P3S: Pertinent Privacy-Preserving Scheme for Remotely Sensed Environmental Data in Smart Cities

Fahad Algarni, Mohammad Ayoub Khan, *Senior Member, IEEE*, Wedad Alawad, and Nadhir Ben Halima

***Abstract*—Sensing devices, high-performance networking, and privacy preservation algorithms have important roles to play in remotely sensed environmental data in smart cities. The data generated by these sensors are heterogeneous, vast, and sensitive. Therefore, it is imperative that adequate security mechanisms are put in place to protect environmental data from privacy breaches and malicious attacks, remotely sensed environmental data, such as weather conditions (windy, cloudy, or rainy), soil types, and other similar data, must be protected. The biggest risks of remotely connected devices are that sensitive information could be leaked and devices could be compromised. Considering these security threats, this article proposes a pertinent privacy-preserving scheme. The presented scheme is reliable for sensitive geosensed data in thwarting the aforementioned security issues. The data are concealed using two-factor authentication from the transmitter end. In this authentication, the signatures of device and receiver are overlapped for improved authentication. The failure in overlapping is identified by delayed signing time and noncoherent agreements. This identification is recurrently analyzed using federated learning. Therefore, the signing process is paused until the device verification is performed. Hence, if the device verification succeeds, then a new data privacy accumulation session is introduced. Contrarily, the accumulation is dropped, preventing compromised actual data from preserving accuracy. In two-factor authentication, lightweight digital signing cryptography is utilized. The proposed scheme maximizes the average authentication success rate and average overlapping factor by 8.86% and 12.20%, respectively. This scheme further reduces average authentication time, false data, and verification time by 10.14%, 9.70%, and 10.19%, respectively.**

***Index Terms*—Big Data, data privacy, machine learning, privacy preserving, remote sensing, smart city.**

I. Introduction

REMOTE sensing is a process that is used to detect and monitor the physical characteristics of a particular object or phenomenon without making physical contact [1]. Satellites are used in remote sensing to collect data from objects. Satellites gather a group of raw data and store it in computer storage as files or database records. Remotely sensing data is an important process that is mostly used to predict and detect conditions via monitoring systems. Very high-resolution (VHR) sensors are used in remote sensing, which improves the security and safety ratio of data that are collected via wireless sensors [2]. VHR improves the feasibility and efficiency levels of smart cities by ensuring the safety of users from attackers. Geographic information systems (GIS) are also used in remote sensing data management systems [3]. The external data and the technological paradigm utilized are modeled using learning techniques for self-decisions. One such process is the inclusion of learning models in GIS and similar technologies. For example, a deep learning (DL)-based remote sensing technique is used in smart cities to improve predictability [4]. The DL reduces latency and time consumption in computational processes [5].

Privacy preservation and security are complicated tasks to perform in a geosensing-based application. Important information is stored in a GIS [6], [7]. Manual analysis and other privacy schemes are used in securing geodata. An automated extraction method is used for remotely sensed data to reduce the error ratio in privacy and security policies [8]. The automated extraction method achieves high accuracy in decision-making, which enhances the overall performance and effectiveness of the systems [9]. Remotely sensed data contain heterogeneous information related to specific fields and areas. The rapid extraction technique is used in automated extraction, which reduces time and energy consumption in computation [10]. Authentication and authorization policies ensure the security of remotely sensed data. A Chaos-based encryption technique is also used in privacy policies. Encryption techniques give users the best security services possible and make it easier to compute and make decisions [11]. Remotely sensed data contain important information about specific fields [12]. Support vector machines (SVMs) are used in weather forecasting applications to identify important features from the database [13]. Remotely sensed data are also used in rural map applications. The map application is implemented via machine learning techniques, which enhance accuracy in providing services to users and improve the performance ratio of an application [11], [14]. Urban modeling also uses remotely sensed data to provide accurate information for modeling and data processing systems. Remotely sensed data produce exact information about soil, weather, water, and the index of other elements. Both urban and rural modeling applications make sure that third-party members' information is safe [13], [15]. The sensors in remote sensing settings produce diverse and sensitive

Manuscript received 5 November 2022; revised 28 February 2023, 29 March 2023, and 4 May 2023; accepted 19 June 2023. Date of publication 22 June 2023; date of current version 7 July 2023. The work was supported by the Deanship of Scientific Research, Qassim University Saudi Arabia. *(Corresponding author: Wedad Alawad.)*

Fahad Algarni and Mohammad Ayoub Khan are with the College of Computing and Information Technology, University of Bisha, Bisha 67714, Saudi Arabia (e-mail: fahad.alqarni@ub.edu.sa; ayoub.khan@ieee.org).

Wedad Alawad is with the Department of Information Technology, College of Computer, Qassim University, Buraydah 51921, Saudi Arabia (e-mail: wmaoad@qu.edu.sa).

Nadhir Ben Halima is with the Department of Information Technology, Community College of Qatar, Doha 7344, Qatar (e-mail: nadhir.benhalima@ccq.edu.qa).

Digital Object Identifier 10.1109/JSTARS.2023.3288743

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

data. Hence, environmental data must be secured against privacy breaches and malicious attacks. The contributions to privacy preservation in remotely sensed environmental data are listed as follows.

1) A pertinent privacy-preserving scheme (P3S) for remotely sensed environmental data using two-factor authentication is proposed. The proposed scheme is based on a lightweight digital signing process to reduce computational costs.
2) To improve authentication, the signatures of the device and the receiver are overlapped. The failure in overlapping is identified by delayed signing time and noncoherent agreements. This identification is recurrently analyzed using federated learning.
3) A comprehensive simulation of the environmental dataset is conducted to validate the functional correctness and effectiveness of the proposed scheme.

The rest of this article is organized as follows. Section II presents the state-of-the-art of privacy preservation in remotely sensed environmental data. Section III presents the proposed P3S. The results and performance analysis have been discussed in Section IV. Finally, Section V concludes this article.

II. Related Work

Zurbarán et al. [16] introduced a geoprivacy-based evaluation framework to identify characteristics of a location in geospatial analysis. The nearest neighbor index reduces latency in evaluation, which enhances the feasibility of analysis systems. The proposed framework improves the performance and efficiency of location privacy. However, the optimal mechanism did not get the highest score on any of the indices but rather maintained average performance throughout them.

Wang et al. [17] proposed a transmission scheduling method for remote state estimation systems. The main aim of the proposed method is to identify transmission scheduling problems that occur during computation. The proposed scheduling method achieves high accuracy in scheduling, which enhances the effectiveness and reliability of the systems. However, practically, the performance of remote estimation is not known.

Huang et al. [18] developed a blockchain-based continuous data integrity checking protocol for cloud computing (CC) technology. A zero-knowledge privacy protection technique is used here to verify delay functions. Compared to other protocols, the proposed protocol makes CC work better and has more significance. However, the overhead of the mining process is not considered in the performance analysis.

Brahem et al. [19] proposed a privacy-by-design solution for the consent-driven data reuse process in multitasking crowdsensing systems. The main aim of the proposed method is to identify the consent that is presented in the analysis process. The proposed method improves the overall privacy and security levels of crowdsensing systems. The authors have not reported any performance analysis that ensures the integrity and confidentiality of the privacy-preservation solution.

Smahi et al. [20] introduced blockchain-based privacy-preserving SVM classification (BPPSVC) for mobile-cloud-sensed data. Blockchain identifies the features necessary for classification and identification processes. Secure multiparty computation is implemented in BPPSVC, which reduces the latency level in computation. Experimental results show that the proposed BPPSVC maximizes the privacy of data, which enhances the feasibility of the systems. However, the use of blockchain technology has introduced communication and mining overhead.

Ding et al. [21] introduced a new privacy-preserving task allocation method for edge-computing-based mobile crowdsensing (EC-MCS) systems. Accurate users are selected based on the homographic encryption process, which reduces error levels in task allocation. The proposed method ensures both the safety and security of users, which improves the effectiveness and efficiency of EC-MCS. The primary drawback of homomorphic encryption is that it necessitates either modifying existing applications or deploying new, custom client-server programs in order to perform properly.

Sani et al. [22] developed a new scheme for smart communities, named a secure and privacy-preserving mutually dependent authentication and data access scheme (SPrivAD). Cryptographic operations and techniques are used here to encrypt information that is required for privacy-preserving policies. Zero-knowledge proof of knowledge (ZKPK) is used here to identify computational attributes. The proposed SPrivAD protocol maximizes the privacy ratio of users from third-party members. However, the ZKPK technology is a computationally intensive process.

Fakroon et al. [23] introduced a secure remote anonymous user authentication scheme for smart home environments and systems. The proposed scheme is mostly used to identify clock-synchronized problems that occur during authentication. The proposed scheme combines both transaction history and physical context to get feasible information for the authentication process. User authentication schemes improve both the privacy and security levels of users during authentication. The storage and communication cost of the proposed schedule is high, which may not be suitable for real-time embedded applications.

Ge et al. [24] designed resilient and secure remote monitoring for cyber-physical systems. The main aim of the proposed monitoring is to identify ellipsoidal attacks and problems that are presented in the collected data. The set-based evaluation method is used here to predict important features from the database. The proposed method achieves high accuracy in prediction and detection, which enhances the efficiency level of the decision-making process. The ellipsoidal prediction and estimate approach may be vulnerable to certain types of malicious assaults.

Hu et al. [25] introduced a privacy-preserving scheme for wireless sensor networks (WSNs). Sensor nodes are detected and managed via key agreement protocols that reduce latency in computation and identification.

The proposed scheme improves the efficiency of sensed data that are generated from WSN. The proposed scheme ensures the privacy of users' data from unknown third-party members. However, the deployment and implementation processes, which are two components of overhead, have become more time-consuming.

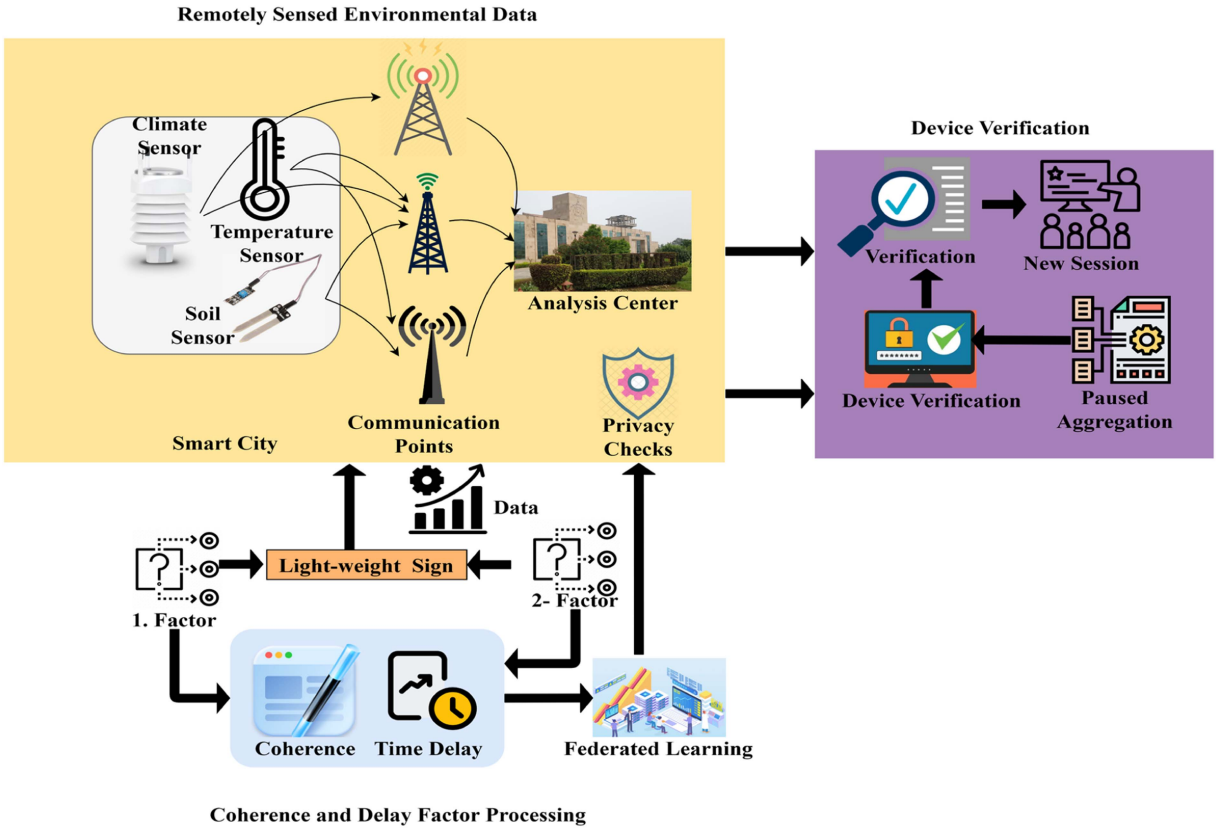

Fig. 1. Proposed P3S scheme for remotely sensed environmental data.

Zhou et al. [26] developed fog and Internet of Things (IoT)-based mechanisms for privacy-preserving policies. Range-max queries are detected from the database that provides optimal information for further processes. Ciphertexts are calculated based on functions and operations that reduce the time consumption ratio in computation. Compared to other methods, the one that is being proposed is more effective and uses less time.

Xie et al. [27] designed a secure, privacy-preserving protocol for WSN. The proposed protocol is mostly used in smart cities that require proper privacy policies for users to ensure safety. The proposed method provides optimal authentication services to users, which improve the security and safety of users' data from third-party members. Experiments show that the proposed protocol improves the level of privacy in WSN systems as much as possible. However, the computational cost is high.

Popa et al. [28] proposed a privacy-aware mobile distributed system for mobile participatory sensing (MPS). The main aim of the proposed method is to reduce location leakage, which enhances the performance and feasibility level of MPS systems. The supporting server infrastructure is used here to identify traditional features that are required for privacy-preserving policies. One of the disadvantages of the proposed model is the high aggregation time. In addition to this, PAMPAS+ costs for an extra phase known as the couple-key exchange, during which each pair of SPs trades a secret key.

The existing literature discussed so far provides privacy preservation for sensed data, as presented in [19], [21], [25], and [28], and location/system, as presented in [16], [26], and [27]. Transmission security is leveraged using individual user authentication and access controls, as discussed in [17], [22], and [23]. The security methods lag a few security demands, such as controlling the false rate, as discussed in [18], [20], and [28], due to intense verification at irregular intervals. In the user authentication and access control process, the problem of data privacy is confined due to unplanned session authentication. The proposed scheme addresses the highlighted issues by identifying overlapping issues in the signing process. Besides, the noncoherent signing processes are paused for preventing irregular verifications.

III. Proposed Privacy Preservation Scheme

The proposed scheme is designed to consider the security threats in smart cities that rely on geosensed data and remotely connected technologies to prevent the chances of data leakage and device compromise. A large amount of data from the climatic sensor, temperature sensor, and soil sensor are sensed and transmitted to different communication points for analysis and securing sensitive geosensed data, as shown in Fig. 1. The remotely sensed data are communicated to the analysis center, such as weather forecast centers. The initial security processes are between the communication infrastructures through digital signing from the sensing device.

This signature is verified by the analysis center for its privacy using coherence and delay factors. The analysis center performs device and data verification to ensure precise data are received.

The remotely sensed environmental data are to be secured before performing analysis. Autonomous and remotely connected geoapplications have fewer chances of data leakage, device compromise, and failure. Before performing the data analysis, the sensed remote raw data are secured through a two-factor authentication process at the transmitter end to identify failures. However, the large amount of remotely sensed data modifies the device compromise based on the type of systems that are observed in the smart city environment. This process leads to an explosion in geosensed data and analysis over sensing devices and sophisticated technologies to support making smart decisions. In this work, the identification of security threats in sensed data is a critical task that must be analyzed to check if the signatures of the device and the receiver are overlapped for augmenting authentication. The failure is identified at the time of overlapping, which is detected using delayed signing time and noncoherent agreements through two-factor authentication. This approach prevents security issues in sensitive geosensed data. If any failures are identified at the time of device verification or a data drop has occurred in that session, the particular sessions are halted. The identification of failure is recurrently analyzed through a federated learning process, and the digital signature process is paused until the device verification is performed based on a coherence-less and time-delayed lightweight signature. From the multiple communication points, precise smart city data augmentation and management are achieved. Multiple transmitters are used for sharing a large amount of data from a sensor to an analytical center, where data transmission time failures are detected. If the device verification succeeds, a new data privacy accumulation session is generated. In this proposed scheme, lightweight digital signing cryptography is utilized using a two-factor authentication process. The device verification is performed for delayed signing time and coherent agreement in geosensed data analysis to reduce false data. The false data are observed as the miscommunicated or interrupted data in any sensing interval other than actually observed. The geodata (Geo^D) are sensed by various sensors (s) in smart cities. The sensed data from the open environment are transmitted to different communication points for secured data analysis using two-factor authentication for accurate device verification. Device compromise is used to manage big data augmentation and management, and data privacy output is analyzed to ensure accuracy. Hence, the P3S is focused on two operations, namely data leakage and device compromise, in real-time applications. The proposed schemes augment and manage the big data while concealing geosensed data at the transmitter end. For improving authentication, data privacy and device verification are analyzed. This ensures that the signing time is delayed and that the agreements are incoherent in multiple device verifications at different time intervals.

A. Privacy Preservation

The geosensed data observed in the open environment rely on sensing devices and connected technologies for improving device compromise. The sensed data are concealed for thwarting security issues. The multiple devices are autonomous and remotely connected for reducing the chances of data leakage at the transmitter end. The data augmentation $(\text{BigData}_{\text{Aug}})$ and remotely sensed data are computed as follows:

$$\text{BigData}_{\text{Aug}} = \left(\frac{s* \left(\text{Geo}^D_{\max} - \text{Geo}^D_{\min} \right)}{\text{Geo}^D} \right) \tag{1}$$

$$R_{\text{SD}} = \frac{1}{\sqrt{2\pi}} \left[\frac{\left(\frac{\text{Geo}^D_{\min}}{\text{Geo}^D_{\max}} - \frac{s}{S} \right)}{N\left(d_l - d_c\right)} \right] \tag{2}$$

where s is the active sensor data observed, $s \in \text{Geo}^D$; $\text{Geo}^D_{\min}$ and $\text{Geo}^D_{\max}$ are the minimum and maximum geosensed data at different periods, respectively. Symbols R_{SD}, d_l, and d_c are used to represent the remotely sensed data, data leakage, and device compromise, respectively, for further device verification and privacy preservation. The sensed raw data are secured using two-factor authentication, and the number of devices N in a smart city sensing application is calculated in all the sessions. In some cases, the device signature D_S and received signature R_S are overlapped for augmenting authentication A_A based on failure in overlapping is identified due to delayed signing time and noncoherent agreements in the digital signature process. The augmenting authentication process is represented in Fig. 2.

Therefore, the digital lightweight signing process impact Geo^D at any period, in which the data privacy $\text{Data}_{\text{Privacy}}$ is computed as follows:

$$\text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right) = \left\| \left(\text{Geo}^D_{\max} - \text{Geo}^D_{\min} \right)_i \right\| * \sqrt{\frac{\text{SD}_t(\text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right) - \text{OV})^2}{\text{SD}_t\left(\frac{\text{Geo}^D_{\min}}{\text{Geo}^D_{\max}} - \text{OV}\right)^2} + \frac{R_{\text{SD}}}{s} - F} \tag{3}$$

where

$$\text{SD}_t = \frac{1}{\text{Geo}^D} \sqrt{\frac{1}{s-1} \sum\nolimits_{i=1}^{\text{Geo}^D} \left(\frac{\text{OV} - F}{N} \right)^2}. \tag{4}$$

Therefore

$$\text{OV} = s\left\{ \left\| \left(\text{Geo}^D_{\max} - \text{Geo}^D_{\min} \right)_i \right\| - \left\| \text{Geo}^D_{\max} - \text{Geo}^D_{\min} \right\| \right\} + \text{SD}_t * \text{NC}_a - F \tag{5}$$

$$F = s\left\{ \left\| \left(\text{Geo}^D_{\max} - \text{Geo}^D_{\min} \right)_i \right\| + \left\| \text{Geo}^D_{\max} - \text{Geo}^D_{\min} \right\| \right\} \leq s\left\{ \left\| \left(\text{Geo}^D_{\max} - \text{Geo}^D_{\min} \right)_i \right\| - \left\| \text{Geo}^D_{\max} - \text{Geo}^D_{\min} \right\| \right\} - \text{OV}\left(D_S + R_S\right). \tag{6}$$

As per (3)–(6), the privacy preservation relies on geosensed data and analysis with existing data, then considering the delayed signing time (SD_t), non-coherent agreement NC_a, overlaps OV, and failures F in active sessions. Here, OV is identified at the time of performing two-factor authentication for data privacy from the transmitter end.

The R_{SD} is accumulated at different sensing intervals that generate $\text{Geo}^D_{\min}$ and $\text{Geo}^D_{\max}$ depending on s operations. Post the classification, the s status for transmission and authentication is

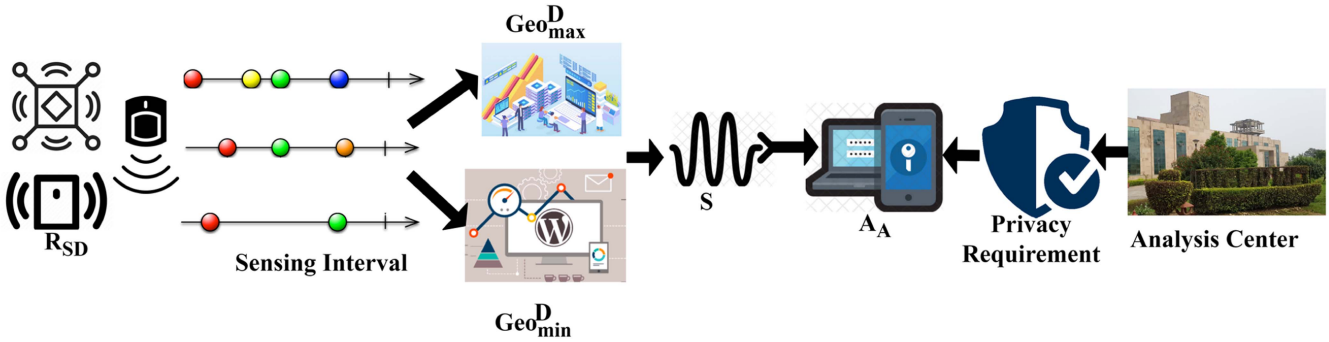

Fig. 2. Augmenting authentication process.

determined at the analysis center. Authentication initialization is performed using mutual acceptance between sensors and the analysis center. If the s status is ready, then overlapping (mutual acceptance) is verified for data exchange. This process is required for $A_A \in (\text{Geo}^D_{\text{min}} + \text{Geo}^D_{\text{max}})$, which is intense over the different intervals (refer to Fig. 2). The signing delay and nonmatched data are identified through a lightweight signing process, in which precise geosensed data are required. Based on the Geo^D and $\text{Data}_{\text{Privacy}}(\text{Geo}^D)$, the sequential identification I_d of signing delay and noncoherent agreement in overlapping is estimated as follows:

Equation (7) shown at the bottom of this page computes continuous smart city big data augmentation and management for the instance until sensors s are active in sending information to the communication points. The sensed data need to be concealed before analytical disclosures, and the devices should be remotely connected to prevent compromised data and leakage. The sequence of device compromise and data augmentation using two-factor authentication and this proposed scheme is reliable for geosensed data. Consider that the data privacy at the transmitter end is to be verified and secured using a lightweight signature for better privacy-preserving accuracy, which mainly focused on device and receiver signatures overlapping in any situation being analyzed. This overlapping is said to fail in privacy-preserving solutions for remotely sensed environmental data of smart cities to improve the digital signing processing. In addition, it is crucial to ensure the privacy of the sensitive geosensed data, as all the data collected from various locations undergoes real-time analysis. Therefore, data augmentation and management based on identifying failure are continuously analyzed using federated learning. If failure is identified at the time of device compromise, then that session will be halted. The autonomous and sophisticated remotely connected devices pose risks of data compromise and leakage; therefore, the failure occurring in that session is detected and rectified through federated learning paradigm. The learning process is configured with the $s \in$ different intervals. Coherence verification is performed using the input features OV and A_A. This is initially performed across different time intervals. In the latter, the independent configurations for N and I_d are considered. The learning process for coherence analysis is presented in Fig. 3. The initial state of these remotely sensed environmental data is protected through two-factor authentication, and then further sensing operation is observed and analyzed. The privacy-preserving output for remote sensing data performs the condition $(1 - \frac{F}{\text{Geo}^D})\text{OV}$ from different transmitter ends for reliable and precise authentication, which is provided to the smart city data.

From this instance, the aforementioned two security issues in geosensed data are analyzed for improving authentication. Let d_l and d_c be used for computing privacy-preserving solutions using federated learning. For this privacy-preserving output computation PP^k, the sequence of remote sensing geoapplications is modeled as per (8) and (9)

$$d_l + d_c = PP^k. \tag{8}$$

For the consecutive instance

$$\text{fl} = \left(I_d(F) + \frac{\text{OV}}{N}\right). \tag{9}$$

This federated learning "fl" is performed to identify failures in active sessions at the transmitter end, following the lightweight signature to conceal data from theft. These geodata are analyzed based on coherence and time delay in data transmission to prevent data leakage and device compromise. The learning for coherence (see Fig. 3) is a reverse process in which C_a is segregated from NC_a. First, for $(\text{Geo}^D_{\text{min}} + \text{Geo}^D_{\text{max}})$, I_d for the sensed intervals and s are identified. This identification is split across OV and F computations; if A_A is to be performed, then $\text{OV} \subseteq I_d$, else noncoherent output is generated. Such instances (post) are halted for preventing false data. The identified halts are separately analyzed for $(1\text{to}\,t)$ across $\text{Geo}^D_{\text{min}}$ and $\text{Geo}^D_{\text{max}}$ occurrences for extracting the least possible I_d.

$$I_d\left[\text{Geo}^D, \text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\right] = \sqrt{\left[\frac{\text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)}{\text{Geo}^D}\right]_1^2 + \left[\frac{\text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)}{\text{Geo}^D}\right]_2^2 + \ldots + \left[\left(1 - \frac{F}{\text{Geo}^D}\right)\text{OV}\right]_s^2}. \tag{7}$$

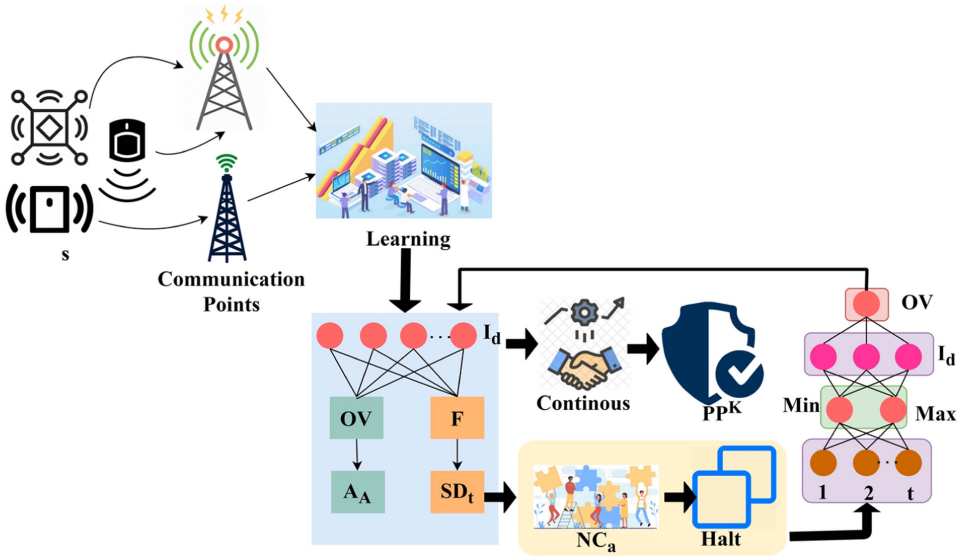

Fig. 3. Coherence analysis.

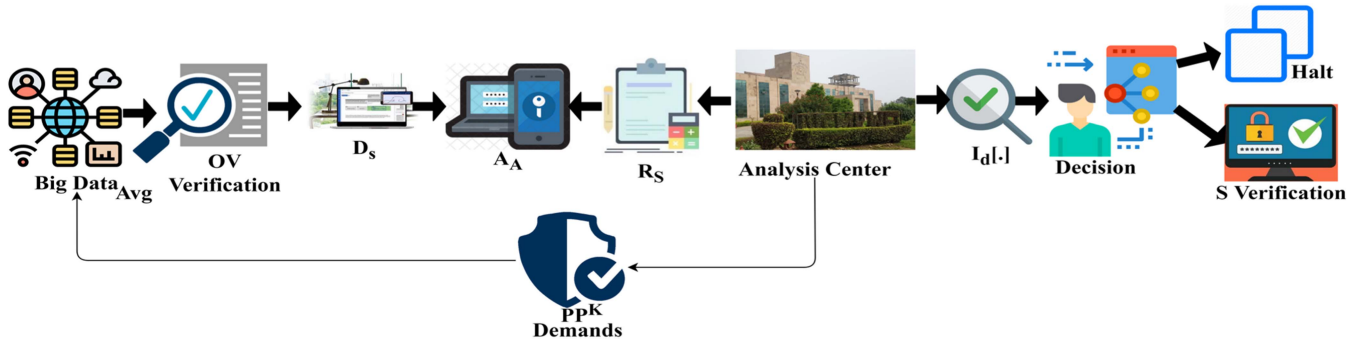

Fig. 4. Authentication flow.

This process is repeated through OV for authentication. This authentication is therefore different for $I_d \subseteq NC_a$ and $I_d \subseteq C_a$, whereas for SD_t instances, the authentication is halted.

B. Lightweight Signing Process

The EI Gamal algorithm is used for lightweight signatures; it first selects the prime numbers p and q and then two integers, α and X, where $\alpha < p$; The estimation of Y is given as $Y = \alpha^X \bmod p$. The prime numbers p and q should be selected; hence, $(p-1)\cdot(q-1)$ has a large prime factor r. When signing a device D and a receiver R, a random integer K will be selected for further process, where K must not be used before satisfying the condition $0 < K < pq - 1$ and is relatively prime to $(p-1)$ and $(q-1)$.

The lightweight signature in the device and receiver (D and R) is performed through $R = \alpha^K \bmod pq$ and $R = K - 1(D - XR)\mathrm{mod}(p-1)\cdot(q-1)$, where K^{-1} is the multiplicative inverse of $K \bmod (p-1).(q-1)$; hence, $K * K^{-1} = 1 \bmod (p-1)\cdot(q-1)$. When verifying the device-compromised data, the public key XY is used to estimate $Y^R D^r \bmod pq$ and determine if it is equivalent to $\alpha^D \bmod pq$. The proposed model performs the public key generation and encryption at the leaf node to decrease the communication and computation overhead of the sensor nodes, as shown in Fig. 4.

The digital signature algorithm (DSA) is also known as the digital signature standard. DSA is referred to as two-factor authentication with a few limitations, which are as follows.

1) The size of p and q is fixed at $3^{602} < pq < 2^{513}$, which makes p and q about 180 decimal digits long.
2) r , which is the largest prime factor of $(p-1)\cdot(q-1)$, is chosen, so that $2513 < r < 3602$.
3) The hash value $H(D*R)$ is used, instead of using all the device-compromised data D.
4) The computations of the device and receiver signatures are taken $\bmod r$,

This authentication clearly states that two-factor authentication and lightweight signature are two completely different algorithms for improving device performance and reducing data leakage; lightweight signature can go up to 4096 b, whereas two-factor authentication has to be exactly 1024 b.

The Big Data_{Avg} is prepared for OV verification with the analysis center (receiver) demands. The requirement is the PP^k satisfaction for generating D_s and R_S in A_A. Therefore, the received A_A is verified for $I_d[.]$ and PP^k demands satisfaction. If any discrepancy occurs in this process, then decisions on halting and/or s verification occurs. Therefore, the false/incomplete data are prevented from entering the actual analysis and verification (see Fig. 4). The above-mentioned representation is different from Fig. 2, where the augmenting process is illustrated. In the representation shown in Fig. 4, the in-depth signing process is illustrated. The Fig. 2 covers the overview between the devices and the intervals, whereas the Fig. 4 specifies the authentication variables and their demands in the former interval. Therefore, the first privacy-preserving output is achieved through a lightweight signature and two-factor authentication. Therefore, $D_S = \text{Geo}^D$ and $R_S = 0$ outputs in failure in communication points, and it increases the time delay in the signing process and coherence agreement at the time of device verification. From this instance, $D_S = \text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)$ and $R_S = \frac{F}{N}$. Therefore, in this proposed scheme, the active session's performance is analyzed with device verification based on the condition $D_S + R_S = \text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right) + \frac{F}{N}$, which is computed for preventing the time delay in signing. Federated learning checks the privacy of the device and recurrently analyzes any failure in active sessions for preserving accuracy. If failure is identified in the active session, the signing processes are paused, and operations are halted until accurate device verification succeeds. Once the device verification process is successfully completed, a new session is initiated to analyse the geosensed data, which is then followed by the generation of output. The effective verification process minimizes the computation overhead. The smart city data augmentation and management operations rely on optimal device verification performed through federated learning, which is represented as follows:

$$F\|\text{Data}_{\text{Privacy}i}\left(\text{Geo}^D\right)\|^2 \le \|\text{Data}_{\text{Privacy}}\left(\text{Geo}^{\text{D}}\right)\|^2 D_S + \|\text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\|^2 R_S - \frac{F}{N} \tag{10}$$

$$F\|\text{Data}_{\text{Privacy}i}\left(\text{Geo}^D\right) - \text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\|^2 \le \|D_S^2\| \tag{11}$$

$$\|\text{Data}_{\text{Privacy}i}\left(\text{Geo}^D\right) - \text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\|^2 \le \left\{\text{OV}_i + C_a\left(F\text{OV}_i + NPP^k\right)\right\} \tag{12}$$

where $C_a = \sum_{i \in N} D_{S_i} + R_{S_i} + I_{d_i}$

$$F\|\text{Data}_{\text{Privacy}i}\left(\text{Geo}^D\right) - \text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\|^2$$

$$= F\|\text{Data}_{\text{Privacy}i}\left(\text{Geo}^D\right)\|^2 - 2F\|\text{Data}_{\text{Privacy}i}\left(\text{Geo}^D\right)\| \|\text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\| + F\|\text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\|^2$$

$$= F\|\text{Data}_{\text{Privacy}i}\left(\text{Geo}^D\right)\|^2 - F\|\text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\|^2. \tag{13}$$

First, we analyze the identified halts across $\text{Geo}^D_{\text{min}}$ and $\text{Geo}^D_{\text{max}}$ to represent the convergence at different time instances as follows:

$$\begin{aligned} &F\left\{\|\text{Geo}^D_{\text{min}} - \text{Geo}^D_{\text{max}}\|\right\}^2 \\ &= F\left\{\|\text{Geo}^D_{\text{min}} - PP^k\left(\text{Data}_{\text{Privacy}i}\left(\text{Geo}^D\right)\right) - \text{Geo}^D_{\text{max}} + PP^k\left(\text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\right)\|\right\} \\ &\le F\{\|\text{Geo}^D_{\text{min}} - \text{Geo}^D_{\text{max}}\| + PP^k\|\,\text{Data}_{\text{Privacy}i}\left(\text{Geo}^D\right) - \text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\| \\ &\quad + PP^k\left(\text{OV}_i + C_a\left(F\text{OV}_i + NPP^k\right)\right)\}. \end{aligned} \tag{14}$$

The performance is analyzed using authentication success and overlapping failures that are responsible for performing device verification at different instances. In two-factor authentication, lightweight digital signing cryptography is utilized for preventing false rates. Based on the analytical disclosure, the sensitive remote sensing geoapplications for preventing compromised data with remotely connected devices are computed as shown in the following equations:.

$$\begin{aligned} \text{Geo}^{\text{D}} = \sum PP^K - F\|\text{Geo}^D_{\text{min}} - PP^k\left(\text{Data}_{\text{Privacy}i}\left(\text{Geo}^D\right)\right) \\ - \text{Geo}^D_{\text{max}} + PP^k\left(\text{Data}_{\text{Privacy}}\left(\text{Geo}^D\right)\right)\| \end{aligned} \tag{15}$$

$$\begin{aligned} = \sum\Big(D_S \text{ in } \text{Geo}^D + \Big(\sum R_S \text{ in the } \text{Geo}^D \times \text{Device}_{\text{verification}}\Big) \\ - PP^k\left(F_i + C_a\left(F\text{OV}_i + NPP^k\right)\right)\Big) \end{aligned} \tag{16}$$

where

$$\rho_{PP^K} = \frac{\left[\text{count}\ \left(\text{Geo}^D\right)\right]^{\text{SD}_t} - (\text{OV})^{\text{SD}_t - 1}}{\sum_{i \in D^t}\left[\text{count}\left(\text{Geo}^D\right)\right]^{\text{SD}_t} \times \left(1 - \text{Device}_{\text{verification}}\right)^{\text{SD}_t - 1}}. \tag{17}$$

From (15)–(17), the probability of privacy-preserving accuracy is computed based on remotely connected devices. The privacy-preserving process is shown in Fig. 5.

The privacy-preserving process requires PP^k satisfaction $\forall A_A \in [t, t+N)$, reducing $\rho(PP^k)$. The learning process decides the NC_a occurrences for which I_d is halted. Therefore, decisions to halt A_A until device verification is performed for improving Geo^D. This ensures freedom from false impressions and leakage (I_d failures) so that SD_t is used for identifying D_S and R_s. Therefore, the remotely sensed environmental data are sequentially improved through successful authentication, preventing compromised data.

IV. Results and Discussion

This section presents the self-analysis of the proposed scheme using the data available in [29] and [30]. The data are generated

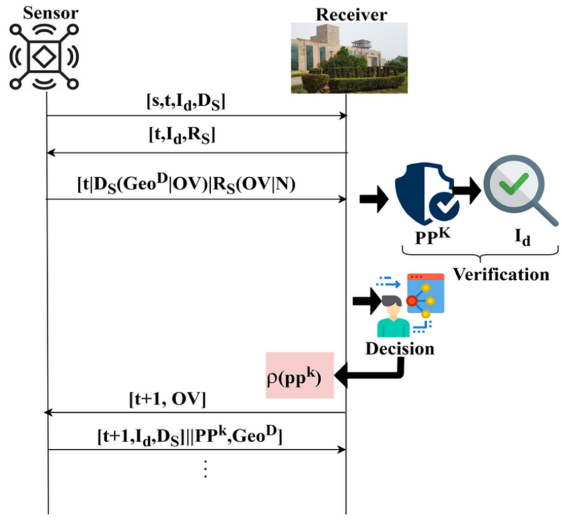

Fig. 5. Privacy-preserving process.

TABLE I
SD_t AT DIFFERENT TIME INTERVALS

t	A_A Instances	D_S Time (min)	R_S Time (min)	SD_t	Transmission Halts
5	3	0.05	0.04	0.01	1
10	8	0.96	0.59	0.37	1
15	6	0.81	0.65	0.16	1
20	8	0.96	0.05	0.91	1
25	7	0.71	0.69	0.02	1
30	10	1.25	0.78	0.47	1
35	11	1.89	1.21	0.68	1
40	8	0.81	0.69	0.12	1
45	9	1.25	1.59	0.34	1
50	12	2.01	1.89	0.12	1
55	10	1.25	2.01	0.76	1
60	14	2.19	2.57	0.38	1

by observing daily climatic changes at different locations from January 2013 to April 2017. The locations are separated by a minimum of 4 km and a maximum of 70 km in the same geospatial city location of a country. The dataset provides 1462 instances of 5 features: date, average temperature, humidity, wind velocity, and pressure. The training is provided on approximately 80% of the data, which is about 1169 instances. The testing is performed using 293 (approximately 20%) random instances. A varying number of data points are used in the validation phase. For example, to predict the temperature, the date, humidity, wind velocity, and pressure are used. To predict the wind velocity, the date, average temperature, humidity, and pressure are used. The feature encoding is performed automatically by the inbuilt library of scikit-learn preprocessing functions, which handles both continuous and categorical variables. However, in our case, the time (months, days, weekdays, hours, minutes, seconds, etc.) is all cyclical in nature; therefore, we have utilized the widely used method of sine and cosine transformations of each to encode these variables.

Data are sensed at 12 accumulation instances from 4- to 60-min intervals and used for deciding the prediction outcome. The security concept for privacy preservation is verified by identifying (verifying) the reception of unchangeable values in the same instance.

The National Climatic Data Center database of historical meteorological and climate data from throughout the world, as well as station history information, is available for free via Climate Data Online [30]. In addition to radar readings and 30-year climate information, these records also include quality-controlled daily, monthly, seasonal, and annual readings of temperature, precipitation, wind, and degree. The collected data are integrated and processed by applying the discussed privacy-preserving process. The effectiveness of the system is evaluated using the authentication rate, overlapping failure analysis, false rate, and verification time. The possible adverse effects in data sensing, accumulation, and reception are presented in Fig. 6.

The device compromise and data leakage adversaries result in false data and missing inputs due to the transmission. The variants of Geo^D for Geo_min and Geo_ $\max \notin A_A$ are considered as the false data. These variants of Geo^D disturb the privacy demands of sensitive geographical data. If this information is processed, then false/improper forecast (or) data unavailability occurs. Therefore, administering privacy-concerned security for data and devices becomes mandatory. In a conventional authentication process, a sensing device is operated remotely through password-protected access. Similarly, the mode of authentication for data privacy is determined by the service provided. The A_A is implemented for the Big Data_{Avg} in t using D_s and R_s. Practically, D_S represents remote access authentication, and R_S represents the mutually agreed transmission privacy. The first analysis is performed to verify if the data integrity is sustained at different intervals, as shown in Fig. 7(a). The proposed scheme is analyzed for its impact on the A_A for device compromise and false data. This scheme ensures SD_t less authentication using D_s in mutual coherence with the R_S. Therefore, concealed data transmission takes place at any t. It should be noted that the $A_A \in t$ is not initiated in $(t \pm N)\ \forall\ N\ \{1, 2, ..t\}$; this prevents the signing delay due to nonmutual agreement. Therefore, device-level compromise is thwarted at the preliminary stage.

For transmission and data-sharing privacy, the El Gamal algorithm is used, which verifies $R = \alpha^k\ |pq|$ in both the sender and the receiver. This ensures maximum data integrity, whereas $\alpha^D|pq|$ ensures data availability for reducing adversary impact. Data integrity denotes the accuracy, completeness, and consistency of remotely sensed environmental data in smart cities. At different time intervals, data integrity has been calculated. However, under limited sensing intervals as the data accumulated is less, the integrity and Geo^D are precisely high, as shown in Fig. 7(b). Pursuing the data-level security outcomes, SD_t, the different values of t are tabulated in Table I.

The above-mentioned tabulation identifies the SD_t depending on the available authentication and transmission initializations.

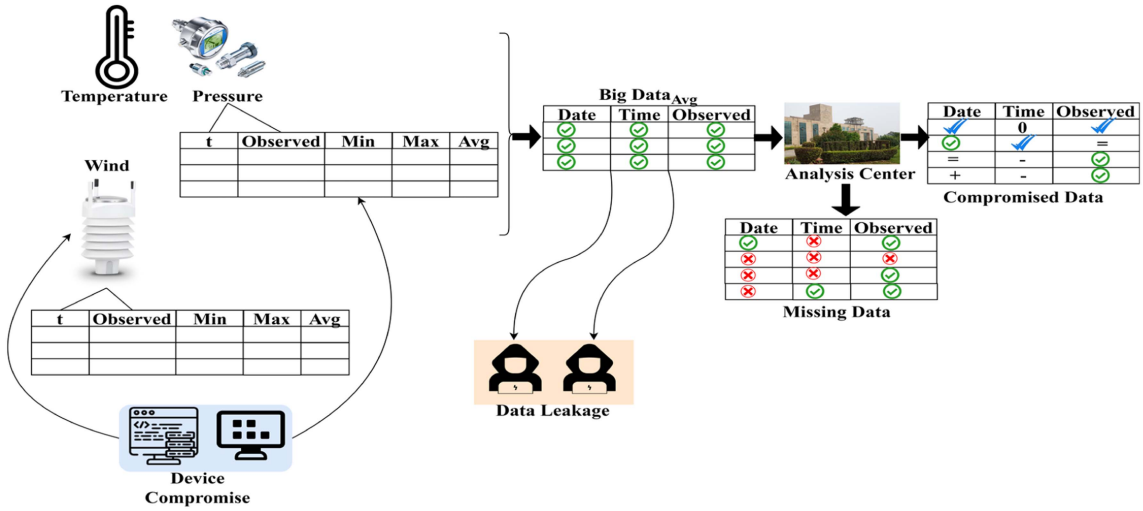

Fig. 6. Possible adversary effect representation.

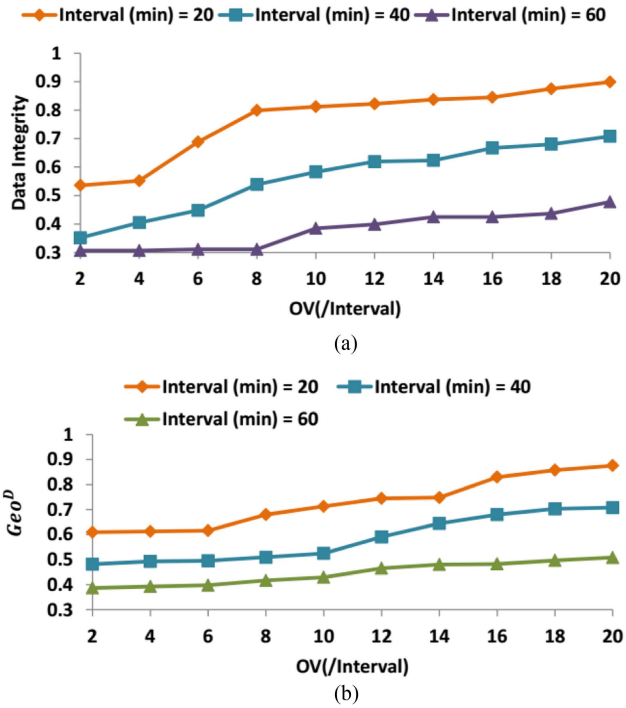

Fig. 7. (a) Data integrity analysis. (b) Geo^D analysis.

The changes in t between the actual sensing interval and transmission time are recorded as SD_t. In particular, if the SD_t is major (high), then the transmission is halted, and therefore, device verification is performed. The above-mentioned tabulation is identified from the missing intervals in the input data. Similarly, the difference in transmission and delay between the receiver and the successive $\mathrm{BigData}_{\mathrm{Avg}} \in (t+N)$ surpasses the current authentication. Therefore, $F(\mathrm{Geo}^D, \mathrm{Data}_{\mathrm{privacy}}(\mathrm{Geo}^D)]$ is performed for D_S $(\mathrm{Geo}^D|\mathrm{OV})$ and $R_s(\mathrm{OV}|N)$. In this case, the OV replication in D_S and R_S is required to be the same for reducing transmission halts (see Table I). The above-mentioned tabulation is performed for all the $\rho(PP^k)$ existence from T to $(T+N)$.

TABLE II
$\rho\,(PP^k)\forall F$

Data Accumulation	F	$\rho(PP^K)$	NC_a	Geo^D
2	0	0.608	0.031	0.91
4	2	0.731	0.098	0.85
6	1	0.691	0.051	0.89
8	2	0.731	0.098	0.85
10	2	0.731	0.098	0.85
12	3	0.823	0.140	0.62

Therefore, the $\rho(PP^k)$ for the varying halted/paused A_A is tabulated in Table II and Fig. 8(a).

As the $\rho(PP^k)$ increases, if the F increases, the F is increased, provided SD_t is observed. Depending on the NC_a occurrence, the OV verification is initiated by verifying the device validity and uncompromised data. Federated learning identifies A_A feasible instances from $F \in \mathrm{SD}_t$ for I_d detection. In consecutive intervals, I_d is verified if Ov is present in the same t without $(t \pm N)$ $\forall N \in \{1, 2, \ldots, t\}$. Therefore, the $\rho(PP^k)$ is satisfied for NC_a fewer sensing instances for preventing failures and adversaries. This is further verified for identifying if F is present in I_d (post the OV verification). Such analyses are presented in Fig. 8(b).

The F is considerably less for OV as the SD_t occurrence is confined due to limited data accumulated and analyzed. The verification is performed for $\rho(PP^k)$ induced I_d. Therefore, I_d verification for A_A and OV is recurrent using the learning for stabilizing Geo^D. The front and tailing validations for consecutive t considering $\mathrm{Geo}^D_{\mathrm{min}}$ and $\mathrm{Geo}^D_{\mathrm{max}}$ are jointly handled for addressing NC_a. In this case, the I_d breaks are confined ensuring prompt data verification (see Fig. 8).

The following section presents the comparative analysis using the metrics of authentication success rate, overlapping factor,

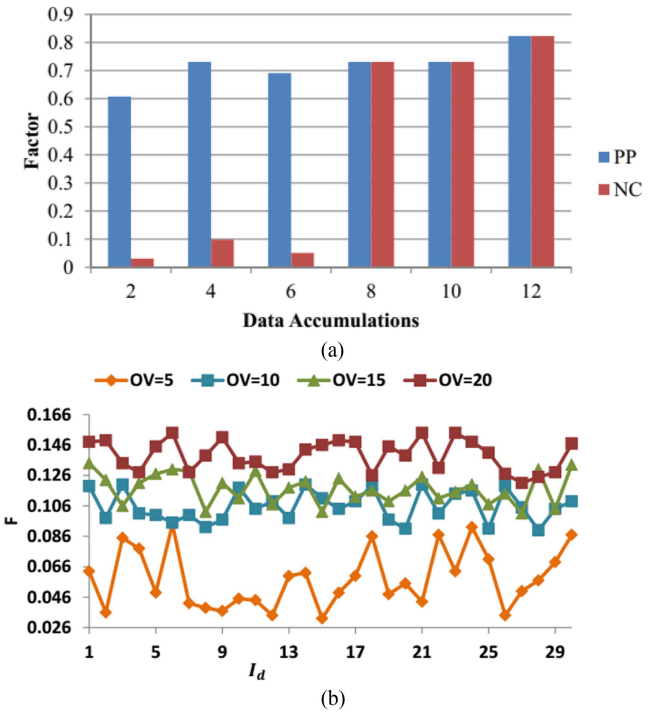

Fig. 8. (a) PP and NC analyses. (b). F analysis in I_d.

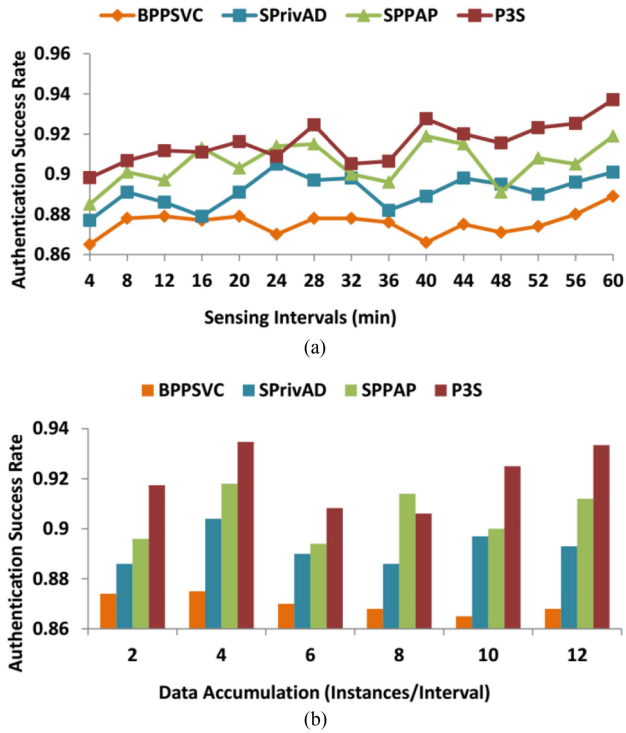

Fig. 9. Authentication success rate analysis. (a) Authentication success rate at different sensing intervals. (b) Authentication success rate versus data accumulation.

authentication time, false data, and verification time. The variants considered are sensing intervals and data accumulation instances. In this comparison, the existing BPPSVC [20], SPrivAD [22], and SPPAP [27] methods are considered.

A. Authentication Success Rate

This proposed P3 scheme satisfies high authentication success rate in device verification using federated learning and a lightweight signature process. This is achieved by reducing data leakage and device compromise in remotely connected devices (refer to Fig. 9). The overlapping failure identified at the transmitter end relies on the device due to consumption variation and receiver signature during data transmission intervals using geosensed data analysis. Transmitting data across different communication points for performing device compromise modification prevents security threats. The identification of device compromise and data drops improves authentication. In the open environment, the use of sensing devices and sophisticated connected technologies is essential for the overall development of the smart city. The failure is identified in sensitive geosensed data for improving authentication. Therefore, device verification is performed based on $s \in \text{Geo}^D$, $\text{Geo}^D_{\min}$, and $\text{Geo}^D_{\max}$. Smart city data privacy is to satisfy the device and receiver signatures for identifying different coherent agreements.

B. Overlapping Failures

In Fig. 10, the weather, temperature, and soil information in smart city applications are analyzed for transmitting data in an open environment to achieve successive device verification and reduce overlapping failures. This identification of failures in device performance enhances privacy preservation based on sensed data from multiple-location verification and mitigates the security threats through federated learning at different periods. The changes in sensed data are analyzed with existing data for reducing authentication time. The successive device verification relies on the overlapping of digital signing delay, and noncoherent agreement for the condition $(1 - \frac{F}{\text{Geo}^D})\text{OV}$ is recurrently computed using the learning process. The device verification fails in the particular session, and as a result, further operation is halted and the aggregation is paused in that session by federated learning. In this proposed scheme, the device-compromised data prevents leakage and security issues. The retransmission of data is performed for identifying accurate device verification in an active session. The sensed data from the smart city are analyzed for controlling different threat mitigations in this proposed scheme to satisfy fewer overlapping failures.

The authentication time is reduced in this proposed scheme, which improves authentication in remote sensing geoapplications. The use of two-factor authentication and a lightweight signature prevents compromised actual data. The security issues of big data augmentation are analyzed and compared to the other factors for succeeding in the device verification, as shown in Fig. 11.

In this work, the communication points rely on the identification of data drops and utilization of lightweight digital signing cryptography from the different transmitter ends. The device compromise and chances of data leakage are analyzed for improving the environment based on privacy preservation through P3S. The overlapping failure is recurrently identified

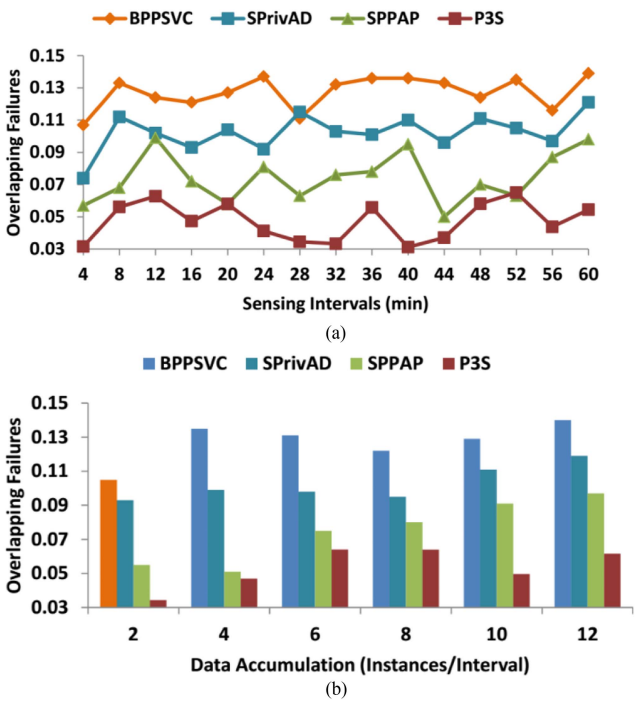

Fig. 10. Overlapping failures analysis. (a) Overlapping failures at different intervals. (b) Overlapping failures versus data accumulation.

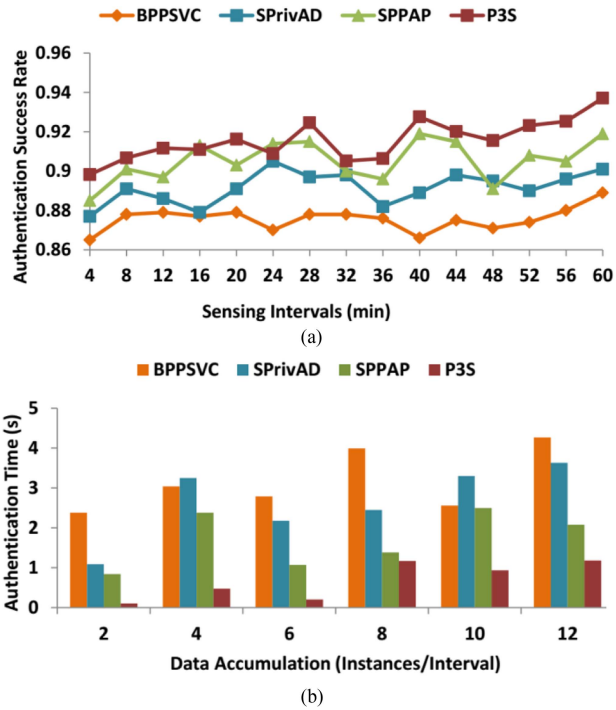

Fig. 11. Authentication time analysis. (a) Authentication success rate at different intervals. (b) Authentication time versus data accumulation.

using federated learning, as shown in (10)–(12). In this proposed scheme, the signatures of the device and receiver are jointly analyzed to prevent security threats. In this signing process, the aforementioned security issues occur, and the session is paused until the device verification is performed. In this proposed

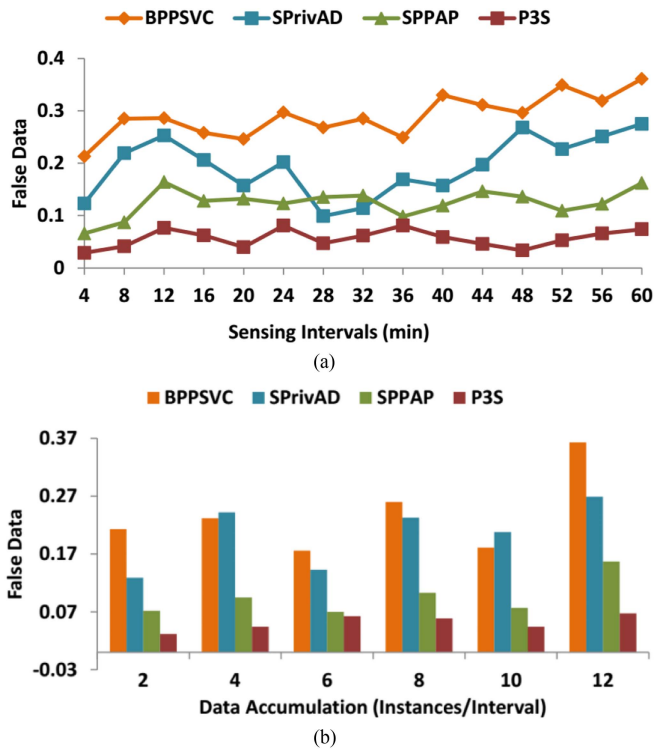

Fig. 12. False-data analysis. (a) False data at different sensing intervals. (b) False data versus data accumulation.

scheme, the smart city device verification is performed to reduce the authentication time.

C. False Data

In Fig. 12, a comparison is made between the existing smart city environmental data and the current geosensed data for identifying changes through communication points at different periods to prevent data drops. The high data leakage and device compromise in the remotely connected devices rely on a different coherent agreement and delayed signing time. From the communication points, a large amount of data is transmitted for big data augmentation, and the raw data are concealed using two-factor authentication for overall development.

The federated learning process is aided in detecting the overlapping failure of performing the device and receiver signing at a similar time. This failure does not require constant devices for processing the data at different periods. The associated sessions have compromised the devices through a learning process and performed verification based on two types of digital signature processes recurrently performed in a continuous manner. The learning process is used for identifying the overlapping failure at the time of device verification failure in the active session. The proposed P3S achieves less false data in autonomous and remotely connected technologies.

D. Verification Time

The device verification time computation is performed to enhance the smart city application performance and maximizing

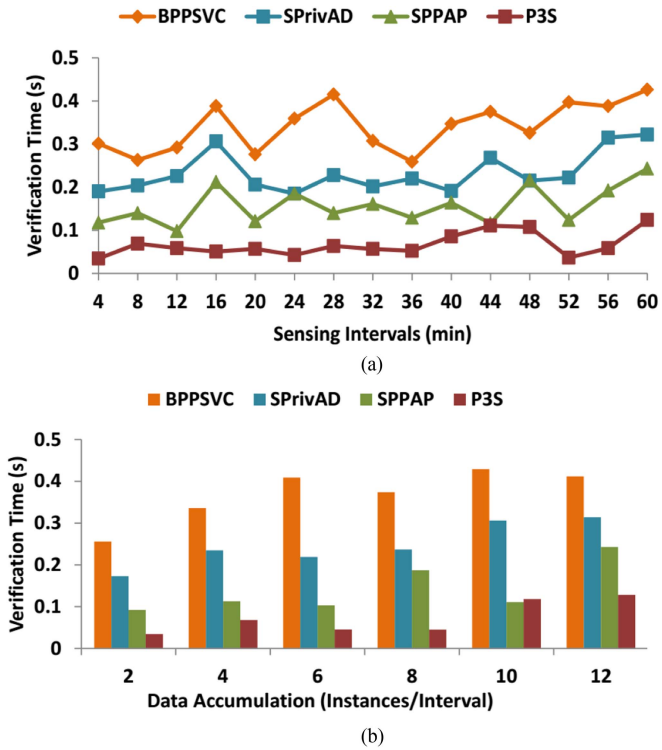

Fig. 13. Verification time analysis. (a) Verification time at different sensing intervals. (b) Verification time versus data accumulation.

TABLE III
COMPARATIVE ANALYSIS FOR SENSING INTERVALS

Metrics	BPPSVC	SPrivAD	SPPAP	P3S
Authentication Success Rate	0.889	0.901	0.919	0.937
Overlapping Factor	0.139	0.121	0.098	0.054
Authentication Time (s)	4.170	3.020	2.360	1.363
False Data	0.361	0.275	0.162	0.073
Verification Time (s)	0.426	0.322	0.243	0.123

the security levels for concealing the environmental data from the sensors, as illustrated in Fig. 13. In this proposed P3S, a large amount of data transmission takes place, and the success of device verification through two-factor authentication and a lightweight signing process for identifying data leakage and device compromise is high. In this article, the device and receiver signature overlapping failure is identified through the estimation of $D_S = \text{Data}_{\text{Privacy}}\ (\text{Geo}^D)$ and $R_S = \frac{F}{N}$ for preventing coherence and time delay. Federated learning is performed for improving authentication, big data augmentation, and management. In this approach, sensitive geosensed data are processed and secured from the transmitter end.

With this recurrent analysis of identifying failures for preventing security threats and overlapping failures using two-factor authentication and a lightweight signing process, the device verification time is less for big data authentication. The comparative analysis results are presented in Tables III and IV, respectively, for the sensing intervals and data accumulation instances. In

TABLE IV
COMPARATIVE ANALYSIS FOR DATA ACCUMULATION INSTANCES

Metrics	BPPSVC	SPrivAD	SPPAP	P3S
Authentication Success Rate	0.868	0.893	0.912	0.933
Overlapping Factor	0.140	0.119	0.097	0.061
Authentication Time (s)	4.270	3.630	2.080	1.182
False Data	0.363	0.269	0.157	0.067
Verification Time (s)	0.412	0.314	0.243	0.128

TABLE V
COMPARATIVE ANALYSIS (AVERAGE)

Metrics	Sensing Interval	Data Accumulation	Average
Authentication Success Rate	9.23	8.48	8.86
Overlapping Factor	12.99	11.41	12.20
Authentication Time (s)	9.54	10.73	10.14
False Data	9.61	9.78	9.70
Verification Time (s)	10.33	10.05	10.19

Tables III and IV, the final values observed from the graphs for the varying sensing intervals and data accumulation instances are presented. The findings given below are estimated as a mean cumulative value of the existing methods to the single proposed value.

The proposed scheme maximizes the authentication success rate and overlapping factor by 9.23% and 12.99%, respectively. This scheme further reduces authentication time, false data, and verification time by 9.54%, 9.61%, and 10.33%, respectively.

The proposed scheme maximizes the authentication success rate and overlapping factor by 8.48% and 11.41%, respectively. This scheme further reduces authentication time, false data, and verification time by 10.73%, 9.78%, and 10.05%, respectively, as compared to existing methods, as mentioned in Table IV.

The mean cumulative values obtained from sensing interval and data accumulation have been averaged in Table V. The proposed scheme maximizes the average authentication success rate and average overlapping factor by 8.86% and 12.20%, respectively. This scheme further reduces average authentication time, false data, and verification time by 10.14%, 9.70%, and 10.19%, respectively.

V. CONCLUSION

Considering the privacy and significance of remotely sensed data in smart city applications, this article introduced a P3S. This scheme incorporates federated learning and lightweight signing authentication for ensuring end-to-end data integrity. More specifically, this scheme counterfeits the impacts due to device compromise and false-data adversaries. The proposed scheme establishes coherent sequential two-factor authentication for sensed data sharing. In the mutual authentication process, the receiver and sensor device signatures are required for sustaining privacy requirements. The learning process identifies lags in sequential transmission using the coherence factor and delayed signing. The proposed scheme identifies failures in

overlapping coherence before and after data exchange. This coherence factor is recurrently analyzed using federated learning, such that the halting and sensor device verification decisions are performed. The proposed scheme maximizes the average authentication success rate and average overlapping factor by 8.86% and 12.20%, respectively. This scheme further reduces average authentication time, false data, and verification time by 10.14%, 9.70%, and 10.19%, respectively. Although the proposed scheme is reliable for the overall privacy process, a setback in pausing the signing process is observed. In nonperiodic sensing intervals, this is less feasible due to which the chances of the false rate increase. This problem is considered in our future work by incorporating multilevel adaptable authentication based on the time of arrival metric. This is planned to be performed with less complexity by preventing signing replications.

ACKNOWLEDGMENT

The authors would like to thank the Deanship of Scientific Research, Qassim University for funding the publication of this project.

REFERENCES

[1] H.-H. Chang and W.-C. Chan, "Automatic registration of remote sensing images based on revised SIFT with trilateral computation and homogeneity enforcement," *IEEE Trans. Geosci. Remote Sens.*, vol. 59, no. 9, pp. 7635–7650, Sep. 2021, doi: 10.1109/TGRS.2021.3052926.

[2] G. Zhou, X. Bao, S. Ye, H. Wang, and H. Yan, "Selection of optimal building facade texture images from UAV-based multiple oblique image flows," *IEEE Trans. Geosci. Remote Sens.*, vol. 59, no. 2, pp. 1534–1552, Feb. 2021, doi: 10.1109/TGRS.2020.3023135.

[3] A. Sharifi, "Development of a method for flood detection based on Sentinel-1 images and classifier algorithms," *Water Environ. J.*, vol. 35, pp. 924–929, 2021, doi: 10.1111/wej.12681.

[4] J. D. Michler, A. Josephson, T. Kilic, and S. Murray, "Privacy protection, measurement error, and the integration of remote sensing and socioeconomic survey data," *J. Develop. Econ.*, vol. 158, pp. 1–25, 2022, doi: 10.1016/j.jdeveco.2022.102927.

[5] A. Sharifi et al., "Agricultural field extraction with deep learning algorithm and satellite imagery," *J. Indian Soc. Remote Sens.*, vol. 50, pp. 417–423, 2022, doi: 10.1007/s12524-021-01475-7.

[6] Y. Liu et al., "COMP: Online control mechanism for profit maximization in privacy-preserving crowdsensing," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 7, pp. 1614–1628, Jul. 2020, doi: 10.1109/JSAC.2020.2999697.

[7] S. Jalayer, A. Sharifi, D. Abbasi-Moghadam, A. Tariq, and S. Qin, "Modeling and predicting land use land cover spatiotemporal changes: A case study in Chalus Watershed, Iran," *IEEE J. Sel. Topics Appl. Earth Observ. Remote Sens.*, vol. 15, pp. 5496–5513, 2022, doi: 10.1109/JSTARS.2022.3189528.

[8] S. Sodagari, "Trends for mobile IoT crowdsourcing privacy and security in the Big Data era," *IEEE Trans. Technol. Soc.*, vol. 3, no. 3, pp. 199–225, Sep. 2022, doi: 10.1109/TTS.2022.3191515.

[9] F. Zhao et al., "Night-time light remote sensing mapping: Construction and analysis of ethnic minority development index," *Remote Sens.*, vol. 13, no. 11, 2021, Art. no. 2129, doi: 10.3390/rs13112129.

[10] Y. Wang et al., "Privacy protection in mobile crowd sensing: A survey," *World Wide Web*, vol. 23, no. 1, pp. 421–452, 2020, doi: 10.1007/s11280-019-00745-2.

[11] M. Li, Z. Tian, X. Du, X. Yuan, C. Shan, and M. Guizani, "Power normalized cepstral robust features of deep neural networks in a cloud computing data privacy protection scheme," *Neurocomputing*, vol. 518, pp. 165–173, 2023, doi: 10.1016/j.neucom.2022.11.001.

[12] O. Odebiri et al., "Modelling soil organic carbon stock distribution across different land-uses in South Africa: A remote sensing and deep learning approach," *ISPRS J. Photogrammetry Remote Sens.*, vol. 188, pp. 351–362, 2022, doi: 10.1016/j.isprsjprs.2022.04.026.

[13] J. Ma and J. Hu, "Safe consensus control of cooperative-competitive multi-agent systems via differential privacy," *Kybernetika*, vol. 58, no. 3, pp. 426–439, 2022, doi: 10.14736/kyb-2022-3-0426.

[14] R. Sun, L. Fu, Q. Cheng, K.-W. Chiang, and W. Chen, "Resilient pseudorange error prediction and correction for GNSS positioning in urban areas," *IEEE Internet Things J.*, vol. 10, no. 11, pp. 9979–9988, Jun. 2023, doi: 10.1109/JIOT.2023.3235483.

[15] S. Jeong et al., "Incorporation of machine learning and deep neural network approaches into a remote sensing-integrated crop model for the simulation of rice growth," *Sci. Rep.*, vol. 12, no. 1, pp. 1–10, 2022, doi: 10.1038/s41598-022-13232-y.

[16] M. A. Zurbarán, A. Salazar, M. A. Brovelli, and P. M. Wightman, "An evaluation framework for assessing the impact of location privacy on geospatial analysis," *IEEE Access*, vol. 8, pp. 158224–158236, 2020, doi: 10.1109/ACCESS.2020.3019631.

[17] L. Wang et al., "Transmission scheduling for privacy-optimal encryption against eavesdropping attacks on remote state estimation," *Automatica*, vol. 137, 2022, Art. no. 110145, doi: 10.1016/j.automatica.2021.110145.

[18] Y. Huang et al., "Blockchain-based continuous data integrity checking protocol with zero-knowledge privacy protection," *Digit. Commun. Netw.*, vol. 8, no. 5, pp. 604–613, 2022, doi: 10.1016/j.dcan.2022.04.017.

[19] M. Brahem et al., "Consent-driven data reuse in multi-tasking crowdsensing systems: A privacy-by-design solution," *Pervasive Mobile Comput.*, vol. 83, 2022, Art. no. 101614, doi: 10.1016/j.pmcj.2022.101614.

[20] A. Smahi et al., "A blockchainized privacy-preserving support vector machine classification on mobile crowd sensed data," *Pervasive Mobile Comput.*, vol. 66, 2020, Art. no. 101195, doi: 10.1016/j.pmcj.2020.101195.

[21] X. Ding et al., "Privacy-preserving task allocation for edge computing-based mobile crowdsensing," *Comput. Elect. Eng.*, vol. 97, 2022, Art. no. 107528, doi: 10.1016/j.compeleceng.2021.107528.

[22] A. S. Sani et al., "SPrivAD: A secure and privacy-preserving mutually dependent authentication and data access scheme for smart communities," *Comput. Secur.*, vol. 115, 2022, Art. no. 102610, doi: 10.1016/j.cose.2022.102610.

[23] M. Fakroon et al., "Secure remote anonymous user authentication scheme for smart home environment," *Internet Things*, vol. 9, 2020, Art. no. 100158, doi: 10.1016/j.iot.2020.100158.

[24] X. Ge et al., "Resilient and secure remote monitoring for a class of cyber-physical systems against attacks," *Inf. Sci.*, vol. 512, pp. 1592–1605, 2020, doi: 10.1016/j.ins.2019.10.057.

[25] X. Hu et al., "Efficient sharing of privacy-preserving sensing data on consortium blockchain via group key agreement," *Comput. Commun.*, vol. 194, pp. 44–54, 2022, doi: 10.1016/j.comcom.2022.07.035.

[26] M. Zhou et al., "Efficient and privacy-preserving range-max query in fog-based agricultural IoT," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 4, pp. 2156–2170, 2021, doi: 10.1007/s12083-021-01179-2.

[27] Q. Xie et al., "A secure and privacy-preserving authentication protocol for wireless sensor networks in smart city," *EURASIP J. Wireless Commun. Netw.*, vol. 2021, pp. 1–17, 2021, doi: 10.1186/s13638-021-02000-7.

[28] I. S. Popa et al., "Mobile participatory sensing with strong privacy guarantees using secure probes," *Geoinformatica*, vol. 25, no. 3, pp. 533–580, 2021, doi: 10.1007/s10707-019-00389-4.

[29] Daily Climate Time Series Data. Accessed: Nov. 1, 2019. [Online]. Available: https://www.kaggle.com/datasets/sumanthvrao/daily-climate-time-series-data

[30] Climate Data Online. Accessed: Mar. 24, 2023, [Online]. Available: https://www.ncei.noaa.gov/cdo-web/

Fahad Algarni received the bachelor's (First Class Hons.) degree in computer sciences from the Department of Computer Science, King Abdul-Aziz University, Jeddah, Saudi Arabia, in 2004, the master's degree in information technology (computer networks) from La Trobe University, Melbourne, VIC, Australia, in 2009, and the Ph.D. degree in information technology from the Clayton School of Information Technology, Monash University, Melbourne, VIC, Australia, in 2015.

He is currently the Dean of the College of Computing and Information Technology, University of Bisha, Bisha, Saudi Arabia. His research interests include wireless sensor networks, cloud computing, systems' reliability, Internet of Things, and cybersecurity.

Mohammad Ayoub Khan (Senior Member, IEEE) received the master of technology degree in computer science and engineering from Guru Gobind Singh Indraprastha, New Delhi, India, in 2005, and the Ph.D. degree in electrical engineering from Jamia Millia Islamia, New Delhi, India, in 2012.

He worked with many leading organizations, like the Ministry of IT and Communications, India, and Sharda University. He is currently an Associate Professor with the University of Bisha, Bisha, Saudi Arabia.

Wedad Alawad received the B.Sc. degree in computer science from Qassim University, Buraydah, Saudi Arabia, in 2008, the M.Sc. degree in computer science from Bowling Green State University, Bowling Green, OH, USA, in 2014, and the Ph.D. degree in computer science from Oakland University, Rochester, MI, USA, in 2018.

She is currently an Assistant Professor of computer science with Qassim University. Her research interests include artificial intelligence, cyber security, Internet of Things, and cloud computing.

Nadhir Ben Halima received the B.Sc. degree in computer engineering from the National School of Computer Sciences (ENSI), Manouba, Tunisia, in 2005, the M.Sc. degree in communication networks engineering from the Sant'Anna School of Advanced Studies, Pisa, Italy, in 2006, and the Ph.D. degree in information and communication technologies from the University of Trento, Trento, Italy, in 2009.

In 2009, he was a Visiting Researcher with the Department of Electrical and Computer Engineering, North Carolina State University, Raleigh, NC, USA. He is an Associate Professor with the Community College of Qatar, Doha, Qatar, and a Cybersecurity and Networking Expert. He is an educational leader and consultant with more than 15 years of experience in higher education.