Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Computer Communications 199 (2023) 87–97

Contents lists available at ScienceDirect

Computer Communications

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

COVID-19 health data analysis and personal data preserving: A homomorphic privacy enforcement approach

Chandramohan Dhasarathan [a], Mohammad Kamrul Hasan [b,*], Shayla Islam [c,*], Salwani Abdullah [b], Umi Asma Mokhtar [b], Abdul Rehman Javed [d,e], Sam Goundar [f,g]

[a] Thapar Institute of Engineering & Technology, ECED, Department of Computer Science & Engineering, Punjab, India
[b] Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), 43600 Bangi, Selangor, Malaysia
[c] Institute of Computer Science and Digital Innovation, UCSI University, Malaysia
[d] Department of Cyber Security, Air University, Islamabad, Pakistan
[e] Department of Electrical and Computer Engineering, Lebanese American University, Byblos, Lebanon
[f] School of Computing and Innovative Technologies, British University Vietnam, Viet Nam
[g] School of Science, Engineering, and Technology, RMIT University, Viet Nam

ARTICLE INFO

Dataset link: https://doi.org/10.21227/scr5-pr80

Keywords:
Deep learning system
Homomorphic
Healthcare
Privacy preserving
Privacy metrics
Security

ABSTRACT

COVID-19 data analysis and prediction from patient data repository collected from hospitals and health organizations. Users' credentials and personal information are at risk; it could be an unrecoverable issue worldwide. A Homomorphic identification of possible breaches could be more appropriate for minimizing the risk factors in preventing personal data. Individual user privacy preservation is a must-needed research focus in various fields. Health data generated and collected information from multiple scenarios increasing the complexity involved in maintaining secret patient information. A homomorphic-based systematic approach with a deep learning process could reduce depicts and illegal functionality of unknown organizations trying to have relation to the environment and physical and social relations. This article addresses the homomorphic standard system functionality, which refers to all the functional aspects of deep learning system requirements in COVID-19 health management. Moreover, this paper spotlights the metric privacy incorporation for improving the Deep Learning System (DPLS) approaches for solving the healthcare system's complex issues. It is absorbed from the result analysis Homomorphic-based privacy observation metric gradually improves the effectiveness of the deep learning process in COVID-19-health care management.

1. Introduction

A multidisciplinary machine learning approach can diagnose COVID-19 with a scientific paradigm to personalize the distribution of significant medical symptoms. Patient health ecosystem building should be decentralized in an ideal environment. Virus transmission was noted in clinical trials from previous pandemics. The patient's symptoms are monitored, analyzed, and predicted as prior information for possible viral infection. In the past ten decades, many viral infections have been caused by a variety of flu worldwide. The Daily life of societal functionality gets affected due to multivariate viruses, which leads to the global pandemic. Holistic studies of crowd monitoring, social spreading cause research, diagnosing fake news delivery, predicting virus infection and its peak analysis. The machine learning technique allows personalizing promising health eco-system analysis and prediction. To make smart integration for gathering the history of virus-infected patients and empowering the flu tracking and appearance of new variants prediction and its risk. Personal health data pattern concerns multiple factors with appropriate isolation, correlated to reducing risk factors. The Internet of Things (IoT) utilizes for accessing, tracing, screening, monitoring, and diagnosing corresponding symptoms for prediction and clinical trials. Predicting COVID-19 by analyzing the blood sample and various symptoms minimizes the spread of vulnerable viruses. The Multi-filtering process helps to diagnose typical spreading among patients and the public as a victim and gets infected. Scanning chest X-rays and CT offers radiation safety measures with certain limitations. Researchers highlight cleanliness as the key promo for avoiding the spreading chain. It is observed that untreated wastewater management in regional-level surveillance could boost the estimation of specific flu spreading and lead to pandemics. Prognosis evaluation by hematological features identifying hybrid genetic algorithm-based machine learning techniques. Clinical symptoms of patient data are normalized, and it might be validated into a statistically trained data set for feature selection to identify the best relevant patient data for treatment. The severity of symptoms is extracted for discriminant analysis and intubation risk

* Corresponding authors.
E-mail addresses: mkhasan@ukm.edu.my (M.K. Hasan), Shayla@ucsiuniversity.edu.my (S. Islam).

https://doi.org/10.1016/j.comcom.2022.12.004
Received 1 July 2022; Received in revised form 13 November 2022; Accepted 1 December 2022
Available online 14 December 2022
0140-3664/

based on ML evaluation criteria. When users store their data in the cloud, a TPA (Third Party Administer) will be allotted to check the integrity of the data. A lightweight encryption scheme for COVID-19 health data needs to focus on a secure range and query for confidential data.

Section 1 deals with the protection of personal data, the importance of privacy in COVID-19 patients, and the need for data to be encrypted. So, mobile users should be able to query data and get the results per their requests. Timestamp routing by various intelligent optimization techniques to analyze the COVID-19 patient data is expressed in Section 2. In Section 3, we designed and proposed a Homomorphic privacy protection enforcement and its metrics to build a system that uses the optimization model by incorporating the artificial bee colony approach in the framework. The need for a data analytics system for analyzing the COVID-19 data collected from various patients and hospitals for testing and formulating a protective mechanism. The analytical result analysis is discussed, and the efficiency variations are illustrated and plotted in Section 4. In Section 5 we concluded the privacy metric needed for a COVID-19 healthcare system, and enhancement features for future research are discussed.

2. Literature study

Firouzi et al. [1] contemporary interrelated pandemic research with digital technology help to discover COVID-19 symptoms analysis and prediction. The paper discusses the risk factors, drug development, early prediction, and alerting the global spreading. However, it focuses on AI-based developments in COVID-19 pandemic research. Rahman et al. [2] to meet the global pandemic, machine learning is the best technology to adopt and improve the situations argued in the world at complete lockdown. Mobility of human activity expects few daily survival needs are exempted from shutting down. Machine learning is one of the most potent pandemic problem solvers and improves the mitigation of the spread of flu in a different form. Abdulkareem et al. [3] to diagnose the symptoms of COVID-19 using machine learning by filtering the datasets with original and normalized values. Features selection is used for diagnosing positive clinical symptoms are directed to a trusted prediction. It minimizes the health risk for practitioners and the public to safeguard themselves from the infection. Fedele et al. [4] predict the inhabitation of patients with mild and moderate symptoms for disease severity and neutralize the persistence of COVID-19. It is observed from the data collected from various hospitals with privacy concerns regarding patient health information. A Spike of virus infection is observed from the disease severity, and the monitoring process helps to anti-Spike less flu infection.

Bezzan and Rocco [5] Uniform Manifold Approximation And Projection (UMAP) technique is followed to cluster essential medical data to filter the diagnostic process, and its outcome is observed. A systemic hematological fraction to discover the illness and new patterns of infection. Rikan et al. [6] correlations and coefficient of regular blood sample testing sensitive medical data and artificial intelligent interpretation among samples are illustrated. Its accuracy mainly focuses on clinical blood samples applying a statistical t-test for filtering unique pandemic diagnosis tools for positive cases. Varzaneh et al. [7] 3D representation empirical mode decomposition techniques for classification and extracting block of backbone components using deep CNN approach. Context-aware attention classifies the main features of pneumonia cases which helps to detect COVID-19.

Li et al. [8] wastewater quantification concentration by mitigating environmental correlation for an early prediction and detection of SARS-CoV-2 from the clinical data of public health monitoring system. Sampling scientific data with limited availability of numerous flu infection provide prior warning to the public noted symptoms. Sevinç [9] decision tree estimation of the severity of patients by adaptive boost machine learning algorithm to reduce the effect of spreading COVID-19 with competitive accuracy prediction by using advanced ML algorithm. To fight against the global virus, a random selection model was used in the COVID-19 test study for unveils and fight against the medical complexities. Miikkulainen et al. [10] World is unprepared to face COVID-19 restless information collection about the community spread. They were monitoring the quality predictors and reducing trade-offs among NPI simulators. The proposed epidemiological models help the system with a trustworthy explanation to improve the interactive symptoms collected for COVID prediction. The synchrophasor measurements identify the classification of regression modeling in all transmission lines. The magnetic flux from the transmission lines is in ideal condition for the projects with faults location. Privacy-preserving in a distributed web service environment with a framework dealing with an ad-hoc scenario. The service requester's demands are not fulfilled by the quality of retrieved services [11]. Privacy policy extensibility is applicable for the service providers in all constraint-based satisfactions. It is validated by optimization algorithms to check efficiency.

Fog-enabled environmental services are delayed, and their load is estimated [12] in a shared service. The requirements are tested in real-time test cases and industrial standards to check their efficiency. Virtual and physical validation is verified in a contemporary data environment. The delay in transmission delay gets improved, and the optimization approaches improve the delivery rate. Patient-care amenities related to healthcare services are taken into intensive care by Edge of Things (EoT) [13] as persuasive healthcare management. The edge computing service providers (ECSP) and cloud computing service providers (CCSP) observe the patient's health at regular intervals and get all health information using body area networks (BAN). The article proposed a portfolio optimization solution based on the virtual machine (VM) with the deliverable cloud service. To achieve service distribution, centralized service monitoring and EoT introduces portfolio optimization. It supports a cost-effective system in personalized healthcare management system using VM-supportable techniques to improve innovative healthcare services. Moreover, it improves intelligent devices and mobile applications to support healthcare services in secure and safe incarceration.

The patient details would be categorized based on the data analytics techniques [14] for identifying the low-power devices utilized in real-time microbiome monitoring. The portable devices are neutral; it has an ambiguous architecture that needs ubiquitous analysis in all diversified environments. To process the data collectively integrated from resources of the universal environment, devices have a vast amount of relevant and irrelevant data that needs to be communicated and converted into useful information. A scheduling mechanism is adopted for reliable communication to pipeline the cloud-based services and edge computing devices. It is proposed that efficient information interaction, multimodal data fusion, and automatic production [15] improve edge computing. The interaction-based systems are highly in demand utilizing e-health services in a robotic architectural neutral system management. The cognitive control of multimodal fusion is carried out in traditional and real-time scenarios. The artificial intelligent driving force highlights resource scheduling. Edge computing techniques expand all computing resources to promote economic growth. Sentimental analysis is endorsed as unsupervised learning, with artificial intelligence (AI) as the core competitiveness. The efficiency of cognitive manufacturing adopts a highly interconnected structure and composition to improve chip assembly significantly.

The article discussed the need for a multi-agent-based cloud service endorsement in ubiquitous computing scenarios [16]. The agents would analyze the possibilities of proper communications with minimum resource utilization in all circumstances. The cloud-enabled devices would share the device information with all service providers on demand. It could increase the privacy issue of the device owners and put them at personal risk—multi-agent-based service utilization with proactive privacy-preserving measures and ineffective resource sharing and communication. Internet of Things (IoT) -based learning for network communications to improve human–computer interaction [17] for the

betterment of enormous service sharing and utilization. It involves vast sensible data processing and transformation in every service cattalo. The researchers are forecasting proper and rescindable research has been highlighted with limited privacy-preserving information. There is a need to concentrate on contextual and content-based privacy preservation in IoT-based communications. It is focused on identity-based encryption schemes based on resource availability for data transfer.

Healthcare emergency monitoring using a bio-inspired approach has a predictive measure for the effective recovery of patients from health risks, as illustrated by Dhasarathan et al. [11], Hasan et al. [18,19]. The current study dealt with the contemporary computing and routing architecture which inculcate randomly and cannot develop trust in cooperative systems. It has crypto mechanisms for ensuring the handshake process between the devices. There is a need to create a privacy metric with a collaboration of mathematical approach, statistical data, privacy policy customized, and advanced encryption mechanism to better the user's trust. Security is focused on high priority by designing protocols with current industrial needs, Hasan et al. [20] discussed enhancing the intelligent control IoT security to handle critical challenges by the cryptographic lightweight process. Encryption and decryption are tested in a real-time network for their efficiency. Dynamic global communication [21] proposed an intelligent grid for effective data processing and transmission to collect and analyze the power grid [18,19,22]. Genetic Deep Learning Convolutional Neural Network (GDCNN) [23,24] designed an approach to predict COVID-19 with a partial swam intelligent optimization model and huddle particle swarm optimization. Numerous techniques and methodologies were proposed in the literature study for personal data prevention [25–27]. Statistical data collaboration and indicating the cause of information breaches are challenging. Researchers face different attacks on stored data, and there is a need for an advanced approach to balance data prevention and computation. The homomorphic encryption technique is one such approach that could balance data encryption and analysis, which fulfills current needs and gives a tricky time for attackers. Patients affected by COVID-19 health condition is tested for marginal deviations in the immune system [28]. The patients who follow the regular diet and physical activity are noticed with perfect immune systems, whereas the rest are found dangerous for take-ups in the next wave. A deep learning-based fake news filtering to get the real news. It uses classification concerning COVID-19 awareness and checks the correctness of information spreading in social media and communication [29] sentimental feature extraction as an information fusion.

3. The homomorphic privacy protection enforcement

The homomorphic encryption system description level metric states the activities involved in the description level with the help of the following parameters development, application, and publication. Fig. 1. states that the development parameter includes the integration of agent idea id_a, dynamics dyn, and its documentation $doc.development\ dev = id_a + dyn + doc$. The application displays the documentation doc of various users. $application\ app = [doc]_0^n$. Publication measures the marketing aspect mk_{as} of multi-agent systems and the user acceptance acc_{user} of agent systems $publication\ pub = \left(mk_{as} + acc_{user}\right)$.

$$PPM(x,y) = \frac{1}{PM}\sum_{i=1}^{P}\sum_{j=1}^{M}\frac{(x_i-\mu_x)(y_{ij}-\mu_y)}{\sigma_x\sigma_y} \tag{1}$$

PPM→ Privacy Preserving model similarity metrics
PM→ Privacy Metrics
x, y are two-way request and response

μ_x *and* μ_y *are average request and response*

$\sigma_x\ \sigma_y$ *are standard deviations of* x *and* y *respectively*

P and M are privacy, metrics for user

$$P^* = \arg Max_T PPM(MSL(m,1), MSL(P(l,-1))) \tag{2}$$

Where 'm' is mathematical induction and 'l' is privacy law.
MSL→ Metric Security Level
Where,
(M, l) is health patient data-related to privacy law.
P*is privacy endurance that produces the alignment pair (m, P(l)).
D: P→ A { Data- D, Privacy-P, Authorised user-A, m ∈ P, l ∈ A.}

$$PL^{\varepsilon} = \sum_{\Omega_\mu}\varepsilon(P(AU), l) \tag{3}$$

Privacy law → PL^{ε}
Privacy (Authorized User)→P(AU)
Law enforcement → l

$$PPAU(x,y) = \frac{(2\mu_{x_i}\mu_{y_j} + U_x)(2\sigma_{ij} + U_y)}{(\mu^2{}_{x_i}\mu^2{}_{y_j} + U_x)(\sigma^2{}_{ij} + \sigma^2{}_{y_{ij}} + U_y)} \tag{4}$$

$PPAU(x,y)$→ Privacy-preserving for an authorized user
U_x, U_y→ User request
$\sigma^2{}_{y_{ij}}, \sigma^2{}_{ij}$→ Unauthorized request
$\mu_{x_i}\mu_{y_j}$→ Mathematical inclusion, statistical metrics
$\mu^2{}_{x_i}\mu^2{}_{y_j}$→ Privacy law, mathematical inclusion, statistical metrics

$$Homomorphic\ System\ desing\ level = size + component\ structure + complexity + function$$

$$Homomorphic\ System\ desing\ level = \sum_{i=1}^{n}\left(act_a + mtr\right) + \left(org_{hr} + org_{fn}\right) + \{re, env, ph, soc\} + fn_{sreq} \tag{5}$$

$$\begin{aligned} Homomorphic\ system\ working\ level &= communication + interaction + knowledge + lifeness \\ &+ conflict\ management + community + management \\ &+ application + stability + performance + organization \end{aligned} \tag{6}$$

$$\begin{aligned} Homomorphic\ system\ working\ level == &\left[lang\left(sof_a + other_a\right) + act\right] \\ &+ md_{ty}\left(sof_a + other_a\right) + lear_{outc} + \left(adp_a + ssmain_{eff}\right) \\ &+ \left(neg_a + sys_{ts}\right) + \left[\left(comm_a\right)_0^n collb_a\right] + \left(coor_a\left(sstr_a\right)\right) \\ &+ \left(appar + [coop]_0^n\right) + \sum selrp_a + \left(perf + perf_a\right) \\ &+ r(cu, pl, ar, md, comm, ob, dmk) \end{aligned} \tag{7}$$

Data metrics are followed to ensure the encryption standard is given in Eqs. (1)–(7) respectively. The privacy-preserving relevant frameworks have an adequate methodology for healthcare to maintain the coordinators' and the tradeoff between energy-efficient architectural interfaces. It cannot organize and sustain the coordinator's private information safety and trust. Identifying the appropriate user's privilege and confidentiality level needs to be considered more concerned with the support of multi-level computing. A Peer-to-Peer opportunistic computing and routing system also socializes with tolerable message transmission with privacy metrics. The software interface for effective machine optimization would support the critical emergence of COVID-19 health monitoring. An emergency is caused in any circumstance to handle it with cooperative information sharing to the centralized system for the betterment of recovery. To monitor the regular activity with intensive care and react in time to speed up the monitoring and medication process. The monitoring activity could be organized periodically to collect the patient medical data for appropriate treatment and action. A specified agent could regularize the movement of a patient to monitor the active process. Multiple agents cooperatively monitor the process for an organized medication process to prolong the COVID-19 health integral structure. COVID-19 health monitoring is a good activity for a balanced medication process for complex maintenance integrated by multi-agent cooperation. Each agent monitors the patient health activity and periodically reports to the COVID-19 health centralized

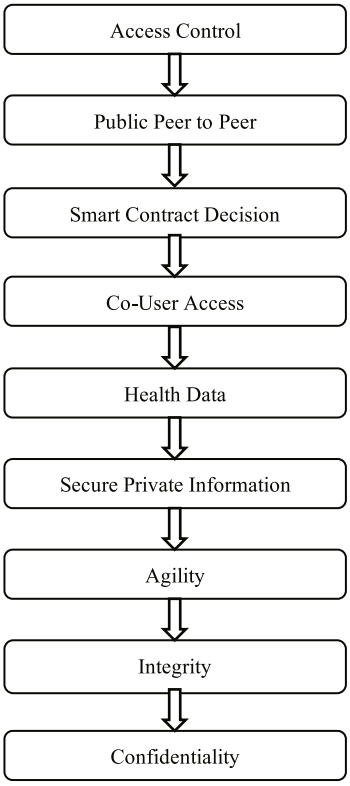

Fig. 1. Private data metrics using homomorphic enforcement for COVID-19 big data.

agent for medication by appropriate experts in time. To collect a patient's regular exercise, the deployed agents run all time as an active depict.

The main objective is the proper treatment at the right time to avoid a patient's critical situation. The medication must be processed during exceptional cases with a cooperative multi-agent hierarchy approach. Emergency and urgent COVID-19 health organizations with multi-agent unified monitoring by on-demand computing lead to a risk of collaborative device participation in the communication for appropriate medication. The devices handle the critical situations provided by agreeing to the multi-agent terms and conditions. To develop an acceptable feature to improve the confidentiality level Fig. 1 with algorithm 3.1 would act as a trust for the devices participating in the cooperative task which handles the emergencies. Participative agent's data privacy-preserving strategy by adopting the mathematical approach, statistical information, information policy act, and encryption techniques to ensure the multi-agent coordination with privacy metrics.

3.1. Algorithm for homomorphic enforcement and working principle for data protection

Fun_Setup_Selection

Web User Group – (WUG)

WUG1, WUG2, WUG3, … WUGn {whereas WUG1, WUG2 belongs to web user such that <WUG1> = WU1, <WUG2>=WU2, which describes and define the bonding of participative users (PU):

PU: WU1 X WU2 → WUn on applying electrical cryptographic (ECC) hash functions such as ECCH1, ECCHz, and ECCH it will give

$ECCH_1$: {T, F}* →{T, F}n,

$ECCH_z$: {T, F}δ x {T, F}* →{T, F}n, for z ∈ {T, F}δ and n ∈ no.of. UsersRequest, and

$ECCH : WU_n \rightarrow WU_2, WU_n \rightarrow WU_z$

Return UsersData (UD):= {u, WUG_1, WUG_2, WU_1, WU_2, *pu,* $ECCH_1, ECCH_z, ECCH$*}*

End Fun_Setup_Selection

Fun_Key_Generation $(UD, W)_\alpha$

T→ Transaction, R→ Request,
$T, R \in_r U^*_{pu}$

$t \leftarrow pu(WUG_1, WUG_2)^j$

Function Data LatenceyUserRequest UR:

fun_Privacy_Sustainability

Input: UR Service

Input: UR Node

Input: CloudUserCredential

User Service ← Null;

For Users in the UR Service list of CloudDataContainers do

If CloudDataStorage is not present on CloudProvider, then

User Service ← Verifying the CloudDataStorage;

End

End

CloudBandWidth ← UserBandwidth[UserIdentity][UserDevice];

AccessPermission ← UserService/ CloudServiceBandwidth;

Return AccessPermission;

While Data Intruder is identified do

Pi← Private Data identification

~Pi ← False User Private Request Identification (Px, Distributed Request-DR)

DR= GenerateDistributedService(Px, DR, ~Pi)

If DR Navigates as DistributedService then do

BlockRequest= DR[0] sum of DR[n]

Else if DR Navigates as AuthenticatedDistributedService Then

AllowRequest= DR[0] sum of DR[n+i]

Else if DR Navigates as UnAuthenticatedDistributedService Then

BlockRequest= DR[0] sum of DR[n+i]

Else if DR Navigates as UnKnownAuthenticatedDistributedService Then

BlockRequest= DR[0] sum of DR[n+i]

Else if DR Navigates as KnownAuthenticatedSimillarDistributedService Then

BlockRequest= DR[0] sum of DR[n+i]

Else if DR Navigates as UnKnownAuthenticatedSimillarDistributedService Then

BlockRequest= DR[0] sum of DR[n+i]

Else

EndService= ServiceRequest[0, n+i]

End while End fun_Privacy_Sustainability

Send to DS

Return VaidService

End

$$\Rightarrow \text{IC}\ (HU_1, HU_2, HU_3, \ldots, HU_n)$$

$$\Rightarrow; \text{Where, } HU_n = HU_x * \begin{bmatrix} HU_{x11} & HU_{x12} & HU_n \\ HU_{x21} & HU_{x22} & \vdots \\ HU_{x31} & HU_{y32} & \vdots \\ \vdots & \vdots & \vdots \\ HU_{xm} & \ldots & HU_{mn} \end{bmatrix} * [\text{d, p, b, m}]$$

$$HU_{x_{ij}} * \begin{bmatrix} HU_{d11} & HU_{p12} & HU_{b13} & HU_{m14} \\ HU_{d21} & HU_{p22} & HU_{b23} & HU_{m24} \\ HU_{d31} & HU_{p32} & HU_{b33} & HU_{m34} \\ \vdots & \vdots & \vdots & \vdots \\ HU_{dm1} & HU_{pm2} & HU_{bm3} & HU_{mm} \end{bmatrix} \begin{bmatrix} HU_{d11} & HU_{p12} & HU_{b13} & HU_{m14} \\ HU_{d21} & HU_{p22} & HU_{b23} & HU_{m24} \\ HU_{d31} & HU_{p32} & HU_{b33} & HU_{m34} \\ \vdots & \vdots & \vdots & \vdots \\ HU_{dm1} & HU_{pm2} & HU_{bm3} & HU_{mm} \end{bmatrix}$$

$$\cdots \begin{bmatrix} HU_{d1} & \cdots & HU_{m1} \\ \vdots & \ddots & \vdots \\ HU_{dm} & \cdots & HU_{mm} \end{bmatrix} n$$

EON = $HU_{x_{ij}}$ [$\because (x_i)_j$ => i ={d, p, b, m} and j= {number of mobile opportunistic nodes}]

$$\begin{bmatrix} MON_x & MON_y & MON_\infty \\ MON_{x1} & MON_{y1} & \vdots \\ MON_{x2} & MON_{y2} & \vdots \\ \vdots & \vdots & \vdots \\ MON_{xn} & MON_{yn} & MON_\infty \end{bmatrix} \begin{bmatrix} HU_{d11} & HU_{p12} & HU_{b13} & HU_{m14} \\ HU_{d21} & HU_{p22} & HU_{b23} & HU_{m24} \\ HU_{d31} & HU_{p32} & HU_{b33} & HU_{m34} \\ \vdots & \vdots & \vdots & \vdots \\ HU_{dm1} & HU_{pm2} & HU_{bm3} & HU_{mm} \end{bmatrix}$$

$$\begin{bmatrix} HU_{d11} & HU_{p12} & HU_{b13} & HU_{m14} \\ HU_{d21} & HU_{p22} & HU_{b23} & HU_{m24} \\ HU_{d31} & HU_{p32} & HU_{b33} & HU_{m34} \\ \vdots & \vdots & \vdots & \vdots \\ HU_{dm1} & HU_{pm2} & HU_{bm3} & HU_{mm} \end{bmatrix} \cdots \begin{bmatrix} HU_{d1} & \cdots & HU_{m1} \\ \vdots & \ddots & \vdots \\ HU_{dm} & \cdots & HU_{mm} \end{bmatrix} n$$

Different algorithms are used to analyze the COVID-19 data, and its result variations are noted carefully. It is illustrated in Table 2. Moreover, improving the analyzing strategy, a deep learning-based approach would improve. It is also used in the proposed approach, as shown in algorithm 3.1. Electronic health records of patients affected by COVID-19 are collected from various open-source datasets and validated by different available algorithms and techniques highlighted in the literature study. Every algorithm is designed to solve one particular issue, such as one algorithm for patient identification with symptoms and another for analyzing the possibility of spreading and the cause. From the study, it is clear that to target solve issues related to electronic health data prediction, analysis, and prevention of personal information of COVID-19 patients hybrid model is needed to address these issues. Homomorphic enforcement of data prevention hybrid algorithm outperforms these perspectives illustrated in Section 3.1.

$$\Rightarrow EON_{x_{ij}}\ (\text{x}_{\text{dpbm}})_n [\because (x_i)_j]$$

$$\Rightarrow IC_n \cdot \prod_{n=1}^{\infty} HU_n$$

$$\therefore Emergency\ Health\ Information = IC_n \cdot \prod_{n=1}^{\infty} HU_n$$

The algorithm at 3.1 describes the information of energy getting used in all circumstances and is highlighted with homomorphic privacy metrics. Fig. 2. shows the structure of collective on-demand classification of nodes with the help of the Multi-Agent system working

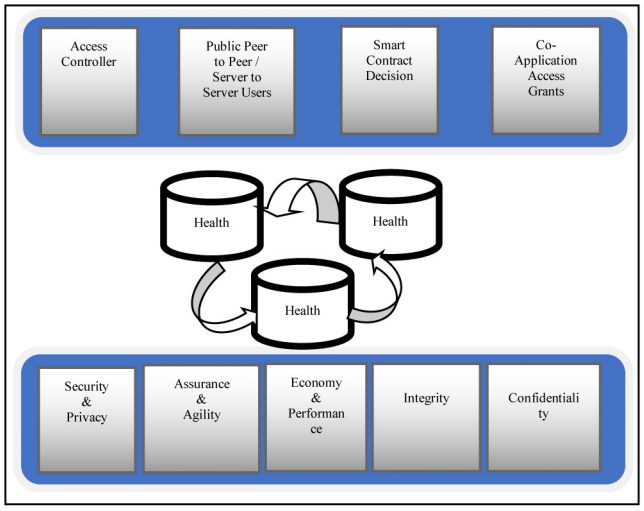

Fig. 2. Deep learning-based privacy preserving system for a Health Care Management Model.

level deals with the agent communication, level of agent interaction, knowledge, lifelessness, conflict management, community, management, application, stability, performance, and organization. Agent communication is stated as the various communication languages of other agents and the action to be carried out $communication\ comm = [lang\ (sof_a + other_a) + act]$. Interaction states the type of interaction with the software agent and another agent, $interaction\ int = md_{ty}(sof_a + other_a)$. Knowledge refers to the outcome of agent learning $knowledge\ kng = lear_{outc}$. Liveness refers to the agent's adaptation symbolizing system maintenance efforts $lifenes\ lif = (adp_a + ssmain_{eff})$. Conflict management deals with agent negotiation and system tasks. $conflict\ mangement\ conf_{mg} = (neg_a + sys_{ts})$. Community refers to the different levels of agent communication regarding agent collaboration. $community\ cmty = [(comm_a)_0^n\ collb_a]$. Management level refers to the various level of agent coordination concerning agent system structures. $management\ level\ mg = (coor_a\ (sstr_a))$. Application level refers to the application area and different agent role cooperation. $application\ level\ app = (appar + [coop]_0^n)$. The stability level states the measure of agent self-reproduction. $stability\ level\ stb = \sum selrp_a$. Performance level states the performance and performance of an environment. $performance\ level\ prf = (perf + perf_a)$. Organization-level parameters deal with an agent's roles, such as customer, planner, archivist, mediator, communicator, observer, and decision-maker. $organization\ level\ org = r(cu, pl, ar, md, comm, ob, dmk)$.

Homomorphic system description level for DPLS

$$Homomorphic\ system\ description\ level = development + application + publication$$

$$Homomorphic\ system\ description\ level = (id_a + dyn + doc) + [doc]_0^n + (mk_{as} + acc_{user}) \quad (8)$$

$$Homomorphic\ development\ life\ cycle = phase\ level + milestone\ level + requirement\ workflow\ level$$

$$Homomorphic\ development\ life\ cycle = \{str, sz, c\} + \sum_{i=1}^{n} ms_a + [req_a] \quad (9)$$

The homomorphic development method level states the various stages involved in the development method level and its parameters, such as methodology level, paradigm level, and case level. The methodology level tries to find out suitable development method for agent implementation $Dmd_a.methodolgy\ levelmth = \prod Dmd_a$. Paradigm levels used

to identify the relevance of selected development paradigm Dmd_{pard}, $paradigm\,level = \prod Dmd_{pard}$. Case-level parameters state the tools that support tl_{sp} for the agent implantation.

$$Homomorphic\,development\,method\,level = methodology\,level + paradigm\,level + case\,level$$

$$Homomorphic\,development\,method\,level = \prod Dmd_a + \prod Dmd_{pard} + tl_{sp} \tag{10}$$

The homomorphic development management level metric deals with all management level activity parameters, project management level as shown in Eqs. (8), (9) and (10), configuration management level, and quality management level. Project management level state the developer risks dev_{rs} and the method m_a involved in the agent development.$project\,mangement\,level\,proj_{mgl} = dev_{rs} + m_a$. Configuration management level states the success of the version control concerning the agent. Thus $configuration\,management\,level = (\frac{n}{k})p^k q^{n-k}$, where 'n' stands for the number of trails, 'k' denotes the number of success, n − k represents the number of failures, p indicates the probability of success of version control based on the agent in one trail, $q = 1 - p$ probability of failures in one trail. Quality management level parameter state the quality assurance technique qtec_a involves in software agents. $quality\,management\,level\,q_{mgl} = [\text{qtec}_a]$.

Homomorphic developer-level metrics state the parameters involved in the development of an agent, such as skill level, communication level, and productivity level. Agent skill level involves the developer skill dev_{sk} and implementation of agent imp_a. $skill\,level\,sk_l = (dev_{sk} + imp_a)$. Agent communication level parameter deals with the work advance based on collaboration $collb$ and cooperation $coop.communication\,level\,comm_l = wk_{adv}(collb + coop)$. Productivity level states the amount of work done $w = f * d$.

$$Agent\,development\,management\,level = project\,management\,level + configuration\,management\,level + quality\,management\,level$$

$$Agent\,development\,management\,level = \left(dev_{rs} + m_a\right) + \left(\frac{n}{k}\right)p^k q^{n-k} + [\text{qtec}_a] \tag{11}$$

$$Homomorphic\,developer\,level = skill\,level + communication\,level + productivity\,level$$

$$Homomorphic\,developer\,level = \left(dev_{sk} + imp_a\right) + wk_{adv}\,(collb + coop) + (f * d) \tag{12}$$

The homomorphic software resource level states the necessary resource required for the development of agent software and is based on the parameters paradigm level, performance level, and replacement level. The paradigm level, as shown in Eqs. (11) and (12), states the relevance of the selected development paradigm dev_{prg}. $paradigm\,level\,prg_l = \prod dev_{prg}$. Performance level represents the component $comp$ and effectiveness $eff.performance\,level\,perf_l = (comp + eff)$. The replacement level parameter states the version of adaptation adp when using various software $replacement\,level\,rep_l = [adp]_{vr}$.

Homomorphic software resource level for DPLS

Agent hardware resource level metric deals with reliability, performance, and availability. Reliability level states the reliable hardware $plaf_a$ required for running an agent. $relaiblity\,level\,rel_l = [plaf_a]_0^n$. Fig. 3. shows the performance level deals with the various platform used by the software agent $performance\,level = [plat]_{a=1}^n$. Availability level states the availability of various platforms $avil.availablity\,level = [avil]_{plat}$

$$Homomorphic\,software\,resource\,level = paradigm\,level + performance\,level + replacement\,level$$

$$Homomorphic\,software\,resource\,level = \prod dev_{prg} + (comp + eff) + [adp]_{vr} \tag{13}$$

$$Homomorphic\,hardware\,resource\,level = Realibility\,level + Performance\,level + Availability\,level$$

$$Homomorphic\,hardware\,resouce\,level = [plaf_a]_0^n + [plat]_{a=1}^n + [avil]_{plat} \tag{14}$$

$$Homomorphic\,System\,development\,life\,cycle = phase\,level + milestone\,level + requirement\,workflow\,level$$

$$Homomorphic\,System\,development\,life\,cycle = \{str, sz, c\} + \sum_{i=1}^{n} ms_{mas} + [req_{mas}] \tag{15}$$

Homomorphic System Development Method level for DPLS

$$Homomorphic\,System\,development\,method\,level = methodology\,level + paradigm\,level + case\,level$$

$$Homomorphic\,System\,development\,method\,level = \prod Dmd_{mas} + \prod Dmd_{pard} + tl_{sp} \tag{16}$$

$$Homomorphic\,System\,development\,management\,level = project\,management\,level + configuration\,management\,level + quality\,management\,level$$

$$Homomorphic\,System\,development\,management\,level = \left(dev_{rs} + m_{mas}\right) + \left(\frac{n}{k}\right)p^k q^{n-k} + [\text{qtec}_{mas}] \tag{17}$$

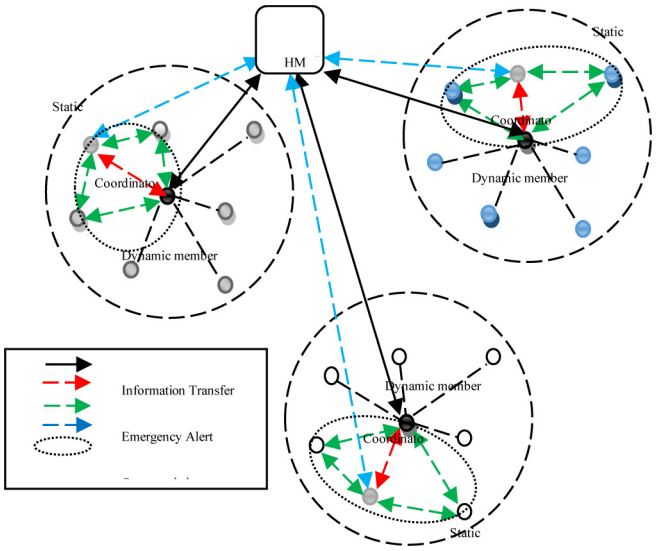

Fig. 3. DPLS — A coordinator-specific Intra-cluster Information Updating system.

The coordinator-specific intra-cluster information system for a health management system is demonstrated in Fig. 3. The virtual coordinators have a limitation with static boundaries for communication. It searches for an appropriate resource for effective communication in deprived regions, and the management level of data protection and privacy levels are illustrated in Eqs. (13) and (14). Homomorphic and Development life cycle, Method, developer, and management level for DPLS. The Homomorphic System Development life cycle and Development management level for DPLS as shown in Eqs. (15), (16), and (17), respectively.

4. Result evaluation and discussion

Homomorphic system development model to analyze the COVID-19 data for managing the entire life cycle of hardware resource monitoring. Resource allocation under developer model and methods with software description. To remain safe and protected and complete maximum

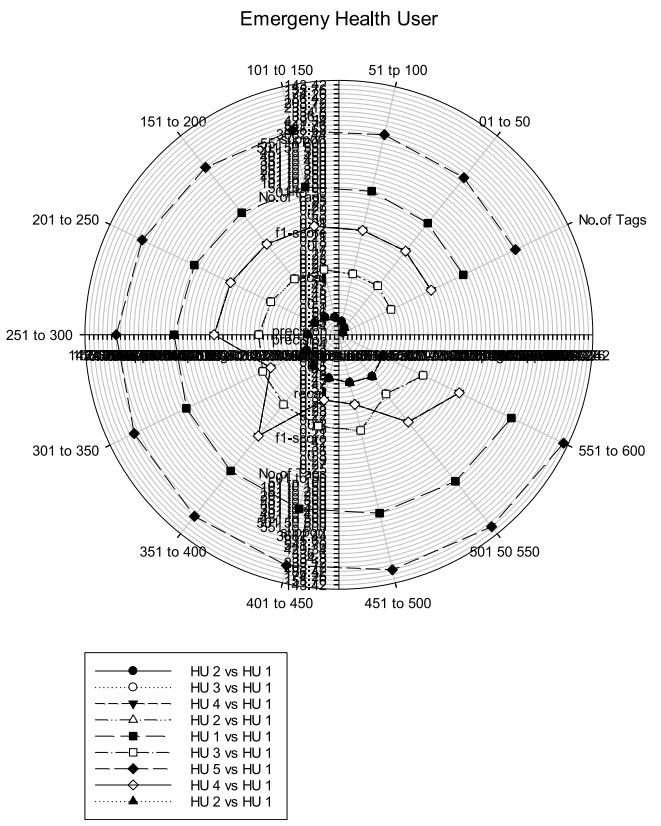

Fig. 4. COVID patient analysis eligible to prevent personal information.

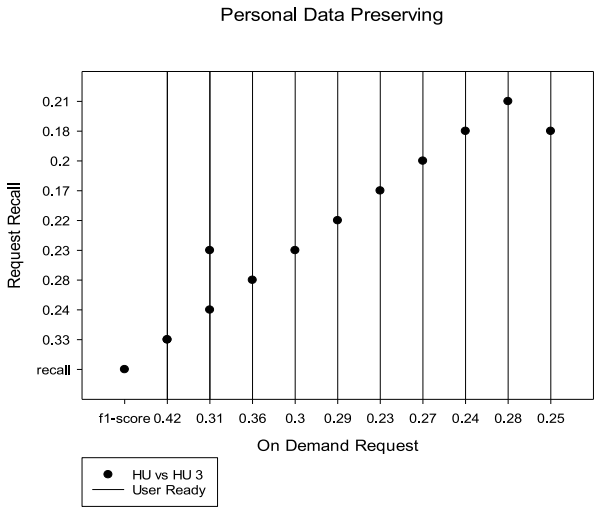

Fig. 5. Homomorphic enforcement in critical scenario.

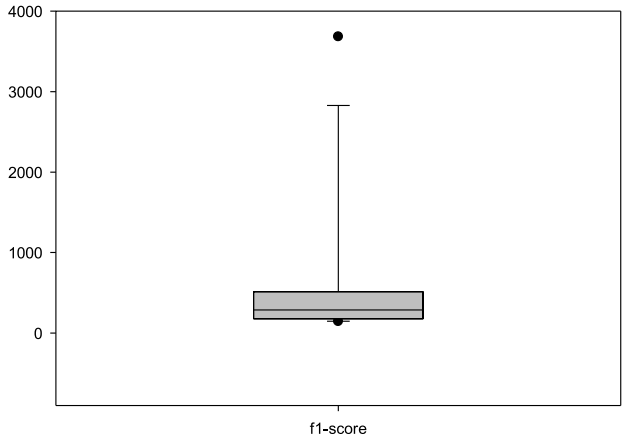

Fig. 6. Opportunistic health data analysis and homomorphic metric for COVID patients.

efficiency with minimum futile effort or disbursement communication system under network problems which intrude an event activity without believing a reliable another part is still persistent as a challenging issue. In three parts, the user's data investigator scrutinizes a crime locomotive as the core of a careful trailing obstructive contrivance. The number of file block facsimiles has no meaning in the design of manifold users with the sole data center. The number of potential electronic health information needs to be prevented from various breach activities and influencing unusual activity. The number of tags is noted from individual responses identified from various symptoms collectively illustrated in Fig. 4. The hit ratio of different ranges concerning COVID-19 data is tested under fifty degrees of other circumstances as defined by user 1 to user n. The on-demand request is calculated based on the recall value of the patient's f1-score to improvise personal data during critical scenarios. The readiness of users after homomorphic encryption is also noticed, as shown in Fig. 5.

Data security is a mandatory research work that needs immediate consideration without any delay. Researchers focus rather than reactively; it would be better to be proactive in data preservation. There are cryptographic techniques to solve these issues actively in preventing data breaches. Mathematical imposed models give a high probability of protection in all scenarios. Elliptical curve cryptography (ECC) is a secure encryption and decryption standard algorithm that can serve the issue until a few hits. Similarly, hashing-based techniques resemble hash tables to protect a few more attempts from data breaches. Comparatively, homomorphic encryption standard algorithms (HMA) prove with the help of distributed mathematical model in-built to withhold maximum hit ratio and attacks to prevent the data identity. It motivated us to incorporate the model into the proposed approach to solve privacy issues, specifically in the healthcare system.

Suppose there is an opportunity to collaborate with various users to perform a computation. In that case, it might help a critical health user recover from danger as a homomorphic metric-based health cooperation analysis is illustrated in Fig. 6.

Preventing user information whenever a critical attack is initiated on the storage region is noted for possible breach. Health users having credentials to various features of storage regions might lead to improper guidance in handling precious data. An electric health record holder would use multiple applications that might provide free access to the rest of the world by agreeing to the vendors' terms and agreements. The agreement is not so easy to explore the users from time to time, leading to mishandling of the data by the application owner and their partnering agency. To avoid exploring inside electronic information without the concern of providers or users, a multi-constrained access control mechanism is used as a shield to protect all data from intruders. Service requests are generated and validated by multi-environment protection levels deployed on top of the storage region by incorporating necessary homomorphic prevention mechanisms.

Privacy metrics are collectively used to reduce the risk factors of health informatics for individual users to improve effective personal data prevention. Fig. 7. shows the eligible metrics adopted by incorporating the homomorphic standard for preventing the data breach. Figs. 4, 5, 6 and 7 illustrate the multi-objective opportunity of COVID-19 analysis prediction and homomorphic enforcement to avoid user's information. The homomorphic system adapts to solving complex tasks more optimally by splitting the problem into various sub-tasks. To

Table 1
Deep learning based privacy metrics system tested under different scenarios (DS).

Different	Critical/ Emergency computing-Kbps					Critical/ Emergency computing-Kbps				
scenarios	Random	SPOC	PPBOC	DPLS	CSOHM	Random	SPOC	PPBOC	DPLS	CSOHM
DS1	7576.7	5992	2231	1915	1241	6573.3	4691	2927	1915	1032
DS2	8853.89	4232	3421	2323	2241	6253.33	3382	3594	2829.03	1174
DS3	10746.45	5442	3952	2424	3141	8303.33	7743	3105	2637.33	1092
DS4	18594.74	9215	4841	3342	4035	13269.33	11215	3182	2102.82	1047
DS5	17978	6456	4315	3562	5221	15449.35	14826	3215.5	2948	1210
DS6	13087.33	7020	2532	4888	6214	11768.97	10420	3853	2008.88	1038
DS7	23527	9983	3123	5333	6533	22341	21983	4013	3133.33	1104

Table 2
Privacy metrics evaluation of cooperative system tested in the healthcare system.

Performance criteria	Privacy-preserving metrics														
	Privacy policy & encryption					Statistical analysis					Mathematical model				
	Random	SPOC	PPBOC	DPLS	CSOHM	Random	SPOC	PPBOC	DPLS	CSOHM	Random	SPOC	PPBOC	DPLS	CSOHM
Confidentiality	✗	✔	✔	✔	✔	✗	✔	✔	✔	✔	✗	✔	✔	✔	✔
Integrity	✗	✔	✔	✔	✔	✗	✔	✔	✔	✔	✗	✔	✔	✔	✔
Availability	✗	✔	✔	✔	✔	✗	✔	✔	✔	✔	✗	✔	✔	✔	✔
Accountability	✗	✗	✗	✗	✔	✗	✗	✗	✗	✔	✗	✗	✗	✗	✔
Service Assurance	✗	✗	✗	✗	✔	✗	✗	✗	✗	✔	✗	✗	✗	✗	✔
Data Reliability	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔
Scalability	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔
Fault tolerance	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔
Robustness	✗	✗	✗	✔	✔	✗	✗	✗	✔	✔	✗	✗	✗	✔	✔
Search time	✗	✗	✗	✔	✔	✗	✗	✗	✔	✔	✗	✗	✗	✔	✔
Computing time	✗	✗	✗	✔	✔	✗	✗	✗	✔	✔	✗	✗	✗	✔	✔
Privacy Risk Factor	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔
Preserving Strategy	✗	✗	✗	✔	✔	✗	✗	✗	✔	✔	✗	✗	✗	✔	✔
Data delivery rate	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔
Node Coordination	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔	✗	✗	✔	✔	✔

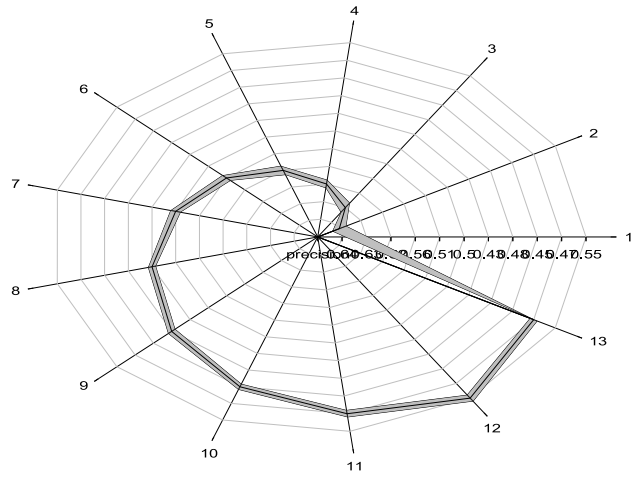

Fig. 7. Homomorphic opportunistic computing with eligible privacy metrics.

maintain the system's reliability, suitable quality metrics should be represented as agents and supports for empirical analysis. The deep learning process would be applied with appropriate metrics for improving DPLS performance, specialization, Interaction, learning, negotiation, and self-reproduction in various fields. A vast area of research needs to be addressed, and available analysis calls for the digital world.

Privacy metrics system evaluation under different scenarios for searching and identifying the nodes which need critical care and emergency computing. They are notably tested for information preservation identified from the shareable participative nodes. Table 1 illustrates the process of random access, searching, and identification of resource sharing to perform emergency communication. Data breaches and computing observed by SPOC, PPBOC, DPLS, and CSOHM are tested, and their metrics are noted with different scenarios. Results show improved performance to do cooperative tasks comparatively high respectively.

Data privacy can be addressed with various methodologies, Such as mathematical models, statistical algorithm analysis, cryptographic logic, and advanced encryption algorithms. Blockchain technologies are one of the advanced technology to be adapted for distributed data storage and decentralized managing strategy. A future extension of the proposed work is further improved by using blockchain-based information protection. Since healthcare patient data is controlled by hospital management or doctors in the current perspective, it can be framed as a decentralized model without disturbing core healthcare management. Homomorphic encryption techniques can be inculcated into blockchain technology to prevent the block of data in the chain. Data created in a genesis block would consist of original patient data where it needs to be stopped. Inside the blockchain, a cryptographic algorithm must be incorporated to generate hashing of every block. Privacy metrics in the healthcare management system is evaluated for the betterment of privacy-preserving; it is compared with various algorithms, privacy policy, encryption techniques, statistical analysis, and mathematical model for effectiveness. It is observed that the proposed privacy metric has a comparatively high data-preserving rate in all circumstances. Table 2 shows various parameters and their illustration with algorithms testing and manipulation of statistical and thematical models wrapped with the privacy policy as a backbone. Encryption techniques adopted for end-to-end data preserving with high risk and low data breaches to achieve a cent percent data delivery. The vast increase in resource sharing would increase the scalability risk, so deep learning-based data navigation needs to reduce the failure rate in information prevention.

Service assurance is an essential preserving strategy in node coordination which help for building trust among providers and to do practical computing. The future research focus might be more concerned with the data prevention mechanism coupled with a framework in-built with deep learning and an artificial intelligence-based approach that would improvise the trust factor. Table 3 illustrates the COVID-19 prediction data collected from hospital management. Moreover, various disease symptoms and patients' illnesses are shown in the table. Patient data is analyzed with all possible opportunities and the prediction mechanism, as shown in Fig. 8a, 8b, and 8c.

Table 3
COVID-19 data analysis and illustration with various diseases.

SL.No	Sex	Pneumonia	Age	Pregnancy	Diabetes	COPD	Asthma	Inmsupr	Hypertension	Other_disease	Cardiovascular	Obesity	Renal_chronic	Tobacco
1.	F	2	71	2	2	2	2	2	1	2	2	2	1	2
2.	M	2	38	+VE	2	2	2	2	2	2	2	1	2	2
3.	F	2	49	2	1	2	2	2	1	2	2	1	2	2
4.	M	1	67	NA	2	2	2	2	1	2	2	2	2	2
5.	F	1	56	2	2	2	2	2	1	2	2	2	2	2
6.	M	2	45	NA	2	2	2	2	2	2	2	2	2	2
7.	M	1	51	NA	2	2	2	1	1	1	1	2	1	2
8.	F	2	48	2	1	2	2	2	1	2	2	2	2	2
9.	M	2	77	NA	1	2	2	2	1	2	2	2	2	1
10.	F	2	30	2	2	2	2	2	2	2	2	1	2	2
11.	M	1	68	NA	1	2	2	2	2	2	2	2	2	2
12.	F	2	42	2	2	2	2	2	2	1	2	1	2	2
13.	M	2	49	NA	2	2	2	2	2	2	2	2	2	2
14.	F	2	59	2	1	2	2	2	1	2	2	2	2	2
15.	M	1	29	+VE	2	2	2	2	2	2	2	2	2	2
16.	M	1	89	NA	1	2	2	2	1	2	2	2	2	2
17.	F	1	67	2	2	2	2	2	2	2	2	2	2	2
18.	M	1	52	NA	2	2	2	2	2	2	2	2	2	2
19.	M	1	63	NA	2	2	2	2	2	2	2	2	2	2
20.	M	2	48	NA	2	2	2	2	2	2	2	2	2	2
21.	F	1	76	2	2	2	2	2	1	2	2	1	2	2
22.	M	2	36	+VE	2	2	2	2	2	2	2	1	2	2
23.	M	2	52	NA	2	2	2	2	2	2	2	1	2	2
24.	M	2	48	NA	1	2	2	2	2	2	2	2	2	2
25.	M	1	60	NA	2	2	2	2	1	2	2	1	2	2
26.	M	2	25	+VE	1	2	2	2	2	2	2	2	2	2
27.	M	1	67	NA	2	2	2	2	2	2	2	2	2	2
28.	M	2	40	NA	2	2	2	2	2	2	2	2	2	2
29.	F	2	54	2	2	2	2	2	2	2	2	2	2	2

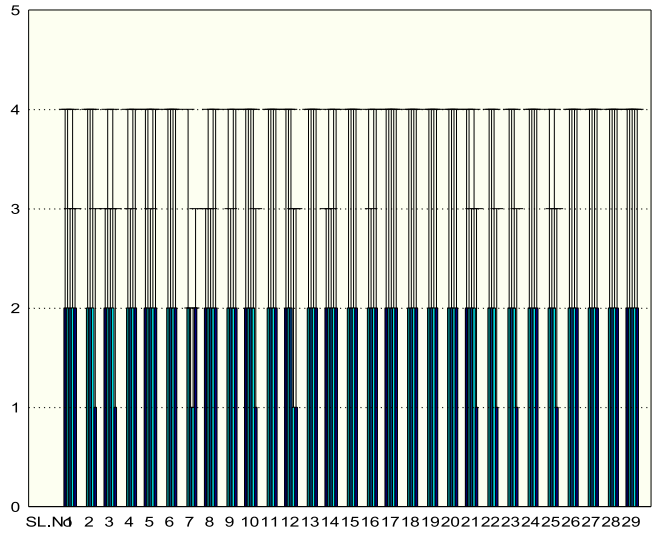

Fig. 8a. COVID-19 patient data analysis.

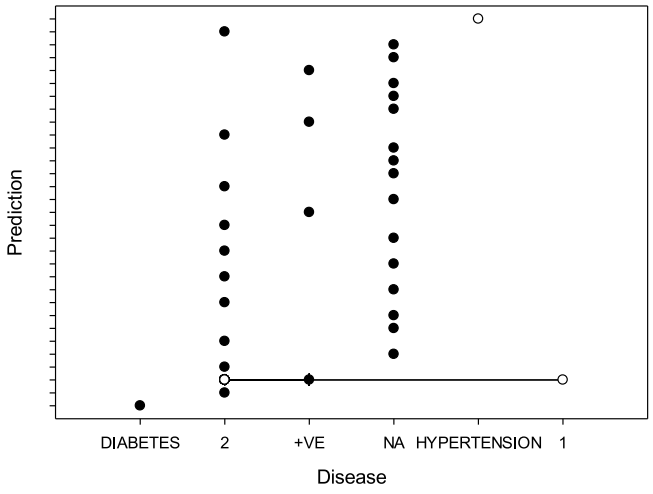

Fig. 8b. COVID-19 prediction.

The literature study explores the need for personal health data prevention from various perspectives. There is a research gap in personal heal record prevention. Available prevention mechanisms are holding the breach for notable iterations because of the vibrant advantages and the adequate performance of the advanced approach to preventing personal data motivated to propose a system that enhances the prevention mechanism in critical cases. Healthcare issues can be handled with homomorphic encryption-based data protection. The multi-constrain data prevention would support the electronic health report holders to collaborate with exemplary practitioners in relevant research communities worldwide. Figs. 8a–8c show the prediction mechanism and its analysis in all scenarios mainly based on the metrics utilized for developing a unique model by incorporating standard homomorphic encryption. COVID-19 patients data is analyzed with acute symptoms of those with other notable diseases under medication.

It is observed from the literature study that virus infection and its vast spreading led to a global pandemic that destroyed all nations' economies. Many cases have come across from time to time with a different virus, which caused much human life in this world. From the study, it is must to predict the cause and procedure to prevent the wide spreading of any virus to the next level or the rest of the world. A research gap is identified in predicting the virus cause, and the chance of affecting internal organs or disturbing the functionality of routine work may lead to critical danger. Patient health information is highly confidential and must be protected by hospitals and doctors. Electronic health records are stored in many hospitals, and cloud storage creates a critical risk for patients' health data. Much research concentrates on personal health record protection by using standard approaches. In the proposed model, the utilization of homomorphic encryption shows an improved performance in personal health record maintenance. The article tested the COVID-19 dataset to evaluate the proposed approach's

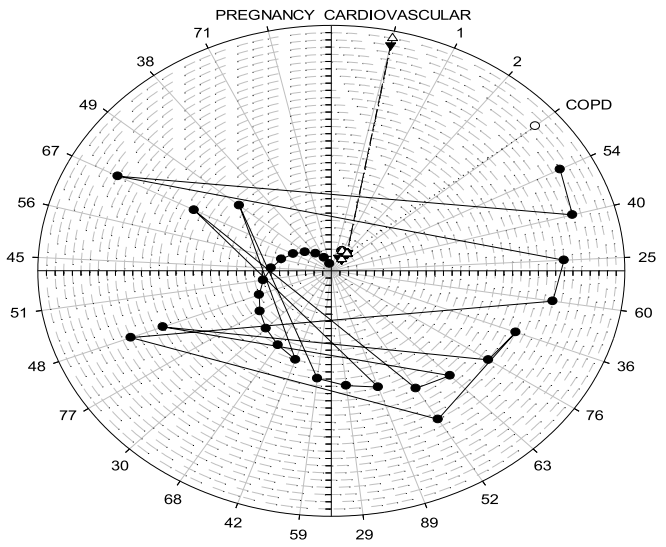

Fig. 8c. COVID-19 health data metric privacy performance compared with other approaches.

effectiveness. The unexpectedly presented system outperformed in all perspectives and showcased the need for applying such methods to prevent the COVID-19 patient details and predict the wide spread of the virus in stipulated time.

5. Conclusion

A deep learning approach for analyzing user requests on demand with an appropriate search process and identifying the right resource is challenging. This paper demonstrates and describes the mining process by coordinator-specific bee colony-based architecture. In decentralized maintenance under virtual coordination, searching and allocating the resource in a wireless region is unmanageable. The nomadic agent supports the knowledgebase with sufficient resources based on the artificial bee colony behavior as the nature-inspired deep learning approach for searching and identifying eligible resources. In this article, it is brought to the notice of the research forum that there is a need for a deep learning process to map the fitness of the learning system using multi-agent. However, deep learning systems might reach a better era if the applicability and maintenance could be performed by improving the efficiency, portability, trustworthiness, functionality, reusability, testability, and security of current social impacts.

Observation and future work

The proposed homomorphic encryption strategy could be more suited to include in the block to improve the prevention mechanism. Cooperative Secure Opportunistic Homomorphic Management (CSOHM) for data integrity encourages health users' awareness to address data breaches. Data protection in various research criteria would be evaluated based on a few parameters considered the highest metrics to mitigate privacy breaches. Metrics that have the most priority like Confidentiality, Integrity, Availability, Accountability, Service assurance, Data Reliability, Scalability (Comparatively High), Fault Tolerance (Very low, Low, Medium/Average, High, Very High), Robustness (Very low, Low, Medium/Average, High, Very High), Search time (ms), Computing time (Kbps), Privacy Risk Factor (Very low, Low, Medium/Average, High, Very High), Preserving Strategy (Very low, Low, Medium/Average, High, Very High), Reliability (Very low, Low, Medium/Average, High, Very High), Data delivery rate %, Node Coordination in %, No. of opp. nodes to do a collaborative task. These privacy metrics must determine adequate personal data protection in various storage services. The performance evaluation is illustrated in Table 2 and its plotting is shown in Figs. 8a, 8b, and 8c evidence of which outperformance of the proposed approach with concrete proof of the proposed system's effectiveness.

CRediT authorship contribution statement

Chandramohan Dhasarathan: Conceptualization, Methodology, Software, Validation, Data curation, Formal analysis, Investigation, Project administration, Resources, Writing – original draft. **Mohammad Kamrul Hasan:** Data curation, Formal analysis, Funding acquisition, Methodology, Resources, Software, Supervision, Writing – original draft, Writing – review & editing, Funding. **Shayla Islam:** Visualization, Investigation, Software. **Salwani Abdullah:** Software, Writing – review & editing. **Umi Asma Mokhtar:** Writing – reviewing and editing. **Abdul Rehman Javed:** Writing – reviewing and editing. **Sam Goundar:** Writing – analysis, Reviewing and editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The dataset used is made available as an open source for the research community. The proposed system preserves patient health records during the pandemic and in all situations. Relevant healthcare data sets are considered for testing the proposed approach's effectiveness, as illustrated in the result and discussion section. Dataset: Chandramohan D, May 25, 2022, "Privacy_COVID", IEEE Dataport, doi: https://doi.org/10.21227/scr5-pr80.

Acknowledgments

This work is supported by the Universiti Kebangsaan Malaysia (UKM) under FRGS/1/2020/ICT03/UKM/02/6, and Thapar Institute of Engineering & Technology, ECED, Patiala, Punjab, India.

References

[1] F. Firouzi, et al., Harnessing the power of smart and connected health to tackle COVID-19: IoT, AI, robotics, and blockchain for a better world, IEEE Internet Things J. 8 (16) (2021) 12826–12846, http://dx.doi.org/10.1109/JIOT.2021.3073904.

[2] M.M. Rahman, K.C. Paul, M.A. Hossain, G.G.M.N. Ali, M.S. Rahman, J.-C. Thill, Machine learning on the COVID-19 pandemic, human mobility and air quality: A review, IEEE Access 9 (2021) 72420–72450, http://dx.doi.org/10.1109/ACCESS.2021.3079121.

[3] K.H. Abdulkareem, et al., Realizing an effective COVID-19 diagnosis system based on machine learning and IoT in smart hospital environment, IEEE Internet Things J. 8 (21) (2021) 15919–15928, http://dx.doi.org/10.1109/JIOT.2021.3050775.

[4] G. Fedele, G. Russo, I. Schiavoni, P. Leone, E. Olivetta, V. Perri, M.A. Zingaropoli, M.R. Ciardi, P. Pasculli, C.M. Mastroianni, P. Stefanelli, Early IgG/ IgA response in hospitalized COVID-19 patients is associated with a less severe disease, Diagn Microbiol Infect Dis. 102 (1) (2022) 115586, http://dx.doi.org/10.1016/j.diagmicrobio.2021.115586, Epub 2021 Oct 23. PMID: 34742119; PMCID: PMC8539217.

[5] Vitor P. Bezzan, Cleber D. Rocco, Using bi-dimensional representations to understand patterns in COVID-19 blood exam data, Inform. Med. Unlocked (ISSN: 2352-9148) 28 (2022) 100828, http://dx.doi.org/10.1016/j.imu.2021.100828.

[6] Samin Babaei Rikan, Amir Sorayaie Azar, Ali Ghafari, Jamshid Bagherzadeh Mohasefi, Habibollah Pirnejad, COVID-19 diagnosis from routine blood tests using artificial intelligence techniques, Biomed. Signal Process. Control (ISSN: 1746-8094) 72 (Part A) (2022) 103263, http://dx.doi.org/10.1016/j.bspc.2021.103263.

[7] Zahra Asghari Varzaneh, Azam Orooji, Leila Erfannia, Mostafa Shanbehzadeh, A new COVID-19 intubation prediction strategy using an intelligent feature selection and K-NN method, Inform. Med. Unlocked (ISSN: 2352-9148) 28 (2022) 100825, http://dx.doi.org/10.1016/j.imu.2021.100825.

[8] Lin Li, Lauren Mazurowski, Aimee Dewan, Madeline Carine, Laura Haak, Tatiana C. Guarin, Niloufar Gharoon Dastjerdi, Daniel Gerrity, Casey Mentzer, Krishna R. Pagilla, Longitudinal monitoring of SARS-CoV-2 in wastewater using viral genetic markers and the estimation of unconfirmed COVID-19 cases, Sci. Total Environ. (ISSN: 0048-9697) 817 (2022) 152958, http://dx.doi.org/10.1016/j.scitotenv.2022.152958.

[9] Ender Sevinç, An empowered AdaBoost algorithm implementation: A COVID-19 dataset study, Comput. Ind. Eng. (ISSN: 0360-8352) 165 (2022) 107912, http://dx.doi.org/10.1016/j.cie.2021.107912.

[10] R. Miikkulainen, N. Iscoe, A. Shagrin, R. Rapp, S. Nazari, P. McGrath, C. Schoolland, E. Achkar, M. Brundage, J. Miller, J. Epstein, Sentient ascend: AI-based massively multivariate conversion rate optimization, in: Thirty-second AAAI conference on artificial, intelligence 27 Apr, 2018.

[11] C. Dhasarathan, M. Kumar, A.K. Srivastava, et al., A bio-inspired privacy-preserving framework for healthcare systems, J. Supercomput. (2021) http://dx.doi.org/10.1007/s11227-021-03720-9.

[12] Nandor Verba, Kuo-Ming Chao, Jacek Lewandowski, Modelling industry 4.0 based fog computing environments for application analysis and deployment, Future Gener. Comput. Syst. (2018) 1–31.

[13] Golam Rabiul Alam, Shirajum Munir, Zia Uddin, Edge-of-things computing framework for cost-effective provisioning of healthcare data, J. Parallel Distrib. Comput. (2018) 1–20.

[14] D. D'Agostino, L. Morganti, E. Corni, D. Cesini, I. Merelli, Combining edge and cloud computing for low-power, cost-effective metagenomics analysis, Future Gener. Comput. Syst. (2018) http://dx.doi.org/10.1016/j.future.2018.07.036.

[15] Long Hu, Yiming Miao, Gaoxiang Wu, An intelligent robot factory based on cognitive manufacturing and edge computing, Future Gener. Comput. Syst. (2018) http://dx.doi.org/10.1016/j.future.2018.08.006.

[16] D. Chandramohan, D. Sathian, D. Rajaguru, T. Vengattaraman, P. Dhavachelvan, A multi-agent approach: To preserve user information privacy for a pervasive & ubiquitous environment, Egyptian Inform. J. (Elsevier) (ISSN: 1110-8665) 16 (2015) 151–166, http://dx.doi.org/10.1016/j.eij.2015.02.002.

[17] Rihab Boussada, Balkis Hamdane, Mohamed Elhoucine Elhdhili, Leila Azouz Saidane, Privacy-preserving aware data transmission for IoT-based e-health, Comput. Netw. (2019) http://dx.doi.org/10.1016/j.comnet.2019.106866.

[18] M.K. Hasan, S. Islam, I. Memon, A.F. Ismail, S. Abdullah, A.K. Budati, N.S. Nafi, A novel resource oriented DMA framework for internet of medical things devices in 5G network, 2022,

[19] M.K. Hasan, S. Islam, I. Memon, A.F. Ismail, S. Abdullah, A.K. Budati, N.S. Nafi, A novel resource oriented DMA framework for Internet of Medical Things devices in 5G network, IEEE Trans. Ind. Inform. (2022).

[20] Mohammad Kamrul Hasan, Muhammad Shafiq, et al., Lightweight cryptographic algorithms for guessing attack protection in complex Internet of Things applications, 13, 2021, 5540296, http://dx.doi.org/10.1155/2021/5540296.

[21] A. Ghasempour, Internet of Things in smart grid: Architecture, applications, services, key technologies, and challenges, Inventions J. 4 (1) (2019) 1–12.

[22] M.K. Hasan, T.M. Ghazal, A. Alkhalifah, K.A.A. Bakar, A. Omidvar, N.S. Nafi, J.I. Agbinya, Fischer linear discrimination and quadratic discrimination analysis–based data mining technique for Internet of Things framework for healthcare, Front. Public Health 9 (2021).

[23] R.G. Babukarthik, Dhasarathan Chandramohan, Diwakar Tripathi, Manish Kumar, G. Sambasivam, COVID-19 identification in chest X-ray images using intelligent multi-level classification scenario, Comput. Electr. Eng. (ISSN: 0045-7906) 104 (Part A) (2022) 108405, http://dx.doi.org/10.1016/j.compeleceng.2022.108405.

[24] R.G. Babukarthik, V.A.K. Adiga, G. Sambasivam, D. Chandramohan, J. Amudhavel, Prediction of COVID-19 using genetic deep learning convolutional neural network (GDCNN), IEEE Access 8 (2020) 177647–177666, http://dx.doi.org/10.1109/ACCESS.2020.3025164.

[25] S.A. Lashari, R. Ibrahim, NSAM Taujuddin, N. Senan, S. Sari, Thresholding and quantization algorithms for image compression techniques: A review, Asia Pacific J. Inf. Technol. Multimedia 7 (1) (2018) 83–89.

[26] Z.R. Mahayuddin, A.S. Saif, A comprehensive review towards segmentation and detection of cancer cell and tumor for dynamic 3D reconstruction, Asia-Pacific J. Inform. Technol. Multimedia 9 (1) (2020) 28–39.

[27] M.I.A. Latiffi, M.R. Yaakub, Sentiment analysis: An enhancement of ontological-based using hybrid machine learning techniques, Asia-Pacific J. Inform. Technol. Multimedia 7 (2018) 61–69.

[28] Desire Ngabo, Wang Dong, Ebuka Ibeke, Celestine Iwendi, Emmanuel Masabo, Tackling pandemics in smart cities using machine learning architecture, Math. Biosci. Eng. 18 (6) (2021) 8444–8461, http://dx.doi.org/10.3934/mbe.2021418.

[29] Celestine Iwendi, Senthilkumar Mohan, Suleman khan, Ebuka Ibeke, Ali Ahmadian, Tiziana Ciano, COVID-19 fake news sentiment analysis, Comput. Electr. Eng. (ISSN: 0045-7906) 101 (2022) 107967, http://dx.doi.org/10.1016/j.compeleceng.2022.107967.