Thing: The "*Thing*" can be a sensor node, actuator or an RFID tag.
   - A *sensor node* also called a mote is a node in an IoT network which can process, gather sensitive information and communicate with other connected nodes or users in the network.
   - An *actuator,* is a device which responds through a physical action by converting an electrical control signal into an action through which an agent acts upon the physical environment.
   - *Radio-Frequency IDentification (RFID) Tags,* are tiny electronic devices having a small chip and an antenna. The chip can carry 2000 bytes of data approximately. The RFID device has a unique identity for an object and can be read by scanning using the RFID reader.

b) The *Local network,* which includes a gateway node, which translates proprietary communication protocols to Internet Protocol.

c) The *Internet*

d) *Back-end services*, enterprise data systems, or PCs and mobile devices.

Security and privacy in IoT networks are critical, as the nodes are mostly in unattended environments [27]. Any remote user can access any IoT service from the network. The IoT node and the gateway node need to be totally assured of the legitimacy of the user, since he/she can access nodes data or might send commands to the nodes. Also, user needs that both the IoT node and gateway node are legitimate; so that the attacker cannot masquerade as node and transmit wrong data.

3.2. Authentication and session key exchange in IoT

Authentication lies at the core of any security protocol. It allows the communicating entities to prove the identity of each other and exchange session keys. Whenever a user needs to access any device from the IoT network, the authentication process is initiated based on the identity information of the user or the device. The authentication process is generally divided into two parts:

a) **Authentication phase:** During this phase, the two entities establish the identity of each other and ensure only the legitimate entity can access the network.

b) **Key establishment phase:** During this phase, secure session keys are exchanged by the communicating entities. A session key is a single-use symmetric key used to encrypt all messages transferred in one communication session. Similar to all cryptographic keys, session keys must be computed in a way that they are impossible to guess by an attacker. Whenever any control information needs to be exchanged between nodes and/or user it must be done in an encrypted and secure manner. For that reason, key agreement is needed to generate a secure shared session key to guarantee the security and privacy of the communication before any information exchange begins.

3.3. Threat model

Since the devices in IoT networks are always present in unattended environments, it becomes necessary to consider all the situations in which devices may be compromised. From the security strength point of view assumptions of the existence of a stronger adversary will result in stronger security guarantee, which is a prerequisite for certain critical applications, such as smart grids,

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

healthcare, smart homes. Similar to the Internet, there exist following security threats in the IoT networks exists:

a) **Eavesdropping attack:** It refers to the process of listening to an ongoing communication, which is an initial step for launching the other attacks. Such attacks are easier to perform on unprotected wireless channels, because the communication takes place in an open insecure wireless channel.
b) **Impersonation attack:** This attack occurs when an illegal user pretends to be a legal entity by replaying a genuine message intercepted from a previous successful communication.
c) **Man-in-the-middle attack:** This attack occurs when the adversary silently listens to the communication of two legal parties with the intent to delay, alter or delete messages exchanged during communication. Such attacks are mostly present within the context of Public Key Cryptography (PKC). In case of PKC, the adversary does not try to break the keys of the communicating parties, rather it tries to become the falsely trusted man-in-the-middle. This is achieved by replacing the exchanged session key with its own. Thereby each of the parties establishes a secure channel with the adversary, who gains access to messages in plaintext.
d) **Denial of Service attack:** The DoS attack hinders the availability of a system offering services. During this attack the illegal entity consumes the resources exhaustively, thereby making the system unavailable to the legal entities. This attack is generally achieved by launching resource consuming activities. Such an attack becomes vital for constrained devices in IoT networks, where the resources are already limited.
e) **Stolen smart device attack:** The user's smart device is a tamper-resistant device. If the smart device of a user is lost or stolen, an attacker can retrieve all the sensitive information stored in the stolen smart device's memory using the power analysis attack. Then, using this retrieved information, the attacker can retrieve other secret information of the communicating parties.
f) **Parallel session attack:** In this attack the illegitimate entity might start multiple parallel runs of the protocol using information captured from the initial successful runs of the protocol.
g) **Password change attack:** In this attack, the attacker can try a series of password change attempts correlated with a successful password change.
h) **Gateway node bypassing attack:** The illegitimate entity can bypass the legal gateway node and get connected to an IoT node without performing the authentication process.
i) **Offline guessing attack:** Any illegal entity can acquire passwords using a "Brute-force" attack to guess the passwords. Using offline guessing mode the attacker can steal the password file or can guess the passwords easily.

3.4. Security requirements

While designing an authentication protocol several security requirements must be considered which are discussed in this section.

a) **Mutual authentication**: It refers to a two-way authentication process wherein both parties involved in a communication authenticate each other. This is one of the most crucial requirements for IoT authentication for enabling secure communication. It is required to eliminate spoofing and mimicking attacks.
b) **Confidentiality:** This requirement means that the secret information must be transmitted securely during all communications between the communicating parties. For that reason, the communicating parties must exchange all information in an encrypted form so as to ensure confidentiality, so that only they can recognize it.
c) **Anonymity:** This requirements enforces that the attacker should not be able to get access of the information of a legal party. If the attacker gets access to the information he/she can easily get access into the system and even pass the authentication process.
d) **Availability:** This requirements enforces the check that the server or the nodes must be continuously available to the user to access information or send commands to the nodes, as and when required.
e) **Forward secrecy:** It is necessary the protocol generates random public key each session without using a deterministic algorithm. With this requirement the compromise of one message cannot compromise other messages.
f) **Scalability:** This requires that device authentication scheme should be scalable enough to dynamically add nodes as and when required. With IoT the number of devices getting connected will increase with time, hence the computational workload should not get affected much by this increase. However, if the computational load increases, it means the protocol lacks scalability.
g) **Attack resistance:** To guarantee secure communication within the IoT network, the authentication process should be secure against several potential attacks, such as replay attacks, masquerade attacks, spoofing attacks, man-in-the-middle attacks, etc.

4. Proposed protocol

The proposed multi-factor biometric user authentication consists of four phases:

Phase 1: User registration phase
Phase 2: Login phase
Phase 3: Authentication phase
*Phase 4:*Password change phase

Table 1 summarizes the notations used in the protocol.

4.1. Preliminaries

In this section, we have discussed one-way hashing and perceptual hashing, which are used in the proposed protocol.

4.1.1. One-way hash function

A one-way hash function also called a message digest takes a variable length string as input, and generates a fixed-length n-bits string. A hash function can be applied to the fingerprint of a file, a message, or other data blocks. The fundamental property of one-way hash function is that its output is very sensitive to even a slight change in input. The process is hard to reverse, i.e., given the hash value and the hash function, it is impossible to find the input value. The hash functions produce hash values of 128 bits and higher. Table 2 shows various lightweight hashing algorithms along with power consumption and technology values [51].

4.1.2. Perceptual hashing

When using biometrics for user authentication schemes, the standard encryption or hashing algorithms cannot be used to encrypt the biometric template. This is because biometric data, e.g., fingerprint scanning, voice, etc. changes with time and environment. To resolve this issue, researchers have suggested using perceptual hashing (P-Hash) [47]. Hashing refers to computing a digest value from the input data. The digest value is a short binary string

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

Table 1
Notations.

Notation	Description
Ui	User
Nj	IoT node
GW	Gateway node
Xg	Secret parameter known only to the gateway node, GW
Xgu	Secret parameter shared with the user by the gateway node. Initiated during user's registration phase
Xgn	Shared secret parameter known to IoT node exchanged during the deployment phase
IDi	Unique identity of the users
PWi	Strong user password
Bi	User personal biometric information e.g., fingerprint, etc.
ri, rj	secret random nonces used by the user and the IoT node, for calculating masked user password and masked node identity
ei,fi	Stores the password masked with identity andStores the biometric masked with the identity
MPi	User's masked password
MIi	Masked identity of user
MBi	User's masked Biometric
SIDj	Regular sensor node's identity
MNj	Masked nonce of the sensor node
RMPj	Masked password of sensor node XOR-ed with the masked nonce
TS1,TS2,TS3,TS4,T	Timestamps used
△T	Permissible time interval for the allowed delay
UNi	User calculated parameter which is sent to gateway node via IoT node. Used to check the validity of the user.
UZi	User calculated parameter which is sent to IoT node. Used for masking the user's session key portion.
Aj	Used to mask xj of node so that the gateway node is valid or not.
Fij	Computed by the GW and used by the sensor node to get the Ki from Zi.
Hj	Used by the IoT node to validate gateway node.
Si	Calculated by the gateway node GW to validate the sensor node and gateway node GW.
Rij	Calculated by the IoT node to mask the node's session key.
SK	Shared session key generated using secret information from the user and IoT nodes.
||	Concatenation operation
⊗	XOR operation
H(.), h(.)	One way irreversible Hash Operation, perceptual hashing operation

Table 2
Hash functions and its characteristics [51].

Algorithm	Area (GE)	Mean power (μW)	Technology (μm)
Spongent	738	1.57	0.13
Photon-80	865	1.59	0.18
Keccak	1300	–	0.13
D-quark	1702	3.95	0.18

referred to as a hash value. Perceptual hashing technique generates a hash value dependent on the multimedia content and it remains approximately the same if the content is not significantly modified. The P-Hash value is compact representation of the original biometric. This hash algorithm offers the advantage that they can handle the quality and format differences, i.e., the binary representation does not matter anymore; the same content always maps to the same hash value. The size of the hash value generated by perceptual hashing varies from 64 bits to 128 bits. The process is shown in Fig. 3.

4.2. User registration phase

After deployment of the IoT network, two separate registration phases are needed, separately for the registration between gateway node and sensor node. The second registration is needed between the user and gateway node.

4.2.1. Registration between the user Ui and the gateway node GW

During this phase, the user who wishes to access IoT service through his/her smart device application will need to register itself with the Gateway Node (GW). Once the user is registered with the gateway node he can on demand access the IoT service provided by the corresponding sensor nodes. The user executes the authentication phase to generate a shared session key which is used for secure communication. In addition, on successful registration, the user can mutually authenticate with the IoT network and the nodes of the network. The phase is explained in Fig. 4.

The following steps are used by the user, Ui, to carry out the registration process with the gateway node, GW, and with IoT nodes:

- **Step 1:** The user, Ui, generates his/her identity, IDi, password, PWi, personal biometric, Bi, and also generates a random number, ri.
- **Step 2:** The user, Ui, next computes the masked password using MPi = H(ri || PWi).
- **Step 3:** User, Ui, computes a masked identity MIi = H(ri || IDi).
- **Step 4:** User, Ui, computes a masked biometric using perceptually hashing MBi = h(ri||Bi). Then, the user sends

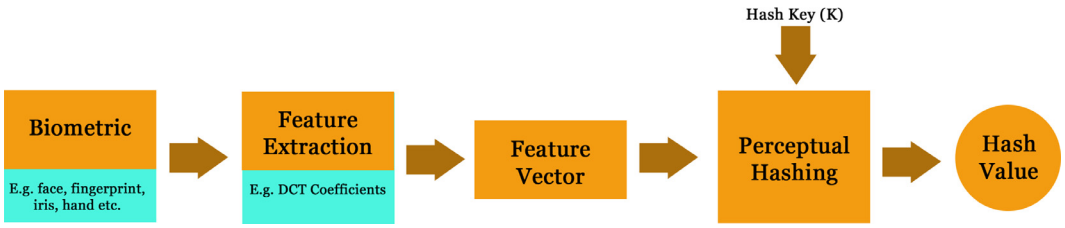

Fig. 3. Perceptual hashing process.

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

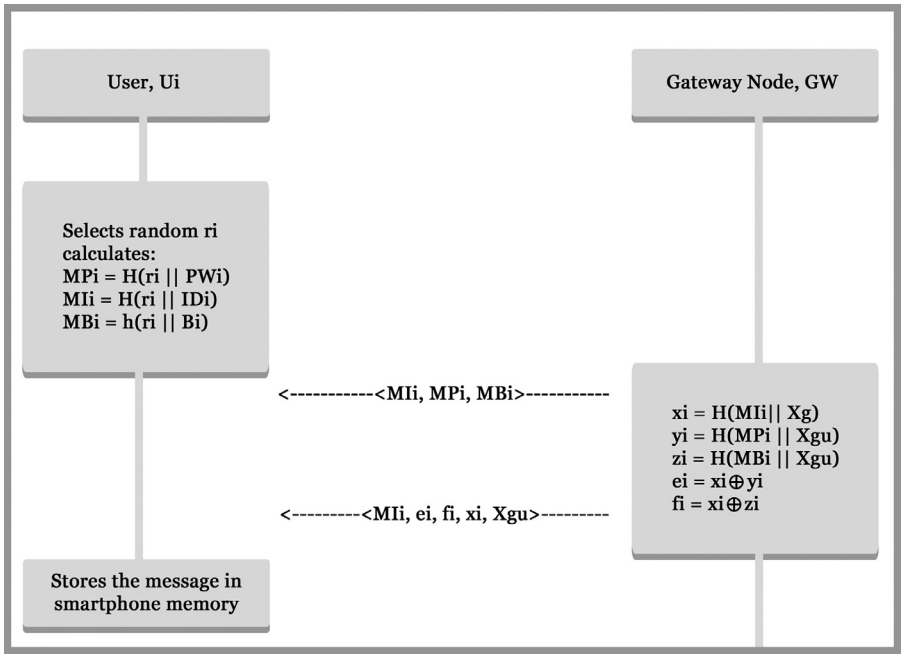

Fig. 4. Registration phase of user with the gateway node.

<MIi,MPi,MBi> as a request message to the gateway node, GW, via a secure channel.

- **Step 5:** On receiving MIi, MPi and MBi from user, Ui, the gateway node, GW, calculates xi = H(MIi||Xg), yi = H(MPi||Xgu) and zi = H(MBi||Xgu).
- **Step 6:** The gateway node, GW, then computes ei = fi ⊗ xi and fi = zi ⊗ xi.
- **Step 7:** The gateway node, GW, sends to the user, Ui's, the computed parameters: <MIi,ei,fi,Xgu>.
- **Step 8:** The User, Ui, receives the parameters and stores them into smart device's memory.

4.2.2. Registration between the IoT node Nj and the gateway node GW

The second registration phase performs the registration of the IoT nodes with the gateway node, GW. This process is also needed for the adding nodes dynamically to the network because the IoT network can grow dynamically with IoT devices being added at any point of time. The process is depicted in Fig. 5. Following steps are performed during registration of IoT node, Nj, with the gateway node, GW.

- **Step 1:** The IoT node, Nj, chooses a random number, rj.
- **Step 2:** The IoT node has a shared secret of the gateway node, GW, Xgn and unique identity, NIDj. It calculates MPj = H(Xgn||rj||NIDj) and MNj = rj ⊗ Xgn.
- **Step 3:** Next, it calculates RMPj = MPj⊗MNj.
- **Step 4:** The IoT node then sends <NIDj,RMPj, MNj,TS1> to the gateway node, GW, through open insecure wireless channel.
- **Step 5:** Next, the gateway node checks for timestamps |TS1-T|< △T, and calculates MPj=RMPj⊗MNj. If the time at which the gateway node received the message is less than the time interval for transmission delay △T, it means the message has not been intercepted and the gateway node proceeds further. Otherwise, the registration phase terminates indicating intrusion by illegitimate entity.
- **Step 6:** The gateway node uses the shared password-key, Xgn, and the received parameter MNj to compute rj*=MNj⊗Xgn.
- **Step 7:** Next, the gateway node using received NIDj, shared secret, Xgn, computes MPj* = H(Xgn|| rj*||NIDj).
- **Step 8:** Next, the gateway node checks if MPj = MPj*. If they are equal, the IoT node, Nj, is legitimate. Otherwise, the gateway node terminates any further operation and sends a denial message to the IoT node, Nj.
- **Step 9:** The gateway node, GW, computes xj = H(NIDj || Xg) and yj = H(MPj || Xgn) and also calculates yj=H(MPj || Xgn) and ej = yj ⊗xj and sends <ej, xj,TS2> via an insecure open wireless channel to the IoT node Nj.
- **Step 10:** On receiving the <ej,xj,TS2> from the gateway node, GW, the IoT node, Nj, checks |TS2-T|< △T to check for any interception or retransmission of any previously intercepted message. If the difference in the received timestamp, TS2, and current timestamp, T, is within the defined transmission delay, △T, it indicates the received message has not been intercepted and the node stores ej, xj and TS2 into smart device's memory.

4.3. Login phase

Once the registration of user, Ui, is accomplished, the user can connect to any desired node within the IoT network through authentication phase. To begin with the authentication phase, user needs to first login into desired IoT service application such as health monitoring, smart home monitoring, etc. on his/her smart device. The proposed scheme uses biometrics and password for user to register and authenticate. Fig. 6 shows login phase of the proposed scheme. The user, Ui, needs to perform following steps in order to send login request message to IoT node, Nj, for authentication purpose:

- **Step 1:** The user, Ui, opens up the IoT service application, enters the identity IDi*, password PWi* and his/her biometric Bi*. The smart device then calculates perceptual hash of input biometric MBi* = h(Bi*||ri) and MPWi* = H(PWi*||ri).
- **Step 2:** The smart device then calculates yi* = H(MPi*||Xgu) and zi* = H(MBi*||Xgu).
- **Step 3:** Next, it calculates original values of yi and zi as yi = xi⊗ei, zi = xi⊗fi.
- **Step 4:** It then checks whether the original yi and zi values are the same as calculated yi* and zi*, i.e., if yi = yi* and zi = zi*. If

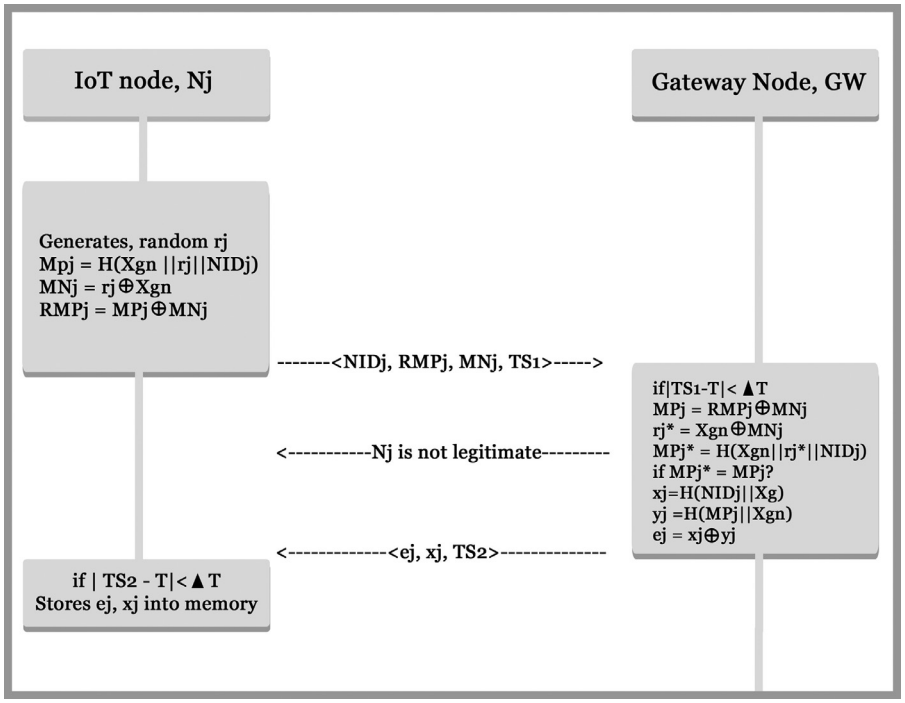

Fig. 5. Registration phase of IoT node with the gateway node.

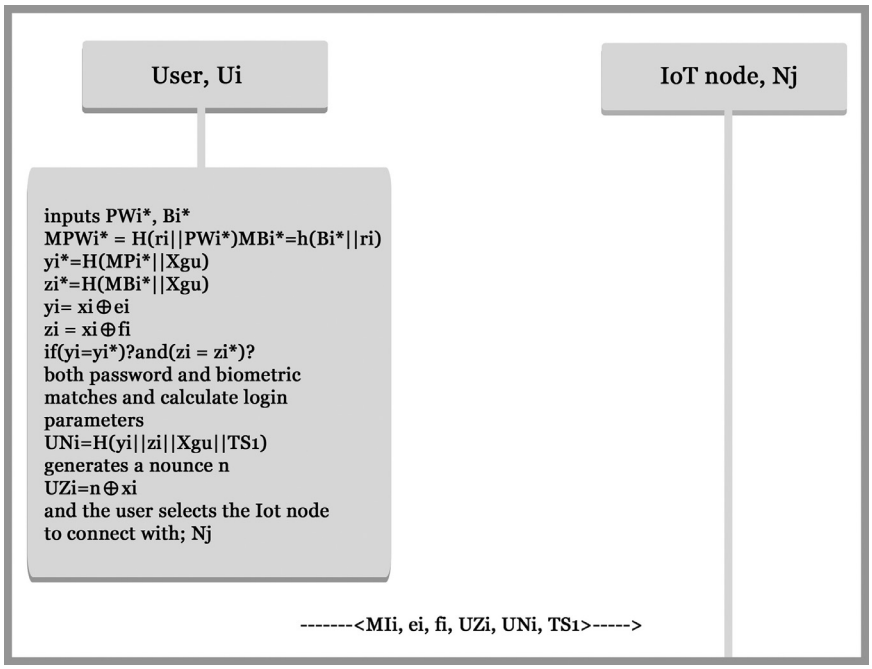

Fig. 6. Login phase of proposed authentication scheme.

both the conditions hold, the user passes the verification process and proceeds further. Otherwise, the user provided either invalid password or invalid biometric information or both and login process is terminated.

- **Step 5**: If the verification is cleared, it computes UNi=H(yi||zi||Xgu||TS1) and a random nonce n is generated. Next, UZi = $n \otimes$xi is computed. The nonce, n, is used for generating the shared session key with the chosen IoT node. Finally, the user, Ui,chooses a IoT node, Nj, providing the respective service and transmits the message via an unsecure channel to the IoT node < MIi, ei, fi UZi, UNi,TS1>.

4.4. Authentication phase

In order to access any IoT service provided by any node, the user will send the authentication message request to desired node within the IoT network and not the gateway node, GW. During this phase, the user and the node in the IoT network generates a one-time use shared secret session key. Once negotiated, they can use the session key to communicate securely in an encrypted manner. The proposed protocol mutually authenticates remote user and the IoT node. Since the user can directly connect with any node in the IoT network, therefore, it needs to be validated by IoT node using

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

gateway node, GW. The steps for the authentication phase are as follows:

- **Step 1:** The user sends authentication message <MIi, ei, fi,UZi, UNi, TS1> to the IoT node, the node, Nj, then checks whether the timestamp value, TS1, received, is greater than the current time stamp, i.e., |T1-T| < △T, this check avoids replay attacks. If the condition holds, the process begins, otherwise it is terminated.
- **Step 2:** Using the stored values ej and xj, the node calculates yj = ej ⊗ xj.
- **Step 3:** Next, the node computes Aj = H(Xgn||TS1||TS2)⊗yj, Aj will be used for mutually authenticating the node, Nj and Gateway node, GW. The node then sends the message <MIi,ei,fi,UNi,NIDj,ej,Aj,TS2,TS1> to the gateway node.
- **Step 4:** Now, the gateway node, GW, will use the received message parameters to authenticate the user and send the user, Ui's authenticity status to the node. The node passes the parameters passed by the user, Ui, directly to the gateway node, GW. The node also passes its identity, NIDj, along with the message. The timestamp values TS1 and TS2 are used to prevent the message replay attack by the attacker.
- **Step 5:** The gateway node, GW, will next check for the received timestamp, TS2, i.e., whether |TS2-T| < △T, where T is the present timestamp. If the condition fails, the gateway node, GW, will terminate the next action and will send a rejection message to IoT node, Nj. If the condition holds, the gateway node, GW, will calculate xj*=H(NIDj||Xg).
- **Step 6:** The gateway node, GW, will next calculate yj* = ej⊗xj*. Also, the gateway node, GW, will calculate its own yj = Aj ⊗ H(Xgn||TS1||TS2). Now, it will check for the equality of yj* and yj, i.e., yj = yj*, if they are equal, the gateway node will authenticate the node, Nj, as a valid registered node from the IoT network. If the condition fails, the gateway node, GW, will terminate the process, because node, Nj, failed to prove its authenticity. The gateway node, GW, will then send authentication failed message to the node, Nj.
- **Step 7:** On successful authentication of the node by the gateway node, GW, it will next calculate xi* as xi* = H(MIi||Xgn). Then, it calculates yi* = ei⊗xi* and zi* = fi⊗xi*. Using xi* and yi* the gateway node computes Qi = H(yi*||Xgu||TS1||zi*). Qi is used by the gateway node to authenticate the user Ui.
- **Step 8:** The gateway node, GW, checks whether the received UNi is same as the calculated Qi, i.e., Qi = UNi, if the condition holds, the gateway node, GW, will successfully authenticate the user, Ui, and continues with the process. However, if the condition fails, the gateway node, GW, will terminate the process and sends an authentication failed message as the user is not registered under it. In this case, the node Nj will further terminate its process and sends a 'failed authentication' message to the user, Ui.
- **Step 9:** On successful verification in step 8, the gateway node, GW, computes Pij = xi*⊗H(xj*||Xgn) to be used by the node, Nj, to derive the value of the nonce, *n*, generated by the user, Ui, during the login phase. Then, Hj, will be calculated to be used by the node, Nj, to verify the authenticity of the gateway node, GW, and resist any impersonation attacks Hj= H(xj*||Xgn||TS1||TS2||TS3). Also, the gateway node, GW, computes Vi = H(Qi||TS1||TS2||TS3) to be sent to the user, Ui, to check the authenticity of the gateway node, GW, and the node Nj. The gateway node GW then sends the authentication parameters to the node Nj <Pij,Hj,Vj,TS1,TS2,TS3>.
- **Step 10:** After receiving the message from the node Nj, the user, Ui, firstly checks whether |TS4-T|<△T. If the condition fails, the user terminates the authentication phase and sends a denial message to the node Nj, thereby avoiding replaying of the messages.
- **Step 11:** If the condition holds, the user, Ui, checks for the equality of Vi = H(H((ei⊗xi)||TS1)||TS1||TS2||TS3). If the condition holds, then the user, Ui, confirms the authenticity of gateway node, GW, and the node, Nj. It will then generate the session key. If the condition fails, the user, Ui, will terminate the authentication phase and will send a denial message to the node, Nj, as either the gateway node, GW, or the node, Nj, is illegitimate.
- **Step 12:** On receiving the message <Pij,Hj,Vi,TS1,TS2,TS3> IoT node Nj will check if Hj=H(xj||Xgn||TS1||TS2||TS3)? If the condition holds, node Nj will compute xj*=Fij⊗H(xj||Xgn) and n=UZi⊗xj*.
- **Step 13:** IoT Node Nj will generate a nonce 'm' and computes Rij=H(xj*||NIDj||TS1||TS2||TS3||TS4)⊗m and computes session key SK=H(n⊗m).
- **Step 14:** IoT node Nj will send the authentication message <Rij,Nj,TS1,TS2,TS3,TS4,Vi> to the user.
- **Step 15:** On successful verification in step 14, the user, Ui, extracts the nonce value of the node, Nj as: n = Rij⊗ H(xi||NIDj||TS1||TS2||TS3||TS4). Finally, the user Ui can compute the final session key SK = H(m⊗n) and the authentication phase terminates successfully.

Fig. 7 shows the authentication phase of the proposed authentication scheme.

4.5. Password-change phase

For security reasons the user must periodically update his/her password. The proposed biometric and password based scheme allows the user to easily change his/her password. Fig. 8 shows the password change process of the proposed scheme. The steps needed to change user's password are:

- **Step 1:** The user, Ui, opens up the IoT application on his smart device and enters his/her old password PWi* and biometric Bi*.
- **Step 2:** The user calculates masked password MPi* = H(ri||PWi*) and masked biometric using perceptual hash function MBi* = h(ri||Bi*). Then, the user calculates yi* = H(MPi*||Xgu) and zi* = H(MBi*||Xgu).
- **Step 3:** The user retrieves the stored ei and fi values from the smart device memory and calculates original yi = xi ⊗ei and zi = xi⊗fi.
- **Step 4:** The user then checks for the equality of yi with yi* and zi with zi*, i.e., yi = yi* and zi = zi*. If either of the condition fails, the user failed to input correct information, i.e., password and biometric information, and the process is terminated.
- **Step 5:** If both conditions hold then the user is a legitimate one and the smart device IoT application asks the user, Ui, to input his/her new password.
- **Step 6:** The user then inputs the new password NPWi and calculates the new masked password NMPi = H(ri||NPWi). It also calculates new version of nyi = H(NMPi||Xgu).
- **Step 7:** The user then can calculate the new ei as nei = xi⊗ nyi.
- **Step 8:** Finally, the user replaces the old ei stored in the smart device memory with nei and the phase terminates successfully.

5. Security analysis

Security is essential for any authentication scheme. This section presents the informal security analysis of the proposed scheme. The proposed scheme establishes a secure key, provides mutual authentication, ensures password protection and is resistant to several attacks discussed in the threat model.

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

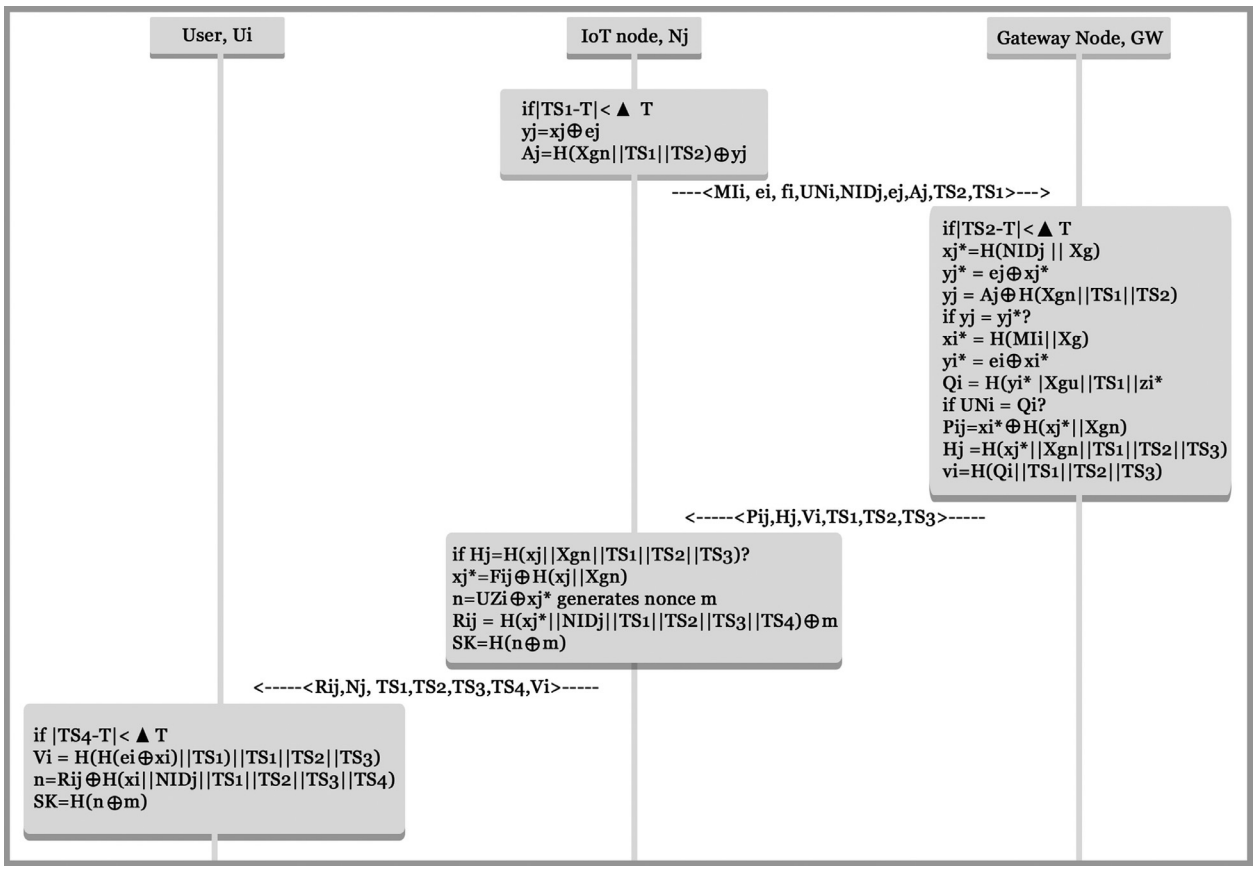

Fig. 7. Authentication phase between user, IoT node and gateway node.

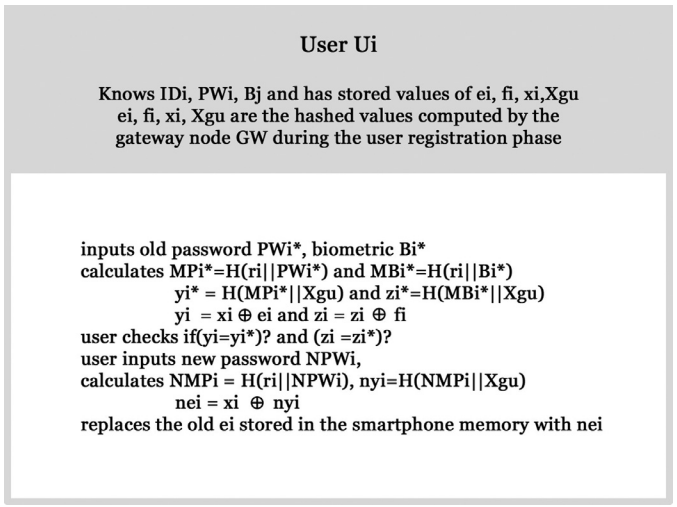

Fig. 8. Password change phase of proposed authentication scheme.

5.1. Security analysis and system requirement analysis

Nodes in IoT are resource-constrained pervasive devices. They are small in terms of size and computational ability. For this reason, it is essential to analyze the performance of the proposed authentication scheme to ensure that the operating cost is minimal. Such an analysis can be done based on various criteria including computational cost, memory requirements and communication overhead.

5.1.1. Key agreement

A session key is agreed upon between the user, Ui, and node, Nj, using a key agreement protocol. In the proposed scheme, both the user, Ui, and node Nj independently and individually generate a shared session key. Both user and node compute the same session key SK=H(n⊗m). The session key is communicated securely through open wireless channel; hence, it uses masked nonces. In the proposed scheme, only the authentic user, Ui, and node, Nj, can find out the nonces, proving the security of the key.

5.1.2. Security to stolen smart device attacks

Assume that the smart device of user, Ui, is lost or stolen. Having the smart device, the attacker can still retrieve all the sensitive information stored in the stolen device's memory using the power analysis attack . Thus, it is assumed that the attacker knows the information <MIi,ei,fi,xi,Xgu>. In fact, the user, Ui's, identity, IDi, is not stored directly in the memory; it is stored in masked form. Furthermore, to guess the password, PWi, of exact, *n,* characters from yi, the attacker has to guess the identity, IDi, of exact m characters and the biometric key, Bi. In addition, the attacker has no way to obtain Bi from zi due to secure perceptual hashing of the original biometric with the secret random ri, and also ri is not communicated across the channel. Hence, the proposed scheme is secure against smart device stolen attacks.

5.1.3. Security against replay attack

Assume that the attacker intercepted the transmitted messages < MIi,ei,fi,UZi,UNi,TS1> either during login phase or <MIi,ei,fi,UNi,NIDj,ej,Aj,TS2,TS1> during the authentication phase of a previous session. The attacker starts a new session with the login request message < MIi', ei',fi',UZi', UNi',TS1'> the process will

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

terminate, because during every transmission the proposed protocol verifies the timestamps.

5.1.4. Security against impersonation attacks

In the proposed scheme, the attacker might try to imitate itself to the gateway node. The proposed authentication scheme is resistant to such attacks, because even if an illegal user eavesdrops on a legal transmitted message and retransmits it to the IoT node, still he/she can not calculate the session key. Moreover, the attacker needs to provide the biometric information of the user which is impossible for the attacker to impersonate. Assume that the attacker intercepts the transmitted messages < MIi, ei, fi UZi, UNi,TS1> during the login phase and <MIi,ei,fi,UNi,NIDj,ej,Aj,TS2,TS1> during the authentication phase. To start a new session, the attacker will have to modify the login request message UNi to UNi‘=H(xi‘||Xgu‘||TS1‘) and UZi to UZi‘= n‘⊗xi‘. The attacker's attempt to login will fail at the gateway node, GW, as UNi‘ will not match with Qi computed during authentication phase.

5.1.5. Security against man-in-the-middle attack

Assume that the attacker intercepts the transmitted messages < MIi, ei, fi UZi, UNi,TS1> during the login phase, and <MIi,ei,fi,UNi,NIDj,ej,Aj,TS2,TS1> during the authentication phase. The attacker modifies the login request message to < MIi‘,ei‘, fi‘, UZi‘, UNi‘,TS1‘>. The attacker can only pass the authentication if he/she successfully computes UNi‘=H(xi‘||Xgu‘||TS1‘) using the shared secret value Xgn and xi. The probability of successfully guessing Xgn and xi is very low. As a consequence, the attacker can not alter all the transmitted messages during the login and authentication phases and hence, the proposed scheme is secure against man-in-the-middle attacks.

5.1.6. Security against offline guessing attacks

An off-line dictionary attack occurs whereby a malicious user can find out the passwords of other legitimate users using the intercepted messages of previous communications. Assume that an attacker tries to extract secret information by interrupting all communicated messages < MIi, ei, fi UZi, UNi,TS1> during the login phase and <MIi,ei,fi,UNi,NIDj,ej,Aj,TS2,TS1> during the authentication phase. If the attacker can guess Xgu, MPi and MBi correctly, he/she can compute UNi and UZi. However, the probability to guess both is very negligible. On the other hand, if it is assumed that the smart device of a user is lost or stolen, then also it is clear that this is a computationally infeasible problem for the attacker to derive the password PWi and personal biometrics Bi of the user Ui. Thus, the proposed scheme is also secure against offline guessing attacks.

5.1.7. Security against denial-of-service attacks

The proposed scheme, the user, Ui, is secure against denial of service. This is possible because he user receives a confirm or reject message from the node which allows the user to know that the response message was authentic. Besides, the use of timestamps in the scheme mitigates any momentous request. Consequently, the proposed scheme is resistant against DoS attacks.

5.1.8. Security against parallel session attacks

Suppose an attacker intercepts the login request message < MIi, ei, fi UZi, UNi,TS1> during the login phase and wants to initiate a parallel session. This attack is not possible, because in the proposed scheme the user's personal biometric information is used for login and authentication.

Table 3
Comparison of computational cost of proposed scheme with other schemes.

Authentication scheme	User	Node	Gateway node/server
Proposed scheme	$\mathbf{8T_h}$	$\mathbf{6T_h}$	$\mathbf{8T_h}$
An et al. [3]	$4T_h$	$5T_h$	$6T_h$
Chen et al. [12]	$4T_h$	$1T_h$	$5T_h$
Das et al. [13]	$5T_h+1T_{E/D}$	$4T_h+1T_{E/D}$	$2T_h+1T_{D/E}$
Turkanovic et al. [26]	$7T_h$	$5T_h$	$7T_h$
He et al. [31]	$5T_h$	$1T_h$	$5T_h$
Xue et al. [32]	$7T_h$	$6T_h$	$13T_h$

5.1.9. Security against password change attack

An attacker cannot impersonate the personal biometric of a legitimate user to change a user's password. Moreover, even if the attacker gets access to the smart device, to change the password, he/she requires old password. Even if the attacker is able to breach into the smart device and extract secret information stored in it, it is still infeasible know the password PWi and biometric information Bi from the known data. Therefore, the proposed scheme is resilient to password-change attacks.

5.1.10. Security against gateway node bypassing attack

This attack is not possible in the proposed protocol because to access IoT service, the user firstly needs to connect with the node, Nj, in IoT network to start the authentication phase and not the gateway node. The node, Nj, connects with the gateway node, GW, after starting the authentication process by the user, Ui. The node, Nj, passes the authentication process to the gateway node, GW, and it verifies both the node, Nj, and the user, Ui.

5.1.11. User anonymity

The user communicates with the node in IoT network in an open insecure wireless channel. The proposed scheme uses masked identity MIi as unique identification for the user, masked password MPWi and masked biometric MBi thus preventing any private information disclosure in case an attacker tries to intercept the communication.

5.1.12. Mutual authentication

Mutual authentication occurs when all the parties involved in communication mutually authenticates each other. In the proposed scheme, all three parties viz. the gateway node GW, user Ui, and the node nj mutually authenticates each other before beginning the information exchange.

5.2. Computation and communication cost analysis

In this section, the cost analysis of the proposed scheme with other related authentication schemes is done. The evaluations prove the effectiveness of the proposed scheme. Table 3 summarizes the computational cost analysis of the proposed scheme with the similar schemes proposed by other authors. Table 4 presents the comparison of the proposed scheme on the basis of security features and resistance to popular known attacks on the authentication protocols.

The scheme proposed uses only xor operations and hash computations which makes it a secure and lightweight, thereby providing better performance for resource constrained devices in IoT. Rifa-Pous and Herrera-Joancomartí [50] conducted a thorough analysis on the computational costs of various symmetric, asymmetric, hash chain functions, elliptic curves cryptography. In comparison with the energy costs of symmetric algorithms, the asymmetric cryptography is more expensive. Also, hash functions give a similar throughput as symmetric algorithms and consume low processing power. One way hash function is less expensive as compared to the ECC operations or encryption/decryption operations.

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

Table 4
Comparison of security features of proposed scheme with other schemes.

Security feature	Proposed scheme	An et al. [3]	Chen et al. [12]	Das et al. [13]	Turkanovic et al [26]	He et al [31]	Xue et al. [32]
Mutual Authentication	**Yes**	No	Yes	Yes	Yes	No	Yes
Key agreement	**Yes**	Yes	No	Yes	Yes	No	Yes
Password change	**Yes**	No	No	Yes	Yes	Yes	Yes
User anonymity	**Yes**	No	Yes	No	Yes	Yes	Yes
Replay attack	**Yes**	Yes	No	Yes	Yes	Yes	Yes
Impersonation attack	**Yes**	No	No	No	Yes	No	Yes
Gateway node bypassing attack	**Yes**	No	No	No	Yes	No	Yes
Denial-of-Service attack	**Yes**	Yes	No	Yes	Yes	No	No
Man-in-the-Middle attack	**Yes**	No	No	Yes	Yes	No	No
Password change attack	**Yes**	No	No	No	Yes	No	No
Parallel session attack	**Yes**	Yes	No	No	Yes	No	No
Smart card/ Smart device Stolen attack	**Yes**	Yes	No	No	Yes	No	Yes

Moreover, the size of the hash value generated by both hash operations is 128 bits. The proposed protocol is also resistant to several attacks such as stolen smart device attack, denial-of-service attack, man-in-the-middle attack, etc. The proposed scheme is thus lightweight and provides higher security compared to the other schemes.

6. Formal verification of proposed protocol using AVISPA

AVISPA is a push-button tool developed for analyzing large-scale Internet security protocols and applications. The protocols are coded in a language called the HLPSL (High Level Protocol Specification Language).

HLPSL consists of basic roles that represents different participants and composition of roles for representing scenarios of basic roles. Each role is independent from the other role, getting some initial information by parameters, communicating with the other roles by channels [48]. First, the protocol written in HLPSL is first translated into a lower level specification by a translator called the hlpsl2if, which further generates a specification in an intermediate format called the Intermediate Format (IF). The Output Format (OF) of AVISPA is produced using one of the four back-ends, i.e., OFMC (On-the-fly Model-Checker), SATMC (SAT-based Model-Checker), CL-AtSe (Constraint Logic based Attack Searcher) and TA4SP (Tree Automata based on Automatic Approximations for the Analysis of Security Protocols) [49].

In the implementation, there three basic roles, namely, Alice, bob and gateway, representing the user Ui, the IoT node Nj and the gateway node GW respectively. Fig. 9 shows the specification in HLPSL language for the role of the initiator, the user Ui. The user Ui first receives the start signal and changes its state from 0 to 1 and sends the registration request message <MIi,ei,fi,Xgu> securely to the gateway node GW using the Snd<> operation. In Figs. 10 and 11 depicts the specification in HLPSL language for the role of the IoT node Nj and gateway node GW. The roles for the session, and the goal and environment of the proposed scheme are specified in Figs. 12 and 13. All the basic roles: alice, bob and gateway are instanced with concrete arguments in the session segment. The top-level role (environment) defined in the specification of HLPSL language contains the global constants and a composition of one or more sessions.

The analysis of the OF is made as follows.

- The first section is called SUMMARY which depicts whether the protocol is safe, unsafe, or whether the analysis is inconclusive.
- The second section is called DETAILS which describes the condition on which the protocol is declared safe, or what conditions have been used for finding an attack, or finally why the analysis was inconclusive.

```
role alice(Ui,Nj,GW :agent,
           SKun,SKng,SKug :symmetric_key,
           %H is hash function
           H : hash_func,
           Snd,Rcv: Channel(dy))
played_by Ui
def =
local State :nat,
% variables
MPi,MIi,MBi,IDi,Xgu,Bi,PWi,ri :text,
% message

% protocol id's
subs1,subs2,subs3,subs4,subs5,subs6 :protocol_id

init State:=0
transition
1. State = 0 /\ Rcv(start)=|>
% Registration phase
State' :=1 /\ MPi':= H(ri.PWi)
           /\ MIi':= H(ri.IDi)
           /\ MBi':= H(ri.Bi)
           /\ Snd({MPi'.MIi'.MBi'}_SKug)
           /\ secret({Xgu},subs1,{Ui,GW})
           /\ secret({IDi,PWi,Bi,ri},subs2,Ui)

2. State=1 /\ Rcv({MIi'.ei'.fi'.xi'.Xgu}_SKug)=|>
% Login phase
State':=2 /\ n':=new()
          /\ TS1':=new()
          /\ yi':=xor(xi'.ei')
          /\ zi':=xor(xi',fi')
          /\ UNi':=H(yi'.zi'.Xgu.TS1')
          /\ UZi':=xor(ri',xi')
          /\ Snd({MIi'.ei'.fi'.UZi'.UNi'.TS1'}_SKun)
%Ui has a new randomly generated nonce value n' for node Nj
          /\ witness(Ui,Nij,alice_bob_rb,ri')

3. State:=4 /\ Rcv({Rij'.Nj'.TS1'.TS2'.TS3'.TS4'.Vi'}_SKun)
          /\ Vi':=H(H(xor(ei'.xi').TS1').TS1'.TS2'.TS3'.TS4')
          /\ SK':=H(xor(ri',m'))
%Ui's acceptance of the value m'
          /\ request(Nj,Ui,bob_alice_ra,m')
end role
```

Fig. 9. Role specification in HLSPL for the user Ui of proposed scheme.

- The remaining sections are called PROTOCOL, GOAL and BACK-END, are the name of the protocol, the goal of the analysis and the name of the back-end used, respectively.
- After some possible comments and the statistics, the trace of the attack (if any) is finally printed in a standard Alice-Bob format.

The three different phases of the protocol i.e. Registration, Login and Authentication have been coded using HLPSL language. The roles of the user, IoT node and gateway node are specified by alice, bob and gateway, respectively. Figs. 9 –11 show the code specifica-

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

```
role bob(Ui,Nj,GW :agent,
         SKun,SKng,SKug :symmetric_key,
         %H is hash function
         H : hash_func,
         Snd,Rcv: Channel(dy))
played_by Nj
def=
local State nat,
% variables
MPi,MIi,MBi,IDi,Xgu,Bi,PWi,ri,
xi,Yi,zi,ei,fi:text,
% protocol id's
subs1,subs2,subs3,subs4:protocol_id
init State:=0
transition
% Registration phase of node

init State:=0
transition
1. State=0 /\Rcv(start)=|>
% Registration phase
State':=1 /\ rj':=new()
          /\ TS1':=new()
          /\ MPj':= H(rj'.Xgn.NIDj)
          /\ MNj':= H(rj'.Xgn)
          /\ RMPj':= xor(MPj,MNj)
          /\ Snd({NIDj.RMPj'.MNj'.TS1'}_SKng)
          /\ secret({Xgn},subs3,{Nj,GW})
          /\ secret({NIDj',rj',Xgn},subs4,Nj')

2. State=1 /\ Rcv({ej'.xj'.TS2')_SKngl)=|>
%Login phase

3. State=2 /\ Rcv({MIi'.ei'.fi'.UZi'.UNi'.TS1'}_SKun)=|>
% Authentication Phase
State':= 3 /\ yj'=xor(xj',ej')
           /\ TS1':=new()
           /\ Aj':= xor(H(Xgn.TS1'.TS2'),yj')
           /\ Snd({MIi'.ei'.fi'.UN'.NIDj'.ej'.Aj'.TS2'.TS1'}_SKng)

4.State= 3 /\ Rcv({Pij'.Hj'.Vi'.TS1'.TS2'.TS3'}_SKng)
 State':= 4 /\ xj':=xor(Pij',H(xj'||Xgn)
            /\ ri':=xor(UZi'.xj')
%Nj has a new randomly generated nonce value m' for user Ui
            /\ m':=new()
            /\ Rij':=xor(H(xj'.NIDj'.TS1'.TS2'.TS3'.TS4'),m')
            /\ SK'::=H(xor(ri',m'))
            /\ Snd({Rij'.Nj'.TS1'.TS2'.TS3'.TS4'.Vi'}_SKun)

%Nj's acceptance of the value n'
State':=5  /\ request(Ui,Nj,alice_gateway_ri,n')
end role
```

Fig. 10. Role specification in HLSPL for the node Nj of proposed scheme.

```
role gateway(Ui,Nj,GW :agent,
      SKun,SICng,SKug :symmetric key,
      %H is hash function H : hash_func,
      Snd,Rcv: Channel(dy))
played_by GW
def=
local State :nat,
% variables
MPi,MIi,MBi,IDi,Xgu,Bi,PWi,ri :text,
% protocol id's
subsl,subs2,subs3,subs4,subs5,subs6,subs7:protocol_id

init State:=0
transition
%Registration phase

1. State = 0 /\ Rcv({MPi'.MIi'.MBi'}_SKug)=|>
  State':=1 /\ secret({Xgu},subs1,{Ui,GW})
            /\ secret({IDi,PWi,Bi,ri},subs2,Ui)
            /\ xi':=xor(Mli,Xg)
            /\ yi':=xor(MPi,Xgu)
            /\ zi':=xor(MBi,Xgu)
            /\ ei':=xor(xi',yi')
            /\ fi':=xor(xi',zi')
            /\ Snd({MIi'.ei'.fi'.xi'.Xgu}_SKug)

2. State =1  /\ Rcv({NIDj.RMPj'.MNj'.TS1'}_SKng)
            /\ TS2':=new()
            /\ secret({Xgn},subs3,{Nj,GW})
            /\ secret({NIDj',rj,Xgn},subs4,Nj)
            /\ MPj':=xor(RMPj',MNj')
            /\ rjs':=xor(MNj',Xgn)
            /\ MPjs':= H(Xgn.rjs'.NIDj')
            /\ xj':= H(NIDj.Xg)
            /\ yj':= H(MPj',Xgn)
            /\ ej':=xor(yj',xj')
            /\ Snd({ej'.xj'.TS2'}_SKng)

% login Phase 3
3. State = 2 /\ Rcv({MIi'.ei'.fi'.UNi'.NIDj'.ej'.Aj'.TS2'.TS1')_SKng)=|>
% Authentication Phase
State':= 3   /\ xj':=H(NIDj'.Xg)
            /\ yj':=xor(ej',xj')
         /\ xi':=H(MIi'.Xg)
            /\ yi':=xor(ei,xi')
            /\ Pij'=xor(xi',H(xj'.Xgn))
            /\ Qi':=H(yi'.Xgu.TS1'.zi)
            /\ Hj':=H(xj'.Xgn.TS1'.TS2'.TS3')
            /\ VI':= H(Qi'.TS1'.TS2'.TS3')
            /\ Snd({Pij'.Hj'.Vi'.TS1'.TS2'.TS3'}_Skng)
end role
```

Fig. 11. Role specification in HLSPL for the gateway node GW of proposed scheme.

tion for the three entities- user, IoT node and gateway node. The entities use the SND() operation to send a message to other entity and RCV() operation to receive a message sent by an entity. To start the protocol communication an entity must receive start signal. On receiving the start signal the user changes its state from 0 to 1 and sends <MIi,MPi,MBi> using SND() operation as a request message to the gateway node, GW, via a secure channel. The gateway node, GW, sends to the user, Ui's, the computed parameters <MIi,ei,fi,Xgu> using RCV() operation. The user Ui receives the acknowledgement message <Rij,Nj,TS1,TS2,TS3,TS4> from the node Nj. The Dolev-yao threat model is used as the threat model in the implementation. In this model, the intruder is denoted by i and he/she can analyze, intercept or modify the exchanged messages on an insecure channel. The witness() command is used for performing weak authentication and request() is used for performing strong authentication.

In the implementation of the IoT node role in Fig. 10 using HLPSL language on receiving start signal the node converts its state from 0 to 1. The node sends a registration request message to the gateway node. It first generates a new random nonce rj and computes the various registration parameters. After computing the necessary parameters the node sends the registration request message <NIDj,RMPj, MNj,TS1> to the gateway node, GW, through open insecure wireless channel. The gateway node in return sends <ej,xj,TS2> . For authentication the node receives the message <MIi, ei, fi,UZi, UNi, TS1> from the user Ui which is again forwarded to the gateway node using the SND() operation. The node then receives the message <Pij,Hj,Vj,TS1,TS2,TS3> using RCV() function from the gateway node. On receiving this message the node does its computations and computes the authentication parameters to be sent to the user. The node then transmits a message of the computed parameters to the user, i.e., <Rij,Nj,TS1,TS2,TS3,TS4,Vi>.

The implementation of role for gateway node is shown in Fig. 11 using HLPSL language on receiving start signal the node converts its state from 0 to 1. The gateway node receives the registra-

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

```
role environment()
def=
  const ui,nj,gw:agent
        skun,skng,skug:symmetric_key,
        h : hash_func,
        pwi,bi,xg,exi,idi :text,
        alice_bob_rb,bob_alice_ra,
        subsl,subs2,subs3,subs4,subs5,subs6,subs7:protocol_id
        intruder_knowledge ={ui,nj,gw,h)

composition
          session(ui,gw,nj,skun,skng,skug,h)
        /\ session(ui,gw,nj,skun,skng,skug,h)
        /\ session(ui,gw,nj,skun,skng,skug,h)
end role

goal
        secrecy_of subs1
        secrecy_of subs2
        secrecy_of subs3
        secrecy_of subs4
        secrecy_of subs5
        secrecy_of subs6
        secrecy_of subs7
        authentication_on alice_gateway_ri
        authentication_on bob_gateway_rj
end goal
environment()
```

Fig. 12. Role specification in HLSPL for the goal and environment of proposed scheme.

```
role session(Ui,Nj,GW :agent,
             SKun,SICng,SKug :symmetric key,
             %H is hash function
             H : hash_func)
def=
composition
              alice(Ui,Nj,GW,SKun,SKng,SKug,H)
             /\ bob(Ui,Nj,GW,SKun,SKng,SKug,H)
             /\ gateway(Ui,Nj,GW,SKun,SKng,SKug,H)
end role
```

Fig. 13. Role specification in HLSPL for the session of proposed scheme.

tion request message <MIi,MPi,MBi> from the user. On receiving which it calculates its necessary parameters and sends the message <MIi,ei,fi,Xgu> back to the user.

The gateway node further receives the registration request message of the IoT node <NIDj,RMPj, MNj,TS1> through the RCV() operation. After doing certain computations using XOR and HASH operations, the gateway node sends the registration parameters <ej,xj,TS2> to the IoT node. Later, it receives the authentication message <MIi,ei,fi,UNi,NIDj,ej,Aj,TS2,TS1> from the IoT node. The gateway node again computes the various parameters required to carry out the authentication between the user, IoT node and the gateway node using the basic HASH and XOR operations. It then sends the authentication message <Pij,Hj,Vj,TS1,TS2,TS3> to the IoT node.

Figs. 12 and 13 defines the role for the session, and goal and environment of the proposed scheme. The session section instances three basic roles alice, bob and gateway. The environment role consists of all global constants and a composition of one or more sessions, where the intruder may play some roles as legitimate users. The intruder also participates in the execution of protocol as a concrete session.

In Figs. 12 and 13, the role specification for the environment and session has been shown. In the implementation, the following secrecy goals and two authentications are verified:

- *secrecy_of subs1*: It means that Xgu is kept secret to the gateway node GW and user Ui only.

```
% OFMC
% Version of 2006/02/13
SUMMARY
    SAFE
DETAILS
    BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
    /home/avispa/web-interface-computation/./tempdir/
    workfilevol3NBQKb.if
GOAL
    as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
    parseTime: 0.00s
    searchTime: 0.38s
    visitedNodes: 208 nodes
    depth: 11 plies
```

Fig. 14. Result of analysis using OFMC of proposed scheme.

- *secrecy_of subs2*: It means that PWi, Bi, ri are kept secret to the user Ui only.
- *secrecy_of subs3*: It means that Xgn is kept secret to the gateway node GW and IoT node only.
- *secrecy_of subs4*: It means that NIDj, rj are kept secret to the IoT node Nj only
- *authentication_on alice_gateway_ri*: Ui (Ci) generates a random nonce ri, where ri is only known to user Ui. When the gateway node GW receives ri from the messages from Ui; gateway node GW performs strong authentication for Ui.
- *authentication_on bob_gateway_rj*: IoT node Nj generates a random nonce rj, where rj is only known to Nj. If the gateway node GW receives rj from the messages from Nj; gateway node performs strong authentication for rj.

6.1. Result analysis

Fig. 14 shows the results of simulation of the proposed protocol using On-the-Fly Model-Checker (OFMC). OFMC is so called because it creates an infinite tree from the protocol analysis using a demand-driven mechanism. OFMC employs the use of symbolic techniques for denoting the state-space. Another advantage of using OFMC is that it allows executing a bounded number of sessions of the protocol and also its speed of performing the execution test is very fast. To check out for replay attacks, the back-end conducts runs of the protocol to check whether the authorized agents can execute the proposed protocol by conducting a search for a passive intruder. After that the back-end gives the intruder the knowledge of some normal sessions between the legitimate agents. For the Dolev–Yao model check, the back-end checks whether there is any man-in-the-middle attack possible by the intruder. The "SUMMARY" section provides the analysis of the protocol simulation. It tells whether the protocol is safe, unsafe or if the analysis is inconclusive. From the results section it is clear that the proposed scheme is safe. The next section called "DETAILS" indicates the condition under which the protocol is marked SAFE, or why the protocol was found to be inconclusive or the conditions applied to find an attack. From the results, it can be found that the proposed protocol is and no attack has been found on it.

7. Conclusion

As security breaches are rising, new authentication techniques need to incorporate users' personal biometrics to increase the security of the system. With IoT several applications and services have been emerging in the areas such as, surveillance, health-

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

care, security, etc. Also, the costs of the embedded sensors or smart devices will come down to a point that connectivity will become a standard feature. This makes security and privacy critical to IoT. Since IoT is based on the idea of connected things, the security challenges are huge; therefore, it becomes crucial that the protocols for IoT include necessary amount of security, even if it stretches the capabilities of the devices. In this paper, a lightweight multi-factor remote user authentication protocol has been proposed. The protocol employs gateway node based architecture for IoT environment which requires the user to first register itself through gateway node. Once registered, the user can directly connect to the desired sensor node using his smart device to access any service. The proposed protocol is lightweight, because it uses only one-way hash, perceptual hash functions and XOR operations which are computationally less expensive, thereby, making the protocol highly suitable for the resource constrained devices in IoT. The security analysis proves that it is robust against multiple security attacks. The formal verification is performed using AVISPA tool, which confirms its security in the presence of a possible intruder. In future, we can setup a testbed to find out the memory requirements of the proposed protocol and prove that the proposed protocol is lightweight for real IoT devices.

References

[1] Yan Z, Zhang P, Vasilakos AV. A survey on trust management for internet of things. J Netw Comput Appl 2014;42:120–34. doi:10.1016/j.jnca.2014.01.014.
[2] Teh TY, Lee YS, Cheah ZY, & Chin JJ IBI-mobile authentication: a prototype to facilitate access control using identity-based identification on mobile smart devices. Wireless Pers Commun, pp. 1–18. doi:10.1007/s11277-016-3320-y.
[3] Atzori L, Iera A, Morabito G. The internet of things: a survey. Comput Netw 2010;54(15):2787–805. doi:10.1016/j.comnet.2010.05.010.
[4] Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed security model and threat taxonomy for the internet of things (IoT). In: Recent trends in network security and applications. Springer Berlin, Heidelberg; 2010. p. 420–9. doi:10.1007/978-3-642-14478-3_42.
[5] Cassar G, Barnaghi P, Wang W, Moessner K. A hybrid semantic matchmaker for IoT services. In: Green computing and communications (GreenCom), 2012 IEEE international conference on, November. IEEE; 2012. p. 210–16. doi:10.1109/GreenCom.2012.40.
[6] Hernández-Ramos JL, Moreno MV, Bernabé JB, Carrillo DG, Skarmeta AF. SAFIR: secure access framework for IoT-enabled services on smart buildings. J Comput Syst Sci 2014;81(8):1452–63. doi:10.1016/j.jcss.2014.12.021.
[7] Mayer CP. Security and privacy challenges in the internet of things. Electron Commun EASST 2009;17:1–12. http://dx.doi.org/10.14279/tuj.eceasst.17.208.
[8] Ham HS, Kim HH, Kim MS, Choi MJ. Linear SVM-based android malware detection for reliable IoT services. J Appl Math 2014;2014. doi:10.1155/2014/594501.
[9] Heer T, Garcia-Morchon O, Hummen R, Keoh SL, Kumar SS, Wehrle K. Security challenges in the IP-based internet of things. Wireless Pers Commun 2011;61(3):527–42. doi:10.1007/s11277-011-0385-5.
[10] Henze M, Hermerschmidt L, Kerpen D, Häußling R, Rumpe B, Wehrle K. A comprehensive approach to privacy in the cloud-based internet of things. Future Gen Comput Syst 2016;56:701–18. doi:10.1016/j.future.2015.09.016.
[11] Gigli M, Koo S. Internet of things: services and applications categorization. Adv Internet Things 2011;1(02):27–41. doi:10.1016/j.future.2015.09.016.
[12] Kuo WC, Wei HJ, Chen YH, Cheng JC. An enhanced secure anonymous authentication scheme based on smart cards and biometrics for multi-server environments. In: Information security (AsiaJCIS), 2015 10th Asia joint conference on, May. IEEE; 2015. p. 1–5. doi:10.1109/AsiaJCIS.2015.11.
[13] Choi Y, Nam J, Lee D, Kim J, Jung J, Won D. Security enhanced anonymous multiserver authenticated key agreement scheme using smart cards and biometrics. Sci World J 2014. doi:10.1155/2014/281305.
[14] Liu M, Shieh WG. On the security of Yoon and Yoo's biometrics remote user authentication scheme. WSEAS Trans Inf Sci Appl 2014;11:94–103.
[15] Xu J, Zhu WT, Feng DG. Improvement of a fingerprint-based remote user authentication scheme. In: Information security and assurance, 2008. ISA 2008. International conference on, April. IEEE; 2008. p. 87–92. doi:10.1109/ISA.2008.62.
[16] Yang D, Yang B. A biometric password-based multi-server authentication scheme with smart card. In: Computer design and applications (ICCDA), 2010 international conference on, 5. IEEE; 2010. p. 540–54. doi:10.1109/ICCDA.2010.5541128.
[17] Lee JK, Ryu SR, Yoo KY. Fingerprint-based remote user authentication scheme using smart cards. Electron Lett 2002;38(12):554–5.
[18] Chang CC, Lin IC. Remarks on fingerprint-based remote user authentication scheme using smart cards. ACM SIGOPS Oper Syst Rev 2004;38(4):91–6. doi:10.1145/1031154.1031165.
[19] Lin CH, Lai YY. A flexible biometrics remote user authentication scheme. Comput Stand Interfaces 2004;27(1):19–23. doi:10.1016/j.csi.2004.03.003.
[20] Khan MK, Zhang J. Improving the security of 'a flexible biometrics remote user authentication scheme. Comput Stand Interfaces 2007;29(1):82–5. doi:10.1016/j.csi.2006.01.002.
[21] Li H, Zhou X. Study on security architecture for Internet of Things. In: Applied informatics and communication. Springer Berlin Heidelberg; 2011. p. 404–11. doi:10.1007/978-3-642-23214-5_53.
[22] Ma HD. Internet of things: objectives and scientific challenges. J Comput Sci Technol 2011;26(6):919–24. doi:10.1007/s11390-011-1189-5.
[23] Thoma M, Meyer S, Sperner K, Meissner S, Braun T. On iot-services: survey, classification and enterprise integration. In: Green computing and communications (GreenCom), 2012 IEEE international conference on, November. IEEE; 2012. p. 257–60. doi:10.1109/GreenCom.2012.47.
[24] Singh D, Tripathi G, Jara AJ. A survey of Internet-of-Things: Future vision, architecture, challenges and services. In: Internet of things (WF-IoT), 2014 IEEE world forum on, March. IEEE; 2014. p. 287–92. doi:10.1109/WF-IoT.2014.6803174.
[25] Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. Internet Things J IEEE 2014;1(1):22–32. doi:10.1109/JIOT.2014.2306328.
[26] Weber RH. Internet of things–new security and privacy challenges. Comput Law Secur Rev 2010;26(1):23–30. doi:10.1016/j.clsr.2009.11.008.
[27] Nguyen KT, Laurent M, Oualha N. Survey on secure communication protocols for the Internet of Things. Ad Hoc Netw 2015;32:17–31. doi:10.1016/j.adhoc.2015.01.006.
[28] Ren CX, Gong YB, Hao F, Cai XY, Wu YX. When biometrics meet IoT: a survey. In: Proceedings of the 6th international Asia conference on industrial engineering and management innovation. Atlantis Press; 2016. p. 635–43. doi:10.2991/978-94-6239-148-2_62.
[29] Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. IEEE Commun Surv Tut 2006;8(2):2–23. doi:10.1109/COMST.2006.315852.
[30] Kumar JS, Patel DR. A survey on internet of things: security and privacy issues. Int J Comput Appl 2014;90(11):20–6.
[31] Chen L, Wei F, Ma C. A secure user authentication scheme against smart-card loss attack for wireless sensor networks using symmetric key techniques. Int J Distrib Sensor Netw 2015;2015:63–73. doi:10.1155/2015/704502.
[32] Das AK, Goswami A. A robust anonymous biometric-based remote user authentication scheme using smart cards. J King Saud Univ-Comput Inf Sci 2015;27(2):193–210. doi:10.1016/j.jksuci.2014.03.020.
[33] An Y. Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards. BioMed Res Int 2012;2012. doi:10.1155/2012/519723.
[34] Huang X, Xiang Y, Chonka A, Zhou J, Deng RH. A generic framework for three-factor authentication: preserving security and privacy in distributed systems. Parallel Distrib Syst IEEE Trans 2011;22(8):1390–7. doi:10.1109/TPDS.2010.206.
[35] Kothmayr T, Schmitt C, Hu W, Brunig M, Carle G. A DTLS based end-to-end security architecture for the internet of things with two-way authentication. In: Local computer networks workshops (LCN workshops), 2012 IEEE 37th conference on. IEEE; 2012, October. p. 956–63. doi:10.1109/LCNW.2012.6424088.
[36] Li CT, Hwang MS. An efficient biometrics-based remote user authentication scheme using smart cards. J Netw Comput Appl 2010;33(1):1–5. doi:10.1016/j.jnca.2009.08.001.
[37] Li CT, Weng CY, Lee CC. An advanced temporal credential-based security scheme with mutual authentication and key agreement for wireless sensor networks. Sensors 2013;13(8):9589–603. doi:10.3390/s130809589.
[38] Liao YP, Hsiao CM. A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Ad Hoc Netw 2014;18:133–46. doi:10.1016/j.adhoc.2013.02.004.
[39] Ndibanje B, Lee HJ, Lee SG. Security analysis and improvements of authentication and access control in the internet of things. Sensors 2014;14(8):14786–805. doi:10.3390/s140814786.
[40] Jing L, Xiao Y, Philip Chen CL. Authentication and access control in the internet of things. 2012 32nd international conference on distributed computing systems workshops. IEEE; 2012. doi:10.1109/ICDCSW.2012.23.
[41] Saied YB, Olivereau A, Zeghlache D, Laurent M. Lightweight collaborative key establishment scheme for the internet of things. Comput Netw 2014;64:273–95. doi:10.1016/j.comnet.2014.02.001.
[42] De Meulenaer G, Gosset F, Standaert FX, Pereira O. On the energy cost of communication and cryptography in wireless sensor networks. In: Networking and communications, 2008. WIMOB'08. IEEE international conference on wireless and mobile computing, October. IEEE; 2008. p. 580–5. doi:10.1109/WiMob.2008.16.
[43] Turkanović M, Brumen B, Hölbl M. A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion. Ad Hoc Netw 2014;20:96–112. doi:10.1016/j.adhoc.2014.03.009.
[44] Yao L, Liu B, Wu G, Yao K, Wang J. A biometric key establishment protocol for body area networks. Int J Distrib Sensor Netw 2011;2011:1–10. doi:10.1155/2011/282986.
[45] He D, Gao Y, Chan S, Chen C, Bu J. An enhanced two-factor user authentication scheme in wireless sensor networks. Ad Hoc Sensor Wireless Netw 2010;10(4):361–71.
[46] Xue K, Ma C, Hong P, Ding R. A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks. J Netw Comput Appl 2013;36(1):316–23. doi:10.1016/j.jnca.2012.05.010.

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003

[47] Niu XM, Jiao YH. An overview of perceptual hashing. Acta Electron Sinica 2008;36(7):1405–11.
[48] AVISPA. Automated validation of internet security protocols and applications. <http://www.avispa-project.org/> (accessed November 2015).
[49] AVISPA. AVISPA web tool. http://www.avispa-project.org/webinterface/expert.php/ (accessed November 2015).
[50] Rifa-Pous H, Herrera-Joancomartí J. Computational and energy costs of cryptographic algorithms on handheld devices. Future Internet 2011;3(1):31–48. doi:10.3390/fi3010031.
[51] Manjulata AK. Survey on lightweight primitives and protocols for RFID in wireless sensor networks. Int J Commun Netw Inf Secur 2014;6(1):29–40.
[52] Hummen R, Shafagh H, Raza S, Voig T, Wehrle K. Delegation-based authentication and authorization for the IP-based internet of things. In: 2014 eleventh annual IEEE international conference on sensing, communication, and networking (SECON), June. IEEE; 2014. p. 284–92. doi:10.1109/SAHCN.2014.6990364.

Please cite this article as: P.K. Dhillon, S. Kalra, A lightweight biometrics based remote user authentication scheme for IoT services, Journal of Information Security and Applications (2017), http://dx.doi.org/10.1016/j.jisa.2017.01.003