sustainability

MDPI

Article

Secure and Lightweight Authentication Protocol for Privacy Preserving Communications in Smart City Applications

Sunil Gupta [1], Fares Alharbi [2,*], Reem Alshahrani [3], Pradeep Kumar Arya [4], Sonali Vyas [1], Dalia H. Elkamchouchi [5] and Ben Othman Soufiene [6]

[1] School of Computer Science and Engineering, University of Petroleum and Energy Studies, Dehradun 248007, India; s.gupta@ddn.upes.ac.in (S.G.); svyas@ddn.upes.ac.in (S.V.)

[2] Department of Computer Science, College of Computing and IT, Shaqra University, Shaqra 15526, Saudi Arabia

[3] Department of Computer Science, College of Computers and IT, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia; rashahrani@tu.edu.sa

[4] Department of Computer Science and Engineering, BML Munjal University, Gurgaon 122413, India; pradeep.arya@bmu.edu.in

[5] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia; dhelkamchouchi@pnu.edu.sa

[6] PRINCE Laboratory Research, ISITcom, Hammam Sousse, University of Sousse, Sousse 4000, Tunisia; ben_oth_soufiene@yahoo.fr

* Correspondence: faalhrbi@su.edu.sa

Abstract: A smart city is a concept that leverages technology to improve the quality of life for citizens, enhance sustainability, and streamline urban services. The goal of a smart city is to use data and technology to manage resources and assets efficiently, make informed decisions, and create a more livable and thriving city for its residents. Smart cities rely on a range of technologies including the Internet of Things (IoT), Artificial Intelligence (AI), big data analytics, and cloud computing to gather, process, and analyze data from various sources. The aim is to create a city that is more connected, responsive, and sustainable, and that provides its residents with a better quality of life, opportunities, and services. A secure and efficient message communication protocol for sensitive information and real-time communication is critical for the functioning of a smart city environment. The main findings of this paper are to develop a new authentication protocol that meets the specific requirements and constraints of smart city applications. The message communication between smart cities is conducted with the help of a gateway. The challenge in constructing a working, viable infrastructure for a smart city is to provide secure authentication for message communication between the user and gateway node in one network, and the gateway node of one network to the gateway node of the other network. The objective for doing research to develop an authentication protocol that ensures the privacy and security of data transmitted in smart city applications while maintaining a lightweight and efficient design. This paper proposes a secure authentication protocol and key establishment scheme for access to the application in smart cities to make feasible access through the IoT environment. The proposed protocol ensures the mutual authentication between user and gateways, and the security analysis shows that the proposed protocol is effective against energy consumption and have less computational cost. The performance of the proposed method is analyzed and tested using BAN Logic and AVISPA security verification to confirm the authenticity of the security protocol. We do compare with past studies of which our proposed method outperformed.

Keywords: smart cities; user authentication; BAN logic; AVISPA; security attacks; efficiency

check for updates

Citation: Gupta, S.; Alharbi, F.; Alshahrani, R.; Kumar Arya, P.; Vyas, S.; Elkamchouchi, D.H.; Soufiene, B.O. Secure and Lightweight Authentication Protocol for Privacy Preserving Communications in Smart City Applications. *Sustainability* **2023**, *15*, 5346. https://doi.org/10.3390/su15065346

Academic Editors: Marc A. Rosen, Iqram Hussain, MD Rashedul Hasan Sarker and Md Azam Hossain

Received: 17 February 2023
Revised: 13 March 2023
Accepted: 14 March 2023
Published: 17 March 2023

1. Introduction

Smart cities are cities that use technology and data to enhance the quality of life for their citizens, increase sustainability, and streamline urban services. In terms of symmetry and asymmetry, these concepts can be applied to different aspects of a smart city. Symmetry in a smart city refers to a balanced distribution of resources and services across the city. For example, a symmetrical city would have equal access to healthcare, education, and public transportation regardless of location within the city. In contrast, an asymmetrical city would have an unequal distribution of resources and services, which can lead to disparities between different neighborhoods and populations. In terms of urban planning and design, symmetry can refer to the visual balance of buildings and public spaces, while asymmetry refers to an intentional imbalance in the design of a city. Both symmetry and asymmetry can be used to create aesthetically pleasing and functional cities, but it is important for cities to consider the effects of their design choices on the overall well-being and livability of the city for all its citizens. In smart cities, technology can also be used to achieve symmetry and address asymmetry. For example, smart transportation systems can help distribute resources more evenly across a city by optimizing traffic flow and reducing congestion, while data analysis can be used to identify areas with unequal access to resources and develop solutions to address these disparities [1].

The smart city application will be possible with the help of interconnected IoT devices [2]. Figure 1 shows all networks are connected to the internet through the specific gateway node. The user exchanges the information from one network to another network using the gateway node [3]. Due to the presence of a connected networks environment, it is imperative to implement security for communication between user to gateway, and gateway of one node to the gateway of another node. Moreover, several sensor devices are brought into contact with each other, raising the need for foolproof security for the fair exchange of information. Many protection methods and protocols were applied in different fields and layers of the networks [4], but, in the literature, many authentication protocols are not adequate for smart city application and environment security [5]. Due to the nature of the sensor having limited computational power and battery constraints, a specific and efficient cryptographic protocol is needed in the smart city scenario [6]. Furthermore, due to the heterogeneity of scenarios, a number of attack types are possible. These attacks can degrade the performance of smart cities application [7].

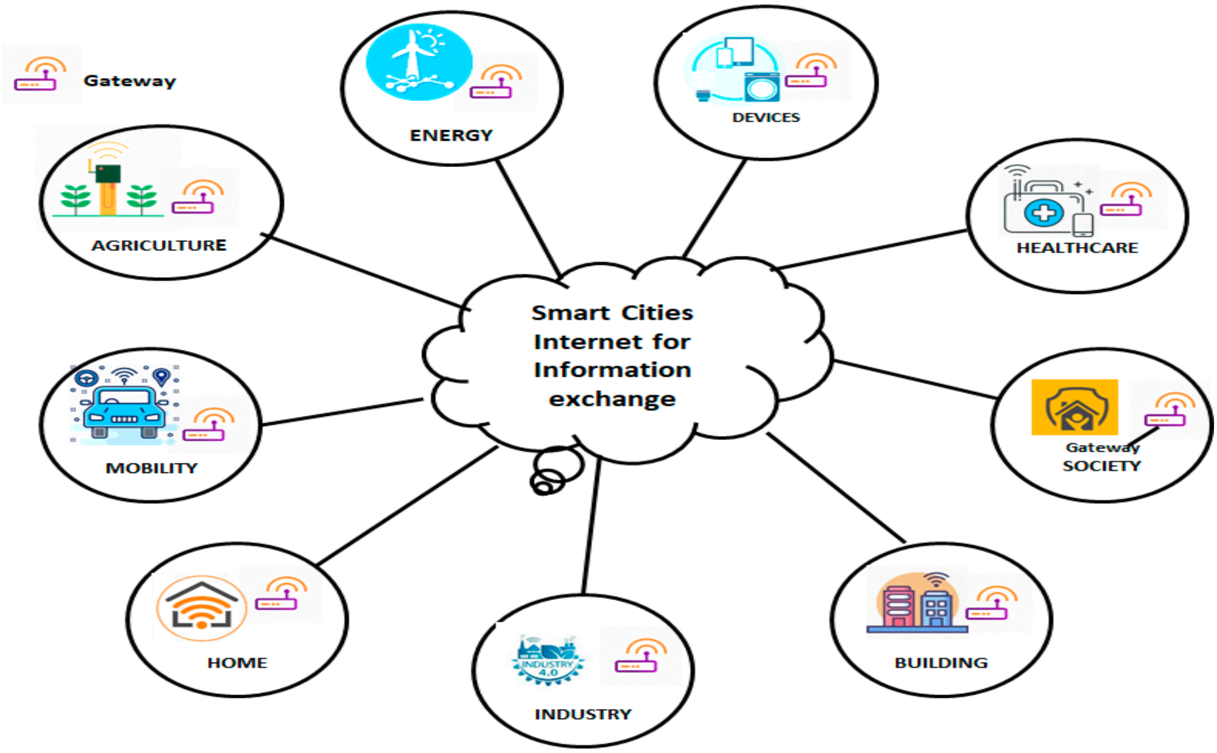


Figure 1. Smart cities model for authentication and key establishment.

The principle of smart cities is associated with the number of security challenges and its requirements; it is necessary to provide a secure environment for the feasible transaction of information. In a smart city, there is communication between users with the gateway using a sensor device for secure authentication from user to gateway, gateway to user, and gateway of one node to another node. There is a need for mutual authentication to communicate each device in this environment. The past studies do not provide the solution of mutual authentication, whereas the present work is based on the authentication with less energy consumption and computational cost.

Following are the contributions given by this paper:

- An authentication protocol and critical exchange for smart cities is presented, and all the possible attacks and challenges are discussed in the paper;
- A proposed authentication protocol is analyzed with the help of Burrows–Abadi–Needham logic (BAN) to show the protocol is proficient and secure;
- The proposed protocol's cryptographic computational cost and energy consumption are calculated to determine the protocol's effectiveness;
- A proposed authentication protocol is simulated using automation validation of the internet security protocol and application (AVISPA) tool to verify the security;
- A proposed authentication protocol is compared with other related work, and the effectiveness in terms of minimization of different types of attacks is demonstrated.

The paper is divided into seven sections. Section 2 provides the related work on authentication protocol for a remote user to access the technology. Section 3 discusses the methodology and various phases to our proposed protocol to provide mutual authentication. Sections 4 and 5 give the detailed security analysis including formal and informal verification. The comparative study is provided in Section 6. This paper is finally concluded in Section 7.

2. Literature Review

Many authentication protocols for sensor networks and communication have been proposed for different active and passive security attacks. These protocols may also deal with smart city authentication frames due to the presence of sensor nodes. The related work uses either symmetric key-based [8] or an asymmetric key-based approach [9]. For multicasting and the broadcasting of communication, symmetric-based public key cryptography is used. Mainly RSA [10] and ECC (elliptic curve cryptography) [11] are used for the sensor-based application. The number of the authentication protocols is based on this category [12–16].

In the literature, different user authentication protocols have been proposed based on smart cards. Turkanovic et al. [17] derived a protocol to provide user authentication for an ad hoc wireless sensor network (WSN). The protocol is lightweight and allows a remote user to generate a key to establish a session and do authentication. However, there is no such evidence that provides mutual authentication between remote users and the gateway. The four-step authentication model was not suitable to fulfill all the requirements such as anonymity and privacy in the network. In 2015 Mishra et al. [18] proposed the use of a password-based authentication. The protocol provides resistance against some known active and passive attacks and maintains user secrecy. In addition, it gives a lot of overhead for gateway nodes and is practically infeasible to implement.

In 2017 Moon et al. [19] provided an improved and efficient password authentication for remote users based on smart card technology. The protocol improved the performance and security functionally but still did not provide user anonymity and was not resistant against hidden gateway node attacks. The spoofing and impersonation attack may also not be ruled out in the alternatives suggested by this aforementioned literature. In 2019, Fatty and Amin proposed a protocol based on the ElGamal cryptosystem to provide security. The author claimed that it is safe against all types of active and passive attacks and provides less computational cost than other protocols [20]. The author claimed that the system overcomes all the other protocols' limitations and provides the authentication framework with a low computational cost [21].

In the year 2020, Basudeb et al. [22] proposed a new biometric-based authentication protocol for smart cities. They allow a registered user to update their password based on biometric authentication. The scheme is robust and dynamically allocates the smart devices to the network. The comparative analysis shows it is secure against all potential attacks. Ghahramani et al. [23] proposed a biometric-based authentication protocol for smart city mobile networks. They remove the time complexity up to 53% in the proposed protocol. Xie et al. [24] proposed a secure authentication protocol for a wireless sensor network in smart cities. They improve the efficiency of resources such as transportation, healthcare, and energy. They use pi calculation-based formal verification to prove the efficiency of the protocol. Xueya et al. [25] proposed an authentication protocol for smart cities. They assure that the protocol provides better privacy and data security for the Internet of Things. They show that the protocol is secure under q-SDM problem and provide better performance than other proposed protocols. Table 1 shows analyses of computational comparison, communication cost, and the challenges in relation with attack possibility in the current authentication protocols.

Table 1. Comparison of communication, computation, and challenges in current authentication protocols.

References	Communication Cost	Computational Cost	Challenges of the Approach, Attacks Possible
[17]	4 messages	$23T_H + 8T_E$	Denial of service attack, privilege attack, ansider attack, untraceability, session key security, no mutual authentication
[18]	3 Messages	$19T_H + 3T_M$	Privilege attack, password guessing attack, untraceability, spoofing attack, no mutual authentication
[19]	4 Messages	$17T_H + 2T_E + 6T_M$	Impersonation attack, anonymity, gateway spoofing attack, sensor spoofing attack, no mutual authentication
[20]	5 Messages	$16T_H + 4T_E + 6T_M$	Password guessing attack, impersonation attack, no mutual authentication
[21]	4 messages	$12T_H + 4T_E + 5T_M$	Anonymity, impersonation attack, denial-of-service attack, no mutual authentication
[22]	3 Messages	$26T_H + 2T_E + 2T_M$	Password guessing attack, anonymity, no mutual authentication
[23]	5 messages	$17T_H + 4T_E + 7T_M$	Denial of service attack, no mutual authentication
[24]	4 Messages	$20T_H + 6T_E + 4T_M$	Impersonation attack, untraceability, no mutual authentication
[25]	4 messages	$10T_H + 7T_E + 11T_M$	Anonymity, impersonation attack, no mutual authentication

On the basis of a sensor tag-based smart healthcare system, Deepak and Al-Turjman [26] suggested a user sign-in authentication approach that leverages single user sign-in for privacy. The protocol's formal verification demonstrates its resistance to denial of service and replay attacks. A lightweight authentication approach for secured computing was put forth by Hammami et al. [27]. To provide a mechanism that establishes the authenticity of the user, the author analyzed the advantages and disadvantages of various protocols. The proposed methodology for supplying security is shown by the author to have lower computational and communication costs. By implementing the concept of multiple keys utilizing the key derivation function for end-to-end encryption and privacy, Masud et al. [28] established a strong and secure access scheme for cloud-based e-healthcare. According to Zhang et al. [29], it is effective to share cloud resources to deliver individualized medical treatment to patients utilizing smart IoT healthcare.

3. Methodology

This section presents the secure authentication protocol and key exchange for access to information in IoT applications. In the Figure 1 scenario, one network user wants to communicate with a user of another network. Authentication is needed between the user to gateways, and gateway 1 to gateway 2 of different network.

The proposed protocol comprises the following seven phases in order to ensure the security and privacy of sensitive information and devices. Firstly, the devices themselves need to be authenticated. This involves verifying that the device is legitimate and authorized to access the network. Secondly, the communication between devices needs to be authenticated. This involves verifying that the data being exchanged are coming from a legitimate device and have not been tampered with in transit. The protocol can be applied to all classes of communication between heterogeneous networks for IoT applications.

1. Setup phase (Gateway);
2. Registration phase (User);
3. Sensor registration phase;
4. Login phase (User);
5. Authentication and key exchange phase (User);
6. Update phase (Password);
7. Revocation phase.

By implementing these various phases of authentication, IoT smart city providers can help to ensure that devices and networks are secure and protected against malicious attacks and unauthorized access. Table 2 shows the notations used in the proposed protocol.

Table 2. Symbolizations used in the paper.

Symbol	**Description**
U_j	User
GW	Gateway
d	Private key of gateway
IS_i	Identity of the sensor
PK_s	Public key of sensor
di	Private key of sensor
IU_j	Identity of user
PU_j	Password of the user
H( )	One-way hash function
SCj	Smart card
a,b	Prime numbers
ΔT	Transmission delay
T_1, T2, T3	Time stamp
$\oplus$	XOR operation
| |	Concatenation

3.1. Gateway Setup Phase:

The gateways of different networks initiate a setup phase in offline mode as follows:

Step 1: The gateway 'GW' first selects the two large prime numbers p and q and computes $n = p$*q.

Step 2: The 'GW' chooses a number e and integer d such that

$$e*d = 1 \bmod n$$
$$d = e - 1 \bmod n$$

where we consider d as a gateway private key and e as a gateway public key for the initial setup phase.

3.2. Sensor Registration Phase:

All the sensor device communicating with the gateway should be registered offline with gateways as follows:

Step 1: For every sensor device 'Si', the GW chooses an identity ISi, private key di, and calculates the sensor public key as PKs = di**p*, where *p* indicates the large prime number.

Step 2: Gateway GW further calculates pseudo-random identity

RSi = h (ISi | | di)

where h indicates a one-way hash function.

Step 3: The gateway 'GW' loads {ISi, di, RSi} in the sensor memory Si and GW itself store (ISi, RSi, Pks) in its database and make PKs key as a public for all the users.

3.3. User Registration Phase:

The user 'U' sends a request to GW for registration and executes the following steps. Figure 2 explains the steps implemented in the registration phase.

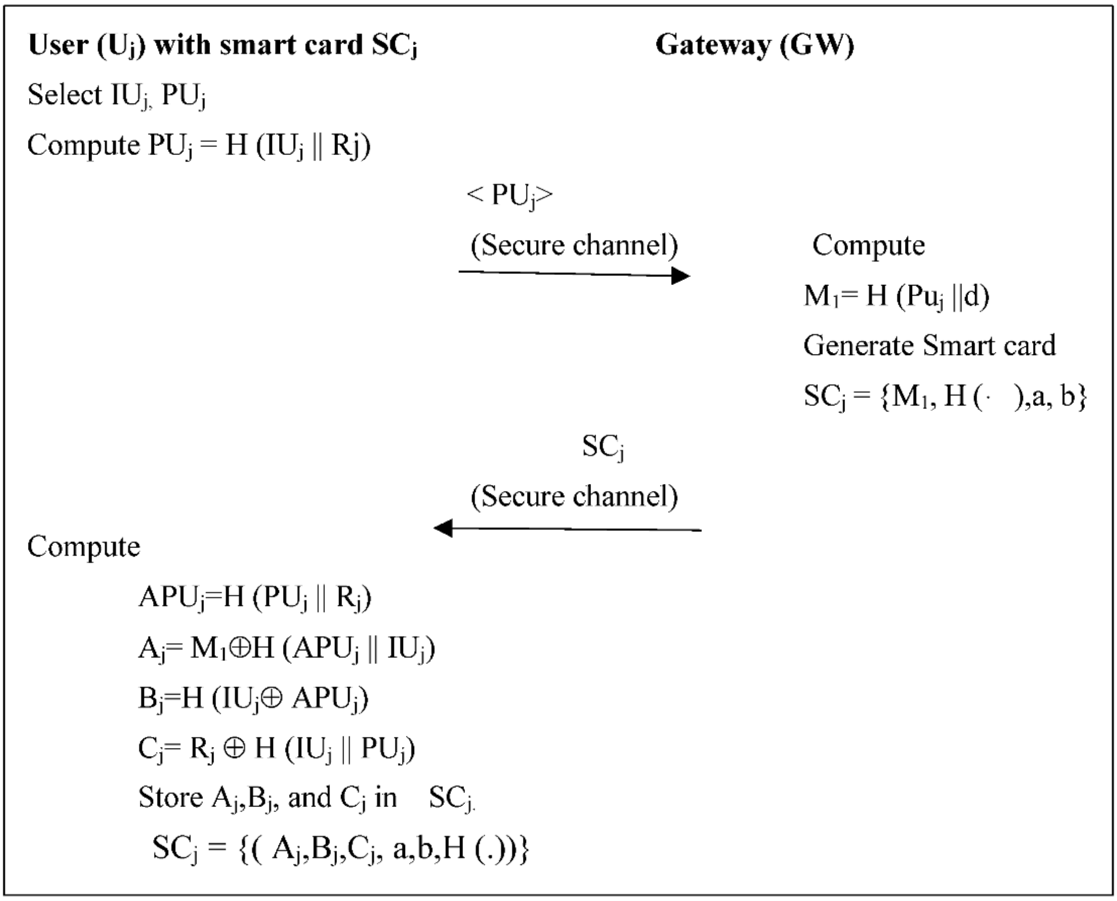

User (U_j) with smart card SC_j
Gateway (GW)
Select $IU_{j,}$ PU_j
Compute $PU_j = H(IU_j \,||\, Rj)$
$< PU_j >$
(Secure channel)
Compute
$M_1 = H(Pu_j \,||d)$
Generate Smart card
$SC_j = \{M_1, H(\cdot\ ), a, b\}$
SC_j
(Secure channel)
Compute
$APU_j = H(PU_j \,||\, R_j)$
$A_j = M_1 \oplus H(APU_j \,||\, IU_j)$
$B_j = H(IU_j \oplus APU_j)$
$C_j = R_j \oplus H(IU_j \,||\, PU_j)$
Store A_j,B_j, and C_j in $SC_{j.}$
$SC_j = \{(A_j, B_j, C_j, a, b, H(.))\}$

Figure 2. User registration phase.

Step 1: The user Uj select its identity IUj, random number Rj and the password PUj.

The user Uj completes the random identity of itself as

PUj = H (IUj | | Rj).

The PUj is sent to the gateway for the registration of the user Uj using a secure communication link.

Step 2: The gateway 'GW', after receiving PUj from user Uj, then computes a message.

Mi = H (PUj | | d),

where H indicates the one-way hash function and d is the private key of the gateway.

Step 3: The gateway generates a smart card SCj = {Mi, H (.), a, b} and sends it to user Uj using a secure communication link.

Step 4: A user Uj receives a smart card SCj and computes another password

$APUj = H\,(PUj\ ||\ Rj)$.

The user also computes three parameter Aj, Bj, Cj as

$Aj = M1 \oplus H\,(APUj\ ||\ IUj)$

$Bj = H\,(IUj \oplus APUj)$

$Cj = Rj \oplus H\,(IUj\ ||\ PUj)$.

All three parameters (Aj, Bj, Cj) are stored into the smart card SCj. The user Uj deletes the stored value M1 from the smart card (SCj) memory. The smart card now contains the information {(Aj, Bj, Cj, a, b, H (.))}.

3.4. User Login Phase:

User Uj executes the following login message to initiate a phase with the gateway node.

Step 1: The user Uj inserts a smart card with their identity IUj and password PUj.

Step 2: The smart card SCj computes the following

$Rj' = Cj \oplus H\,(IUj\ ||\ PUj)$

$PUj' = H\,(IUj\ ||\ Rj')$

$APUj = H\,(PUj\ ||\ Rj')$

$Bj = H\,(IUj \oplus APUj')$

$Mj' = Aj \oplus H\,(APUj'\ ||\ IUj)$.

If $Bj' = Bj$ holds true, it verifies the user Uj and goes to the next phase.

If $Bj' \neq Bj$, i.e., not hold the condition, it does not verify the login request, and it gets rejected.

Step 3: The smart card SCj calculates a pseudo-random number Rs, the current timestamp Ti, and calculates

$Dj = H\,(APUj'\ ||\ Rs\ ||\ M1'\ ||\ T1)$

$Ej = H\,(PUj'\ ||\ APUj'\ ||\ Mj') \oplus Rs$

$Fj = H\,(PUj'\ ||\ APUj'\ ||\ Rs\ ||\ M1'\ ||\ T1)\ a \bmod b$.

After that smart card, SCj sends the message <Dj, Ej, Fj> to the gateway node through a secure communication network.

3.5. User Authentication and Key Exchange Phase

The gateway node GW verifies the user Uj and establishes the key exchange process, accessed between the sensor device and the user Uj of the system. A mutual authentication process between the user and the gateway with a shared session key will be generated as the following steps. Figure 3 explains the authentication phase and the key exchange steps.

Step 1: The gateway node GW received <Dj, Ej, Fj> message from the user Uj and finds the information {PUj′, APUj′, Rs, Mj, Tj}. The gateway node decrypts the Fj by using gateway private key d. The following node is able to find out

$D = (Fj) \bmod b = (PUj', APUj', Rs, Mj, Tj)$.

The gateway GW verifies the validation of time stamp T ie $|T2 - T1| \leq \Delta T$. The timestamp helps to remove the replay attack from the authentication. If the timestamp condition is not satisfied, the procedure will terminate; else, it goes to the next stage of the authentication.

Step 2: Gateway compute $M1' = H\,(PUj\ ||\ d)$ and compare with M1. If $M1' = M1$, it holds true, and the process goes to the next stage; else, it terminates the user login request.

Step 3: If $M1' = M1$ the gateway calculates $Rs' = Ej \oplus H\,(PUj\ ||\ APUj\ ||\ M1)$, and if it find $Rs' = Rs$ it holds true, then goes to the next stage; else, it terminates in this phase.

Step 4: Gateway GW calculates $Dj' = H\,(APUj'\ ||\ Rs\ ||\ M1'\ ||\ Tj)$ and verifies with Dj. If $Dj' = Dj$ it holds true, then the process moves to the next stage; else, the request is terminated.

Step 5: Gateway GW generates a pseudo-random number Rg and current timestamp T2, then calculates the session key as follows.

$Sk = H\,(PUj\ ||\ APUj\ ||\ Rs'\ ||\ Rg\ ||\ T1\ ||\ T2)$

$Gj = Rs' \oplus Rg$

$Kj = H\,(Sk\ ||\ M1'\ ||\ Rg\ ||\ T1\ ||\ Rs\ ||\ T2)$

and then the gateway sends the authentication request <Gj, Kj, T2> to the user Uj.

Step 6: The user Uj with the smart card SCj receives <Gj, Kj, T2>. The user first verifies the time stamp $\mid T2 - T1 \mid \leq \Delta T$. If the time stamp holds true, the session goes to step 7; otherwise, the session is terminated.

Step 7: The user Uj computes

$Rg' = Rs \oplus Gj$

$Sk = H\ (PUj \mid\mid APUj \mid\mid Rs' \mid\mid Rg \mid\mid T1 \mid\mid T2)$

$Kj = H\ (Sk \mid\mid M1' \mid\mid Rg \mid\mid T1 \mid\mid Rs \mid\mid T2)$.

If Kj′ = Kj holds true means, the user and gateway get mutually authenticated, and the authentication phase goes to the next stage; else, the session will terminate.

Step 8: The smart card SCj computes another timestamp T3 and calculates

$Sk' = H\ (Sk \mid\mid M1' \mid\mid PUj \mid\mid T2 \mid\mid T3)$

and sends <Sk′, T3> to the gateway node GW through the secure communication channel.

Step 9: The gateway node GW receives message <Sk′, T3>. The GW first verifies the time stamp and if $\mid T3 - T2 \mid \leq \Delta\ T$ holds true, then it computes

$Sk' = H\ (Sk \mid\mid M1' \mid\mid PUj \mid\mid T2 \mid\mid T3)$

and check Sk = Sk′.

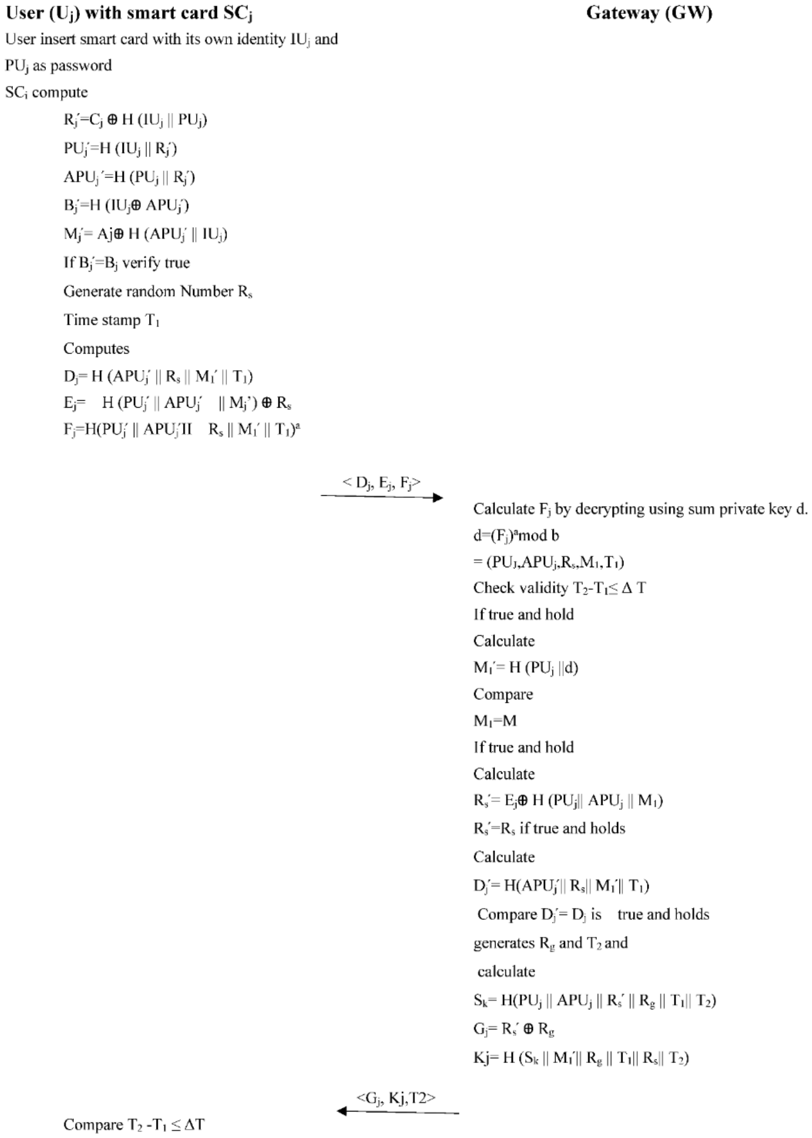

User (U_j) with smart card SC_j
Gateway (GW)
User insert smart card with its own identity IU_j and
PU_j as password
SC_i compute
$R_j' = C_j \oplus H\ (IU_j \mid\mid PU_j)$
$PU_j' = H\ (IU_j \mid\mid R_j')$
$APU_j' = H\ (PU_j \mid\mid R_j')$
$B_j' = H\ (IU_j \oplus APU_j')$
$M_j' = Aj \oplus H\ (APU_j' \mid\mid IU_j)$
If $B_j' = B_j$ verify true
Generate random Number R_s
Time stamp T_1
Computes
$D_j = H\ (APU_j' \mid\mid R_s \mid\mid M_1' \mid\mid T_1)$
$E_j = H\ (PU_j' \mid\mid APU_j' \mid\mid M_j') \oplus R_s$
$F_j = H(PU_j' \mid\mid APU_j' II\ R_s \mid\mid M_1' \mid\mid T_1)^a$
$< D_j, E_j, F_j >$
Calculate F_j by decrypting using sum private key d.
$d = (F_j)^a \mathrm{mod}\ b$
$= (PU_J, APU_j, R_s, M_1, T_1)$
Check validity $T_2 - T_1 \leq \Delta\ T$
If true and hold
Calculate
$M_1' = H\ (PU_j \mid\mid d)$
Compare
$M_1 = M$
If true and hold
Calculate
$R_s' = E_j \oplus H\ (PU_j \mid\mid APU_j \mid\mid M_1)$
$R_s' = R_s$ if true and holds
Calculate
$D_j' = H(APU_j' \mid\mid R_s \mid\mid M_1' \mid\mid T_1)$
Compare $D_j' = D_j$ is true and holds
generates R_g and T_2 and
calculate
$S_k = H(PU_j \mid\mid APU_j \mid\mid R_s' \mid\mid R_g \mid\mid T_1 \mid\mid T_2)$
$G_j = R_s' \oplus R_g$
$Kj = H\ (S_k \mid\mid M_1' \mid\mid R_g \mid\mid T_1 \mid\mid R_s \mid\mid T_2)$
$<G_j, Kj, T2>$
Compare $T_2 - T_1 \leq \Delta T$

Figure 3. *Cont.*

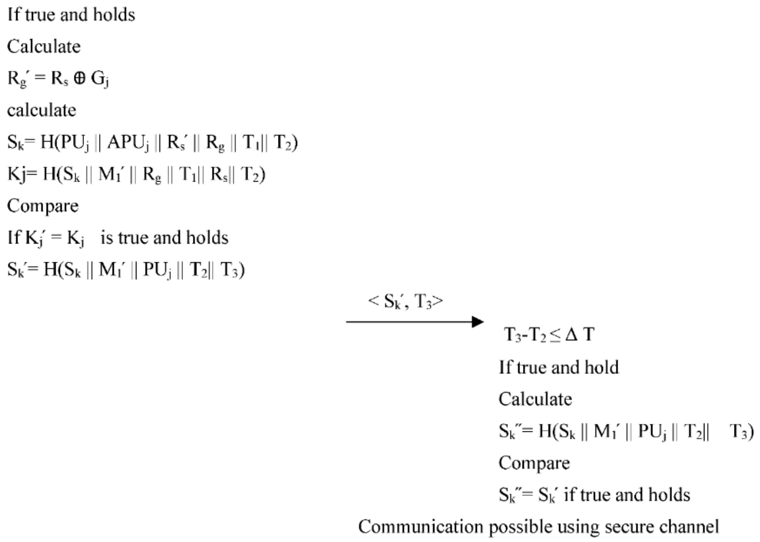

If true and holds
Calculate
Rg′ = Rs ⊕ Gj
calculate
Sk= H(PUj || APUj || Rs′ || Rg || T1|| T2)
Kj= H(Sk || M1′ || Rg || T1|| Rs|| T2)
Compare
If Kj′ = Kj is true and holds
Sk′= H(Sk || M1′ || PUj || T2|| T3)
< Sk′, T3>
T3-T2 ≤ Δ T
If true and hold
Calculate
Sk″= H(Sk || M1′ || PUj || T2|| T3)
Compare
Sk″= Sk′ if true and holds
Communication possible using secure channel

Figure 3. Login and authentication phase between user U_j and gateway GW.

3.6. Password Change Phase:

A user Uj executes this phase internally as follows:

Step 1: User Uj enters their identity IUj and its password PUj using the smart card to the specific sensor terminal 'Si'.

Step 2: The smart card SCj calculates

Rj′ = Ci ⊕ H (IUj | | PUj)
PUj′ = H (IUj | | Rj′)
APUj = H (PUj | | Rj′)
Bj′ = H (IUj ⊕ APUj′)
M1′ = Aj ⊕ H (APUj | | IUj).

It checks the stored Bj in the smart card SCj and compares it with Bj′ if Bj′ = Bj. If it holds true, then verify that the user is authentic and ask for a new password NPUj; otherwise, terminate the session.

Step 3: The user Uj sends the generated new password to the gateway 'GW'.

Step 4: The smart card SCj calculates

ANPUj = H (NPUj | | Rj′)
NAj = M1′ ⊕ H (ANPUj | | IUj)
NBj = H (IUj ⊕ ANPUj)
NCj = Rj′ ⊕ H (IUj | | NPUj).

The smart card replaces all the values of Aj with new Aj (NAj), Bj with new Bj (NBj), and Cj with new Cj (NCj).

3.7. Revocation Phase

If the smart card SCj of any authentic user Uj is stolen or missing, it may be recovered by executing the following steps.

Step 1: The gateway node 'GW' helps users with new requests from users with new passwords. The old value of password and pseudo-random number will not be used again for the new user registration of the user. The reason behind this is to prevent impersonation attacks.

Step 2: The user Uj requests the gateway node GW to revoke the smart card. The gateway node verifies the user Uj with the help of previous known identification or values provided by the user Uj.

Step3: After verification from the user, the gateway node asks for a new password from the user. The user generates a new password PUj′ = H (IUj | | Rj′) and submits the request to the gateway A <PUj′> through a secure communication channel.

Step 4: The gateway node calculates M1′ = H (PUj′ | | d), where d is the gateway private key. The information (M1′a, b, (H)(is sent to the user through a secure communication channel.

Step 5: The user UJ with smart card SCj calculates

AUj′ = H (PUj′ | | Rj′)
Aj = M1 ⊕ H (APUj | | IUj)
Bj = H (IUj ⊕ APUj)
Cj = Rj ⊕ H (IUj | | PUj).

All three parameters Aj′, Bj′, Cj′ are stored into the new smart card. Therefore, the new smart card contains {Aj′, Bj′, Cj′, a, b, h (.)}.

4. Security Analysis

This section shows the informal analysis using BAN logic for proof of authentication in the proposed authentication protocol [30]. Additionally, we offer that the proposed work provides robust security against different types of known attacks. BAN logic helps the protocol to ensure that it works correctly. The logic allows for belief in the trusted parties involved in the communication and provides authenticity.

4.1. Informal Security Proof Using BAN Logic

To provide mutual, trustworthy authentication, we use BAN logic between user Uj, sensor Si, and GW. The following statements and notations prove that the proposed work follows the BAN Logic.

- A beliefs B: A $\mid\rightarrow$ B states that user 'A' believes the statement of user 'B';
- A sees B: A ∇ B, i.e., A receives a B's communication, which may be possible after decryption;
- A said B: A $\mid\sim$ B, i.e., A once said B, means A sent a message that includes a statement of user B;
- A control B: A has jurisdiction over B. A$\mid\Rightarrow$B, i.e., A believes that it is a trusted authority and can generate encryption keys;
- Fresh (B): The B is a new formula; this usually means for nonce includes time stamp or random number, which is used only once;
- A$\overset{K}{\leftrightarrow}$ B: This states that user A and user B shared a key 'K' for the communication;
- $\mid\overset{K}{\rightarrow}$A: This says that A has a public key, 'k';
- A$\overset{X}{\Leftrightarrow}$ B: The formula X is known to only users A and B;
- {B}k: Formula B is hashed with key k;
- < B > Y: this represents B confined with the formula Y.

The following logical hypotheses of BAN logic shows rules concern with the message.

Rule 1: Meaning message rule.

$$\frac{\text{A believes B } \overset{K}{\leftrightarrow} \text{ A, Asees } \{\text{X}\}\text{k}}{\text{A believes B said B}}$$

i.e., the equation says that user 'A' believes that key 'k' is shared with user B and see 'X' is encrypted under 'k'; i.e., shows user A believes user B once said X.

For shared secret key the postulate becomes

$$\frac{\text{A believes B } \overset{Y}{\Leftrightarrow} \text{A, P sees}\langle\text{B}\rangle\text{Y}}{\text{A believes B said X}}$$

Rule 2: Nonce rule of verification.

$$\frac{\text{A believes fresh (B), A believes B said X}}{\text{A believes B believes X}}$$

It says that A believes B believes X, if A believes B once A believes X is fresh.

Rule 3: The jurisdiction rule.

It states that user A believes user B has authority over X, then user A trusts user B's beliefs on X

$$\frac{\text{A believes B control X, A believes B believes X}}{\text{P believes X}}$$

Rule 4: Belief rule if user A sees a formula, then they also see all the component.

$$\frac{\text{A sees }(\text{X},\text{Y})}{\text{A see X}}$$

$$\frac{\text{A believes k}|\text{ B, A sees }\{\text{X}\}\text{K}-1}{\text{A see X}}$$

Rule 5: Freshness rule.

It says that the complete formula is said to be fresh, if one part of the formula is fresh.

$$\frac{\text{A believes fresh }(\text{X})}{\text{A believes fresh}\langle\text{X},\text{Y}\rangle}$$

Theorem 1. *The proposed authentication protocol provides the mutual authentication between user Uj and gateway node GW.*

Proof. The following procedure shows the mutual authentication between user Uj and gateway with their goal.

Our goals:

G1: $\text{Uj} \mid \equiv \text{ Uj } \overset{Sk}{\leftrightarrow}\text{GW}$

G2: $\text{GW} \mid \equiv \text{ UJ } \overset{Sk}{\leftrightarrow} \text{ GW}$

A1: $\text{Uj } \mid\equiv \#\ (\text{Ti}), \text{Uj } \mid\equiv \#\ (\text{Tj});$

A2: $\text{GW } \mid\equiv \#\ (\text{Ti}), \text{Uj } \mid\equiv \#\ (\text{Tk});$

A3: $\text{GW } \mid\equiv \#\ (\text{Ti}), \text{GW } \mid\equiv \#\ (\text{Tk}), \text{GW } \mid\equiv \#\ (\text{Tj});$

A4: $\text{GW} \mid \equiv\ (\text{GW } \overset{e,d}{\leftrightarrow}\text{Uj});$

A5: $\text{SCj} \mid \equiv\ (\text{GW } \overset{e,d}{\leftrightarrow} \text{ Scjj});$

A6: $\text{SCj } \mid\equiv (\text{GW} \Rightarrow \text{GW } \mid\sim \text{X};$

A7: $\text{Uj} \mid \equiv\ (\text{Uj } \overset{RSi}{\leftrightarrow} \text{ SCj});$

A8: $\text{SCj} \mid \equiv\ (\text{Uj } \overset{RSi}{\leftrightarrow} \text{ SCj})$

A9: $\text{Uj } \mid\equiv \text{SCj} \Rightarrow (\text{Uj } \overset{Sk}{\leftrightarrow} \text{ SCj}).$

A10: $\text{Uj} \mid \equiv \text{ Uj } \overset{Sk}{\leftrightarrow} \text{ GW}$

A11: $\text{GW} \mid \equiv \text{ Uj } \overset{Sk}{\leftrightarrow} \text{ GW}$

Goal G1 and G2 clearly shows that the user is mutually authenticated with the sensor and the gateway. □

4.2. Security Analysis on the Different Attacks

In this section, we examined the ways in which our proposed protocol protects against different types of known security attacks.

Property 1. *The proposed protocol is resistant against user impersonation attacks.*

The proposed authentication protocol provides resistance against impersonation attacks. Let the intruder I intercept the communicated message < Dj, Ej, Fj> during the login phase, where

$\text{Dj} = \text{H}\ (\text{APUj}' \mid\mid \text{Rs} \mid\mid \text{Mj}' \mid\mid \text{Tj})$
$\text{Ej} = \text{H}\ (\text{PUj}' \mid\mid \text{APUj}' \mid\mid \text{Mj}') \oplus \text{Rs}$
$\text{Fj} = \text{H}\ (\text{PUj}' \mid\mid \text{APUj}' \mid\mid \text{Rs} \mid\mid \text{Mj}' \mid\mid \text{Tj})\ \text{a mod b}.$

The intruder does not have knowledge of the parameter PUj′, Rs, Ej for logging into the session. So, the proposed work is secure against the impersonation attack.

Property 2. *The proposed work provides protection against denial-of-service attacks.*

The proposed protocol uses the concept of current timestamp T1, T2, T3 during user authentication and key exchange phase. In the proposed protocol, the gateway GW verifies the user Uj with identity IUj and password PUj before providing access to the information. Hence, the proposed work is secure against denial-of-service attacks.

Property 3. *The proposed work provides protection against privileged insider attacks.*

A privileged user at the gateway node may be the intruder I and obtain RIUj, which may be the user Uj information during the registration phase. Let the smart card be stolen and lost. Intruder A may not be able to guess the password PUj and APUj due to the presence of a masked password APUj, which is not directly shared with the smart card SCj. Further, the information is protected through the one-way hash function, and it is infeasible to calculate the hash.

Property 4. *The proposed work provides protection against insider attacks.*

Let the intruder I be at the gateway node and able to obtain PUj. The user UJ does the hash function on the password and a random number PUj = H (IUj II Rj). Intruders are not able to get the identification because the hash function is a one-way function and not reversible. In addition, PUj is not used in any authentication procedure for any computation. Hence, intruders 'I' may not be able to forge any information used PUj.

Property 5. *The proposed work provides protection against lost/stolen smart card attacks.*

Let us assume that the intruder gets the smart card of any legitimate user Uj. The security parameter that the smart card contains is {Aj′, Bj′, Cj′, a,b,h()}. An intruder may perform several attacks to known Ai, Bi, and Ci, but intruder I will never be able to find out these parameters.

$Aj = M1 \oplus H\ (APUj \mid\mid IUj)$
$Bj = H\ (IUj \oplus APUj)$
$Cj = Rj \oplus H\ (IUj \mid\mid PUj).$

Hence, all the parameters are collision resistance hash function (h). So, intruder I cannot forge and find out any information if the smart card is stolen or lost.

Property 6. *The proposed work provides protection against offline password guessing attacks.*

This is a common type of attack that any intruder tries to attempt. Let us suppose the intruder steals the smart card of any user Uj and is able to see {Aj, Bj′, Cj′ (a,b,h)} where

$Aj = M1 \oplus H\ (APUj \mid\mid IUj)$
$Bj = H\ (IUj \oplus APUj)$
$Cj = Rj \oplus H\ (IUj \mid\mid PUj)$
and $APUj = H\ (Puj \mid\mid Rj).$

Due to the presence of polynomial time, the intruder cannot find IUj or PUj and these values are not directly stored into the smart card due to the presence of a one-way hash function. The intruder may not be able to calculate or guess the password and identity of users.

Property 7. *The proposed work provides protection against man-in-the-middle attacks.*

Suppose the intruder I intercept in the login phase where the smart card sends a message <Dj, Ej, Fj> to the gateway node. They may try to acquire the message and modify the message for another login request, for this intruder will have to select a random number Rs* and current timestamp T1* and try to able to calculate.

Dj = H (APUj′ | | Rs* | | M1′ | | T1*)
Ej = H (Puj′ | | APUj′ | | M1′) ⊕ Rs*
Fj = H (Puj′ | | APUj′ | | Rs* | | M1′ | | T1*) a mod b.

However, this is infeasible for an intruder to find PUj, M1, and APUj and again all the parameters Dj,Ej,Fj are hashed which is not reversible. Consequently, the MIMA is not possible in the proposed protocol.

Property 8. *The proposed work provides protection against anonymity and is untraceable.*

Let us assume intruder I calculates and tries to find out login request < Dj, Ej, Fj > and <Dj*, Ej*, Fj*>

where
Dj = H (APUj′ | | Rs* | | M1′ | | T1*)
Ej = H (PUj′ | | APUj′ | | M1′) ⊕ Rs*
Fj = H (PUj′ | | APUj′ | | Rs*| | M1′ | | T1*) a mod b.

To find the intruder and legitimate user, both have the same parameter and value. The value of Rs and T1 should be the same, and the importance of random number Rs is constantly changing. The intruder is unable to find out the exact value Rs and the time stamp T1. Further, user identity is not identified in any message, hence the proposed scheme provides anonymity and intractability.

Property 9. *The proposed work provides the mutual authentication.*

The proposed work provides the mutual authentication between users Uj with the gateway GW. Both user and gateway validate each other. Similarly, the user with sensor Sj also authenticates itself to the gateway. Thus, the gateway and sensor provide mutual authentication with each other. Overall, there is authentication needed at each level of sharing of information in the communication channel.

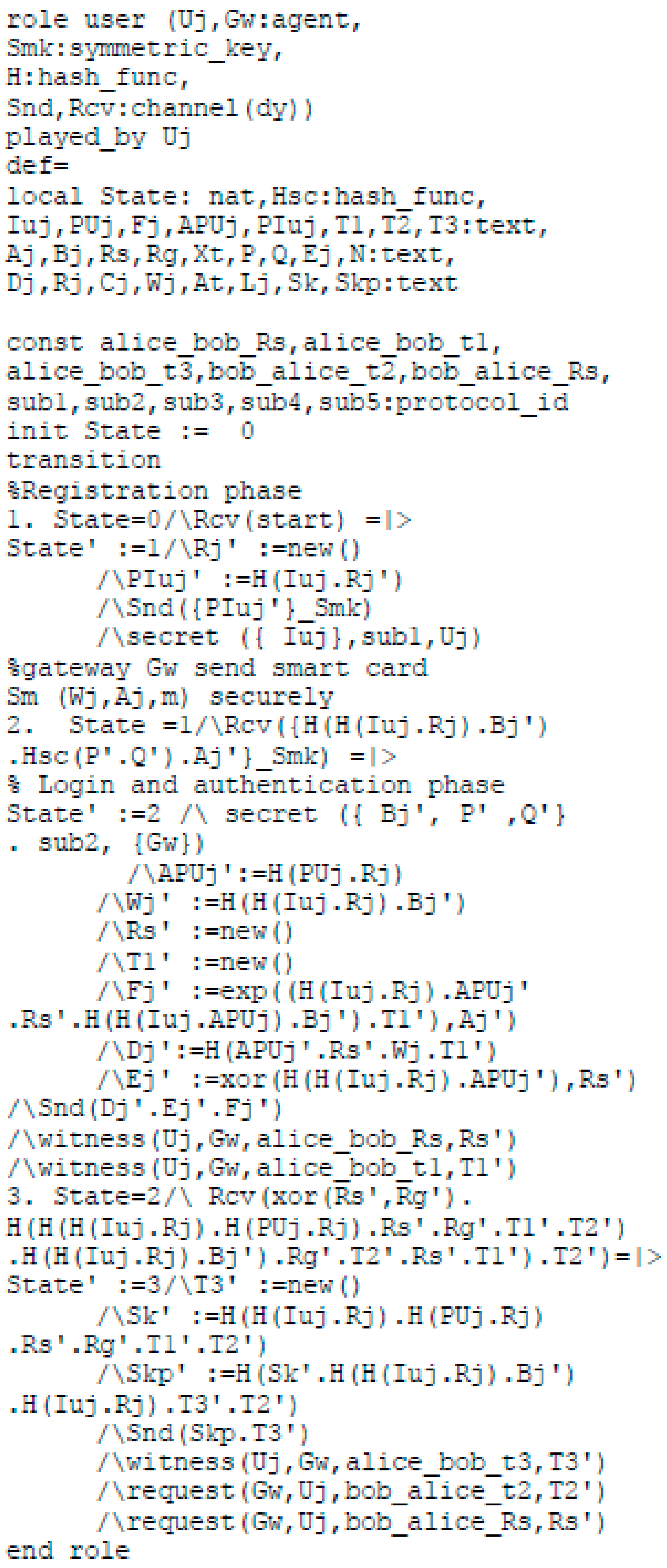
Property 10. *The proposed work provides the security of the session key.*

The session key Sk = H (PUj′ | | APUj′ | | Rs′ | | Rg | | T1 | | T2) is secure, due to presence of random number Rs and Rg. In the session key, there is no clear indication of user identification IUj and password PUj, so the intruder may not be able to find out the value of APUj and <Dj, Ej, Fj> using these parameters. Thus, the proposed work provides security for the shared session key.

5. Formal Validation Using Avispa

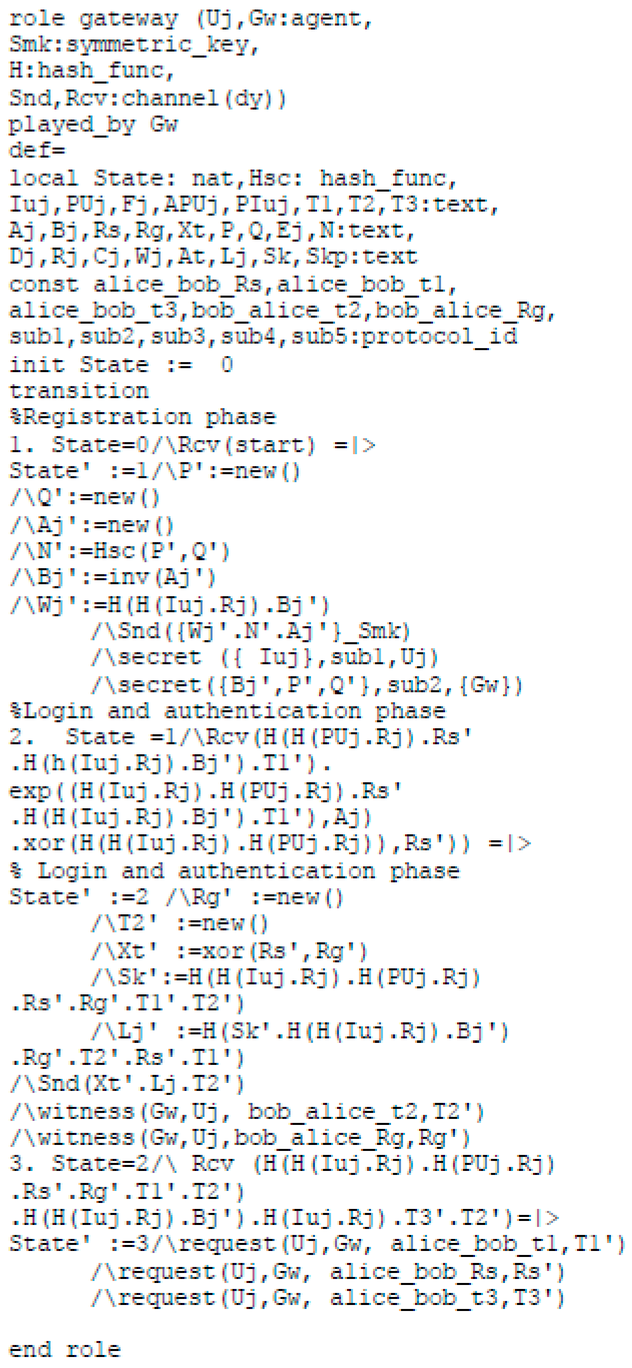
In this section, we make a presentation for the simulation of authentication and key exchange protocol using automation validation of internet security protocol and application (AVISPA) [31,32]. AVISPA is coded in high-level protocol specification language (HLPSL) [33–35].

This is a compelling language for the authentication protocol. Using the simulation, we find that our protocol is free from all types of known attacks. The HLPSL code for the proposed protocol with all entities (such as user Uj and gateway GW) is provided in Figures 4 and 5. The HLPSL code for goal, session, and environment is shown in Figures 6 and 7. The result of the simulation is shown in Figures 8 and 9. From these figures, our proposed work confirmations resist all types of known attacks. Figures 8 and 9 show that our protocol is SAFE in both simulation environments, that is, OFMC and CI-Atse model. This indicates that the protocol is secure against reply attacks, MITM attacks, and other active and passive attacks.



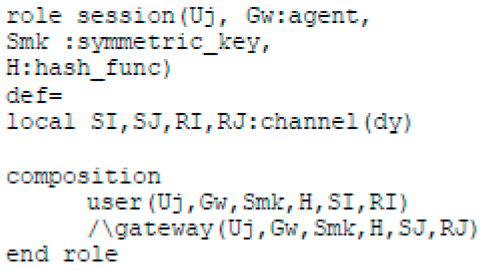
```
role user (Uj,Gw:agent,
Smk:symmetric_key,
H:hash_func,
Snd,Rcv:channel(dy))
played_by Uj
def=
local State: nat,Hsc:hash_func,
Iuj,PUj,Fj,APUj,PIuj,T1,T2,T3:text,
Aj,Bj,Rs,Rg,Xt,P,Q,Ej,N:text,
Dj,Rj,Cj,Wj,At,Lj,Sk,Skp:text

const alice_bob_Rs,alice_bob_t1,
alice_bob_t3,bob_alice_t2,bob_alice_Rs,
sub1,sub2,sub3,sub4,sub5:protocol_id
init State :=  0
transition
%Registration phase
1. State=0/\Rcv(start) =|>
State' :=1/\Rj' :=new()
      /\PIuj' :=H(Iuj.Rj')
      /\Snd({PIuj'}_Smk)
      /\secret ({ Iuj},sub1,Uj)
%gateway Gw send smart card
Sm (Wj,Aj,m) securely
2.  State =1/\Rcv({H(H(Iuj.Rj).Bj')
.Hsc(P'.Q').Aj'}_Smk) =|>
% Login and authentication phase
State' :=2 /\ secret ({ Bj', P' ,Q'}
. sub2, {Gw})
        /\APUj':=H(PUj.Rj)
      /\Wj' :=H(H(Iuj.Rj).Bj')
      /\Rs' :=new()
      /\T1' :=new()
      /\Fj' :=exp((H(Iuj.Rj).APUj'
.Rs'.H(H(Iuj.APUj).Bj').T1'),Aj')
      /\Dj':=H(APUj'.Rs'.Wj.T1')
      /\Ej' :=xor(H(H(Iuj.Rj).APUj'),Rs')
/\Snd(Dj'.Ej'.Fj')
/\witness(Uj,Gw,alice_bob_Rs,Rs')
/\witness(Uj,Gw,alice_bob_t1,T1')
3. State=2/\ Rcv(xor(Rs',Rg').
H(H(H(Iuj.Rj).H(PUj.Rj).Rs'.Rg'.T1'.T2')
.H(H(Iuj.Rj).Bj').Rg'.T2'.Rs'.T1').T2')=|>
State' :=3/\T3' :=new()
      /\Sk' :=H(H(Iuj.Rj).H(PUj.Rj)
.Rs'.Rg'.T1'.T2')
      /\Skp' :=H(Sk'.H(H(Iuj.Rj).Bj')
.H(Iuj.Rj).T3'.T2')
      /\Snd(Skp.T3')
      /\witness(Uj,Gw,alice_bob_t3,T3')
      /\request(Gw,Uj,bob_alice_t2,T2')
      /\request(Gw,Uj,bob_alice_Rs,Rs')
end role
```

Figure 4. User role description in HLPSL for the proposed protocol.



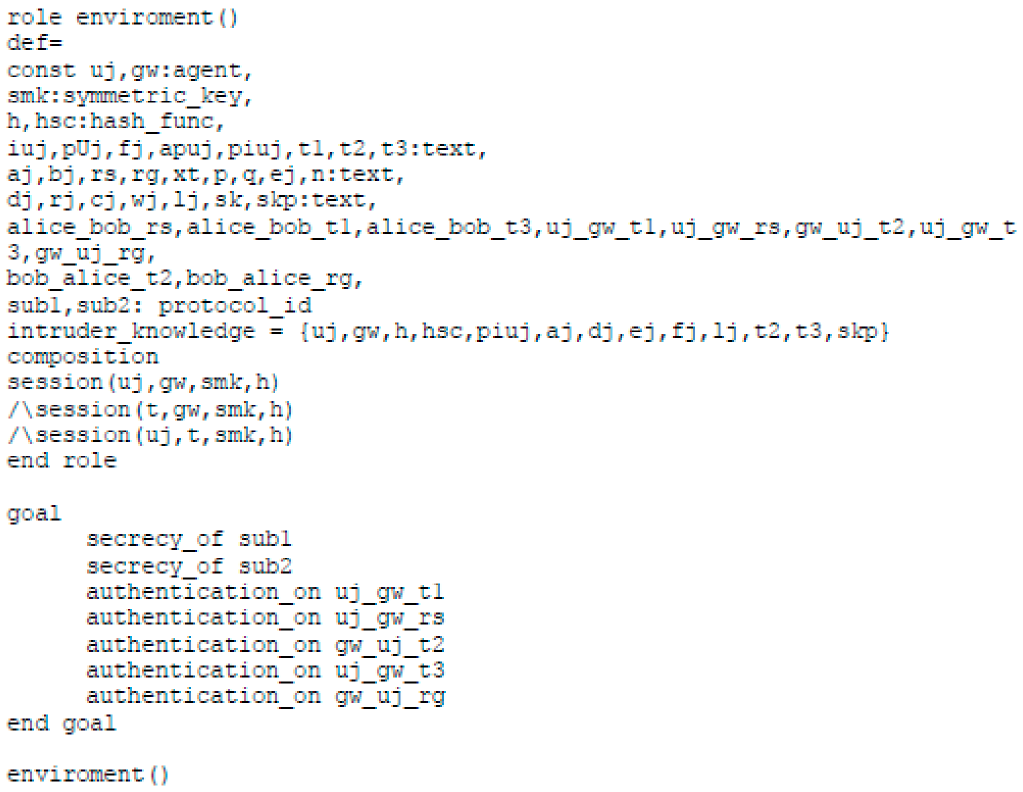
```
role gateway (Uj,Gw:agent,
Smk:symmetric_key,
H:hash_func,
Snd,Rcv:channel(dy))
played_by Gw
def=
local State: nat,Hsc: hash_func,
Iuj,PUj,Fj,APUj,PIuj,T1,T2,T3:text,
Aj,Bj,Rs,Rg,Xt,P,Q,Ej,N:text,
Dj,Rj,Cj,Wj,At,Lj,Sk,Skp:text
const alice_bob_Rs,alice_bob_t1,
alice_bob_t3,bob_alice_t2,bob_alice_Rg,
sub1,sub2,sub3,sub4,sub5:protocol_id
init State :=  0
transition
%Registration phase
1. State=0/\Rcv(start) =|>
State' :=1/\P':=new()
/\Q':=new()
/\Aj':=new()
/\N':=Hsc(P',Q')
/\Bj':=inv(Aj')
/\Wj':=H(H(Iuj.Rj).Bj')
      /\Snd({Wj'.N'.Aj'}_Smk)
      /\secret ({ Iuj},sub1,Uj)
      /\secret({Bj',P',Q'},sub2,{Gw})
%Login and authentication phase
2.  State =1/\Rcv(H(H(PUj.Rj).Rs'
.H(h(Iuj.Rj).Bj').T1').
exp((H(Iuj.Rj).H(PUj.Rj).Rs'
.H(H(Iuj.Rj).Bj').T1'),Aj)
.xor(H(H(Iuj.Rj).H(PUj.Rj)),Rs')) =|>
% Login and authentication phase
State' :=2 /\Rg' :=new()
      /\T2' :=new()
      /\Xt' :=xor(Rs',Rg')
      /\Sk':=H(H(Iuj.Rj).H(PUj.Rj)
.Rs'.Rg'.T1'.T2')
      /\Lj' :=H(Sk'.H(H(Iuj.Rj).Bj')
.Rg'.T2'.Rs'.T1')
/\Snd(Xt'.Lj.T2')
/\witness(Gw,Uj, bob_alice_t2,T2')
/\witness(Gw,Uj,bob_alice_Rg,Rg')
3. State=2/\ Rcv  (H(H(Iuj.Rj).H(PUj.Rj)
.Rs'.Rg'.T1'.T2')
.H(H(Iuj.Rj).Bj').H(Iuj.Rj).T3'.T2')=|>
State' :=3/\request(Uj,Gw, alice_bob_t1,T1')
      /\request(Uj,Gw, alice_bob_Rs,Rs')
      /\request(Uj,Gw, alice_bob_t3,T3')

end role
```

Figure 5. Gateway role description in HLPSL for the proposed protocol.



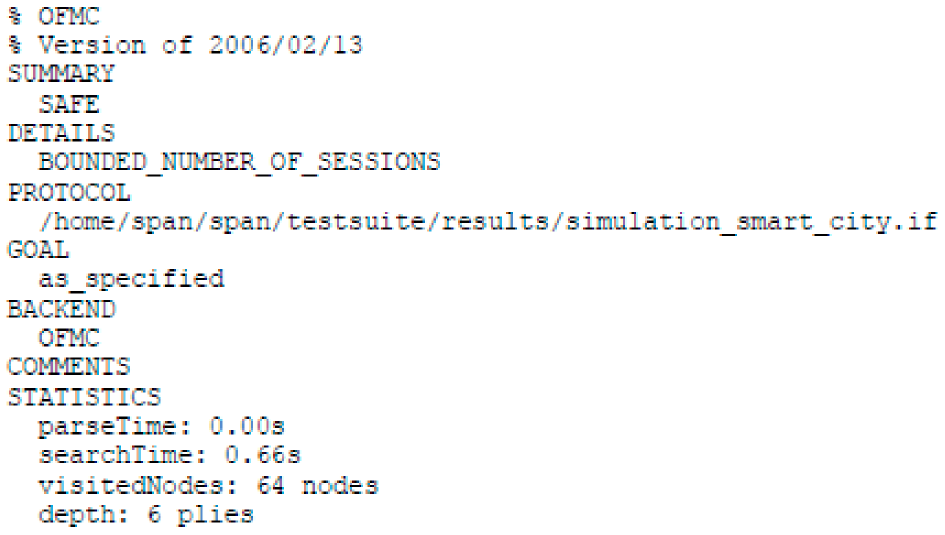
```
role session(Uj, Gw:agent,
Smk :symmetric_key,
H:hash_func)
def=
local SI,SJ,RI,RJ:channel(dy)

composition
      user(Uj,Gw,Smk,H,SI,RI)
      /\gateway(Uj,Gw,Smk,H,SJ,RJ)
end role
```

Figure 6. Session role description in HLPSL for the proposed protocol.



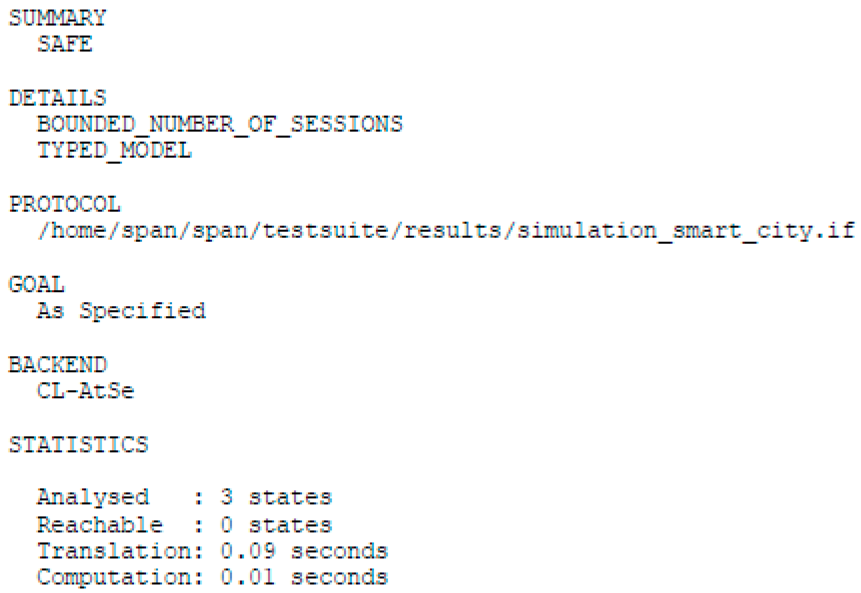
```
role enviroment()
def=
const uj,gw:agent,
smk:symmetric_key,
h,hsc:hash_func,
iuj,pUj,fj,apuj,piuj,t1,t2,t3:text,
aj,bj,rs,rg,xt,p,q,ej,n:text,
dj,rj,cj,wj,lj,sk,skp:text,
alice_bob_rs,alice_bob_t1,alice_bob_t3,uj_gw_t1,uj_gw_rs,gw_uj_t2,uj_gw_t
3,gw_uj_rg,
bob_alice_t2,bob_alice_rg,
sub1,sub2: protocol_id
intruder_knowledge = {uj,gw,h,hsc,piuj,aj,dj,ej,fj,lj,t2,t3,skp}
composition
session(uj,gw,smk,h)
/\session(t,gw,smk,h)
/\session(uj,t,smk,h)
end role

goal
      secrecy_of sub1
      secrecy_of sub2
      authentication_on uj_gw_t1
      authentication_on uj_gw_rs
      authentication_on gw_uj_t2
      authentication_on uj_gw_t3
      authentication_on gw_uj_rg
end goal

enviroment()
```

Figure 7. Environment role description in HLPSL for the proposed protocol.



```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/simulation_smart_city.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.66s
  visitedNodes: 64 nodes
  depth: 6 plies
```

Figure 8. Simulation result analysis using OFMC backend.



```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/simulation_smart_city.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 3 states
  Reachable  : 0 states
  Translation: 0.09 seconds
  Computation: 0.01 seconds
```

Figure 9. Simulation result analysis using CL-AtSe backend.

6. Comparative Analysis

This section presents a comparison of the security feature of proposed work with other related work. Developing a secure and lightweight authentication protocol for privacy preserving communications in smart city applications is a challenging task that involves several technical and non-technical problems. Some of the key problems include:

- Security: One of the main challenges in developing an authentication protocol is ensuring its security against various types of attacks, such as impersonation, replay, and man-in-the-middle attacks. The protocol must be designed to prevent these attacks and protect sensitive data transmitted between devices;
- Privacy: Another challenge is preserving the privacy of user data, which is critical in smart city applications that involve sensitive information, such as location and personal data. The protocol must be designed to prevent tracking, profiling, and other privacy violations;
- Resource constraints: Smart city devices, such as sensors and mobile devices, often have limited computational power, memory, and battery life. The protocol must be lightweight and efficient to minimize resource consumption and avoid impacting device performance;
- Scalability: Smart city applications involve a large number of devices and users, which can make it challenging to scale the authentication protocol. The protocol must be designed to support large-scale deployments and minimize communication overhead;
- Compatibility: Smart city applications may use different communication technologies and protocols, which can make it difficult to ensure compatibility and interoperability between devices. The authentication protocol must be designed to support different communication technologies and ensure interoperability between devices;
- Cost: Developing and deploying a new authentication protocol can be costly, especially in large-scale smart city applications. The protocol must be cost-effective and scalable to minimize the overall cost of the smart city system.

A comparative analysis with selected papers on authentication in IoT smart cities can help to provide a deeper understanding of the various authentication methods and techniques being used in this field, as well as their strengths and limitations. The comparison provides the security feature and usefulness of proposed work. Table 3 shows the assessment of cryptographic computational cost among the proposed work.

Table 3. Comparison of the security feature of proposed work with other related work.

S.No	Security Feature	Mishra et al. [18]	Moon et al. [19]	Turkanovic et al. [17]	Proposed
1	Impersonation attack	Yes	No	Yes	Yes
2	Denial of service attack	Yes	Yes	No	Yes
3	Privilege attack	No	Yes	No	Yes
4	Insider attack	Yes	Yes	No	Yes
5	Smart card stolen	Yes	Yes	Yes	Yes
6	Offline password guessing attack	No	Yes	No	Yes
7	Man in the middle attack	Yes	Yes	Yes	Yes
8	Anonymity	Yes	No	Yes	Yes
9	Untraceability	No	Yes	No	Yes
10	Session key security	Yes	Yes	No	Yes
11	Forgery attack	Yes	Yes	Yes	Yes
12	Mutual authentication	Yes	Yes	No	Yes
13	Smart card revocation	Yes	Yes	No	Yes
14	Forward secrecy	Yes	Yes	Yes	Yes
15	Authentication of smart card	Yes	Yes	Yes	Yes
16	Gateway spoofing attack	No	No	No	Yes
17	Online password guessing attack	No	Yes	No	Yes
18	Malicious user attack	No	Yes	No	Yes
19	Sensor spoofing attack	No	No	No	Yes
20	Hidden gateway attack	No	No	No	Yes

Table 4 uses the notation TE for time required for exponential computation, TH for time needed for hash computation, TM is for multiplication and division, and TF is for fuzzy extraction. The comparison shows the great efficiency of the proposed work. The proposed work is lightweight and uses one-way hash function h() and Exclusive-OR (XOR) operation to better the IoT environment. Table 5 shows the computation cost of cryptographic operations of related work. Our scheme demands less computational cost related to other protocols. For example, according to the data available in Xu et al. [34] the execution time required for the hash function TH is 0.004 ms, and the time for the execution of exponential function TE is 0.16 ms, while the time needed for the performance of multiplication function TM is 0.21ms. These values are calculated by using C/C++ library in MI RACL.

Table 4. Assessment of cryptographic computational cost of proposed protocol with related work.

Protocol	Registration Phase	Login Phase	Authentication Phase	Password Change Phase
Mishra et al. [25]	$3T_H$	$T_E + 3\ T_H$	$3T_E + 6\ T_H$	$4T_E + 11T_H$
Moon et al. [36]	$5T_H$	$2T_M + 4\ T_H$	$4T_M + 2T_E + 5T_H$	$3T_H$
Turkanovic et al. [24]	$7T_H$	$5T_H + T_M$	$7T_H + 2T_M$	-
Proposed	$3T_H$	$T_E + 4T_H$	$2T_E + 5T_H$	$2T_H$

T_E: time for exponential computation, T_H: time for hash, T_M: time for multiplication and division.

Table 5. Time taken and energy consumption of proposed protocol.

Protocol Phase	Mishra et al. [25]	Moon et al. [36]	Turkanovic et al. [24]	Proposed Protocol
Total cost	$23T_H + 8T_E$	$17T_H + 2T_E + 6T_M$	$19T_H + 3T_M$	$14T_H + 3T_E$
Total time taken	1.37 ms	1.64 ms	0.70 ms	0.53 ms
Total energy consumption	32.8 mj	39.36 mj	16.8 mj	12.72 mj

The efficiency of the proposed protocol in terms of time effectiveness and energy consumption is shown in Figure 10. The proposed protocol takes 0.53 ms to complete the execution process and required 12.72 mj of energy consumption. We used the formula E = U *I * t for calculating the energy consumption for the value of I = 8mA and U = 3.0 V at active mode. Table 4 shows significant improvement in the proposed protocol. Figure 10 shows the execution time and the energy consumption of the different authentication protocols.

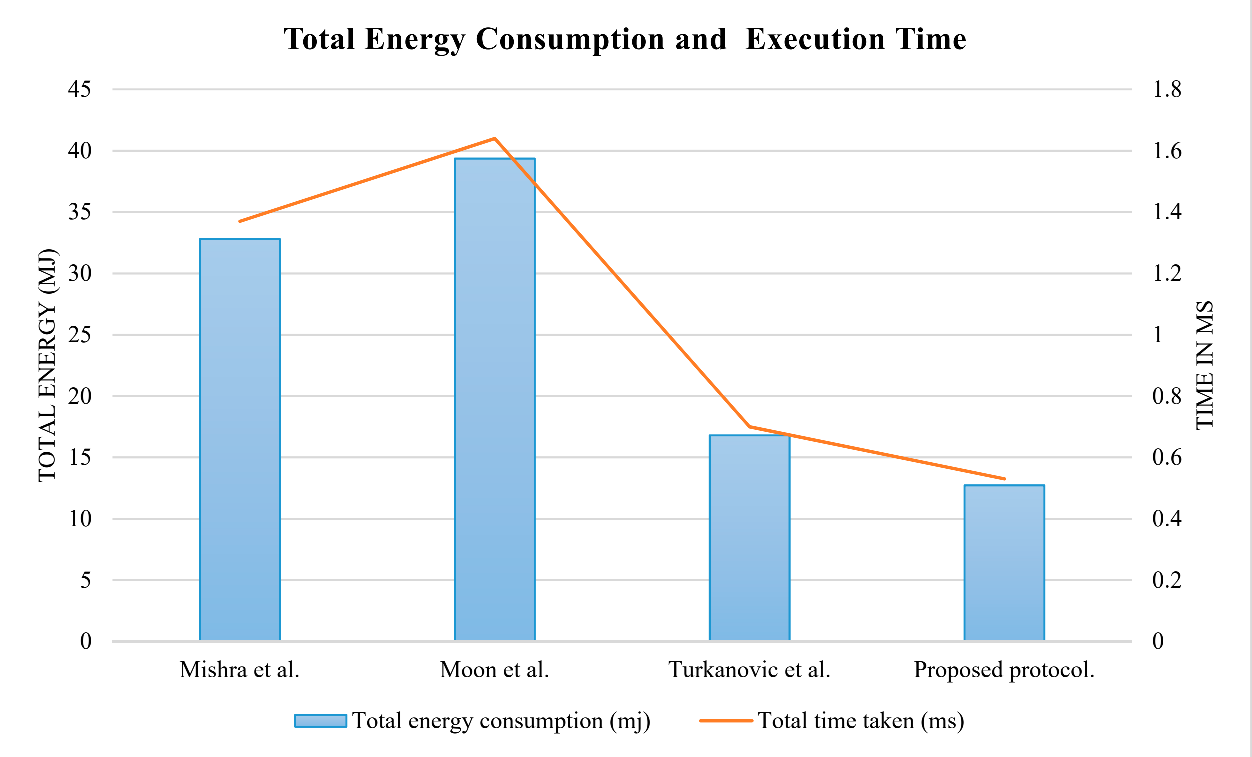


Figure 10. Comparison of execution time (ms) and total energy consumption (mj) of the authentication protocols.

7. Conclusions

We have discussed the smart city scenario based on IoT applications and their security requirements and challenges. The proposed protocol is designed to ensure the privacy and security of data transmitted in smart city applications while maintaining a lightweight and efficient design. The proposed protocol provides efficient authentication between users to the gateway in an IoT network. The key exchange provides the user and gateway for the effective sharing of information. In this paper, proposed work provides mutual authentication for communication between user, sensor, and gateway node. The proposed protocol is scalable and interoperable to support large-scale smart city deployments and different communication technologies. The security analysis using BAN logic helps to provide proof of the proposed protocol and shows that it is perfect and secure against different types of active and passive attacks. The proposed protocol is efficient in terms of computational cost, execution time, energy efficiency, and security features. The AVISPA analysis shows the practical implementation and feasibility in the smart city environment with great security features.

In future work, a more secure protocol for mutual authentication will be designed for intelligent transportation and smart healthcare. In addition, we would also extend this work by using some machine learning techniques.

Author Contributions: Conceptualization, methodology, writing—original draft, results analysis, S.G.; supervising, reviewing, editing, proofreading, F.A.; editing and reviewing, R.A.; methodology, writing—review and editing, P.K.A.; methodology, writing—review and editing, S.V.; methodology, writing—review and editing, D.H.E.; methodology, writing—review and editing, B.O.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R238), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Shaqra University for supporting this work.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets used during the current study are available from the corresponding author on reasonable request.

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

References

1. Li, Y.; Lin, Y.; Geertman, S. The development of smart cities in China. In Proceedings of the 14th International Conference on Computers in Urban Planning and Urban Management, Cambridge, MA, USA, 7–10 July 2015; pp. 7–10.
2. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and privacy in smart city applications: Challenges and solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
3. Ren, K.; Yu, S.; Lou, W.; Zhang, Y. Multi-user broadcast authentication in wireless sensor networks. *IEEE Trans. Veh. Technol.* **2009**, *58*, 4554–4564. [CrossRef]
4. Malan, D.J.; Welsh, M.; Smith, M.D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography. In Proceedings of the 2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, Santa Clara, CA, USA, 4–7 October 2004; pp. 71–80.
5. Yamakawa, S.; Cui, Y.; Kobara, K.; Imai, H. Lightweight broadcast authentication protocols reconsidered. In Proceedings of the 2009 IEEE Wireless Communications and Networking Conference, Budapest, Hungary, 5–8 April 2009; pp. 1–6.
6. Cao, X.; Kou, W.; Dang, L.; Zhao, B. IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks. *Comput. Commun.* **2008**, *31*, 659–667. [CrossRef]
7. Alomair, B.; Poovendran, R. Efficient authentication for mobile and pervasive computing. *IEEE Trans. Mobile Comput.* **2014**, *13*, 469–481. [CrossRef]
8. Wu, T.; Cui, Y.; Kusy, B.; Ledeczi, A.; Sallai, J.; Skirvin, N.; Werner, J.; Xue, Y. A fast and efficient source authentication solution for broadcasting in wireless sensor networks. In *New Technologies, Mobility and Security*; Springer: Dordrecht, The Netherlands, 2007; pp. 53–63.
9. Kothmayr, T.; Schmitt, C.; Hu, W.; Brünig, M.; Carle, G. DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Netw.* **2013**, *11*, 2710–2723. [CrossRef]
10. Rivest, R.L.; Shamir, A.; Adleman, L. A Method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* **1978**, *21*, 120–126. [CrossRef]
11. Miller, V. Uses of elliptic curves in cryptography. In *Advances in Cryptology—CRYPTO 85*; Springer: Berlin/Heidelberg, Germany, 1986; pp. 417–426.
12. Perrig, A.; Szewczyk, R.; Tygar, J.; Wen, V.; Culler, D.E. SPINS: Security protocols for sensor networks. *Wireless Netw.* **2002**, *8*, 521–534. [CrossRef]
13. Ren, K.; Lou, W.; Zeng, K.; Moran, P.J. On broadcast authentication in wireless sensor networks. *IEEE Trans. Wireless Commun.* **2007**, *11*, 4136–4144. [CrossRef]
14. Liu, D.; Ning, P. *Multi-Level MicroTESLA: A Broadcast Authentication System for Distributed Sensor Network*; North Carolina State University at Raleigh: Raleigh, NC, USA, 2003.
15. Shaheen, J.; Ostry, D.; Sivaraman, V.; Jha, S. Confidential and secure broadcast in wireless sensor networks. In Proceedings of the 2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, Athens, Greece, 3–7 September 2007; pp. 1–5.

16. Roy, A.; Karforma, S. Uml based modeling of ECDSA for secured and smart E-governance system. *Comput. Sci. Inf. Technol.* **2013**, *3*, 207–222.
17. 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. [CrossRef]
18. Mishra, D.; Das, A.K.; Chaturvedi, A. A secure password-based authentication and key agreement scheme using smart card. *J. Inf. Secur.* **2015**, *23*, 28–43. [CrossRef]
19. Moon, J.; Lee, D.; Jung, J. Improvement of efficient and secure smart card based password authentication scheme. *Int. J. Netw. Secur.* **2017**, *19*, 1053–1061.
20. Fatty, M.; Salem, R.A. A privacy-preserving RFID authentication protocol based on El-Gamal cryptosystem for secure TMIS. *Inf. Sci.* **2020**, *527*, 382–393.
21. Vijayakumar, P.; Obaidat, M.; Azees, M.; Islam, S.; Kumar, N. Efficient and Secure Anonymous Authentication with Location Privacy for IoT-Based WBANs. *IEEE Trans. Ind. Inform.* **2020**, *16*, 2603–2611. [CrossRef]
22. Basudeb, B.; Ashok, K.D.; Walter, B.; Carlo, M.M. On the design of biometric-based user authentication protocol in smart city environment. *Pattern Recognit. Lett.* **2020**, *138*, 439–446, ISSN 0167-8655. [CrossRef]
23. Ghahramani, M.; Javidan, R.; Shojafar, M. A secure biometric-based authentication protocol for global mobility networks in smart cities. *J. Supercomput.* **2020**, *76*, 8729–8755. [CrossRef]
24. Xie, Q.; Li, K.; Tan, X.; Han, L.; Tang, W.; Hu, B. A secure and privacy-preserving authentication protocol for wireless sensor networks in smart city. *J. Wirel. Com. Netw.* **2021**, *2021*, 119. [CrossRef]
25. Xia, X.; Ji, S.; Vijayakumar, P.; Shen, J.; Rodrigues, J.J. An efficient anonymous authentication and key agreement scheme with privacy-preserving for smart cities. *Int. J. Distrib. Sens. Netw.* **2021**, *17*, 1–13. [CrossRef]
26. Deebak, B.D.; Al-Turjman, F. Secure-user sign-in authentication for IoT-based eHealth systems. *Complex Intell. Syst.* **2021**, *7*, 2157–2177. [CrossRef]
27. Hammami, H.; Yahia, S.B.; Obaidat, M.S. A lightweight anonymous authentication scheme for secure cloud computing services. *J. Supercomput.* **2021**, *77*, 1693–1713. [CrossRef]
28. Masud, M.; Gaba, G.S.; Choudhary, K.; Alroobaea, R.; Hossain, M.S. A robust and lightweight secure access scheme for cloud based E-healthcare services. *Peer Peer Netw. Appl.* **2021**, *14*, 3043–3057. [CrossRef] [PubMed]
29. Zhang, Y.; Sun, Y.; Sun, Y.; Jin, R.; Lin, K.; Lin, K.; Liu, W.; Liu, W. High-performance isolation computing technology for smart IoT healthcare in cloud environments. *IEEE Internet Things J.* **2021**, *8*, 16872–16879. [CrossRef]
30. Burrows, M.; Abadi, M.; Needham, R. A Logic of Authentication. *ACM Trans. Comput. Syst.* **1990**, *8*, 18–36. [CrossRef]
31. AVISPA. Automated Validation of Internet Security Protocols and Applications. Available online: http://www.avispa-project.org/ (accessed on 25 May 2022).
32. AVISPA. Web Tool. Available online: https://www.avispa-project.org/web-interface/index.php (accessed on 25 May 2022).
33. Dang, Q.H. *Secure Hash Standard*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 1995.
34. Xu, L.; Wu, F. Cryptanalysis and improvement of a user authentication scheme preserving uniqueness and anonymity for connected health care. *J. Med. Syst.* **2015**, *39*, 10. [CrossRef]
35. Nyangaresi, V.O. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. *Ad Hoc Networks* **2023**, *142*, 103117. [CrossRef]
36. Bahaa, H.T.; Liu, H.; Firas, A.; Lu, H.; Ali, A.; Yassin, A.; Mohammed, J. A Secure and Lightweight Three-Factor Remote User Authentication Protocol for Future IoT Applications. *J. Sens.* **2021**, *2021*, 8871204. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.