scientific reports

OPEN

Smart city energy efficient data privacy preservation protocol based on biometrics and fuzzy commitment scheme

Vincent Omollo Nyangaresi[1,2], Zaid Ameen Abduljabbar[3,4,5]✉, Keyan Abdul-Aziz Mutlaq[6,7], Salim Sabah Bulbul[8], Junchao Ma[4]✉, Abdulla J. Y. Aldarwish[3], Dhafer G. Honi[3,9], Mustafa A. Al Sibahee[10,11] & Husam A. Neamah[12]

Advancements in cloud computing, flying ad-hoc networks, wireless sensor networks, artificial intelligence, big data, 5th generation mobile network and internet of things have led to the development of smart cities. Owing to their massive interconnectedness, high volumes of data are collected and exchanged over the public internet. Therefore, the exchanged messages are susceptible to numerous security and privacy threats across these open public channels. Although many security techniques have been designed to address this issue, most of them are still vulnerable to attacks while some deploy computationally extensive cryptographic operations such as bilinear pairings and blockchain. In this paper, we leverage on biometrics, error correction codes and fuzzy commitment schemes to develop a secure and energy efficient authentication scheme for the smart cities. This is informed by the fact that biometric data is cumbersome to reproduce and hence attacks such as side-channeling are thwarted. We formally analyze the security of our protocol using the Burrows–Abadi–Needham logic logic, which shows that our scheme achieves strong mutual authentication among the communicating entities. The semantic analysis of our protocol shows that it mitigates attacks such as de-synchronization, eavesdropping, session hijacking, forgery and side-channeling. In addition, its formal security analysis demonstrates that it is secure under the Canetti and Krawczyk attack model. In terms of performance, our scheme is shown to reduce the computation overheads by 20.7% and hence is the most efficient among the state-of-the-art protocols.

Keywords Authentication, Biometrics, Fuzzy commitment, Security, Privacy, Efficiency, Hamming distance, Smart city

A smart city refers to a geographical area where technologies such as energy production, logistics and information communication technology are amalgamated to enhance environmental quality, intelligent development, citizen well-being, participation and inclusion. As explained in[1,2], smart cities utilize data-driven technologies to boost sustainability, efficiency, quality of life of the citizens and streamline city services. In addition, the usage of smart city data and technologies facilitate efficient and optimized management of resources, urban services and assets, as well as aiding in making informed decisions[3,4]. The advancements in big data, cloud computing,

[1]Department of Computer Science and Software Engineering, Jaramogi Oginga Odinga University of Science and Technology, Bondo 40601, Kenya. [2]Department of Applied Electronics, Saveetha School of Engineering, SIMATS, Chennai 602105, Tamilnadu, India. [3]Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq. [4]College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China. [5]Shenzhen Institute, Huazhong University of Science and Technology, Shenzhen 518000, China. [6]IT and Communications Center, University of Basrah, Basrah 61004, Iraq. [7]School of Computer Sciences, UniversitiSains Malaysia, USM, 11800 Gelugor, Penang, Malaysia. [8]Directorate General of Education Basra, Ministry of Education, Basra 61004, Iraq. [9]Department of IT, University of Debrecen, Debrecen 4002, Hungary. [10]National Engineering Laboratory for Big Data System Computing Technology, Shenzhen University, Shenzhen 518060, China. [11]Computer Technology Engineering Department, Iraq University College, Basrah 61004, Iraq. [12]Mechatronics Department, Faculty of Engineering, University of Debrecen, Ótemető U. 4-5, Debrecen 4028, Hungary. ✉email: zaid.ameen@uobasrah.edu.iq; majunchao@sztu.edu.cn

Flying Ad-Hoc Networks (FANET), Wireless Sensor Networks (WSNs), Artificial Intelligence (AI), 5th generation mobile network (5G) and Internet of Things (IoT) have led to considerable traction towards smart cities[5–8]. These technologies enable smart cities to collect, analyze and share data from a myriad of sources such as social media, sensors, vehicles, electronic devices, machines and mobile devices. The capabilities of interconnecting a large pool of heterogeneous smart devices enable seamless connections to the smart city environment devoid of communication loss[9]. This helps improve smart city operations and services in terms of enhanced traffic flow, reduced crime rates, energy efficiency and improved citizen engagement.

According to[10], the deployment of heterogeneous communication modes to interconnect smart devices enables the smart cities to have direct exploitation of resources, facilitating easy access to information. In addition, it offers pervasive computing, comprehensive perception, ubiquitous and reliable services. These services may include smart parking, environmental monitoring[11], smart traffic lights, rescue operations[12], smart transportation, remote health monitoring, surveillance, disaster management, search, and traffic monitoring, which can be accomplished by WSNs or Internet of Drones (IoD). As such, smart cities are characterized by high responsiveness, high connectivity, enhanced sustainability, improved quality of life, elevated intelligence, enhanced resource utilization and affordable cost of living[13]. The low cost, flexibility, ease of deployment wide and range of applications of the WSNs and IoD have all led to rise in smart city adoption[14].

Although smart cities provide numerous services and merits, they are exposed to numerous security, performance and privacy challenges. For instance, a typical smart city is composed of numerous sensors and IoT devices that generate massive volumes of data. Some of these data items contain user-specific information such as habits, location and behavior. Since the collected data are exchanged over the public channels, they are susceptible to attacks[15–17]. In addition, some sensors and drones are placed in unattended environment but accessible locations and hence can be physically captured by the attackers[18]. Thereafter, the data stored in their memories can be extracted. Using the obtained credential, attackers can impersonate as legitimate entities. In addition, the authenticity of users, Cyber-Physical System (CPS), and Customer Premises Equipment (CPE) such as sensors and actuators is a major concern in smart cities. The high number of interconnected heterogeneous devices increases the surface from which adversaries can launch attacks, which can compromise economic development, safety and well-being of the users[19]. It is also possible for the collected data to be misused by the end users, posing serious threat to the smart cities[20]. Moreover, some of the devices in smart cities have vulnerabilities which can be exploited by the adversaries to steal data, gain unauthorized access and manipulate the systems.

Based on the above discussion, it is evident that security and privacy are key challenges that need to be solved in smart cities. There is therefore need for the development of robust security schemes that can protect privacy, authenticity and data integrity[17,21–24]. As explained in[25], reliable data measurement is critical for most IoT applications. As such, there is need of ensuring that data is generated and transferred by only authorized users and devices. To this end, various authentication protocols have been developed for the smart cities. However, majority of them fail to offer user anonymity and are vulnerable to attacks such as Denial of Service (DoS)[13]. In addition, majority of these schemes deploy public key cryptography[26] which is inefficient for the power and energy-limited smart city sensors. As such, the design of secure and truly lightweight security solutions for smart cities is still a challenging activity.

Research contributions

- We leverage on biometrics, error correction codes and fuzzy commitment schemes to develop a secure and energy efficient authentication scheme for the smart cities.
- Unlike majority of the current schemes that deploy timestamps to prevent replay attacks, our protocol incorporates random nonces in all exchanged messages. This is demonstrated to address security issues such as de-synchronization attacks inherent in timestamp-based schemes.
- We execute extensive formal security analysis using the BAN logic to show that our scheme performs strong mutual authentication and key negotiation in an appropriate manner.
- Informal security analysis is carried out to demonstrate that the proposed protocol supports numerous functional and security features such as strong mutual authentication, anonymity and perfect key secrecy. In addition, this analysis shows that our scheme can withstand a myriad of smart city security threats such as session hijacking, privileged insider and side-channeling attacks.
- Elaborate comparative evaluations are carried out to show that the proposed protocol incurs the lowest computation overheads and hence is energy efficient.

The rest of this paper is structured as follows: "Related work" section discusses related works while "The proposed protocol" section presents the proposed protocol. On the other hand, "Security analysis" section discusses the security analysis of our scheme while "Performance evaluation" section describes its performance evaluation. Towards the end of this paper, "Conclusion and future work" section presents the conclusion and future research work.

Mathematical preliminaries

In this section, we provide some mathematical formulations for the key cryptographic building blocks of the proposed scheme. This include fuzzy commitment, one way hashing and error correcting codes.

One way hashing
Suppose that $\boldsymbol{N}$ is a set of all positive integers, P_k is a family of uniform probability distributions and L is a polynomial such that $L(k) > k$. Then, H represents a family of functions which are defined by $H = P_k H_k$, where H_k is a multi-set of functions from $\sum^{\mathcal{L}(k)}$ to $\sum^{k}$. Here, $P_k(x) = 1/2^{\mathcal{L}(k)}$ for all $x \in \sum^{\mathcal{L}(k)}$. H is referred to as a hash function, which compresses $L(k)$-bit input into some k-bit output strings.

Definition 1 Let us consider two strings $a, b \in \sum^{\mathcal{L}(k)}$, where $a \neq b$. We say that string a collides with string b under $h \in H_k$, or (a, b) is a collision pair for h, provided that $h(a) = h(b)$.

Definition 2 H is regarded as polynomial time computable on condition that there exists a polynomial (in k) time algorithm that derives all $h \in H$.

Definition 3 H is regarded as accessible provided that there exists a probabilistic time algorithm which takes input $k \in \boldsymbol{N}$ and outputs homogeneously at random a depiction of $h \in H_k$.

Error correcting codes
In noisy transmission channels, error correcting code (*ecc*) is crucial for accurate reception of the transmitted data. Particularly, error correcting codes are critical in fuzzy commitment systems where they ensure that data is exchanged accurately over noisy transmission channels. Suppose that Ψ is a set of messages, where $\Psi = \{0,1\}^{\varphi}$. Then, an error correcting code is made up of a set of codephrases $CP \subseteq \{0,1\}^{\rho}$. A typical *ecc* comprises of a translation function ω and decoding function f, where ω: $\Psi \rightarrow CP$ and f: $\{0,1\}^{\rho} \rightarrow CP \cup \{\gamma\}$. Denoting the Hamming distance as H, then the decoding function maps a ρ—bit string S to the closest codephrase in CP in terms of H, otherwise it outputs γ. Prior to transmission, any message $\psi \in \Psi$ is mapped to an element in CP. For improved redundancy, $\rho > \varphi$. Suppose that θ is the correction threshold, and $\tau \in \{0,1\}^{\rho}$ is the error term. Then, for codephrase $cp \in CP$ and Hamming weight $||\tau|| \leq \theta$, we have $f(cp \oplus \tau) = cp$.

Fuzzy commitment
Due to the noisy nature of biometric data, the input biometrics is not exactly similar to the biometric templates. Therefore, the biometric template can be deployed in fuzzy commitment schemes. Suppose that h: $\{0,1\}^{\rho} \rightarrow \{0,1\}^{\chi}$ is a collision-resistant one-way hashing function. We also let w be the witness, $\lambda = h(cp)$ and $\varepsilon = w \oplus cp$. Then, the fuzzy commitment scheme F: $(\{0,1\}^{\rho}, \{0,1\}^{\rho}) \rightarrow (\{0,1\}^{\chi}, \{0,1\}^{\rho})$ commits codephrase $cp \in CP$ using a ρ – bit witness w as $F(cp, w) = (\lambda, \varepsilon)$. Provided that witness w^* is fairly close to w but not necessarily equivalent to w, then commitment $F(cp, w) = (\lambda, \varepsilon)$ can be opened using w^*. Suppose that this commitment is sent from T towards R. Therefore, the opening of this commitment at R using w^* involves the derivation of $cp^* = f(w^* \oplus \varepsilon)$. Since $\varepsilon = w \oplus cp$, then cp^* can also be expressed as $cp^* = f(cp \oplus (w^* \oplus w))$. Thereafter, R confirms whether $\lambda \stackrel{?}{=} h(cp^*)$. Provided that this condition holds, then the fuzzy commitment is effectively opened. Otherwise, witness w^* is flagged as invalid. We apply this fuzzy commitment concept in our biometric authentication procedures by treating the biometric template as witness w. As such, the user inputs biometric data (seen as witness w^*) which is deployed to open codephrase cp, provided that w^* is closer to w.

Attack model
In the proposed scheme, the adversary is assumed to have all the capabilities in the Canetti and Krawczyk (CK) threat model. Therefore, the communication process within the smart city is executed over the public internet and hence the attacker can have full control of this channel. In addition, the attacker can eavesdrop, alter, delete and insert bogus messages in the communication channel during message exchanges over the public smart city wireless channels. Moreover, all the sensitive data stored in the sensor nodes can be extracted upon physical capture of these nodes. It is also possible for all secret information, ephemeral secrets and session states to be compromised via session-hijacking attacks.

Related work
Many security techniques have been developed over the recent past to offer security protection in IoT and other devices interconnected in smart cities[27–31]. However, these schemes have extensive communication and computation overheads[32]. Although the protocol in[33] is lightweight and hence can address this issue, it cannot withstand outsider attackers[34]. Blockchain technology[35] can provide authentication and decentralized management of identity as well as authorization policies. Therefore, many blockchain-based security schemes have been presented in[36–43]. However, these schemes incur high storage and computation overheads which are not suitable for the sensors[44]. Therefore, a lightweight authentication scheme is developed in[3]. However, the communication costs analysis of this scheme is missing. In addition, it has not been evaluated against attacks such as side-channeling and de-synchronization.

Based on the Physically Unclonable Function (PUF), mutual authentication schemes are presented in[4,45,46]. Although these protocols can withstand physical capture and side-channeling attacks, PUF-based schemes have stability challenges[47]. On the other hand, biometric-based schemes have been introduced in[48–51]. However, the three-factor authentication protocol in[48] cannot preserve perfect backward secrecy[52]. Therefore, an improved scheme is presented in[52]. Unfortunately, this protocol is susceptible to offline password guessing, forgery, session key disclosure and replay attacks[49]. In addition, it cannot uphold perfect forward secrecy and data confidentiality. On the other hand, the protocol in[50] is vulnerable to impersonation and stolen verifier attacks[51]. In addition, it fails to preserve user untraceability. To prevent single-point of failure attacks, a scheme that is devoid of trusted issuer is developed in[53]. However, comparative security and performance analyses of this scheme have not been carried out. Similarly, feasibility, scalability and comparative analyses against the state of the art techniques are missing in[54].

To mitigate service-oriented attacks in smart cities, a context-based trust model is presented in[55]. However, processing huge volumes of contextual data results in high computation overhead[56]. Similarly, the quantum-inspired technique presented in[57] incurs extensive computation overheads due to the required quantum computing[58]. Although an energy-efficient framework for IoT developed in[59] can address this issue, its comparative performance and security analyses have not be carried out. The verification scheme in[60] is efficient and hence can address the performance issues in[55,57]. However, it fails to provide robust identity check and user anonymity[61]. Similarly, the Elliptic Curve Cryptography (ECC) based protocol in[61] cannot offer anonymity and untraceability. Therefore, an ECC based anonymous authentication protocol is introduced in[13], while an identity based technique is presented in[62] to offer strong unforgeability and anonymity. Although the scheme in[13] is shown to resist DoS attacks, its numerous point multiplications can lead to high computation costs. Similarly, the fuzzy extractor based protocol in[63] incurs heavy computation overheads[32]. On the other hand, identity-based schemes have key escrow problems[64].

To protect smart cities against botnet attacks, an algorithm based on Long Short-Term Memory (LSTM) is developed in[65]. However, its evaluation is carried out on a single dataset of botnet attacks and hence fails to reflect a variety of attack vectors in a typical smart city. In addition, its performance evaluation in terms of the required resources has not been presented. To ensure access control and high security level, Public Key Cryptography (PKC) based protocols have been developed in[66–68]. However, these schemes are susceptible to physical capture attacks and hence their stored secret credentials can be retrieved[4]. Thereafter, the attackers are able to impersonate the entities whose credentials have been extracted. In addition, most of these PKC-based schemes incur extensive communication and computation overheads[69]. Moreover, the homomorphic encryption based protocol in[66] is vulnerable to privileged insider and session key disclosure attacks[4]. On its part, the bilinear pairing based protocol in[67] fails to offer perfect forward secrecy and cannot withstand impersonation attacks[68]. In addition, the deployed bilinear pairing operations incur extensive communication and computation overheads and hence cannot support real-time services provision in smart cities. Regarding the ECC-based developed in[68], it is susceptible to impersonation, replay and privileged insider attacks[70]. In addition, it cannot offer strong mutual authentication among the communicating entities. Therefore, an improved security technique is presented in[70]. However, this protocol is vulnerable to attacks such as server spoofing, session key disclosure and forgery[4]. Although the schemes in[71,72] can solve some of these challenges, they have not been evaluated against de-synchronization attacks. On their part, the three-factor security schemes in[48–52] are susceptible to potential security attacks[4]. Although the protocol in[73] addresses some of the attacks such as ephemeral leakage, it cannot withstand identity guessing attacks[74–76].

Based on the discussion above, it is evident that many schemes have been developed for the smart city environment. However, the attainment of perfect smart city security at low computation and communication is still an open challenge. For instance, many security protocols have been shown to be vulnerable to numerous attacks while others cannot support anonymity, mutual authentication and untraceability. In addition, some of these schemes do not incorporate biometric and password change procedures. Moreover, some of these security techniques incur extensive computation and communication overheads while others deploy centralized architecture which can easily result in central failure, denial of services and privacy breaches[39]. The proposed protocol is demonstrated to address some of these security, performance and privacy challenges. For instance, our scheme incurs the lowest computation overheads among its peers and hence addresses performance challenges in most of the above protocols. In addition, it provides support for anonymity, mutual authentication and untraceability which are features missing in most of the above schemes. Moreover, it mitigates attacks which are rarely considered in most of the existing protocols. Such attacks include de-synchronization, eavesdropping, session hijacking, forgery and side-channeling.

The proposed protocol

The elliptic curve cryptography offer offers strong security at relatively shorter key sizes compared to other public key cryptographies such as RSA. Therefore, we deploy elliptic curve cryptography in the proposed scheme. To address physical and side-channeling attacks, we leverage on biometric, error correction codes and fuzzy commitment schemes.

Motivation

Smart cities have streamlined services in urban centers, leading to the enhancement on the quality of life of the citizens. In a typical smart city, numerous smart devices are interconnected to facilitate activities such as surveillance, shipping, logistics, healthcare and warehousing. As such, high volumes of data are generated and exchanged among these smart devices. Since these message exchanges are carried out over the public internet, many security and privacy threats lurk in this environment. For instance, personal user information can be eavesdropped over the public channels while successful sensor and device capture can facilitate impersonation attacks. Therefore, past research works have presented numerous security techniques to alleviate these challenges. Unfortunately, majority of these schemes are based on computationally extensive cryptographic operations such as bilinear pairings. Consequently, these schemes are inefficient for the computation, bandwidth, storage and energy constrained sensor nodes. In addition, some of the presented security solutions still have security and privacy related issues[77,78] such as susceptibility to physical, impersonation, privileged insider and

Man-in-the-Middle (MitM) attacks. Therefore, the design of provably secure and yet efficient[79] authentication protocols for smart cities is a nontrivial challenge.

Requirements

In smart city environment, security efficiency[80] is critical in ensuring that users can authenticate and access the required data in a timely manner. This is particularly important due to the bandwidth, energy, computation power and storage constraints of the interconnected sensor networks in light of this, the proposed protocol must fulfill the following security and performance requirements.

Mutual authentication All the entities involved in message exchanges within the smart city must verify each other at the onset of the communication process.

Key agreement Upon successful validation of each other, session keys should be setup among the communicating parties. This key is deployed to encipher all the exchanged data within the smart city.

Perfect key secrecy It should be computationally infeasible for the adversary to capture the current session keys and utilize them to derive keys for the previous and subsequent sessions.

Anonymity The adversaries with the capabilities of eavesdropping the communication channel should not be in a position to obtain the real identities of the communicating parties.

Untraceability An adversary should be unable to associate any communication sessions to a particular network entity.

Resilience against threats typical security threats such as de-synchronization, denial of service, physical, eavesdropping, session hijacking, privileged insider, KSSTI, replays, forgery, MitM, impersonation and side-channeling should be curbed in our scheme.

Resource efficiency Owing to the resource-constrained nature of the smart city sensors and devices, the proposed scheme should be computationally efficient.

In our scheme, each user deploys his/her mobile device (MD_i) to interact with the smart city sensor SN_j through some gateway node GW_k. In this environment, the GW_k bridges the connection between MD_i and SN_j as shown in Fig. 1.

Table 1 presents all the notations deployed throughout this paper. The major phases executed in our scheme include the system setup, registration, login, authentication, key negotiation, and password change. The subsections below describe these phases in greater details.

System setup

This phase is carried out by the gateway node GW_k. The goal is to derive the long term keys that will be utilized in the latter phases of our scheme. The following 3 steps are executed during the system setup phase.

Step 1 The GW_k selects some elliptic curve E and additive group G over finite field F_p. Here, the generator is point P whose order is a large prime number q.

Step 2 GW_k generates nonce $n \in Z_q^*$ and sets it as its secret key. Next, it derives its corresponding public key as $P_k = nP$.

Step 3 The GW_k selects M_k as its master key and privately keeps both n and M_k. Finally, it publishes parameter set $\{P, P_k, G, E(F_p)\}$.

Sensor node registration

Prior to actual deployment in their application domains, each sensor node SN_j must be registered at the gateway node GW_k. The aim is to assign these sensors some security values that are deployed during the login, authentication and key negotiation phase. The following 2 steps are executed in this phase.

Step 1 The GW_k chooses $SNID_j$ as sensor node SN_j unique identity. This is followed by the derivation of private key $K_{GS} = h(SNID_j||M_k)$. GW_k sends values $SNID_j$ and K_{GS} to SN_j over secure channels as shown in Fig. 2.

Step 2 Upon receiving parameters $SNID_j$ and K_{GS} from the GW_k, the SN_j stores them in its memory. The sensor node is now ready to be deployed to the field.

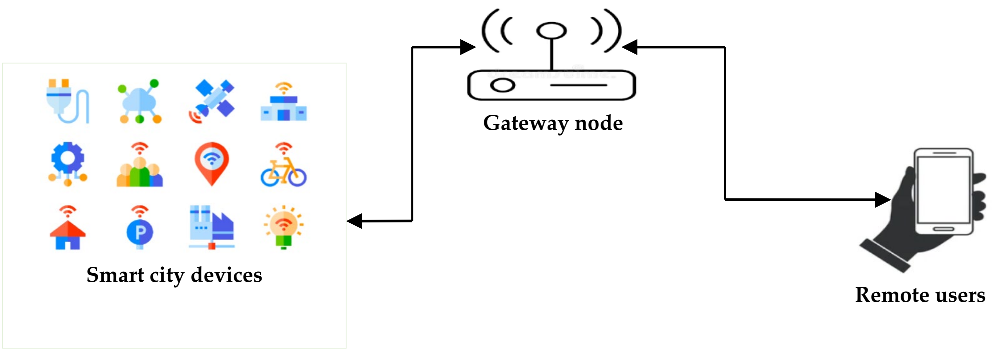

Figure 1. Smart city network model.

Symbol	Description
GW_k	Gateway node k
SN_j	Sensor node j
MD_i	User's mobile device i
n	Secret key for GW_k
P_k	Public key for GW_k
M_k	Master key for GW_k
$SNID_j$	Unique identity for sensor node j
K_{GS}	Secret key shared between GW_k and SN_j
U_i	User i
UID_i	Unique identity for user i
PW_i	Password for user i
SK_S	Session key derived at SN_j
SK_G	Session key derived at the GW_k
SK_D	Session key derived at the MD_i
h (.)	One-way hashing function
||	Concatenation operation
$\oplus$	XOR operation

Table 1. Notations.

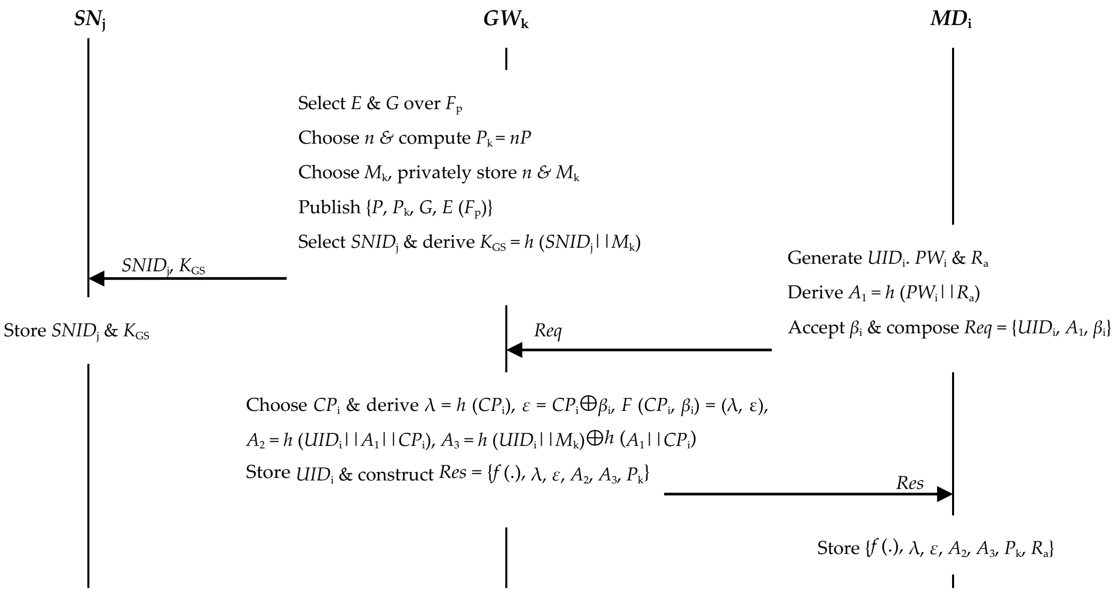

Figure 2. System setup and registration.

User registration

All users within the smart city network must be registered at their respective gateway nodes. During this phase, the users are assigned security tokens that they will deploy to securely acquire data from the sensor devices deployed in a given domain. The following 4 steps are executed during this process.

Step 1 The user U_i through the MD_i generates unique identity UID_i and password PW_i. Next, nonce R_a is generated which is then used to derive value $A_1 = h (PW_i||R_a)$.

Step 2 The U_i imprints biometric data β_i onto the MD_i. Finally, registration request $Req = \{UID_i, A_1, \beta_i\}$ is constructed and forwarded to the GW_k over secure channels as shown in Fig. 2.

Step 3 Upon receiving registration request Req from U_i, the GW_k selects some random codephrase $CP_i \in CP$ for this particular user U_i. Next, it derives tokens $\lambda = h (CP_i)$, $\varepsilon = CP_i \oplus \beta_i$, $F (CP_i, \beta_i) = (\lambda, \varepsilon)$, $A_2 = h (UID_i||A_1||CP_i)$ and $A_3 = h (UID_i||M_k) \oplus h (A_1||CP_i)$. Finally, it stores UID_i in its database before composing registration response $Res = \{f (.), \lambda, \varepsilon, A_2, A_3, P_k\}$ that is sent to the U_i over secured channels.

Step 4 After getting registration response Res from the GW_k, the U_i through MD_i stores value set $\{f (.), \lambda, \varepsilon, A_2, A_3, P_k, R_a\}$ in its memory.

Login, authentication and key negotiation

This phase is activated whenever the user U_i through the MD_i wants some access to the data help by the sensors. Here, the security tokens assigned during the registration phase are deployed to authenticate U_i to the gateway node GW_k. To accomplish this, the following 8 steps are executed.

Step 1 User U_i imprints his/her biometric data β_i^* onto the MD_i upon which value $CP_i^* = f(\varepsilon \oplus \beta_i^*)$ is computed. Since $\varepsilon = CP_i \oplus \beta_i$, CP_i^* can also be expressed as $CP_i^* = f(CP_i \oplus (\beta_i \oplus \beta_i^*))$. Thereafter, the MD_i checks whether $h(CP_i^*) \stackrel{?}{=} \lambda = h(CP_i)$. Basically, the user login session is terminated upon verification failure. Otherwise, U_i has passed the biometric validation and hence proceeds to input unique identity UID_i and password PW_i into the MD_i.

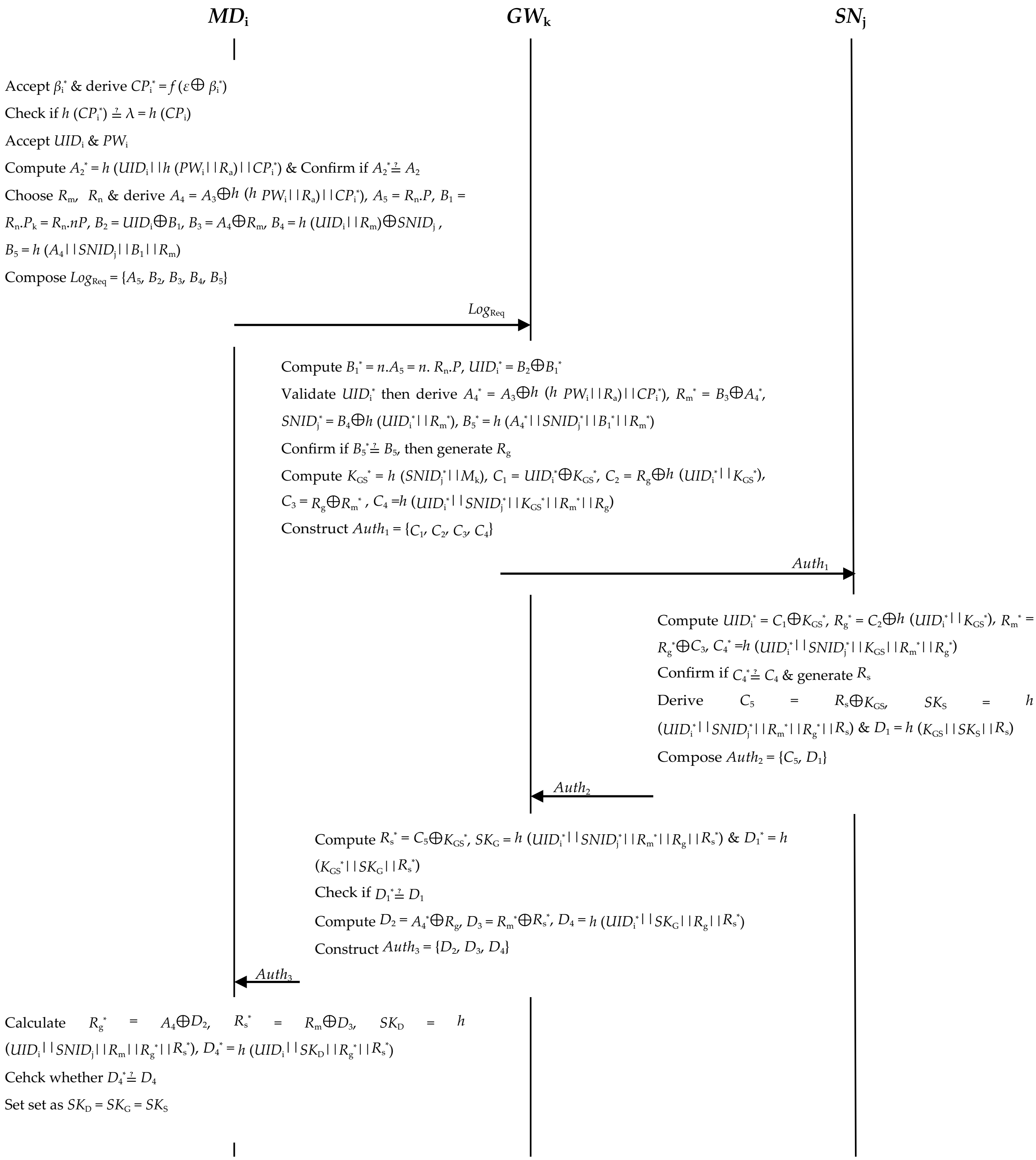

Figure 3. Login, authentication and key negotiation.

Step 2 The MD_i computes $A_2^* = h\ (UID_i||h\ (PW_i||R_a)||CP_i^*)$ and confirms whether $A_2^* \stackrel{?}{=} A_2$. Since $A_1 = h\ (PW_i||R_a)$, this verification should be successful otherwise the session is aborted. However, if this validation is successful, both user identity and password have been authenticated by the MD_i.

Step 3 The MD_i selects nonce R_m and $R_n \in Z_q^*$ and computes values $A_4 = A_3 \oplus h\ (h\ PW_i||R_a)||CP_i^*)$, $A_5 = R_n.P$, $B_1 = R_n.P_k = R_n.nP$, $B_2 = UID_i \oplus B_1$, $B_3 = A_4 \oplus R_m$, $B_4 = h\ (UID_i||R_m) \oplus SNID_j$ and $B_5 = h\ (A_4||SNID_j||B_1||R_m)$. At the end, the MD_i constructs login request message $Log_{Req} = \{A_5, B_2, B_3, B_4, B_5\}$ that is transmitted to the GW_k over public channels as shown in Fig. 3.

Step 4 Upon receiving login request message Log_{Req}, the GW_k derives values $B_1^* = n.A_5 = n.\ R_n.P$, $UID_i^* = B_2 \oplus B_1^*$. This is followed by the confirmation of whether UID_i^* is in its database. Provided that UID_i^* cannot be found in its database, the MD_i login request is rejected. Otherwise, the GW_k calculates $A_4^* = A_3 \oplus h\ (h\ PW_i||R_a)||CP_i^*)$, $R_m^* = B_3 \oplus A_4^*$, $SNID_j^* = B_4 \oplus h\ (UID_i^*||R_m^*)$ and $B_5^* = h\ (A_4^*||SNID_j^*||B_1^*||R_m^*)$.

Step 5 The GW_k checks if $B_5^* \stackrel{?}{=} B_5$ such that the session is terminated if this condition does not hold. Otherwise, it generates nonce R_g and derives values $K_{GS}^* = h\ (SNID_j^*||M_k)$, $C_1 = UID_i^* \oplus K_{GS}^*$, $C_2 = R_g \oplus h\ (UID_i^*||K_{GS}^*)$, $C_3 = R_g \oplus R_m^*$ and $C_4 = h\ (UID_i^*||SNID_j^*||K_{GS}^*||R_m^*||R_g)$. At last, it composes authentication message $Auth_1 = \{C_1, C_2, C_3, C_4\}$ which is sent to the sensor node SN_j over public channels.

Step 6 On receiving authentication message $Auth_1$, the SN_j derives $UID_i^* = C_1 \oplus K_{GS}^*$, $R_g^* = C_2 \oplus h\ (UID_i^*||K_{GS}^*)$, $R_m^* = R_g^* \oplus C_3$ and $C_4^* = h\ (UID_i^*||SNID_j^*||K_{GS}||R_m^*||R_g^*)$. Next, it checks if $C_4^* \stackrel{?}{=} C_4$ such that the session is aborted upon verification failure. Otherwise, the SN_j generates nonce R_s before calculating parameter $C_5 = R_s \oplus K_{GS}$, session key $SK_S = h\ (UID_i^*||SNID_j^*||R_m^*||R_g^*||R_s)$ and value $D_1 = h\ (K_{GS}||SK_S||R_s)$. Finally, SN_j constructs authentication response message $Auth_2 = \{C_5, D_1\}$ which is sent over to GW_k.

Step 7 After getting authentication response message $Auth_2$, the GW_k derives value $R_s^* = C_5 \oplus K_{GS}^*$, session key $SK_G = h\ (UID_i^*||SNID_j^*||R_m^*||R_g||R_s^*)$ and parameter $D_1^* = h\ (K_{GS}^*||SK_G||R_s^*)$. This is followed by the confirmation of whether $D_1^* \stackrel{?}{=} D_1$ such that the session is terminated upon verification failure. Otherwise, the GW_k derives parameters $D_2 = A_4^* \oplus R_g$, $D_3 = R_m^* \oplus R_s^*$ and $D_4 = h\ (UID_i^*||SK_G||R_g||R_s^*)$. At last, it composes authentication message $Auth_3 = \{D_2, D_3, D_4\}$ that is forwarded to the MD_i.

Step 8 On receiving authentication message $Auth_3$, the MD_i calculates $R_g^* = A_4 \oplus D_2$, $R_s^* = R_m \oplus D_3$, session key $SK_D = h\ (UID_i||SNID_j||R_m||R_g^*||R_s^*)$ and value $D_4^* = h\ (UID_i||SK_D||R_g^*||R_s^*)$. It then verifies whether $D_4^* \stackrel{?}{=} D_4$ such that the session is aborted upon validation failure. Otherwise, user U_i, GW_k and SN_j have successfully authenticated each other and negotiated session keys. As such, the session key is set as $SK_D = SK_G = SK_S$ and is shared among these three entities. Afterwards, U_i can securely access sensed data held at SN_j vial GW_k.

Password change

In this phase, the user executes password change upon its compromise. To reduce on communication overheads, this change is carried out without contacting the gateway node GW_k. the following…steps are executed during this phase.

Step 1 The user U_i imprints biometric data β_i^*onto the MD_i. Thereafter, the MD_i derives $CP_i^* = f\ (\varepsilon \oplus \beta_i^*) = f(CP_i \oplus (\beta_i \oplus \beta_i^*))$.Next, the MD_i validates whether $h\ (CP_i^*) \stackrel{?}{=} \lambda = h\ (CP_i)$ such that the password change session is terminated upon verification failure. Otherwise, the user U_i has passed biometric authentication.

Step 2 User U_i inputs UID_i and PW_i into the MD_i after which it calculates $A_2^* = h\ (UID_i||h\ (PW_i||R_a)||CP_i^*)$. This is followed by the confirmation of whether $A_2^* \stackrel{?}{=} A_2$ such that the session is aborted upon verification failure. Otherwise, user U_i is prompted to input new password PW_i^{New}.

Step 3 The MD_i computes $A_2^{New} = h\ (UID_i||h\ (PW_i^{New}||R_a)||CP_i^*)$ and $A_3^{New} = A_3 \oplus h\ (h\ (PW_i||R_a)||CP_i^*) \oplus h\ (h\ (PW_i^{New}||R_a)||CP_i^*)$. Finally, the MD_i updates value set $\{A_2, A_3\}$ with their refreshed counterparts $\{A_2^{New}, A_3^{New}\}$ in its memory.

Security analysis

In this section, we formally and informally analyze the security features provided by the proposed scheme. Whereas the formal security analysis is executed using Burrows–Abadi–Needham logic (BAN) logic, informal security analysis is carried out by formulating and proofing some propositions.

Formal security analysis

The aim of this sub-section is to verify that our scheme performs strong mutual authentication and key negotiation in an appropriate manner. The notations used throughout this proof are described below.

(A): *A* is fresh.

$\langle A \rangle_B$: *A* is enciphered using *B*.

S|≡Y: *S* believes *Y*.

(A, B): *A* or *B* is part of message (*A*, *B*).

S ⊲ Y: *S* sees *Y*.

S|~ A: *S* once said *A*.

$(A, B)_\mu$: *A* or *B* is hashed using *μ*.

S ⇒ A: *S* has jurisdiction over *A*.

$S \stackrel{\mu}{\leftrightarrow} T$: *S* and *T* communicate using shared key *μ*.

In addition to the above BAN logic rules, the following BAN logic rules are used in our proof.

Belief Rule (BR): $\frac{S|\equiv(A), S|\equiv(B)}{S|\equiv(A,B)}$

Message Meaning Rule (MMR): $\frac{S|\equiv S \stackrel{\mu}{\leftrightarrow} T, S \lhd \langle A \rangle_\mu}{S|\equiv T|\sim A}$

Session Keys Rule (SKR): $\frac{S|\equiv\#(A), S|\equiv T|\equiv A}{S|\equiv S \stackrel{\mu}{\leftrightarrow} T}$

Jurisdiction Rule (JR): $\frac{S|\equiv T\Rightarrow A, S|\equiv T|\equiv A}{S|\equiv A}$

Fresh Promotion Rule (FPR): $\frac{S|\equiv \#(A)}{S|\equiv \#(A,B)}$

Nonce Verification Rule (NVR): $\frac{S|\equiv \#(A), S|\equiv T|\sim A}{S|\equiv T|\equiv A}$

To be secure under the BAN logic, the proposed scheme must satisfy the following security goals.

Goal 1: $SN_j| \equiv SN_j \overset{SK_S}{\leftrightarrow} MD_i$

Goal 2: $SN_j| \equiv MD_i| \equiv SN_j \overset{SK_S}{\leftrightarrow} MD_i$

Goal 3: $MD_i| \equiv SN_j \overset{SK_D}{\leftrightarrow} MD_i$

Goal 4: $MD_i| \equiv SN_j| \equiv SN_j \overset{SK_D}{\leftrightarrow} MD_i$

Goal 5: $GW_k| \equiv GW_k \overset{SK_G}{\leftrightarrow} MD_i$

Goal 6: $GW_k| \equiv MD_i| \equiv GW_k \overset{SK_G}{\leftrightarrow} MD_i$

Goal 7: $GW_k| \equiv GW_k \overset{SK_G}{\leftrightarrow} SN_j$

Goal 8: $GW_k| \equiv SN_j| \equiv GW_k \overset{SK_G}{\leftrightarrow} SN_j$

In our scheme, 4 messages are exchanged during the login, authentication and key agreement phase. These messages include $Log_{Req} = \{A_5, B_2, B_3, B_4, B_5\}$, $Auth_1 = \{C_1, C_2, C_3, C_4\}$, $Auth_2 = \{C_5, D_1\}$ and $Auth_3 = \{D_2, D_3, D_4\}$. For ease of analysis, we transform these messages into idealized format as follows.

$MD_i \rightarrow GW_k$: $Log_{Req} = \{A_5, B_2, B_3, B_4, B_5\}$

Idealized format: $\{R_n.P, \langle UID_i\rangle_{R_n.P_k}, \langle R_m\rangle_{h(UID_i||M_k)}, \langle SNID_j\rangle_{h(UID_i||R_m)}, (SNID_j||R_m)_{R_n.P_k, h(UID_i||M_k)}\}$

$GW_k \rightarrow SN_j$: $Auth_1 = \{C_1, C_2, C_3, C_4\}$

Idealized format: $\{\langle UID_i^*\rangle_{KG_S}, \langle R_g\rangle_{h(UID_i^*||KG_S)}, \langle R_m\rangle_{R_g}, (UID_i||SNID_j)_{(R_m, R_g, KG_S)}\}$

$SN_j \rightarrow GW_k$: $Auth_2 = \{C_5, D_1\}$

Idealized format: $\{\langle R_s\rangle_{KG_S}, (R_s)_{(SK_S, KG_S)}$

$GW_k \rightarrow MD_i$: $Auth_3 = \{D_2, D_3, D_4\}$

Idealized format: $\{\langle R_g\rangle_{h(UID_i||KG_S)}, \langle R_s^*\rangle_{R_m^*}, (UID_i^*)_{(R_g, R_s^*, SK_G)}\}$

The following initial state assumptions (SA) are also made.

SA_1: $U_i| \equiv \# R_m$

SA_2: $GW_k| \equiv \# R_g$

SA_3: $SN_j| \equiv \# R_s$

SA_4: $MD_i| \equiv MD_i \overset{nR_n.P}{\leftrightarrow} GW_k$

SA_5: $MD_i| \equiv MD_i \overset{SK_S}{\leftrightarrow} SN_j$

SA_6: $GW_k| \equiv GW_k \overset{R_n.nP}{\leftrightarrow} MD_i$

SA_7: $GW_k| \equiv GW_k \overset{KG_S}{\leftrightarrow} SN_j$

SA_8: $SN_j| \equiv SN_j \overset{SK_S}{\leftrightarrow} MD_i$

SA_9: $SN_j| \equiv SN_j \overset{KG_S}{\leftrightarrow} GW_k$

SA_{10}: $MD_i| \equiv SN_j \Rightarrow R_s, SK_S$

SA_{11}: $MD_i| \equiv GW_k \Rightarrow R_g, SK_G$

SA_{12}: $GW_k| \equiv MD_i \Rightarrow R_m, SK_D, nR_nP$

SA_{13}: $GW_k| \equiv SN_j \Rightarrow R_s \oplus KG_S$

SA_{14}: $SN_j| \equiv GW_k \Rightarrow R_g \oplus h(UID_i||KG_S)$

SA_{15}: $SN_j| \equiv MD_i \Rightarrow R_m, SK_D$

Based on the above BAN logic rules, idealized format of the exchanged messages and the initial state assumptions, we proof that the proposed scheme attains all the above security goals through the following BAN logic proof (*BLP*).

Using the idealized form of Log_{Req} and *BR*, we obtain BLP_1,

BLP_1: $GW_k \triangleleft \{R_n.P, \langle UID_i\rangle_{R_n.P_k}, \langle R_m\rangle_{h(UID_i||M_k)}, \langle SNID_j\rangle_{h(UID_i||R_m)}, (SNID_j||R_m)_{R_n.P_k, h(UID_i||M_k)}\}$

Based on SA_6, BLP_1 and *MMR*, we obtain BLP_2 as follows,

BLP_2: $GW_k| \equiv MD_i \sim \{R_n.P, \langle UID_i\rangle_{R_n.P_k}, \langle R_m\rangle_{h(UID_i||M_k)}, \langle SNID_j\rangle_{h(UID_i||R_m)}, (SNID_j||R_m)_{R_n.P_k, h(UID_i||M_k)}\}$

Using *FPR* and *NVR* on both BLP_2 and SA_1 yields BLP_3 as shown below.

BLP_3: $GW_k| \equiv MD_i| \equiv \{R_n.P, \langle UID_i\rangle_{R_n.P_k}, \langle R_m\rangle_{h(UID_i||M_k)}, \langle SNID_j\rangle_{h(UID_i||R_m)}, (SNID_j||R_m)_{R_n.P_k, h(UID_i||M_k)}\}$

On the other hand, using *JR* on BLP_3, SA_6 and SA_{12} yields BLP_4.

BLP_4: $GW_k| \equiv \{R_n.P, \langle UID_i\rangle_{R_n.P_k}, \langle R_m\rangle_{h(UID_i||M_k)}, \langle SNID_j\rangle_{h(UID_i||R_m)}, (SNID_j||R_m)_{R_n.P_k, h(UID_i||M_k)}\}$

Based on BLP_4, the *SKR* is applied to obtain BLP_5.

BLP_5: $GW_k| \equiv GW_k \overset{SK_G}{\leftrightarrow} MD_i$, hence security **Goal 5** is attained.

On the other hand, *NVR* is applied to both BLP_5 and SA_{12} to yield BLP_6.

BLP_6: $GW_k| \equiv MD_i| \equiv GW_k \overset{SK_G}{\leftrightarrow} MD_i$, achieving security **Goal 6**.

Considering idealized formats of both $Auth_1$ and $Auth_3$, the application of *BR* yields BLP_7 and BLP_8.

BLP_7: $SN_j \triangleleft \{\langle UID_i^*\rangle_{KG_S}, \langle R_g\rangle_{h(UID_i^*||KG_S)}, \langle R_m\rangle_{R_g}, (UID_i||SNID_j)_{(R_m, R_g, KG_S)}\}$

BLP_8: $MD_i \triangleleft \{\langle R_g\rangle_{h(UID_i||KG_S)}, \langle R_s^*\rangle_{R_m^*}, (UID_i^*)_{(R_g, R_s^*, SK_G)}\}$

Using the *MMR* on both BLP_7 and SA_9 results in BLP_9.

BLP_9: $SN_j| \equiv GW_k \sim \{\langle UID_i^*\rangle_{KG_S}, \langle R_g\rangle_{h(UID_i^*||KG_S)}, \langle R_m\rangle_{R_g}, (UID_i||SNID_j)_{(R_m, R_g, KG_S)}\}$

However, the application of *MMR* on both BLP_8 and SA_4 yields BLP_{10}.

BLP_{10}: $MD_i| \equiv GW_k \sim \{\langle R_g\rangle_{h(UID_i||KG_S)}, \langle R_s^*\rangle_{R_m^*}, (UID_i^*)_{(R_g, R_s^*, SK_G)}\}$

Based on BLP_9, SA_2, SA_{14}, FPR and the NVR, we obtain BLP_{11}.
BLP_{11}: $SN_j| \equiv GW_k| \equiv \{\langle UID_i^* \rangle_{KG_S}, \langle R_g \rangle_{h(UID_i^*||KG_S)}, \langle R_m \rangle_{R_g}, (UID_i||SNID_j)_{(R_m, R_g, KG_S)}\}$
Using the FPR and NVR on BLP_{10}, SA_2 and SA_{11}, we get BLP_{12}.
BLP_{12}: $MD_i| \equiv GW_k| \equiv \{\langle R_g \rangle_{h(UID_i||KG_S)}, \langle R_s^* \rangle_{R_m^*}, (UID_i^*)_{(R_g, R_s^*, SK_G)}\}$
On the other hand, the application of JR on BLP_{12} and SA_{11} yields BLP_{13}.
BLP_{13}: $MD_i| \equiv \{\langle R_g \rangle_{h(UID_i||KG_S)}, \langle R_s^* \rangle_{R_m^*}, (UID_i^*)_{(R_g, R_s^*, SK_G)}\}$
According to BLP_{13}, the SKR is applied to get BLP_{14}.
BLP_{14}: $SN_j| \equiv SN_j \overset{SK_S}{\leftrightarrow} MD_i$ and hence security **Goal 1** is achieving.
Based on BLP_{14} and SA_{14}, the SKR is applied to obtain BLP_{15}.
BLP_{15}: $SN_j| \equiv MD_i| \equiv SN_j \overset{SK_S}{\leftrightarrow} MD_i$, achieve **Goal 2**.
On the other hand, using SKR on BLP_{14} yields BLP_{16}.
BLP_{16}: $MD_i| \equiv SN_j \overset{SK_D}{\leftrightarrow} MD_i$ and hence **Goal 3** is realized.
The application of SKR on BLP_{14}, SA_5 and SA_{11} results in BLP_{17}.
BLP_{17}: $MD_i| \equiv SN_j| \equiv SN_j \overset{SK_D}{\leftrightarrow} MD_i$, attaining security **Goal 4**.
Using idealized form of message $Auth_2$, the BR is applied to get BLP_{18}.
BLP_{18}: $GW_k \lhd \{\langle R_s \rangle_{KG_S}, (R_s)_{(SK_S, KG_S)}\}$
However, the usage of MMR on both BLP_{18} and SA_7 results in BLP_{19}.
BLP_{19}: $GW_k| \equiv SN_j \sim \{\langle R_s \rangle_{KG_S}, (R_s)_{(SK_S, KG_S)}\}$
Based on BLP_{19} and SA_3, NVR and FPR are applied to obtain BLP_{20}.
BLP_{20}: $GW_k| \equiv SN_j| \equiv \{\langle R_s \rangle_{KG_S}, (R_s)_{(SK_S, KG_S)}\}$
On the other hand, using JR on BLP_{20}, SA_7 and SA_{13} yields BLP_{21}.
BLP_{21}: $GW_k| \equiv \{\langle R_s \rangle_{KG_S}, (R_s)_{(SK_S, KG_S)}\}$
However, using the SKR on both BLP_{21} and SA_8 yields BLP_{22}.
BLP_{22}: $GW_k| \equiv GW_k \overset{SK_G}{\leftrightarrow} SN_j$, realizing security **Goal 7**.
Based on BLP_{22}, SA_{13} and SA_{15}, the SKR is applied to obtain BLP_{23}.
BLP_{23}: $GW_k| \equiv SN_j| \equiv GW_k \overset{SK_G}{\leftrightarrow} SN_j$ and hence **Goal 8** is attained.

The attainment of all the 8 formulated security goals demonstrates that the proposed scheme achieves strong mutual authentication among the SN_j, MD_i and GW_k. In addition, it confirms that after successful mutual authentication, session key $SK_D = SK_G = SK_S$ is established among these three entities.

Informal security analysis

In this sub-section, we state and proof various propositions to show that our scheme supports numerous security features and is robust against many typical smart city attacks. Based on the attack model in "Attack model" section, an adversary is capable of launching attacks such as de-synchronization, denial of service, eavesdropping, session hijacking, KSSTI, replays, forgery, MitM, privileged insider,physical, side-channeling and impersonation. In this sub-section, we demonstrate that our protocol mitigates all these attacks.

Proposition 1 *Eavesdropping attacks are prevented.*

Proof Suppose that an adversary $\mathring{A}$ is interested in intercepting the exchanged messages after which parameters such as $SNID_j$ and UID_i are retrieved. In our scheme, messages $Log_{Req} = \{A_5, B_2, B_3, B_4, B_5\}$, $Auth_1 = \{C_1, C_2, C_3, C_4\}$, $Auth_2 = \{C_5, D_1\}$ and $Auth_3 = \{D_2, D_3, D_4\}$ are exchanged over public channels. Here, $A_5 = R_n.P$, $B_2 = UID_i \oplus B_1$, $B_3 = A_4 \oplus R_m$, $B_4 = h\ (UID_i||R_m) \oplus SNID_j$, $B_5 = h\ (A_4||SNID_j||B_1||R_m)$, $C_1 = UID_i^* \oplus K_{GS}^*$, $C_2 = R_g \oplus h\ (UID_i^*||K_{GS}^*)$, $C_3 = R_g \oplus R_m^*$, $C_4 = h\ (UID_i^*||SNID_j^*||K_{GS}^*||R_m^*||R_g)$, $C_5 = R_s \oplus K_{GS}$, $D_1 = h\ (K_{GS}||SK_S||R_s)$, $D_2 = A_4^* \oplus R_g$, $D_3 = R_m^* \oplus R_s^*$ and $D_4 = h\ (UID_i^*||SK_G||R_g||R_s^*)$. Clearly, none of these messages contain $SNID_j$ and UID_i in plaintext. Therefore, eavesdropping attacks against our scheme fail.

Proposition 2 *Our scheme thwarts session hijacking and denial of service attacks.*

Proof The aim of adversary $\mathring{A}$ in this attack is to gain access to the MD_i belonging to user U_i, effectively disconnecting him/her from accessing sensory data. To prevent this, our scheme incorporates invalid password, identity and biometric checks. For biometric authentication, the the MD_i checks whether $h\ (CP_i^*) \overset{?}{=} \lambda = h\ (CP_i)$. On the other hand, user password and identity are verified by the MD_i through the confirmation of whether $A_2^* \overset{?}{=} A_2$. In both cases, the session is terminated upon validation failure. Therefore, unauthorized logins that can facilitate session hijacking and denial of service attacks are thwarted.

Proposition 3 *Message replay and de-synchronization attacks are prevented.*

Proof During the login, authentication and session key negotiation phases, random nonces are incorporated in all the exchanged messages. These random nonces include R_m, R_n, R_g and R_s included in parameters $A_5 = R_n.P$, $B_1 = R_n.P_k = R_n.nP$, $B_3 = A_4 \oplus R_m$, $B_4 = h\ (UID_i||R_m) \oplus SNID_j$, $B_5 = h\ (A_4||SNID_j||B_1||R_m)$, $C_2 = R_g \oplus h\ (UID_i^*||K_{GS}^*)$, $C_3 = R_g \oplus R_m^*$, $C_4 = h\ (UID_i^*||SNID_j^*||K_{GS}^*||R_m^*||R_g)$, $C_5 = R_s \oplus K_{GS}$, $D_1 = h\ (K_{GS}||SK_S||R_s)$, $D_2 = A_4^* \oplus R_g$, $D_3 = R_m^* \oplus R_s^*$ and $D_4 = h\ (UID_i^*||SK_G||R_g||R_s^*)$. Therefore, the freshness of messages $Log_{Req} = \{A_5, B_2, B_3, B_4, B_5\}$, $Auth_1 = \{C_1, C_2, C_3, C_4\}$, $Auth_2 = \{C_5, D_1\}$ and $Auth_3 = \{D_2, D_3, D_4\}$ is upheld, thwarting any replay attacks. This is in contrast to most schemes that employ timestamps to prevent replay attacks. In these schemes, these timestamps render them vulnerable to de-synchronization attacks.

Proposition 4 *Our scheme is robust against privileged insider and impersonation attacks.*

Proof The aim of this attack is to allow users with elevated privileges such as system administrators to access users' registration information. Thereafter, the obtained information is utilized to impersonate the legitimate users. During the user registration phase, registration request $Req = \{UID_i, A_1, \beta_i\}$ is constructed by U_i and forwarded to the GW_k over secure channels. Here, UID_i is the user's unique identity, β_i is the user's biometric data and $A_1 = h\ (PW_i||R_a)$. Evidently, privileged users cannot retrieve user's password PW_i from A_1 due to its encapsulation in random nonce R_a and eventual one-way hashing, which is computationally infeasible to reverse.

Proposition 5 *Untraceability and anonymity are preserved.*

Proof Suppose that adversary $\AA$ is interested in tracking particular users and sensors within the network. To realize this, all the messages exchanged over the public channels are intercepted. These messages include $Log_{Req} = \{A_5, B_2, B_3, B_4, B_5\}$, $Auth_1 = \{C_1, C_2, C_3, C_4\}$, $Auth_2 = \{C_5, D_1\}$ and $Auth_3 = \{D_2, D_3, D_4\}$. Thereafter, attempts are made to obtain $SNID_j$ and UID_i. However, according to *Proposition 1*, this attempt will fail. Although parameters $C_2 = R_g \oplus h\ (UID_i^*||K_{GS}^*)$, $C_4 = h\ (UID_i^*||SNID_j^*||K_{GS}^*||R_m^*||R_g)$, and $D_4 = h\ (UID_i^*||SK_G||R_g||R_s^*)$ contain these unique identities, they are scrambled in other security tokens and hashed. This makes it cumbersome for adversary $\AA$ to retrieve them. To prevent traceability attacks, the MD_i generates random nonces R_a, R_m and R_n that are incorporated in values $A_5 = R_n.P$, $B_1 = R_n.P_k$, $B_3 = A_4 \oplus R_m$, $B_4 = h\ (UID_i||R_m) \oplus SNID_j$ and $B_5 = h\ (A_4||SNID_j||B_1||R_m)$. Similarly, the SN_j generates nonce R_s that is incorporated in parameters $C_5 = R_s \oplus K_{GS}$, session key $SK_S = h\ (UID_i^*||SNID_j^*||R_m^*||R_g^*||R_s)$ and value $D_1 = h\ (K_{GS}||SK_S||R_s)$. Therefore, user's login request message Log_{Req} and SN_j's authentication message $Auth_2$ are session-specific. As such, it is difficult for the adversary to associate these two messages to particular users and sensors.

Proposition 6 *Our scheme is resilient against side-channeling and physical attacks.*

Proof The goal of the attacker is to steal user's MD_i and use power analysis techniques to retrieve the stored secrets. In our scheme, the MD_i stores value set $\{f\ (.), \lambda, \varepsilon, A_2, A_3, P_k, R_a\}$ in its memory. Here, $\lambda = h\ (CP_i)$, $\varepsilon = CP_i \oplus \beta_i$, $A_1 = h\ (PW_i||R_a)$, $A_2 = h\ (UID_i||A_1||CP_i)$, $A_3 = h\ (UID_i||M_k) \oplus h\ (A_1||CP_i)$, CP_i is the code-phrase chosen by the GW_k, R_a is the random nonce generated by the MD_i while $P_k = nP$ is the public key computed at the GW_k. Next, an attempt is made to retrieve user's unique identity UID_i and password PW_i. This requires access to security tokens such as CP_i and master key M_k for GW_k. In addition, adversary $\AA$ needs to reverse the one-way hashing function to obtain these parameters from $A_1$and A_2. Since this presents a computationally infeasible activity, this attack flops.

Proposition 7 *Known Session-Specific Temporary Information (KSSTI) attacks are prevented.*

Proof In our scheme, all the three entities derive the session key used to encipher the sensory data. Whereas the SN_j derives the session key as $SK_S = h\ (UID_i^*||SNID_j^*||R_m^*||R_g^*||R_s)$, the GW_k derives it as $SK_G = h\ (UID_i^*||SNID_j^*||R_m^*||R_g||R_s^*)$. Similarly, the MD_i computes the session key as $SK_D = h\ (UID_i||SNID_j||R_m||R_g^*||R_s^*)$. Based on *Propositions 1* and *5*, adversary cannot obtain identities UID_i and $SNID_j$ from the exchanged messages. In addition, *Proposition 6* has detailed the difficulty of obtaining UID_i from MD_i's memory. Therefore, even if temporary information such as random nonces R_m, R_g and R_s are compromised by $\AA$, these session keys cannot be computed.

Proposition 8 *Strong mutual authentication is executed among all network entities.*

Proof In our scheme, the MD_i validates user biometric data by checking whether $h\ (CP_i^*) \stackrel{?}{=} \lambda = h\ (CP_i)$. In addition, it verifies user unique identity UID_i and password PW_i by confirming if $A_2^* \stackrel{?}{=} A_2$. On its part, the the GW_k authenticates MD_i by checking whether $B_5^* \stackrel{?}{=} B_5$, while the SN_j validates GW_k through the confirmation of whether $D_1^* \stackrel{?}{=} D_1$. Finally, the the MD_i authenticates the SN_j by establishing whether $D_4^* \stackrel{?}{=} D_4$. In all these authentication scenarios, the session is aborted upon validation failure.

Proposition 9 *Session keys are negotiated among all network entities.*

Proof To protect the exchanged sensor data, the MD_i, GW_k and SN_j setup session keys amongst themselves. Upon receiving authentication message $Auth_1 = \{C_1, C_2, C_3, C_4\}$, the SN_j computes values $UID_i^* = C_1 \oplus K_{GS}^*$, $R_g^* = C_2 \oplus h\ (UID_i^*||K_{GS}^*)$, $R_m^* = R_g^* \oplus C_3$, $C_4^* = h\ (UID_i^*||SNID_j^*||K_{GS}||R_m^*||R_g^*)$, $C_5 = R_s \oplus K_{GS}$ and session key $SK_S = h\ (UID_i^*||SNID_j^*||R_m^*||R_g^*||R_s)$. Similarly, on getting authentication response message $Auth_2 = \{C_5, D_1\}$, the GW_k derives value $R_s^* = C_5 \oplus K_{GS}^*$ and session key $SK_G = h\ (UID_i^*||SNID_j^*||R_m^*||R_g||R_s^*)$. On its part, the MD_i receives authentication message $Auth_3 = \{D_2, D_3, D_4\}$ after which it derives values $R_g^* = A_4 \oplus D_2$, $R_s^* = R_m \oplus D_3$ and session key $SK_D = h\ (UID_i||SNID_j||R_m||R_g^*||R_s^*)$. These session keys are used by these entities to encipher the sensor data exchanged between the MD_i and SN_j via the GW_k.

Proposition 10 *Our scheme is robust against MitM and forgery attacks.*

Proof The aim of adversary $\mathring{A}$ is to gather information belonging to the network entities and attempt to forge the exchanged messages $Log_{Req} = \{A_5, B_2, B_3, B_4, B_5\}$, $Auth_1 = \{C_1, C_2, C_3, C_4\}$, $Auth_2 = \{C_5, D_1\}$ and $Auth_3 = \{D_2, D_3, D_4\}$. Here, $A_1 = h\ (PW_i||R_a)$, $A_3 = h\ (UID_i||M_k) \oplus h\ (A_1||CP_i)$, $A_4 = A_3 \oplus h\ (h(PW_i||R_a)||CP_i^*)$, $A_5 = R_n.P$, $B_1 = R_n.P_k = R_n.nP$, $B_2 = UID_i \oplus B_1$, $B_3 = A_4 \oplus R_m$, $B_4 = h\ (UID_i||R_m) \oplus SNID_j$, $B_5 = h\ (A_4||SNID_j||B_1||R_m)$, $C_1 = UID_i^* \oplus K_{GS}^*$, $C_2 = R_g \oplus h\ (UID_i^*||K_{GS}^*)$, $C_3 = R_g \oplus R_m^*$, $C_4 = h\ (UID_i^*||SNID_j^*||K_{GS}^*||R_m^*||R_g)$, $C_5 = R_s \oplus K_{GS}$, $D_1 = h\ (K_{GS}||SK_S||R_s)$, $D_2 = A_4^* \oplus R_g$, $D_3 = R_m^* \oplus R_s^*$ and $D_4 = h\ (UID_i^*||SK_G||R_g||R_s^*)$. To forge these messages, $\mathring{A}$ needs access to GW_k's master key P_k, UID_i, $SNID_j$, PW_i, CP_i^*, M_k, SK_S, SK_G, K_{GS} as well as random nonces R_a, R_g, R_m , R_n and R_s. *Proposition 1* , *Proposition 5* and *Proposition 6* have demonstrated the difficulty that $\mathring{A}$ faces in obtaining UID_i and $SNID_j$. On the other hand, *Propositions 4 and 6* have shown the challenges $\mathring{A}$ faces in retrieving PW_i. Similarly, *Proposition 7* has demonstrated the diffulty of adversarial derivation of session keys SK_S, SK_G and SK_D. Since M_k is only known to GW_k and K_{GS} is only known by GW_k and SN_j, $\mathring{A}$ cannot access these values. Similarly, random nonces are independently derived at the MD_i, GW_k and SN_j, hence not available to $\mathring{A}$. As such, forgery attacks against our scheme flops.

Proposition 11 *Backward and forward key secrecy is upheld.*

Proof In our scheme, the SN_j computes session key as $SK_S = h\ (UID_i^*||SNID_j^*||R_m^*||R_g^*||R_s)$ while the GW_k derives the session key as $SK_G = h\ (UID_i^*||SNID_j^*||R_m^*||R_g||R_s^*)$. Similarly, the MD_i calculates the session key as $SK_D = h\ (UID_i||SNID_j||R_m||R_g^*||R_s^*)$. The incorporation of random nonces R_m, R_g^* R_s^* renders the derived session keys one-time such that they are only valid for a particular session. Therefore, although adversary $\mathring{A}$ compromises the current session keys, it is not possible to use the captured parameters to derive session keys for the previous and subsequent communication session.

Performance evaluation

In this section, we present the comparative evaluations of our scheme in terms of computation costs, communication costs, functional and security features. The specific details are elaborated in the sub-sections below.

Computation costs

The proposed scheme is implemented in a laptop with the specifications in Table 2. Using the specifications in Table 2, the execution time times for the the elliptic curve point multiplication (T_{EM}) ≈ 21.74 ms, one-way hashing (T_H) ≈ 0.63 ms and elliptic curve point addition (T_{EA}) ≈ 6.75 ms.

During the login, authentication and key negotiation phase, the MD_i executes 2 ECC point multiplications and 8 one-way hashing operations. On the other hand, the GW_k carries out a single ECC point multiplication and 9 one-way hashing operations. On its part, the SN_j executes only 4 one-way hashing operations. Therefore, the total computation cost of our scheme is $21T_H + 3\ T_{EM}$. Table 3 presents the computation costs comparative evaluation of our scheme against other related schemes.

As shown in Fig. 4, the scheme developed in[71] incurs the highest computation costs of 251.33 ms. This is attributed to the numerous elliptic curve point multiplications which are computationally intensive. This is

Specification	Details
Operating system	Windows 11 Pro 64-bit
Processor	Intel Core i5-10400
Clock speed	2.90 GHz
RAM	8 GB
Programming language	Python
Cryptographic library	Pycryptodome

Table 2. Implementation environment.

Scheme	Time (ms)
Li et al.[31]	$24T_H + 6T_{EM} \approx 145.56$
Kumar et al.[61]	$5T_H + 6\ T_{EM} \approx 133.59$
Nikooghadam et al.[68]	$19T_H + 4\ T_{EM} \approx 98.93$
Wang et al.[71]	$11T_H + 10T_{EM} + 4T_{EA} \approx 251.33$
Bera et al.[72]	$18T_H + 10T_{EM} + 3T_{EA} \approx 248.99$
Bagga et al.[73]	$10T_H + 9T_{EM} + 2T_{EA} \approx 215.46$
Proposed	$21T_H + 3\ T_{EM} \approx 78.45$

Table 3. Computation costs comparisons.

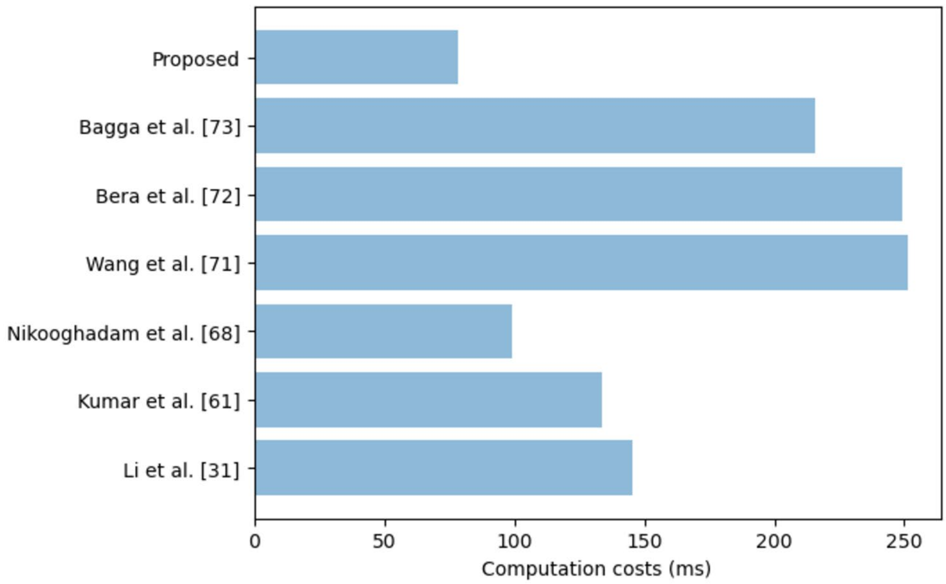

Figure 4. Computation costs comparisons.

Scheme	Size (bits)
Li et al.[31]	1792
Kumar et al.[61]	1760
Nikooghadam et al.[68]	2336
Wang et al.[71]	1376
Bera et al.[72]	1952
Bagga et al.[73]	1856
Proposed	2176

Table 4. Communication costs comparisons.

followed by the protocols in[31,61,68,72,73] which incur computation overheads of 248.99 ms, 215.46 ms, 145.56 ms, 133.59 ms and 98.93 ms respectively.

On the other hand, the proposed scheme incurs the lowest computation costs of only 78.45 ms. Based on the scheme in[68], our protocol reduced the computation costs by 20.7%. Since the sensors in smart cities are limited in terms of the computation power, our scheme is the most ideal for deployment in this environment.

Communication costs

In the course of the login, authentication and session key setup phase, 4 messages are exchanged among the MD_i, GW_k and SN_j. These messages include $Log_{Req} = \{A_5, B_2, B_3, B_4, B_5\}$, $Auth_1 = \{C_1, C_2, C_3, C_4\}$, $Auth_2 = \{C_5, D_1\}$ and $Auth_3 = \{D_2, D_3, D_4\}$. Here, ECC point multiplication = 160 bits, identities = 32 bits, one way hashing = 160 bits and random nonces = 128 bits. Using these values, $Log_{Req} = 160 + 160 + 160 + 160 + 160 = 800$ bits, $Auth_1 = 160 + 160 + 128 + 160 = 608$ bits, $Auth_2 = 160 + 160 = 320$ bits and $Auth_3 = 160 + 128 + 160 = 448$ bits. As such, the total communication overhead is 2176 bits. Table 4 provides comparative evaluation of the communication costs of our scheme against other related protocols.

As shown in Fig. 5, the protocol in[68] has the highest communication costs of 2336 bits. This is followed by the proposed scheme which inclurs a communication overhead of 2176 bits. This is attributed to the strong mutual authentication that must be executed among the MD_i, GW_k and SN_j.

Although the protocols in[31,61,71–73] incur relatively lower communication costs, they are insecure since they cannot offer functional and security features supported by our scheme, as evidenced in Table 5.

Functional and security features

In this sub-section, we discusses the comparative evaluation of our scheme in terms of offered functional and security features. Table 5 presents the security features supported by our scheme as well as the attacks that this scheme is resilient against. The security features and resilience of its peers are also detailed.

As shown in Table 5, the protocol in[68] supports only 7 functionalities and hence is the most insecure. This is followed by the scheme in[31] which supports 8 security features. On the other hand, the protocols in[71–73] support

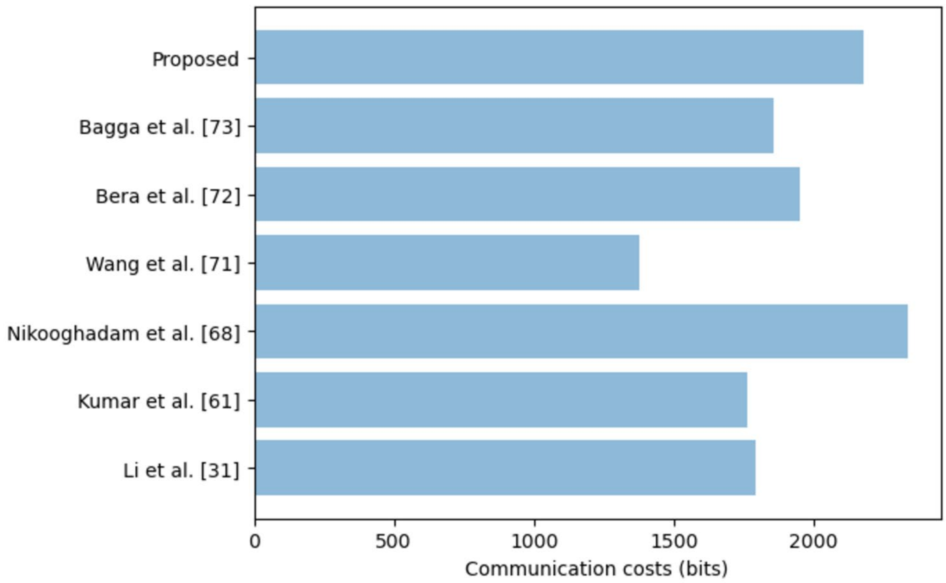

Figure 5. Communication costs comparisons.

	[72]	[71]	[73]	[31]	[61]	[68]	**Proposed**
Security features							
Mutual authentication	√	√	√	√	√	×	√
Key agreement	√	√	√	√	√	√	√
Backward key secrecy	×	√	√	×	√	√	√
Forward key secrecy	×	√	√	×	√	√	√
Anonymity	√	√	×	√	√	√	√
Untraceability	√	√	×	√	×	√	√
Password change	×	√	×	√	×	×	√
Formal verification	√	√	√	√	√	√	√
Resilient against							
De-synchronization	×	×	×	×	×	×	√
Denial of service	×	×	×	√	√	×	√
Eavesdropping	×	×	×	×	×	×	√
Session hijacking	×	×	×	×	×	×	√
KSSTI	×	×	×	×	√	×	√
Replays	√	√	√	×	×	×	√
Forgery	×	×	×	×	×	×	√
MitM	√	×	√	×	√	×	√
Privileged insider	√	×	√	×	√	×	√
Physical	√	×	√	√	√	√	√
Side-channeling	×	×	×	×	×	×	√
Impersonation	√	√	√	×	√	×	√
	√ Supported × Not supported or not considered						

Table 5. Functional and security features.

10 functionalities each. However, the protocol developed in[61] supports 12 functionalities while the proposed scheme offers support for all the 20 security features and functionalities. Although our scheme incurs slightly higher communication overheads, it supports the highets number of security and privacy functionalites. In addition, it incurs the lowest computation costs. As such, it offers a good trade-off between privacy, security and performance.

Some of the anticipated limitations that are likely to crop up during the practical implementation of our scheme is its slightly high communication costs and the need for biometric reader at the user mobile device MD_i. Specifically, the accurate recovery of biometric tokens via fuzzy extraction is not a trivial exercise.

Conclusion and future work

The security, privacy and performance issues in smart cities have attracted a lot of attention from the industry and academia. Therefore, past research works have developed a myriad of security solutions for this environment. In majority of these approaches, public key cryptography, blockchain and bilinear pairing operations are utilized. As such, the resulting authentication process is computationally extensive and hence long latencies can be experienced. In addition, they place high communication, energy and storage overheads on the resource-limited smart city sensor devices. Motivated by this, we have presented a biometric-based scheme that has been demonstrated to incur the least computation overheads. Its formal security analysis has shown that it performs strong mutual authentication and key negotiation in an appropriate manner. In addition, informal security analysis has shown that it is secure under all the threat assumptions in the Canetti and Krawczyk attack model. Future research work will involve further reductions in the communication overheads which are observed to be slightly higher compared with some of its peers.

Data availability

The datasets generated and/or analyzed during the current study are not publicly available due to university policy but are available from the corresponding author on reasonable request.

Received: 1 March 2024; Accepted: 8 July 2024
Published online: 13 July 2024

References

1. Kolhe, R. V., William, P., Yawalkar, P. M., Paithankar, D. N. & Pabale, A. R. Smart city implementation based on Internet of Things integrated with optimization technology. *Meas.: Sens.* **27**, 100789. https://doi.org/10.1016/j.measen.2023.100789 (2023).
2. Ghahramani, M., Javidan, R. & Shojafar, M. A secure biometric-based authentication protocol for global mobility networks in smart cities. *J. Supercomput.* **76**, 8729–8755. https://doi.org/10.1007/s11227-020-03160-x (2020).
3. Gupta, S. *et al.* Secure and lightweight authentication protocol for privacy preserving communications in smart city applications. *Sustainability* **15**(6), 5346. https://doi.org/10.3390/su15065346 (2023).
4. Yu, S., Das, A. K., Park, Y. & Lorenz, P. SLAP-IoD: Secure and lightweight authentication protocol using physical unclonable functions for internet of drones in smart city environments. *IEEE Trans. Veh. Technol.* **71**(10), 10374–10388. https://doi.org/10.1109/TVT.2022.3188769 (2022).
5. Hajjaji, Y., Boulila, W., Farah, I. R., Romdhani, I. & Hussain, A. Big data and IoT-based applications in smart environments: A systematic review. *Comput. Sci. Rev.* **39**, 100318. https://doi.org/10.1016/j.cosrev.2020.100318 (2021).
6. Yu, S., Lee, J., Park, K., Das, A. K. & Park, Y. IoV-SMAP: Secure and efficient message authentication protocol for IoV in smart city environment. *IEEE Access* **8**, 167875–167886. https://doi.org/10.1109/ACCESS.2020.3022778 (2020).
7. Khan, M. A. *et al.* An efficient and secure certificate-based access control and key agreement scheme for flying ad-hoc networks. *IEEE Trans. Veh. Technol.* **70**(5), 4839–4851. https://doi.org/10.1109/TVT.2021.3055895 (2021).
8. Nyangaresi, V. O., Abduljabbar, Z. A. & Abduljabbar, Z. A. Authentication and key agreement protocol for secure traffic signaling in 5G networks, in *2021 IEEE 2nd International Conference on Signal, Control and Communication (SCC)* 188–193 (IEEE, 2021). https://doi.org/10.1109/SCC53769.2021.9768338.
9. Alhudhaif, A. *et al.* Block cipher nonlinear confusion components based on new 5-D hyperchaotic system. *IEEE Access* **9**, 87686–87696. https://doi.org/10.1109/ACCESS.2021.3090163 (2021).
10. Dawaliby, S., Bradai, A. & Pousset, Y. Joint slice-based spreading factor and transmission power optimization in LoRa smart city networks. *Internet of Things* **14**, 100121. https://doi.org/10.1016/j.iot.2019.100121 (2021).
11. Ma, X., Dong, Z., Quan, W., Dong, Y. & Tan, Y. Real-time assessment of asphalt pavement moduli and traffic loads using monitoring data from Built-in Sensors: Optimal sensor placement and identification algorithm. *Mech. Syst. Signal Process.* **187**, 109930. https://doi.org/10.1016/j.ymssp.2022.109930 (2023).
12. Boccadoro, P., Striccoli, D. & Grieco, L. A. An extensive survey on the Internet of Drones. *Ad Hoc Netw.* **122**, 102600. https://doi.org/10.1016/j.adhoc.2021.102600 (2021).
13. Chen, R., Mou, Y. & Zhang, M. An improved anonymous DoS-resistant authentication protocol in smart city. *Wirel. Netw.* **28**(2), 745–763. https://doi.org/10.1007/s11276-021-02820-x (2022).
14. Kandris, D., Nakas, C., Vomvas, D. & Koulouras, G. Applications of wireless sensor networks: An up-to-date survey. *Appl. Syst. Innov.* **3**(1), 14. https://doi.org/10.3390/asi3010014 (2020).
15. Yahuza, M. *et al.* Internet of drones security and privacy issues: Taxonomy and open challenges. *IEEE Access* **9**, 57243–57270. https://doi.org/10.1109/ACCESS.2021.3072030 (2021).
16. Al Sibahee, M. A. *et al.* Lightweight secure message delivery for E2E S2S communication in the IoT-cloud system. *IEEE Access* **8**, 218331–218347. https://doi.org/10.1109/ACCESS.2020.3041809 (2020).
17. Hussain Ali, Y. *et al.* Multi-layered non-local bayes model for lung cancer early diagnosis prediction with the internet of medical things. *Bioengineering* **10**(2), 138. https://doi.org/10.3390/bioengineering10020138 (2023).
18. Yang, Z., Lai, J., Sun, Y. & Zhou, J. A novel authenticated key agreement protocol with dynamic credential for WSNs. *ACM Trans. Sens. Netw. (TOSN)* **15**(2), 1–27. https://doi.org/10.1145/3303704 (2019).
19. Zeb, H. *et al.* Zero energy IoT devices in smart cities using RF energy harvesting. *Electronics* **12**(1), 148. https://doi.org/10.3390/electronics12010148 (2022).
20. Yassein, H. R., Al-Saidi, N. M. & Farhan, A. K. A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure. *J. Discrete Math. Sci. Cryptogr.* **25**(2), 523–542. https://doi.org/10.1080/09720529.2020.1741218 (2022).
21. Nurelmadina, N. *et al.* A systematic review on cognitive radio in low power wide area network for industrial IoT applications. *Sustainability* **13**(1), 338. https://doi.org/10.3390/su13010338 (2021).
22. Abduljabbar, Z. A. *et al.* Session-dependent token-based payload enciphering scheme for integrity enhancements in wireless networks. *J. Sens. Actuator Netw.* **11**(3), 55. https://doi.org/10.3390/jsan11030055 (2022).
23. Tawalbeh, L. A., Muheidat, F., Tawalbeh, M. & Quwaider, M. IoT Privacy and security: Challenges and solutions. *Appl. Sci.* **10**(12), 4102. https://doi.org/10.3390/app10124102 (2020).

24. Khalil, U., Malik, O. A. & Hussain, S. A blockchain footprint for authentication of IoT-enabled smart devices in smart cities: State-of-the-art advancements, challenges and future research directions. *IEEE Access* **10**, 76805–76823. https://doi.org/10.1109/ACCESS.2022.3189998 (2022).
25. Liu, C., Wu, T., Li, Z., Ma, T. & Huang, J. Robust online tensor completion for IoT streaming data recovery. *IEEE Trans. Neural Netw. Learn. Syst.* https://doi.org/10.1109/TNNLS.2022.3165076 (2022).
26. Li, H., Huang, Q., Huang, J. & Susilo, W. Public-key authenticated encryption with keyword search supporting constant trapdoor generation and fast search. *IEEE Trans. Inf. Forensics Secur.* **18**, 396–410. https://doi.org/10.1109/TIFS.2022.3224308 (2022).
27. Dammak, M., Boudia, O. R. M., Messous, M. A., Senouci, S. M. & Gransart, C. Token-based lightweight authentication to secure IoT networks, in *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)* 1–4 (IEEE, 2019).https://doi.org/10.1109/CCNC.2019.8651825.
28. Gupta, A., Tripathi, M., Shaikh, T. J. & Sharma, A. A lightweight anonymous user authentication and key establishment scheme for wearable devices. *Comput. Netw.* **149**, 29–42. https://doi.org/10.1016/j.comnet.2018.11.021 (2019).
29. Lyu, Q. *et al.* Remotely access "my" smart home in private: An anti-tracking authentication and key agreement scheme. *IEEE Access* **7**, 41835–41851. https://doi.org/10.1109/ACCESS.2019.2907602 (2019).
30. Renuka, K., Kumari, S., Zhao, D. & Li, L. Design of a secure password-based authentication scheme for M2M networks in IoT enabled cyber-physical systems. *IEEE Access* **7**, 51014–51027. https://doi.org/10.1109/ACCESS.2019.2908499 (2019).
31. Li, X. *et al.* A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. *IEEE Syst. J.* **14**(1), 39–50. https://doi.org/10.1109/JSYST.2019.2899580 (2019).
32. Taher, B. H. *et al.* A secure and lightweight three-factor remote user authentication protocol for future IoT applications. *J. Sens.* **2021**, 1–18. https://doi.org/10.1155/2021/8871204 (2021).
33. Wu, F., Xu, L., Kumari, S. & Li, X. An improved and provably secure three-factor user authentication scheme for wireless sensor networks. *Peer-to-Peer Netw. Appl.* **11**, 1–20. https://doi.org/10.1007/s12083-016-0485-9 (2018).
34. Ryu, J., Lee, H., Kim, H. & Won, D. Secure and efficient three-factor protocol for wireless sensor networks. *Sensors* **18**(12), 4481. https://doi.org/10.3390/s18124481 (2018).
35. Guo, Y., Zhang, C., Wang, C. & Jia, X. Towards public verifiable and forward-privacy encrypted search by using blockchain. *IEEE Trans. Dependable Secure Comput.* https://doi.org/10.1109/TDSC.2022.3173291 (2022).
36. Ammi, M., Alarabi, S. & Benkhelifa, E. Customized blockchain-based architecture for secure smart home for lightweight IoT. *Inf. Process. Manag.* **58**(3), 102482. https://doi.org/10.1016/j.ipm.2020.102482 (2021).
37. Esposito, C., Ficco, M. & Gupta, B. B. Blockchain-based authentication and authorization for smart city applications. *Inf. Process. Manag.* **58**(2), 102468. https://doi.org/10.1016/j.ipm.2020.102468 (2021).
38. Ahmad, M. O. *et al.* BAuth-ZKP—A blockchain-based multi-factor authentication mechanism for securing smart cities. *Sensors* **23**(5), 2757. https://doi.org/10.3390/s23052757 (2023).
39. Goyat, R., Kumar, G., Saha, R. & Conti, M. Pribadi: A decentralized privacy-preserving authentication in wireless multimedia sensor networks for smart cities. *Clust. Comput.* https://doi.org/10.1007/s10586-023-04211-7 (2023).
40. Khalid, U. *et al.* A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Clust. Comput.* **23**(3), 2067–2087. https://doi.org/10.1007/s10586-020-03058-6 (2020).
41. Gong, L., Alghazzawi, D. M. & Cheng, L. BCoT sentry: A blockchain-based identity authentication framework for IoT devices. *Information* **12**(5), 203. https://doi.org/10.3390/info12050203 (2021).
42. Zhaofeng, M., Jialin, M., Jihui, W. & Zhiguang, S. Blockchain-based decentralized authentication modeling scheme in edge and IoT environment. *IEEE Internet Things J.* **8**(4), 2116–2123. https://doi.org/10.1109/JIOT.2020.3037733 (2020).
43. Li, C. *et al.* Efficient privacy-preserving in IoMT with blockchain and lightweight secret sharing. *IEEE Internet Things J.* https://doi.org/10.1109/JIOT.2023.3296595 (2023).
44. Al Sibahee, M. A. *et al.* Efficient encrypted image retrieval in IoT-cloud with multi-user authentication. *Int. J. Distrib. Sens. Netw.* **14**(2), 1550147718761814. https://doi.org/10.1177/1550147718761814 (2018).
45. Bansal, G. *et al.* Lightweight mutual authentication protocol for V2G using physical unclonable function. *IEEE Trans. Veh. Technol.* **69**(7), 7234–7246. https://doi.org/10.1109/TVT.2020.2976960 (2020).
46. Alladi, T., Bansal, G., Chamola, V. & Guizani, M. SecAuthUAV: A novel authentication scheme for UAV-ground station and UAV-UAV communication. *IEEE Trans. Veh. Technol.* **69**(12), 15068–15077. https://doi.org/10.1109/TVT.2020.3033060 (2020).
47. Nyangaresi, V. O. & Petrovic, N. Efficient PUF based authentication protocol for internet of drones, in *2021 International Telecommunications Conference (ITC-Egypt)* 1–4 (IEEE, 2021).https://doi.org/10.1109/ITC-Egypt52936.2021.9513902
48. Wazid, M., Das, A. K., Kumar, N., Vasilakos, A. V. & Rodrigues, J. J. Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment. *IEEE Internet Things J.* **6**(2), 3572–3584. https://doi.org/10.1109/JIOT.2018.2888821 (2018).
49. Deebak, B. D. & Al-Turjman, F. A smart lightweight privacy preservation scheme for IoT-based UAV communication systems. *Comput. Commun.* **162**, 102–117. https://doi.org/10.1016/j.comcom.2020.08.016 (2020).
50. Srinivas, J., Das, A. K., Kumar, N. & Rodrigues, J. J. TCALAS: Temporal credential-based anonymous lightweight authentication scheme for Internet of drones environment. *IEEE Trans. Veh. Technol.* **68**(7), 6903–6916. https://doi.org/10.1109/TVT.2019.2911672 (2019).
51. Ali, Z., Chaudhry, S. A., Ramzan, M. S. & Al-Turjman, F. Securing smart city surveillance: A lightweight authentication mechanism for unmanned vehicles. *IEEE Access* **8**, 43711–43724. https://doi.org/10.1109/ACCESS.2020.2977817 (2020).
52. Alladi, T., Chamola, V. & Kumar, N. PARTH: A two-stage lightweight mutual authentication protocol for UAV surveillance networks. *Comput. Commun.* **160**, 81–90. https://doi.org/10.1016/j.comcom.2020.05.025 (2020).
53. Sucasas, V., Aly, A., Mantas, G., Rodriguez, J. & Aaraj, N. Secure multi-party computation-based privacy-preserving authentication for smart cities. *IEEE Trans. Cloud Comput.* https://doi.org/10.1109/TCC.2023.3294621 (2023).
54. Duraisamy, A. & Subramaniam, M. Attack detection on IoT based smart cities using IDS based MANFIS classifier and secure data transmission using IRSA encryption. *Wirel. Pers. Commun.* **119**, 1913–1934. https://doi.org/10.1007/s11277-021-08362-x (2021).
55. Altaf, A. *et al.* Mitigating service-oriented attacks using context-based trust for smart cities in IoT networks. *J. Syst. Arch.* **115**, 102028. https://doi.org/10.1016/j.sysarc.2021.102028 (2021).
56. Al Sibahee, M. A., Lu, S., Hussien, Z. A., Hussain, M. A., Mutlaq, K. A.-A. & Abduljabbar, Z. A. The best performance evaluation of encryption algorithms to reduce power consumption in WSN, in *2017 International Conference on Computing Intelligence and Information System (CIIS)* 308–312 (IEEE, 2017). https://doi.org/10.1109/CIIS.2017.50.
57. Abd El-Latif, A. A. *et al.* Quantum-inspired blockchain-based cybersecurity: Securing smart edge utilities in IoT-based smart cities. *Inf. Process. Manag.* **58**(4), 102549. https://doi.org/10.1016/j.ipm.2021.102549 (2021).
58. Irshad, R. R. *et al.* An Intelligent buffalo-based secure edge-enabled computing platform for heterogeneous IoT network in smart cities. *IEEE Access* https://doi.org/10.1109/ACCESS.2023.3288815 (2023).
59. Jiang, H. *et al.* An energy-efficient framework for internet of things underlaying heterogeneous small cell networks. *IEEE Trans. Mobile Comput.* **21**(1), 31–43. https://doi.org/10.1109/TMC.2020.3005908 (2020).
60. Dhillon, P. K. & Kalra, S. Multi-factor user authentication scheme for IoT-based healthcare services. *J. Reliab. Intell. Environ.* **4**, 141–160. https://doi.org/10.1007/s40860-018-0062-5 (2018).
61. Kumar, A., Abhishek, K., Liu, X. & Haldorai, A. An efficient privacy-preserving id centric authentication in IoT based cloud servers for sustainable smart cities. *Wirel. Pers. Commun.* **117**, 3229–3253. https://doi.org/10.1007/s11277-020-07979-8 (2021).

62. Li, J., Zhang, Z., Hui, L. & Zhou, Z. A novel message authentication scheme with absolute privacy for the internet of things networks. *IEEE Access* **8**, 39689–39699. https://doi.org/10.1109/ACCESS.2020.2976161 (2020).
63. Chen, Y., Ge, Y., Wang, W. & Yang, F. A biometric-based user authentication and key agreement scheme for heterogeneous wireless sensor networks. *KSII Trans. Internet Inf. Syst.* https://doi.org/10.3837/tiis.2018.04.021 (2018).
64. Nyangaresi, V. O. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. *High-Confid. Comput.* **3**(4), 100154. https://doi.org/10.1016/j.hcc.2023.100154 (2023).
65. Salim, M. M., Singh, S. K. & Park, J. H. Securing Smart Cities using LSTM algorithm and lightweight containers against botnet attacks. *Appl. Soft Comput.* **113**, 107859. https://doi.org/10.1016/j.asoc.2021.107859 (2021).
66. Cheon, J. H. *et al.* Toward a secure drone system: flying with real-time homomorphic authenticated encryption. *IEEE Access* **6**, 24325–24339. https://doi.org/10.1109/ACCESS.2018.2819189 (2018).
67. Ever, Y. K. A secure authentication scheme framework for mobile-sinks used in the internet of drones applications. *Comput. Commun.* **155**, 143–149. https://doi.org/10.1016/j.comcom.2020.03.009 (2020).
68. Nikooghadam, M., Amintoosi, H., Islam, S. H. & Moghadam, M. F. A provably secure and lightweight authentication scheme for Internet of Drones for smart city surveillance. *J. Syst. Arch.* **115**, 101955. https://doi.org/10.1016/j.sysarc.2020.101955 (2021).
69. Mutlaq, K. A.-A., Nyangaresi, V. O., Omar, M. A. & Abduljabbar, Z. A. Symmetric key based scheme for verification token generation in Internet of Things communication environment, *in EAI International Conference on Applied Cryptography in Computer and Communications* 46–64 (Springer, 2022). https://doi.org/10.1007/978-3-031-17081-2_4
70. Ali, Z. *et al.* TC-PSLAP: Temporal credential-based provably secure and lightweight authentication protocol for IoT-enabled drone environments. *Secur. Commun. Netw.* **2021**, 1–10. https://doi.org/10.1155/2021/9919460 (2021).
71. Wang, J. *et al.* A secure and efficient multiserver authentication and key agreement protocol for internet of vehicles. *IEEE Internet Things J.* **9**(23), 24398–24416. https://doi.org/10.1109/JIOT.2022.3188731 (2022).
72. Bera, B., Das, A. K., Garg, S., Piran, M. J. & Hossain, M. S. Access control protocol for battlefield surveillance in drone-assisted IoT environment. *IEEE Internet Things J.* **9**(4), 2708–2721. https://doi.org/10.1109/JIOT.2020.3049003 (2021).
73. Bagga, P. *et al.* On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. *IEEE Trans. Veh. Technol.* **70**(2), 1736–1751. https://doi.org/10.1109/TVT.2021.3050614 (2021).
74. Bagga, P., Das, A. K. & Rodrigues, J. J. Bilinear pairing-based access control and key agreement scheme for smart transportation. *Cyber Secur. Appl*> **1**, 100001. https://doi.org/10.1016/j.csa.2022.100001 (2023).
75. Nyangaresi, V. O., Abduljabbar, Z. A., Refish, S. H. A., Al Sibahee, M. A., Abood, E. W. & Lu, S. Anonymous key agreement and mutual authentication protocol for smart grids, in *International Conference on Cognitive Radio Oriented Wireless Networks*, 325–340 (Springer, 2021). https://doi.org/10.1007/978-3-030-98002-3_24.
76. Hussien, Z. A. *et al.* Lightweight integrity preserving scheme for secure data exchange in cloud-based IoT systems. *Appl. Sci.* **13**(2), 691. https://doi.org/10.3390/app13020691 (2023).
77. Jiang, H., Wang, M., Zhao, P., Xiao, Z. & Dustdar, S. A utility-aware general framework with quantifiable privacy preservation for destination prediction in LBSs. *IEEE/ACM Trans. Netw.* **29**(5), 2228–2241. https://doi.org/10.1109/TNET.2021.3084251 (2021).
78. Nyangaresi, V. O., Ibrahim, A., Abduljabbar, Z. A., Hussain, M. A., Al Sibahee, M. A., Hussien, Z. A. & Ghrabat, M. J. J. Provably secure session key agreement protocol for unmanned aerial vehicles packet exchanges, in *2021 International Conference on Electrical, Computer and Energy Technologies (ICECET)* 1–6 (IEEE, 2021). https://doi.org/10.1109/ICECET52533.2021.9698744.
79. Al Sibahee, M. A., Ma, J., Nyangaresi, V. O. & Abduljabbar, Z. A. Efficient extreme gradient boosting based algorithm for QoS optimization in inter-radio access technology handoffs, in *2022 international congress on human-computer interaction, optimization and robotic applications (HORA)* 1–6 (IEEE, 2022). https://doi.org/10.1109/HORA55278.2022.9799997.
80. Xu, H., Han, S., Li, X. & Han, Z. Anomaly traffic detection based on communication-efficient federated learning in space-air-ground integration network. *IEEE Trans. Wirel. Commun.* **22**(99), 1–1. https://doi.org/10.1109/TWC.2023.3270179 (2023).

Author contributions
All authors have contributed equally to this article.

Funding
Natural Science Foundation of Top Talent of SZTU (grant no. GDRC202132).

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to Z.A.A. or J.M.