C-NEST: cloudlet based privacy preserving multidimensional data stream approach for healthcare electronics.

SRIVASTAVA, G., MEKALA, M.S., HAJAR, M.S. and KALUTARAGE, H.

2024

C-NEST: Cloudlet based Privacy Preserving Multidimensional Data Stream Approach for Healthcare Electronics

Gautam Srivastava, M S Mekala, Muhammad Shadi Hajar, Harsha Kalutarage

***Abstract*—The Medical Internet of Things (MIoT) facilitates extensive connections between cyber and physical "things" allowing for effective data fusion and remote patient diagnosis and monitoring. However, there is a risk of incorrect diagnosis when data is tampered with from the cloud or a hospital due to third-party storage services. Most of the existing systems use an owner-centric data integrity verification mechanism, which is not computationally feasible for lightweight wearable-sensor systems because of limited computing capacity and privacy leakage issues. In this regard, we design a 2-step Privacy-Preserving Multidimensional Data Stream (PPMDS) approach based on a cloudlet framework with an Uncertain Data-integrity Optimization (UDO) model and Sparse-Centric SVM (SCS) model. The UDO model enhances health data security with an adaptive cryptosystem called Cloudlet- Nonsquare Encryption Secret Transmission (C-NEST) strategy by avoiding medical disputes during data streaming based on novel signature and key generation strategies. The SCS model effectively classifies incoming queries for easy access to data by solving scalability issues. The cloudlet server measures data integrity and authentication factors to optimize third-party verification burden and computational cost. The simulation outcomes show that the proposed system optimizes average data leakage error rate by 27%, query response time and average data transmission time are reduced by 31%, and average communication-computation cost are reduced by 61% when measured against state-of-the-art approaches.**

***Index Terms*—Cloudlet, C-NEST, UDO model, data-integrity measurement index, SCS model.**

I. Introduction

THE cloud-integration of Internet of Things (IoT) frameworks has become an essential paradigm in cyberspace, enabling seamless connections between healthcare systems. The convergence of wireless technology advancements and statistical machine learning (ML) has extended the exponential growth of medical IoT data analysis within cloud-based healthcare centers which is an Industry 5.0 emerging challenge [1]. Healthcare professionals utilize electronic health records (EHR) to facilitate patient-centric healthcare services. However, the storage of patient data in third-party cloud computing services and personal devices raises security concerns due to its sensitivity. In response to these challenges, innovative technologies such as Artificial Intelligence (AI)-driven software-defined networks (SDN), fog computing, statistical machine learning, and blockchain have been introduced in the past few years to fortify Industry 4.0 [2], [3], [4]. Now, as we transition towards Industry 5.0, there is a need to adapt and apply these advancements to realize healthcare case studies. This includes the implementation of virtual care, intelligent healthcare decision-making, and remote monitoring using wearable sensors to enhance the efficiency of healthcare electronic business operations, ensuring consistency throughout the entire value chain.

The integration of Cloudlet within the MIoT (Medical Internet of Things) paradigm coupled with automated decision-making systems enables efficient remote monitoring and control of patient diagnosis, as discussed in [5], [6]. MIoT frameworks are resource-limited because they typically include battery-powered devices with limited network lifetime and constrained computational resources. For instance, some wearable biomedical sensors, such as the Sphygmomanometer, Blood oxygen (SPO2) sensors, and Electromyography (EMG) as well as Electrocardiogram (ECG) devices/sensors are enabled with batteries but cannot compute and analyze data for optimal clinical decision-making. However, modern wireless telecommunication is not restricted to computer networks but also can be used to integrate consumer electronics through global Internet access. As consumer electronics become more interconnected, IoT continues to expand, particularly in the healthcare domain, where wearable health tracking solutions are becoming increasingly popular [5], [7], [8]. For instance, in 2019, 463 million people were affected by diabetes [9] which has prompted healthcare companies to innovate their diagnostic devices due to the high prevalence of this chronic disease. Over the past five years, wearable Continuous Glucose Monitors (CGM) have replaced traditional finger stick blood glucose measurement as the preferred diagnostic device. Moreover, healthcare social frameworks like PatientsLikeMe[1] collect and share patient's sensitive data over networks, which have the potential to be leaked or stolen, leading to privacy issues [10]. Therefore, maintaining consistent privacy protection has become a challenging endevour due to the ever changing landscape of the ntersection between consumer electronics and healthcare.

The advances of Cloudlets allow for storing large

Gautam Srivastava is with the Dept. of Math and Computer Science, Brandon University, Brandon R7A 6A9, Canada, and the Research Centre for Interneural Computing, China Medical University, Taichung 40402, Taiwan as well as Dept. of Computer Science and Math, Lebanese American University, Beirut 1102, Lebanon (email: srivastavag@brandonu.ca).

M S Mekala, Muhammad Shadi Hajar, and Harsha Kalutarage are with School of Computing, Robert Gordon University, Garthdee Road, Aberdeen, AB10 7QB, Scotland, UK (E-mail: ms.mekala@rgu.ac.uk, s.hajar@rgu.ac.uk, & h.kalutarage@rgu.ac.uk).

Corresponding Author: Gautam Srivastava

[1]https://www.patientslikeme.com/

amounts of data and facilitates intensive computation services. Cloudlets serve as an intermediary between IoT and end-users while also enabling clinical decisions based on medical data analysis at Cloudlets/IoT-Hubs rather than sending data directly to the cloud [11], [12]. This mechanism decreases latency and improves system reliability and performance. IMoT data is transmitted through access points and IoT-Hubs to carry out initial processes at a Cloudlet to make clinical decisions, which are shared with end-users and medical professionals, as shown in Fig. 1. However, Cloud-based IoT healthcare frameworks have the following fundamental challenges:

1) Protecting data while sharing to a Cloudlet to avoid data leakage and/or data theft issues.
2) IMoT data that is stored at third-party servers may lead to the disclosure of sensitive information without user consent [13], [14]. .

Motivation: The use of Cloudlets facilitates robust computing and data storage services near the data generation point, significantly reducing third party involvement in data authentication and transmission. In this regard, we design a secure key exchange mechanism called Cloudlet-Novel Encryption Secret Transmission (C-NEST). The Cloudlet forwards encrypted data to the server, where data is decrypted using a secret key before sharing the data with doctors and end-users. In most cases, data integrity verification is required, where end-users send a request to a Cloudlet for effective integration, which is time-consuming. Therefore, public-key infrastructure management is omitted in our proposed system to achieve low latency. Based on our knowledge, this proposed method is a reliable and effective privacy solution based on Cloudlets.

Our approach incorporates a User Defined Object (UDO) to enhance health data security by avoiding medical disputes during data streams. Subsequently, the Sparse-Centric Support Vector Machines (SCS) model design helps in classifying query results to simplify data access and solve scalability issues. Furthermore, the Cloudlet server measures data integrity and authentication to optimize third-party verification burden and computational cost. Our main contributions can be summarized as follows:

1) Design a 2-step privacy-preserving multidimensional data stream (PPMDS) approach based on a Cloudlet framework.
2) Develop a UDO model to enhance health data security with adaptive cryptosystem by avoiding medical disputes during data stream.
3) Develop a SCS model for effective classification of queries for easy access of data by solving scalability issues.
4) Develop a data integrity measurement method to optimize the third-party verification burden and computation cost.

The remainder of this article is structured as follows: Section II focuses on related work related to data integrity, quality-aware data searches, and multi-objective sensor data fusion. Section III describes the proposed PPMDS system and its functional methods, including UDO, C-NEST, and SCS. The algorithm's performance is discussed based on expewrimental evaluation results in Section IV, and the article concludes with Section V.

II. Related Work

The increased number of recent publications is evidence of the importance of privacy-preserving computation for multi-dimensional data.

A. Attribute-Aware Security Methods

An attribute-based encryption (ABE) method was developed to achieve fine-grained access control with privacy [15] instead of relying on a server-centric mechanism based on Bayesian theory [26], [27]. An attribute-based electronic health record (EHR) security system was developed in [28], [29]. Additionally, the data redundancy method has been developed in [16] to reduce the storage cost of the server and lower computational as well as communication costs. The CINEMA approach was developed based on secure permutation mechanisms for online health data privacy in [17]. This approach allows users to make query operations without decryption. However, service request execution demands inadequate computing and storage resources to achieve a reliable service rate. Here, three different issues of multidimensional data fusion are listed as follows:

1) Security issues of heterogeneous networks [18].
2) Authenticate crypto-model design issues for effective data transmission [30].
3) Network cost optimization by classifying the terminology of sensors (such as low-end and high-end sensors) [19].

Low-end sensors are often used to optimize network costs. In contrast, mobile sensors reduce the number of active sensors and optimize real-time data transmission costs, sensor coverage, and network congestion. However, the authors in [20] neglected to design a data search mechanism and concentrated on data transmission efficiency. As an extension of this work, a searchable encryption system was developed in [31], but the privacy preservation system is not up to the mark. The authors developed two searchable encryption systems but neglected data-sharing privacy services and substantial index generation methods. In [32], a defector tracking system was designed based on legal user authentication, and the white-box trace model was developed to assess the affinity among search attributes for identifying private keys. However, the system is only suitable for data sharing and does not focus on data searching privacy services. In [21], keyword search and data decryption schemes are developed, independent of any key integrity checks, which could potentially result in data leakage.

B. Data Integrity Models

Data integrity verification is essential in various fields of data research, particularly in the case of dynamic data [22], [33]. Some examples of dynamic data include social data, music, and movies, which are often stored on the cloud due to frequent changes in the data such as additions, modifications, or deletions. However, the major challenge in Cloudlet storage

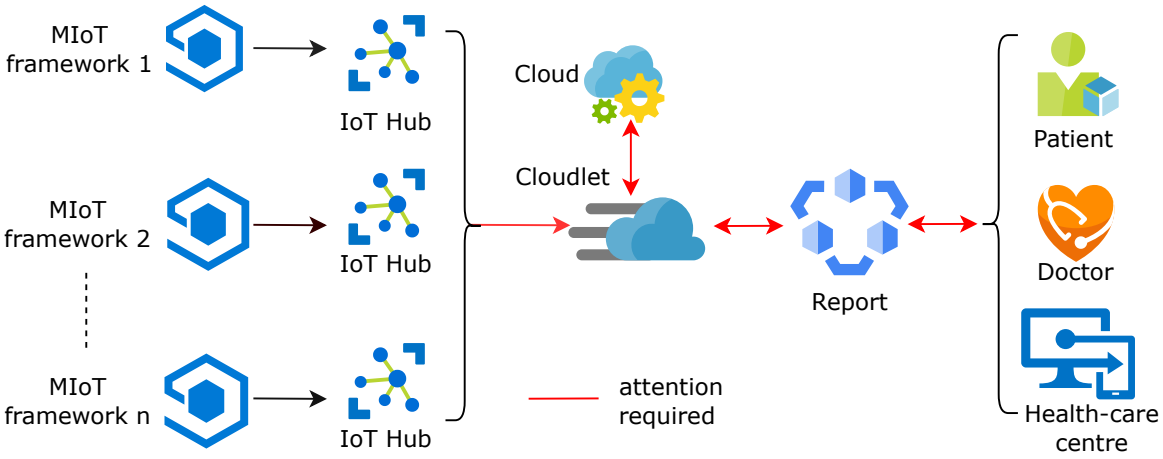


Fig. 1: Graphical problem illustration

TABLE I: Summary of related work

Work	Protection mechanisms			Privacy disclosure			Data Analytics		
	(methods)	(models)	(metrics)	(input)	(output)	(model)	(preparation)	(exploration)	(mining)
[15] to [16]	✓	✓	✓	✓	✗	✗	✓	✗	✗
[17]	✓	✗	✓	✓	✗	✗	✓	✗	✓
[18] to [19]	✗	✓	✓	✓	✗	✗	✓	✗	✓
[20] to [21]	✓	✓	✓	✓	✗	✗	✓	✓	✓
[22] & [23]	✓	✗	✓	✓	✗	✓	✓	✗	✓
[24]	✓	✗	✓	✗	✓	✓	✓	✗	✓
[25]	✓	✓	✗	✓	✗	✓	✓	✗	✓
Our work	✓	✓	✓	✓	✓	✓	✓	✓	✓

privacy includes authentication and authorization of data identity for secure transmission [34], data storage [35], as well as access control [36]. A such, there is a need to develop a novel data integrity verification scheme to enhance data privacy for cloud-assisted systems. During data integrity verification, a zero-knowledge proof strategy is employed to prevent third-party consideration while acquiring user data in [37]. It is crucial to hide user-sensitive information before sharing it in any environment. Data integrity verification mechanisms are vital assessing data damage. An extended dynamic data integrity verification method that uses a block-based signature policy and an identity-based cryptography system was described in [38]. Another method used was an integrity verification method based on attribute revocation functions, which uses a dual encryption-based Merkle hash function to optimize data privacy. However, the system's computational complexity was not adequately considered, making it unsuitable for IoT frameworks [23]. The SPPDA model [24] utilizes a bi-linear pairing scheme based on the Diffie–Hellman key mechanism to address data privacy and aggregation issues. However, the model inaccurately addresses data leakage issues. In [25], data was encrypted and shared with the edge server using the Equilibrium Point Analysis (EPA) model. Here, a public cloud center (PCC) accommodates a secure storage service for all aggregated data from an edge server, and a private key is used for data integrity and authentication. However, the computational complexity was not moderated and was shown to be not equivalent to traditional methods. We propose a PPMDS approach to address these issues to enable effective privacy preservation and data searching schemes, providing seamless access to IoT frameworks. A summary of the related work is given in Table I, while a the notation used in this paper is summarized in Table II.

III. Proposed Model

In this section, we theoretically formulate the proposed framework, which allows for the interconnection of IoT devices with a Cloudlet. We derive mathematical methods aimed at optimizing integrity and security.

Fig. 2 illustrates the fundamental mechanism of a two-step PPMDS approach based on Cloudlets. This approach comprises an UDO model and a SCS model. The deployment of Cloudlets, IoT-Hub, and wearable sensors enables medical data fusion services. IoT-Hub plays a crucial role in data authentication by generating a private key for each entity, which helps identify intruders and classify medical data for easy access. End-users or patients can access data from the Cloudlet using an authentication key generated by IoT-Hub. Usera receive ciphertext as search results, which can be converted into plaintext using a private authentication key. This procedure remains the same for all end-users. The Cloudlet stores patient data and provides easy access based on search operations by bringing cloud services close to the network's edge with secure computation and storage capacity.

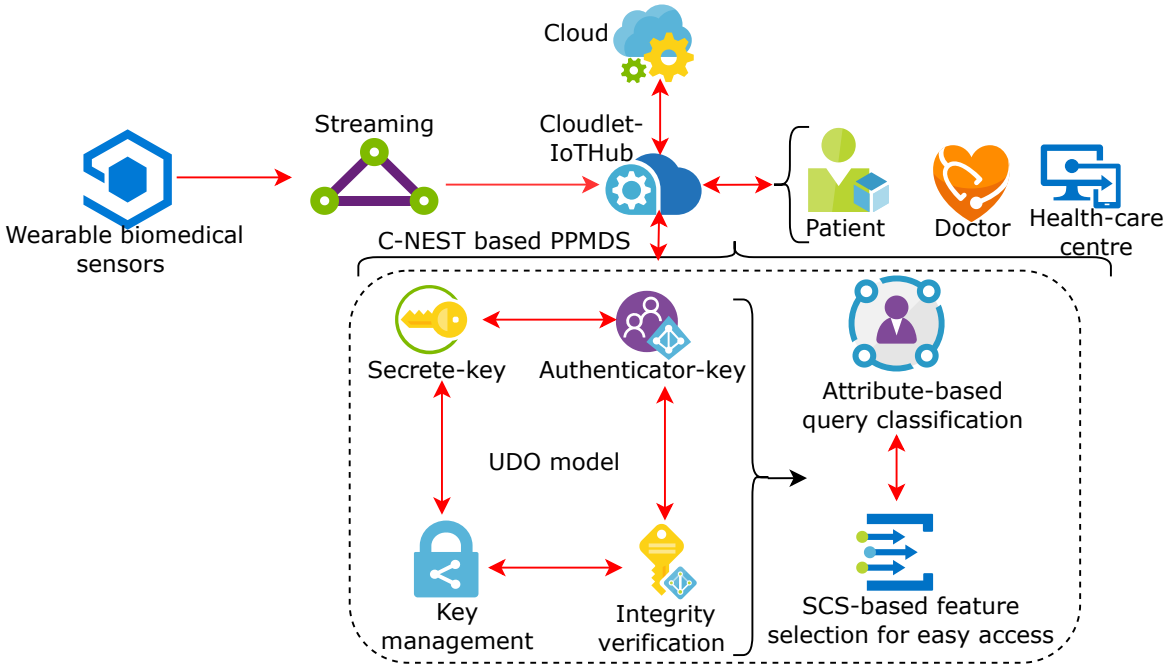


Fig. 2: PPMDA System Model

TABLE II: Notation table

Variable	Definition
E_{id}	Patient ID
Υ	Patient uncertain data-integrity
X	Valid and identical data of patient
$\overline{\text{X}}$	Invalid and non-identical data of patient
φ_t	Data authentication factor
ς_t	Signature for effective data processing
C_{id}	Cloudlet ID of patient record
C_{sk}	Cloudlet security key of the particular record
ϕ_C	secure key generator
ς_t	Non-singular covariance matrices
q_t	A sequence of each record data points or values
q_{t-i}	Data points or values at previous time steps
K	a fixed positive integer representing the number of previous time steps

A. PPMDS Functional-Flow

For the process of validating stored data, UDO $\Upsilon\left(E_{id}\right) \rightarrow \left(\text{X}, \overline{\text{X}}\right)$, involves cross-validation. Here, E_{id} represents the patient ID, Υ indicates uncertain data integrity, X indicates valid and identical data, while $\overline{\text{X}}$ indicates invalid and non-identical data. Typically, the Cloudlet sends a request to the server for data integrity verification, and the server shares a report based on the stored data with authenticators in response. The same request is verified by the Cloudlet when sent by an end-user. If the outcome is X, then the stored data is secure, whereas if it is not X, then the data has been tampered with. Where $\Delta_{t,o} \rightarrow (\varphi_t, \varsigma_t)$ helps classify data for easy access with adaptable security. $\Delta_{t,o}$ is the encrypted medical data fused at time t of the objective/parameter o, $\nabla_{t,o}$ is the decrypted medical data fused at time t of the objective/parameter o, φ_t is data authentication, and ς_t is a signature for effective data processing. The Key-Management process $(E_{id}) \rightarrow (E_{sk}, \phi)$ is responsible for providing secure communication using the Nonsquare Encryption Secure Transmission (NEST) protocol, influenced by Diffie-Hellman. Here, E_{id} represents the patient ID, E_{sk} represents the patient security key and ϕ represents a private key. The Key-Generation model $(E_{sk}, C_{id}) \rightarrow (E_{sk}, C_{sk}, \phi_C)$ generates secure keys for effective privacy preservation. C_{id}, C_{sk}, ϕ_C represent the Cloudlet ID, cloudlet security key, and secure key generator, respectively. These keys enable easy access to medical data with data authenticators.

B. UDO Model based on C-NEST

Algorithm 1: Key Management

1 [t]
input : $E_{id}, E_{sk}, C_{pk}, \phi$
output: Secure key generation ϕ_C
2 Initialize $E_{sk} \neq 0, C_{pk} \neq 0, \phi \neq 0$;
3 **for** *each i= 1 to* E_i^{id} **do**
4 Generation of new keys E_{sk}, C_{sk};
5 **for** *each i= 1 to* ϕ_n **do**
6 Compute Encryption $\alpha_{ij} = \left\{E_j^{id}, h_i, \alpha\left\{E_j^{pk}, \left(C_i, E_j^{id}\right)\right\}\right\}$;
7 Estimate Signature $\sigma_i = Sign\left(E_{sk}, \hbar\left(E_{id}, t, \alpha_{ij}\right)\right)$;
8 **end**
9 **end**

The key generation process for each patient and Cloudlet is managed by Algorithm 1. Line 1 initializes the parameters

such as patient secret key, cloudlet public key, and private key generated by the data authenticator, which is not equal to zero. Lines 2-6 assess the key for each patient and doctor for encryption and signature generation processes.

Algorithm 2: Data security

input : $E_{pk}, C_{pk}, IoT_{data}$
output: Secure data communication
1 Initialize $C_{pk} \neq 0, IoT_{data} \neq 0$;
2 **for** *each t= 1 to T* **do**
3 Estimate $\alpha_{data} = Enc\left(\phi_C, data\right)$;
4 Measure signature;
5 $\sigma_i = Sign\left(E_{sk}, \hbar\left(E_{id}, t, \alpha_{ij}\right)\right)$;
6 Hash function $h_i = \hbar\left(E_{id}, t, \alpha_{ij}, \sigma_i\right)$;
7 Complete hash at end level $h_i^{com} = \{E_{id}, t, \alpha_{ij}, \sigma_i, h_i\}$;
8 **end**

Algorithm 2 ensures security of data during its transfer to the cloud for storage purposes. The initialization of the necessary parameters takes place on Line 1, while Lines 2-7 evaluates the complete encryption of the data using both encryption and signature models, based on the patient ID and the IoT-Hub data authenticator generated key.

Algorithm 3: UDO Model

input : $C_{id}, \partial_E, \partial_c$
output: Integrity verification status
1 Let us initialize $C_{id} \neq 0, a_i \neq 0, b_i \neq 0, h_i \neq 0, \chi_o \neq 0, \varphi_i \neq 0, \eta_o \neq 0, \Upsilon_C = (n, \phi_i, \phi_{i+1})$;
2 **for** *each i= 1 to* DI_n **do**
3 Measure $a_i = \ell_{\phi_i}, \quad b_i = f\left(\phi_{i+1}\right)$; # key attributes
4 Estimate $\varphi = \prod_{i=1}^{DI_n} \varphi_{a_i}^{b_i}$;
5 Estimate hash function for data $\eta_o = \sum_{i=1}^{DI_n} b_i \times \Delta_{t,o} \;\; o \in (\{1, 2, \ldots, O\})$;
6 **if** *Sing is valid* **then**
7 Estimate a_i, b_i, h_i, χ_o;
8 $h_i = h_{i+1}\left(a_i, O, E_{sk}\right)$; ; $\chi_o = h_{i+1}\left(T, o, E_{sk}\right)$;
9 $\Upsilon_C\left(\varphi, \sigma\right) = \left(\prod_{i=1}^{DI_n} h_i^{b_i} \times \prod_{o=1}^{O} \chi_o^{\eta_o}, Sign\right)$;
10 **else**
11 The data is tampered with.
12 **end**
13 **end**

Algorithm 3 is designed to verify the integrity of medical data for each patient. In Line 1, the necessary parameters are initialized, while Line 2 measures the key attributes required for generating the authenticator key, along with Line 4. Storage data is encrypted in Line 5. Lines 6-9 are responsible for verifying data integrity when the signature is valid. If the signature is found to be invalid, it can be inferred that the stored data has been tampered with.

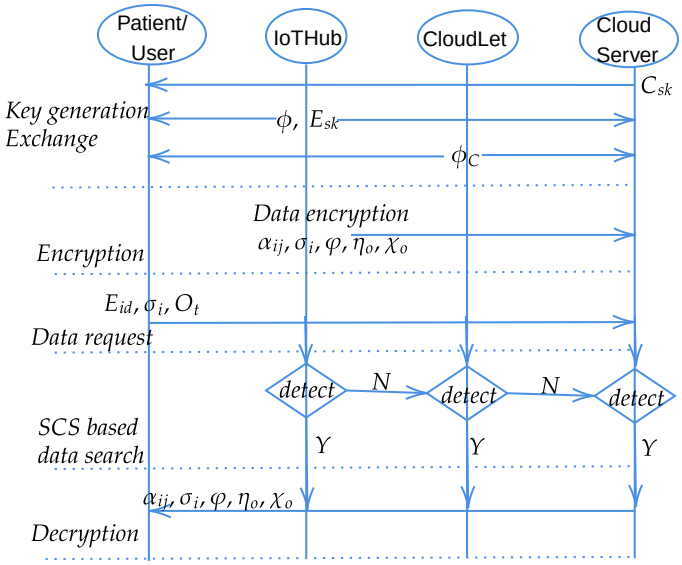


Fig. 3: SCS-based Data Access Model

1) Signature Generation: The PPMDS approach generates a public-key $\left(\delta, \phi_{\sigma_i}^{pk}, P\right)$, where δ is the general public-key, ${\sigma_i}^{pk}$ is the signature public-key, and P is a random prime number. Additionally, it generates a private-key $\left(\phi_{\sigma_i}^{sk}, P\right)$, where ${\sigma_i}^{sk}$ is the signature private-key for C-NEST. The signature keys are formulated as follows: $\phi_{\sigma_i}^{sk} = -e^2 \bmod P$ and $\phi_{\sigma_i}^{pk} = -2e^2 \log, (\bmod P)$. The encrypted signature is also formulated in the approach.

$$\begin{aligned} &\nabla = \Delta p^{\left(\delta + \phi_{\sigma_i}^{pk}\right)} \bmod P, \\ &where\ 1 \leq p \leq P, \ \& \ \gcd\left(p, P\right) = 1 \end{aligned} \tag{1}$$

The signature for the IoT data is as follows

$$\sigma_{\Delta_{t,o}} = \nabla^{\phi_{\sigma_i}^{sk}} \bmod P \tag{2}$$

2) Signature Verification: A valid signature is as follows

$$\overline{\sigma_{\Delta_{t,o}}} = \sigma_{\Delta_{t,o}} \bmod P \tag{3}$$

Substitute Eq. 1 and 2 in Eq. 3, then

$$\begin{aligned} &\overline{\sigma_{\Delta_{t,o}}} = \sigma_{\Delta_{t,o}} \bmod P \\ &= \nabla^{\phi_{\sigma_i}^{sk}} \bmod P \\ &= \left(\Delta p^{\left(\delta + \phi_{\sigma_i}^{pk}\right)}\right)^{\phi_{\sigma_i}^{sk}} \bmod P \\ &= \left(\Delta^{\phi_{\sigma_i}^{sk}} p^{\left(\delta + \phi_{\sigma_i}^{pk} + \phi_{\sigma_i}^{sk}\right)}\right) \bmod P, \\ &\therefore \ \delta + \phi_{\sigma_i}^{pk} + \phi_{\sigma_i}^{sk} = 1, \ \&p.p^{-1} = 1 \\ &\overline{\sigma_{\Delta_{t,o}}} = \Delta^{\phi_{\sigma_i}^{sk}} \bmod P \\ &\overline{\sigma_{\Delta_{t,o}}} = \widehat{\sigma_{\Delta_{t,o}}} \bmod P \end{aligned} \tag{4}$$

If Δ is equal to ∇, then the IoT medical data is considered valid and not tampered with. Otherwise, the data is deemed tampered with.

Theorem 1: Let's assume, the cloudlet verifies the integrity of the data based on user demand, with $\Upsilon_C\left(\varphi, \sigma\right) = \left(\prod_{i=1}^{DI_n} h_i^{b_i} \times \prod_{o=1}^{O} \chi_o^{\eta_o}, Sign_t\right)$

Proof: The signature encryption, hash function, and data

authentication remain used to assess the data integrity and it follows

$$\Upsilon_C(\varphi,\sigma) = \left(\prod_{i=1}^{DI_n} \varphi_{a_i}^{b_i}, \Delta^{\phi_{\sigma_i}^{sk}} \bmod P\right)$$

$$= \left(\prod_{i=1}^{DI_n} h_i^{b_i}, \left(\Delta p^{\left(\delta+\phi_{\sigma_i}^{sk}\right)}\right)^{\phi_{\sigma_i}^{sk}} \bmod P\right)$$

$$= \left(\prod_{i=1}^{DI_n} \left(h_{i+1}\left(a_i, O, E_{sk}\right)\right)_i^{b_i}, \left(\Delta^{\phi_{\sigma_i}^{sk}} \cdot p^{\left(\delta+\phi_{\sigma_i}^{sk}\right)^{\phi_{\sigma_i}^{sk}}}\right) \bmod P\right)$$

$$= \left(\prod_{i=1}^{DI_n} h_i^{b_i} \times \prod_{o=1}^{O} \chi_o^{\sum_{i=1}^{DI_n} b_i \times \Delta_{t,o}}, \left(\Delta^{\phi_{\sigma_i}^{sk}} \cdot p^{\left(\delta+\phi_{\sigma_i}^{sk}\right)} \cdot p^{\phi_{\sigma_i}^{sk}}\right) \bmod P\right)$$

$$= \left(\prod_{i=1}^{DI_n} h_i^{b_i} \times \prod_{o=1}^{O} \chi_o^{\sum_{i=1}^{DI_n} b_i \times \Delta_{t,o}}, \left(\Delta^{\phi_{\sigma_i}^{sk}} \cdot p^{\left(\delta+\phi_{\sigma_i}^{sk}+\phi_{\sigma_i}^{sk}\right)}\right) \bmod P\right)$$

$$= \left(\prod_{i=1}^{DI_n} h_i^{b_i} \times \prod_{o=1}^{O} \chi_o^{\eta_o}, \left(\Delta \cdot p^{\left(\delta+\phi_{\sigma_i}^{sk}\right)}\right) \bmod P\right)$$

As per equation 1, it formulates as follows

$$= \left(\prod_{i=1}^{DI_n} h_i^{b_i} \times \prod_{o=1}^{O} \chi_o^{\eta_o}, \nabla^{\phi_{\sigma_i}^{sk}} \bmod P\right)$$

$$\Upsilon_C(\varphi,\sigma) = \left(\prod_{i=1}^{DI_n} h_i^{b_i} \times \prod_{o=1}^{O} \chi_o^{\eta_o}, Sign_t\right)$$

C. Data Storage Model

The decision of where to store sensed data is evaluated by Algorithm 4, which offers three storage options based on the concerned device's capacity: store at a neighbouring IoT-Hub, Cloudlet, or Cloud server. Line 1 initializes the parameters, including patient ID, old-entry set, storage array, sensed data, and device capacity. Note that we have not focused on estimating device capacity, as it is beyond the scope of this manuscript. Line 2 uses security models discussed previously to determine where data should be stored. Algorithm 4 utilizes a time series to estimate the entire process, as shown in Line 4. If the patient ID and old-entry data are identical, Line 6 cross-checks for the threshold value ($\aleph_\kappa$), then changes it and sends a notification message if necessary. Otherwise, the new arrival encrypted data is updated. Lines 7-20 check for unusual measurements and send an alert notification accordingly.

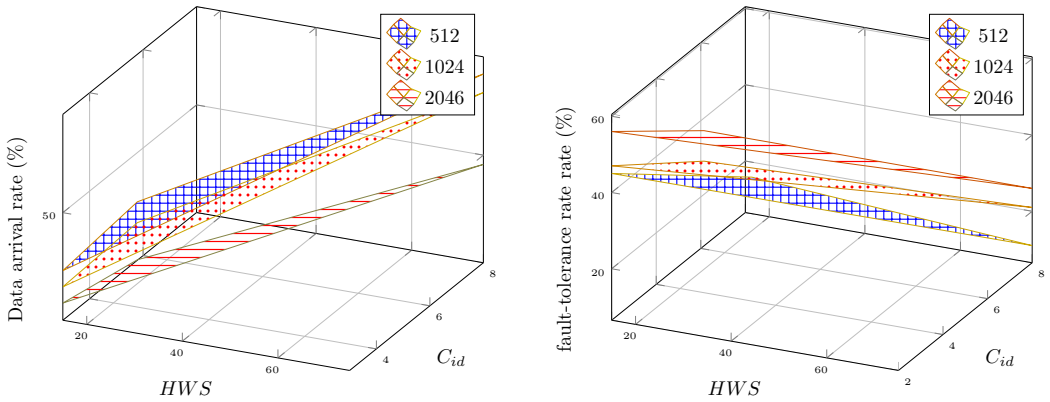
1) SCS-based Data Access Model: In Fig. 3, the data access mechanism based on the SCS model is shown. The key-generation and exchange process involves generating and communicating the key through the C-NEST protocol. At the same time, the data authenticator shares the key with the patient, Cloudlet, and server. To enhance privacy preservation, encryption estimates the encryption of all data stored and shared with the Cloudlet or server. Our research objective is achieved through the Support Vector Machine (SVM)-based SCS model, which facilitates easy access to data based on user requests. The SCS model classifies requests or queries to locate storage (in IoT-Hub, Cloudlet, or server) and, if identified, initiates the decryption process to share data as per user or device request.

Algorithm 4: Device/Server Data Storage

```
1  [!ht]
input : E_id, Old-entry set ε_id[i], Storage array ϖ[i], Fused data
        set κ[i]
output: Data change analysis
2  Initialize threshold-value of objective ℵ_κ ≠ 0, E_id ≠ 0,
   ε_id[i] ≠ 0, ϖ[i] = 0, κ[i] ≠ 0, threshold storage capacity
   ℵ_Θ ≠ 0, storage capacity Θ_t ≠ 0;
3  if Θ_t ≤ ℵ_Θ then
4      while E_id ≠ 0 do
5          for each t= 1 to T do
6              Update κ[i] ← κ[i + 1];
7              if E_id ≡ ε_id then
8                  if κ[i] ≡ κ[i + 1] then
9                      Store data ϖ[i] ≡ κ[i];
10                     if κ_t ≤ ℵ_κ then
11                         update the fused data with privacy;
12                     else
13                         Alert message to the doctor;
14                     end
15                 else
16                     Store data ϖ[i] ≡ κ[i + 1];
17                     Update κ[i] ← κ[i + 1];
18                 end
19             else
20                 Store data ϖ[i] ≡ κ[i];
21                 if κ_t ≤ ℵ_κ then
22                     update the fused data with privacy;
23                 else
24                     Alert message to the doctor;
25                 end
26             end
27         end
28     end
29 else
30     The offloading mechanism will trigger the selection of a
       suitable device (IoT-Hub) or Cloudlet for storing data;
       otherwise, storing data in the cloud.
31 end
```

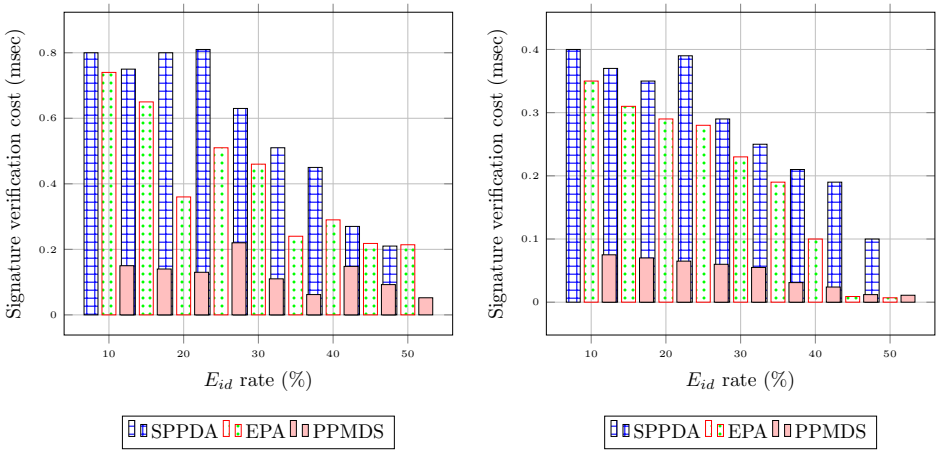
D. Data Streaming Model

Let $\mathbb{Z}$ be the set of k-dimensional coefficient matrices, and let ς_t be a sequence of non-singular covariance matrices. The expression $q_t = \sum_{i=1}^{K} \mathbb{Z}i \times q_{t-i} + \varsigma_t$ refers to the set of influenced data points that are to be streamed to the device or server for storage, to reduce the communication-computation overhead on the server. Algorithm 5 facilitates the streaming of multidimensional data. In Line 1, patient ID, stored information, and fused data are initialized. Line 2 evaluates the data points to effectively reduce their size and optimize the communication overhead. Line 4 and Line 5 determine the subset of points from the IoT data that should be equal by definition, and the threshold distance of points d plays an important role in clustering the subset points, as can be observed in Line 6. Line 7 calculates the model matrix for streaming data according to the sensor objective, while Line 8 maintains the individual j^{th} objective data with column vectors, as follows: $\varpi = \left[\varpi^1, \varpi^1, \ldots, \varpi^j\right]$.



(a) Data fusion analysis (b) Decryption fault-tolerance rate

Fig. 4: Data fusion and fault-tolerance analysis with different sizes



(a) $C_{id} = 4$ (b) $C_{id} = 7$

Fig. 5: Signature verification cost when cloud-lets count is 4 & 7

E. Complexity analysis

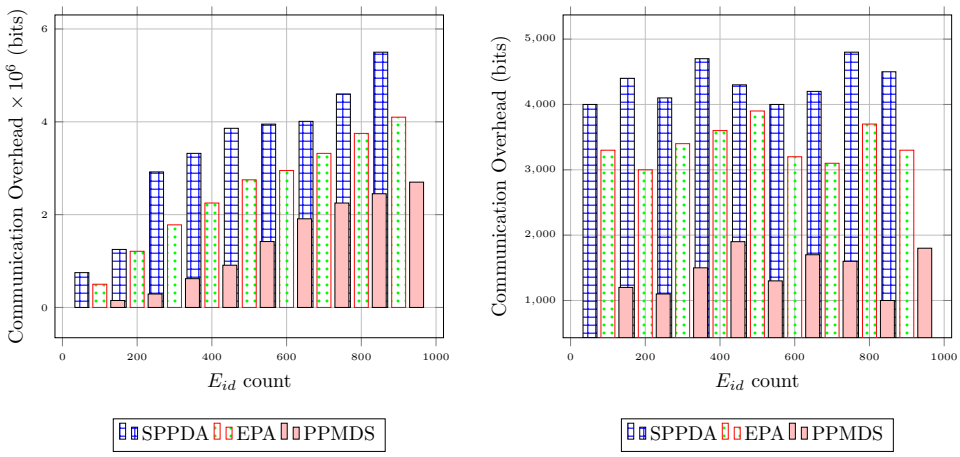
Assuming we split all four algorithms into three sub-modules. First, the complexity of calculating key generation and the signature function for each patient record is in $\mathcal{O}(n^2)$. The complexity of sorting the uncertain data integrity of all records is in $\mathcal{O}(n \log n)$. Finally, the complexity of content-storage update and change analysis at each request is $\mathcal{O}(n^3)$. The overall complexity can be expressed as the sum of the complexities of the three sub-modules:

$$\mathcal{O}\left(n^2\right) + \mathcal{O}\left(n\log_2 n\right) + \mathcal{O}\left(n^3\right) \tag{5}$$

IV. Experimental Analysis

For experimentation, both the Raspberry Pi-4 Model-B Board and a Personal Computer (PC) were used. The PC used 64-bit UBUNTU 18.04.5 LTS on an Intel Core i7-10700 CPU @ 3.80GHz with 16 cores, NVIDIA GeForce RTX3090, and 64 GB RAM. The Raspberry Pi used Ubuntu MATE 16.04 on an ARMv7 Processor rev (v7l) CPU with 4 cores, a maximum clock speed of 600 MHz, and 128 MB RAM. The Pis were utilized for aggregating data from sensors, and the PBC and GMP libraries, along with a C++ program, were employed for cryptographic operations. File sizes of 512-bit or 1024-bit and a communication distance of 50 meters with a communication speed of 2 Mbps were considered between IoTHub and Cloudlet. The data packet density was taken into account to evaluate the bandwidth rate, with each packet being 24 Kb in size.

We have examined two benchmark models, namely EPA [25] and Secure Privacy-Preserving Data Aggregation (SPPDA) [24]. The EPA model, based on the Boneh–Goh–Nissim cryptosystem, ensures data authenticity and integrity, as well as estimates communication costs and emphasizes data aggregation in the context of mobile edge computing (MEC). EPA employs a single key mechanism tailored for lightweight networks, where data is encrypted and shared with the edge server using a private key. The public cloud center (PCC) stores all aggregated data from the edge server, and a private key is utilized for data integrity and authentication. The second benchmark model, SPPDA, introduces an innovative signature scheme to enhance authenticity and integrity of aggregated data. SPPDA relies on the bi-linear Diffie–Hellman assumption



(a) WS-to-CL overhead. (b) CL-to-CS

Fig. 6: Communication overhead comparison

Algorithm 5: Data Streaming to Cloudlet for storage

[!ht]
input : E_{id}, $\Delta_{t,o}$, $\kappa[i]$
output: Streaming data tampering analysis
Let initialize $E_{id} \neq 0$, $\Delta_{t,o} \neq 0$, $\kappa[i] \neq 0$;
Measure IoT-data points for effective compression as follows
$q_t = \sum_{i=1}^{K} \mathbb{Z}_i \times q_{t-i} + \varsigma_t$;
for $each\, t = 1\, to\, T$ **do**
  Estimate the Influence Points of j^{th} IoT-data for effective data compression with low-data size as follows;
  $p^{j}_{ip,t} = \left\{ D_t\left(o_j\right) \geqslant d^2 \right\},\ \therefore p_{ip} \subseteq \mathbb{Q}$;
  Distance-based data clustering is as follows
  $D_t\left(o_j\right) = \widehat{q}_t \mathbb{Q} q_t$;
  $\mathbb{Q} = \sum_{t} \left(\widehat{q}_t q_t\right)^{-1}$;
  The estimation of the model matrix for streaming data is as follows $\varpi_t^{o_j} = \arg\min_{\varpi} \sum_{D_t\left(o_j\right)} \|q_t - \widehat{q}_t \varpi\|^2$;
  Each objective sensor data stream to stored as a block matrix with column vectors as follows
  $\varpi = \left[\varpi^1, \varpi^1, \ldots, \varpi^j\right]$;
end

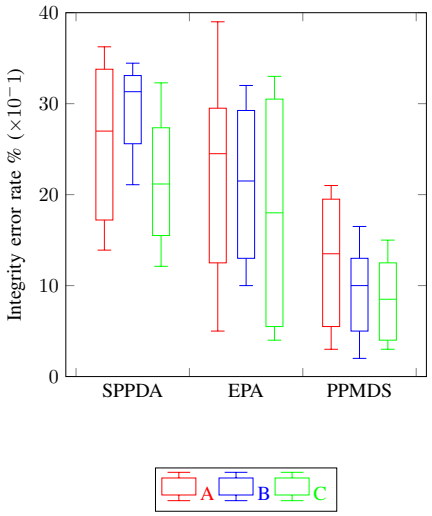


Fig. 7: Integrity error rate comparative analysis, where A, B and C refer to the device, cloudlet and server, respectively

to upscale data confidentiality, authenticity, and privacy. The primary focus of SPPDA is to minimize communication, transmission, and computational costs associated with remote servers to meet the requirements of lightweight networks.

In developing a script for a Cloudlet-integrated IoT-Hub, we assumed 8 Cloudlet instances to handle 10 distinct IoT frameworks, each associated with various data sizes originating from 10 wearable sensors. During simulations, we allocated one instance for each framework that allows to management of ten sensors. Data fusion and fault-tolerance of comparative decryption analysis are depicted in Fig. 4. The data fusion mechanism plays a vital role in the process of streaming multidimensional data to enhance privacy preservation of the data stream. The file size has a significant impact on data fusion and storage rates during encryption and signature generation. In our simulations, an average of $C_{id} = 8$ Cloudlets and an average of 79 human-wearable sensors were considered to evaluate the data fusion rate, as shown in Fig. 4(a).

Increasing the number of Cloudlets significantly increases the data fusion rate, even when sensor count is low. During data storage, the authenticator generates private keys for each sensing unit to enhance data privacy. The decryption time is a crucial metric for assessing and optimizing communication and computational overhead of devices and it is affected by the average C_{id} count when accessing data. The Privacy-Preserving Multidimensional Data Stream (PPMDS) approach, which is based on the C-NEST mechanism and SCS model, and streamlined with the UDO model, has a lower fault-tolerance rate during decryption for all file sizes. However, the fault-tolerance rate is higher for a file size of 2046 bits compared to 512 bits, as shown in Fig. 4(b).

The cost of signature verification is a crucial performance

TABLE III: Signature verification cost

	Resource usage		Execution time per message set [ms]		
Model	Computation cost	Communication cost [bits]	30	50	70
PPMDS	$\Upsilon(\varphi,\eta_o)+(2\Lambda+1)\,\Upsilon_{\mathbb{Z}}+2\Lambda\Upsilon_A$	$\leqslant 2000$	0.72	2.15	3.62
EPA [25]	$2\Upsilon(\varphi,\eta_o)+(3\Lambda+1)\,\Upsilon_{\mathbb{Z}}+\Lambda\Upsilon_A$	$\leqslant 3900$	9.63	9.95	11.31
SPPDA [24]	$(\Lambda+3)\,\Upsilon(\varphi,\eta_o)+(\Lambda+1)\,\Upsilon_A$	$\leqslant 4600$	6.1	10.2	12.25

metric for evaluating our proposed privacy approaches, as shown in Fig. 5. The number of potential Cloudlets affects signature generation cost, and our approach incurs lower costs than State-Of-The-Art (SOA) methods due to its innovative signature generation and verification techniques. Specifically, when accessing data from a Cloudlet or IoT-Hub at $E_{id}=45$, the approach has lower costs, as shown in Fig. 5(a), and it also incurs lower costs when $C_{id}=7$, as shown in Fig. 5(b).

Communication overhead between sensors, Cloudlets, and servers is illustrated in Fig. 6, while Fig. 6(a) specifically depicts the communication overhead between wearable sensors (WS) and Cloudlets, respectively. The PPMDS approach has a lower overhead rate compared to SOA approaches. However, as the number of medical records E_{id} increases, communication overhead is usually significantly increased due to limited computational resources of sensors. Therefore, sensed data is transferred to a Cloudlet with moderate computational and storage capacity. Fig. 6(b) shows the communication overhead between Cloudlet and server. This overhead does not frequently occur, but when the Cloudlet is not capable of processing data, a service offloading strategy is initiated. The average communication overheads for PPMDS, EPA, and SPPDA are $\leqslant$ 2000bits, $\leqslant 3900bits$, and $\leqslant$ 4600 bits, respectively. Nowadays, multi-edge computations can handle up to 8 GB of data storage and computation [39].

The error rate of proposed and existing approaches based on data processing location is presented in Fig. 7. The PPMDA approach exhibits a lower error rate than both SSPDA [24] and EPA [25] approaches at the server, Cloudlet, and IoT-Hub. This is due to the hierarchical independence of computational and storage capacities, where Server $\geqslant$ Cloudlet $\geqslant$ IoT-Hub. Additionally, the UDO model enhances health data security by utilizing an adaptive cryptosystem called C-NEST during the data stream, while the SCS model solves scalability issues in data access. These two models prevent third-party involvement in privacy preservation. Comparatively, the EPA approach has a moderate error rate compared to the SSPDA approach. Table III shows signature verification cost of proposed and SOA approaches. The pairing cost is $\Upsilon(\varphi,\eta_o)=15.79ms$, argumentation cost is $\Upsilon_A,=0.04ms$, exponential cost of $\mathbb{Q}t$ is $\Upsilon_e=1.31ms$, Λ is argumentation order of $\mathbb{Q}$ and exponential cost is $\Upsilon\mathbb{Z}=1.25ms$, respectively.

Impact of proposed model: By leveraging the UDO and SCS models, the PPMDS approach achieves appropriate data security and service reliability rates by effectively classifying service requests. The data integrity measurement model accurately measures and validates data authentication, and its lightweight functionality eliminates the need for third-party involvement during data integrity verification. The complete process of data service request classification is shown in Fig. 3. The signature generation and verification mechanisms are novel and generate public, private, and signed public keys to enhance privacy, primarily suited for Cyber Physical Systems (CPS) and IoT applications to ensure effective network maintenance. Before storing data on IoT devices, data is analyzed and mapped with existing data, and the processing capacity depends on device selection to optimize unauthorized access. The C-NEST protocol provides secure transmission between IoT devices and Cloudlet. In summary, the UDO model simplifies data integrity processes on IoT devices by identifying similar data and providing adequate security during storage based on the C-NEST communication strategy. The communication process begins for data storage only when received data is different from stored data.

V. Conclusion

The Cloudlet-based 2-step PPMDS approach, consisting of the UDO model and the SCS model, aims to optimize data privacy and reduce single-bottleneck issues. The UDO model utilizes an adaptive cryptosystem to optimize data security and reduce the medical dispute rate by 27%, using the Cloudlet-Nonsquare Encryption Secret Transmission (C-NEST) strategy during data streams. The SCS model effectively classifies query requests, with 89% accuracy, to enable easy data access and address scalability issues, as the UDO model reduces data redundancy rates. The Cloudlet measurement system reduces third-party verification burden and computational cost average by 44% and 61%, respectively. Experimental analysis results show that the proposed system outperforms State-Of-The-Art approaches, reducing average data leakage error rate by 27%, query response time, average data transmission time by 31%, and average communication-computational cost by 61%.

Future Work

Future work will focus on designing and developing optimized secure channel selection, trust estimation, and latency-constrained computation models based on offloading schemes. Additionally, a node selection strategy will be designed to improve multidimensional data access, as these are global challenges that drastically affect device and server communication as well as computational service costs.

References

[1] E. Mbunge, B. Muchemwa, J. Batani *et al.*, "Sensors and healthcare 5.0: transformative shift in virtual care through emerging digital health technologies," *Global Health Journal*, vol. 5, no. 4, pp. 169–177, 2021.

[2] J. Li and P. Carayon, "Health care 4.0: A vision for smart and connected health care," *IISE Transactions on Healthcare Systems Engineering*, vol. 11, no. 3, pp. 171–180, 2021.

[3] P. Bhattacharya, S. Tanwar, U. Bodkhe, S. Tyagi, and N. Kumar, "Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications," *IEEE transactions on network science and engineering*, vol. 8, no. 2, pp. 1242–1255, 2019.

[4] G. Muhammad, F. Alshehri, F. Karray, A. El Saddik, M. Alsulaiman, and T. H. Falk, "A comprehensive survey on multimodal medical signals fusion for smart healthcare systems," *Information Fusion*, vol. 76, pp. 355–375, 2021.

[5] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare internet of things: A survey of emerging technologies," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1121–1167, 2020.

[6] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," *IEEE Systems Journal*, vol. 11, no. 1, pp. 118–127, 2017.

[7] F. John Dian, R. Vahidnia, and A. Rahmati, "Wearables and the internet of things (iot), applications, opportunities, and challenges: A survey," *IEEE Access*, vol. 8, pp. 69 200–69 211, 2020.

[8] I. Psychoula, L. Chen, and O. Amft, "Privacy risk awareness in wearables and the internet of things," *IEEE Pervasive Computing*, vol. 19, no. 3, pp. 60–66, 2020.

[9] M. Al-Badri and O. Hamdy, "Diabetes clinic reinvented: will technology change the future of diabetes care?" *Therapeutic advances in endocrinology and metabolism*, vol. 12, p. 2042018821995368, 2021.

[10] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 1, pp. 222–233, 2014.

[11] M. Mekala, G. Srivastava, J. H. Park, and H.-Y. Jung, "An effective communication and computation model based on a hybridgraph-deeplearning approach for siot," *Digital Communications and Networks*, vol. 8, no. 6, pp. 900–910, 2022.

[12] J. Ding, X.-H. Hu, and V. Gudivada, "A machine learning based framework for verification and validation of massive scale image data," *IEEE Transactions on Big Data*, vol. 7, no. 2, pp. 451–467, 2021.

[13] C. Zhang, L. Zhu, C. Xu, K. Sharif, X. Du, and M. Guizani, "Lptd: Achieving lightweight and privacy-preserving truth discovery in ciot," *Future Generation Computer Systems*, vol. 90, pp. 175–184, 2019.

[14] D. Tosh, S. Shetty, X. Liang, C. Kamhoua, and L. L. Njilla, "Data provenance in the cloud: A blockchain-based approach," *IEEE consumer electronics magazine*, vol. 8, no. 4, pp. 38–44, 2019.

[15] Y. Zhang, D. Zheng, and R. H. Deng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

[16] Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, and X. Lin, "Healthdep: An efficient and secure deduplication scheme for cloud-assisted ehealth systems," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 4101–4112, 2018.

[17] J. Hua, H. Zhu, F. Wang, X. Liu, R. Lu, H. Li, and Y. Zhang, "Cinema: Efficient and privacy-preserving online medical primary diagnosis with skyline query," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1450–1461, 2018.

[18] X. Du and H.-H. Chen, "Security in wireless sensor networks," *IEEE Wireless Communications*, vol. 15, no. 4, pp. 60–66, 2008.

[19] J.-Y. Huang, I.-E. Liao, and H.-W. Tang, "A forward authentication key management scheme for heterogeneous sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2011, pp. 1–10, 2011.

[20] Z. Liu, T. Li, P. Li, C. Jia, and J. Li, "Verifiable searchable encryption with aggregate keys for data sharing system," *Future Generation Computer Systems*, vol. 78, pp. 778–788, 2018.

[21] J. Sun, D. Chen, N. Zhang, G. Xu, M. J. Tang, X. Nie, and M. Cao, "A privacy-aware and traceable fine-grained data delivery system in cloud-assisted healthcare iiot," *IEEE Internet of Things Journal*, 2021.

[22] H. Tian, Y. Chen, C.-C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu, "Dynamic-hash-table based public auditing for secure cloud storage," *IEEE Transactions on Services Computing*, vol. 10, no. 5, pp. 701–714, 2015.

[23] L.-Y. Yeh, P.-Y. Chiang, Y.-L. Tsai, and J.-L. Huang, "Cloud-based fine-grained health information access control framework for lightweightiot devices with dynamic auditing andattribute revocation," *IEEE transactions on cloud computing*, vol. 6, no. 2, pp. 532–544, 2015.

[24] A. Ara, M. Al-Rodhaan, Y. Tian, and A. Al-Dhelaan, "A secure privacy-preserving data aggregation scheme based on bilinear elgamal cryptosystem for remote health monitoring systems," *IEEE Access*, vol. 5, pp. 12 601–12 617, 2017.

[25] X. Li, S. Liu, F. Wu, S. Kumari, and J. J. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted iot applications," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4755–4763, 2018.

[26] W. He, Y. Liu, H. Yao, T. Mai, N. Zhang, and F. R. Yu, "Distributed variational bayes-based in-network security for the internet of things," *IEEE Internet of Things Journal*, vol. 8, no. 8, pp. 6293–6304, 2021.

[27] S. Dusmez, H. Duran, and B. Akin, "Remaining useful lifetime estimation for thermally stressed power mosfets based on on-state resistance variation," *IEEE Transactions on Industry Applications*, vol. 52, no. 3, pp. 2554–2563, 2016.

[28] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE transactions on parallel and distributed systems*, vol. 24, no. 1, pp. 131–143, 2012.

[29] M. S. Mekala and P. Viswanathan, "Equilibrium transmission bi-level energy efficient node selection approach for internet of things," *Wireless Personal Communications*, vol. 108, no. 3, pp. 1635–1663, 2019.

[30] R. Ezhilarasie, A. Umamakeswari, and T. Renugadevi, "Key management schemes in wireless sensor networks: a survey," *International Journal of Advanced Intelligence Paradigms*, vol. 7, no. 3-4, pp. 222–239, 2015.

[31] Y. Yang, X. Liu, X. Zheng, C. Rong, and W. Guo, "Efficient traceable authorization search system for secure cloud storage," *IEEE Transactions on Cloud Computing*, vol. 8, no. 3, pp. 819–832, 2018.

[32] S. F. Aghili, H. Mala, P. Kaliyar, and M. Conti, "Seclap: Secure and lightweight rfid authentication protocol for medical iot," *Future Generation Computer Systems*, vol. 101, pp. 621–634, 2019.

[33] C. Thirumallai, M. S. Mekala, V. Perumal, P. Rizwan, and A. H. Gandomi, "Machine learning inspired phishing detection (pd) for efficient classification and secure storage distribution (ssd) for cloud-iot application," in *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*. IEEE, 2020, pp. 202–210.

[34] M. Akter and Gani, "Performance analysis of personal cloud storage services for mobile multimedia health record management," *IEEE Access*, vol. 6, pp. 52 625–52 638, 2018.

[35] E. Luo and M. Bhuiyan, "Privacyprotector: Privacy-protected patient data collection in iot-based healthcare systems," *IEEE Communications Magazine*, vol. 56, no. 2, pp. 163–168, 2018.

[36] Y. Zhang and H. Zheng, "Security and privacy in smart health: Efficient policy-hiding attribute-based access control," *IEEE Internet of Things Journal*, vol. 5, no. 3, pp. 2130–2145, 2018.

[37] T.-Y. Youn, K.-Y. Chang, K.-H. Rhee, and S. U. Shin, "Efficient client-side deduplication of encrypted data with public auditing in cloud storage," *IEEE Access*, vol. 6, pp. 26 578–26 587, 2018.

[38] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 331–346, 2018.

[39] D. Xiao, M. Li, and H. Zheng, "Smart privacy protection for big video data storage based on hierarchical edge computing," *Sensors*, vol. 20, no. 5, p. 1517, 2020.